UNIVERSIDADE FEDERAL DE VIÇOSA

Bioproteção laboratorial, biodefesa e inteligência: um modelo transdisciplinar focado em intersetorialidade e ciberbioproteção para a gestão de riscos biológicos no Brasil

Danilo Coelho Alves de Sousa
Doctor Scientiae

VIÇOSA - MINAS GERAIS
2025

DANILO COELHO ALVES DE SOUSA

Bioproteção laboratorial, biodefesa e inteligência: um modelo transdisciplinar focado em intersetorialidade e ciberbioproteção para a gestão de riscos biológicos no Brasil

Tese apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação em Bioquímica e Biotecnologia, para obtenção do título de *Doctor Scientiae*.

Orientador: Claudio L. M. de Siqueira

Coorientador: Donald Hugh Bouyer

VIÇOSA - MINAS GERAIS
2025

Ficha catalográfica elaborada pela Biblioteca Central da Universidade Federal de Viçosa - Campus Viçosa

T
S725b
2025

Sousa, Danilo Coelho Alves de, 1980-
Bioproteção laboratorial, biodefesa e inteligência: um modelo transdisciplinar focado em intersetorialidade e ciberbioproteção para a gestão de riscos biológicos no Brasil / Danilo Coelho Alves de Sousa. – Viçosa, MG, 2025.
1 tese eletrônica (271 f.): il. (algumas color.).

Inclui anexos.
Orientador: Cláudio Lísias Mafra de Siqueira.
Tese (doutorado) - Universidade Federal de Viçosa, Departamento de Bioquímica e Biologia Molecular, 2025.
Referências bibliográficas: f. 256-268.
DOI: https://doi.org/10.47328/ufvbbt.2025.119
Modo de acesso: World Wide Web.

1. Laboratórios microbiológicos - Medidas de segurança. 2. Biossegurança. 3. Inteligência artificial. 4. Aprendizado do computador. I. Siqueira, Cláudio Lísias Mafra de, 1965-. II. Universidade Federal de Viçosa. Departamento de Bioquímica e Biologia Molecular. Programa de Pós-Graduação em Bioquímica Aplicada. III. Título.

CDD 22. ed. 542.1

Bibliotecário(a) responsável: Euzébio Luiz Pinto CRB-6/3317

DANILO COELHO ALVES DE SOUSA

Bioproteção laboratorial, biodefesa e inteligência: um modelo transdisciplinar focado em intersetorialidade e ciberbioproteção para a gestão de riscos biológicos no Brasil

Tese apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação em Bioquímica e Biotecnologia, para obtenção do título de *Doctor Scientiae*.

APROVADA: 18 de fevereiro de 2025.

Assentimento:

_____

Danilo Coelho Alves de Sousa
Autor

_____

Claudio Lisias Mafra de Siqueira
Orientador

*À mamãe coruja e amiga de sempre, Márcia Almeida Coelho de Mattos (*in memoriam*).*

Também dedico o meu empenho nesta pesquisa ao meu pai Sérgio Alves, professor emérito da Universidade Federal de Pernambuco (UFPE) e exemplo de uma vida inspiradora, voltada ao ensino-aprendizado; à minha querida companheira Mariana Amorim, amor genuíno que não finda; e às minhas filhas e enteada Julia, Lia e Clarice, na certeza de que a vontade de aprender caminha ao lado do afeto e terá valido a pena se o legado for um mundo menos desigual, mais solidário e completamente sustentável.

AGRADECIMENTOS

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

Ao meu orientador, Professor Doutor Cláudio Mafra, obrigado por criar oportunidades e ter a coragem de implementar sonhos: estas páginas mostram uma convergência de interesses em prol da responsabilidade com o trabalho em laboratórios biomédicos, com a ciência brasileira e com um Estado efetivamente comprometido com a saúde dos pesquisadores e a segurança humana como um todo.

Ao Prof. Dr. Elias Medeiros, da Universidade Federal da Grande Dourados (UFGD) pelo importante apoio e programação para esta tese, enquanto parte do seu pós-doutoramento.

À Diretora Dra. Daniela Buosi, ao Epidemiologista e Secretário Dr. Wanderson Kleber de Oliveira, ao Dr. Cristiano Barros de Mello, ao Major Dr. Dornellas e ao Dr. Henrique de Souza Rocha, que, enquanto membros das bancas desta tese e eminentes professores na práxis do trabalho integrado ABIN-Ministério da Saúde-Forças Armadas, foram alicerces robustos de transdisciplinaridade na pesquisa aqui materializada. Saudade dos tempos de interação em Brasília e no Rio de Janeiro, que procurei revisitar e homenagear com estas páginas.

À Universidade Federal de Viçosa (UFV) e seu corpo docente e discente da Pós-Graduação em Bioquímica Aplicada, na pessoa do coordenador Prof. Doutor Thiago Mendes, com quem tanto aprendi remotamente, em anos isoladamente difíceis de pandemia da COVID-19, pela excelente estrutura e seriedade enquanto instituição pública federal de educação superior.

Às equipes envolvidas no planejamento e implementação do Programa de Cooperação Acadêmica em Defesa Nacional da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior do Ministério da Educação (PROCAD-DEFESA/CAPES/ME – Processo n. 88881.682224/2011-01) por tornarem possível pesquisas importantes sobre gestão laboratorial no Brasil.

À Agência Braslieira de Inteligência (ABIN), nas pessoas dos Oficiais de Inteligência Ivana Barros (Superintendente da SEPE), Alexandre Carreira (Superintendente da SEPB), Eduardo Farias (Coordenador de Produção da SEPE) e Marcelo Wilker (Coordenador-Substituto de Produção da SEPE), que tornaram possível a escrita da tese apesar do não afastamento para realizar a pós-graduação.

Ao Oficial de Inteligência veterano Janér Tesch Hosken Alvarenga que,

enquanto Diretor Geral da ABIN, empreendeu o fortalecimento da atuação da inteligência na área de ameaças biológicas; à Oficial de Inteligência veterana Vera Alarcon; e aos Oficiais de Inteligência Marcela de Andrade Costa e Eriton Lincoln Pompeu que foram incentivadores fundamentais de ações pioneiras da ABIN na área de biodefesa e de antecipação e acompanhamento de bioameaças - enquanto diretora do então Departamento de Inteligência Estratégica (DIE), coordenadora-geral da então Coordenação-Geral de Inteligência Externa e primeiro Coordenador da fração de biodefesa da ABIN.

À Sociedade Brasileira de Biossegurança e Bioproteção (SB3), da qual tenho o privilégio ser fundador, cujos membros formam uma rede de apoio mútuo e extremamente engajado na construção de laboratórios mais seguros e protegidos e no debate sobre os principais desafios da gestão de biorriscos.

A todas as pesquisadoras e pesquisadores brasileiros que atuam em laboratórios biomédicos e contribuem para o crescimento da ciência no Brasil, na pessoa do Dr. André Mendonça, “o pioneiro”, que, antes de todos, concluiu seu doutoramento no PROCAD-DEFESA e serviu de exemplo para mim e os demais pesquisadores do Programa.

Aos meus colegas de trabalho e amigos da vida, que me expressaram palavras de estímulo e votos de um ótimo doutoramento: vocês ajudaram grandemente o término deste doutorado, mesmo que possam não saber disso.

Aos que se interessarem pela leitura desta pesquisa, na certeza de que busquei disponibilizar um produto que fosse útil a diversos atores da biossegurança e bioproteção laboratoriais. Bons estudos!

“In an age of explosive development in the realm of medical technology, it is unnerving to find that the discoveries of Salk, Sabin, and even Pasteur remain irrelevant to much of humanity.”
- Paul Farmer[a]

“Não é o bárbaro que nos ameaça; é a civilização que nos apavora.”
- Euclides da Cunha[b]

“Any attempt to find automatically safe channels for the present explosive variety of progress must lead to frustration. The only safe possible is relative, and it lies in an intelligent exercise of day-to-day judgement.”
- John von Neumann[c]

[a] FARMER P. Pathologies of power: health, human rights, and the new war on the poor. Oakland: University of California Press, 2004

[b] CUNHA, E. Temores vãos. In: EUCLIDESITE. Obras de Euclides da Cunha. Contrastes e confrontos. São Paulo, 2020. Disponível em: https://euclidesite.com.br/contrastes-e-confrontos/temores-vaos. Acesso em: 04 out 2024. Publicado originalmente em O País, Rio de Janeiro, 24 jun. 1904. Transcrito de: CUNHA, Euclides da. Contrastes e confrontos. In: Obra completa. org. Paulo Roberto Pereira. 2. ed. Rio de Janeiro: Nova Aguilar, 2009. v. 1. pp. 78-81.

[c] In: BRENT, R.; MCKELVEY, T. G.; MATHENEY, J. The New Bioweapons: How Synthetic Biology Could Destabilize the World. Foreign Affairs. September/October 2024. p. 159.

RESUMO

SOUSA, Danilo Coelho Alves de, D.Sc., Universidade Federal de Viçosa, fevereiro de 2025. **Bioproteção laboratorial, biodefesa e inteligência: um modelo transdisciplinar focado em intersetorialidade e ciberbioproteção para a gestão de riscos biológicos no Brasil**. Orientador: Claudio Lisias Mafra de Siqueira. Coorientador: Donald Hugh Bouyer.

A segurança da saúde e a mitigação de riscos biológicos emergem como prioridades estratégicas para os Estados, demandando abordagens inovadoras e integradas em biossegurança e bioproteção laboratoriais, em segurança da saúde e biodefesa. No entanto, a ausência de um arcabouço normativo robusto no Brasil para a gestão de bioproteção laboratorial e a fragmentação das iniciativas voltadas à inteligência laboratorial e à ciberbioproteção comprometem a eficácia das estratégias de prevenção e resposta a eventos biológicos intencionais. Esta tese propõe um modelo ampliado para a gestão de riscos biológicos, fundamentado na incorporação da inteligência laboratorial como um (sub)sistema da inteligência em saúde e na aplicação de tecnologias emergentes para o monitoramento preditivo de ameaças. Dentre as principais contribuições desta pesquisa, destacam-se a concepção e validação da ferramenta PathoFinder Brazil®, projetada para mapear laboratórios e pesquisadores com potencial de manipulação de agentes biológicos selecionados. A integração dessa ferramenta com inteligência artificial e aprendizado de máquina amplia sua capacidade de detecção precoce de riscos, tornando-a um instrumento estratégico para a biodefesa e para a antecipação de ameaças biológicas. Além disso, o estudo elabora o Checklist RAMPA (CIR), considerando um modelo mais abrangente para avaliação da bioproteção laboratorial, que incorpora medidas de ciberbioproteção e de intersetorialidade de maneira alinhada às melhores práticas internacionais. A tese também examina a necessidade de uma integração mais efetiva entre os setores de saúde, segurança e inteligência, explorando a inclusão da bioproteção laboratorial, da segurança da saúde e da biodefesa na governança da inteligência nacional. Argumenta-se que a formalização da inteligência laboratorial dentro do Sistema Brasileiro de Inteligência (SISBIN) ou outros (sub)sistemas fortaleceria a capacidade do país em antecipar e responder a ameaças biológicas, garantindo maior coordenação interinstitucional. Os resultados obtidos evidenciam que a segurança laboratorial deve evoluir para um modelo integrado que contemple fatores físicos, humanos e digitais, assegurando que os desafios emergentes, como ataques cibernéticos a infraestruturas laboratoriais e acessos indevidos a dados sensíveis sejam tratados de

forma integrada. Nesse sentido, a pesquisa reforça a urgência de uma abordagem transdisciplinar e tecnológica para a proteção da saúde pública e segurança nacional. Com isso, esta tese contribui significativamente para o campo da biossegurança, bioproteção, inteligência e biodefesa, oferecendo ferramentas concretas para a mitigação de riscos biológicos e um novo paradigma para a governança da segurança da saúde no Brasil e no exterior.

Palavras-chave: biossegurança; bioproteção; biodefesa; inteligência em saúde; inteligência laboratorial; ciberbioproteção; segurança da saúde; pathofinder brazil; gestão de riscos biológicos

ABSTRACT

SOUSA, Danilo Coelho Alves de, D.Sc., Universidade Federal de Viçosa, February, 2025. **Laboratory biosecurity, biodefense and intelligence: a transdiscipinary model focused on intersetoriality and cyberbiosecurity for biological risk management in Brazil**. Adviser: Claudio Lisias Mafra de Siqueira. Co-adviser: Donald Hugh Bouyer.

Health security and biohazard mitigation are emerging as strategic priorities for States, demanding innovative and integrated approaches in laboratory biosafety and biosecurity, health security and biodefense. However, the lack of a robust regulatory framework in Brazil for laboratory biosafety management and the fragmentation of initiatives aimed at laboratory intelligence and cyberbioprotection compromise the effectiveness of strategies for preventing and responding to intentional biological events. This thesis proposes an expanded model for biohazard management, based on the incorporation of laboratory intelligence as a (sub)system of health intelligence and the application of emerging technologies for predictive threat monitoring. Among the main contributions of this research, the design and validation of the PathoFinder Brazil® tool, designed to map laboratories and researchers with the potential to manipulate selected biological agents, stand out. The integration of this tool with artificial intelligence and machine learning expands its capacity for early risk detection, making it a strategic instrument for biodefense and anticipation of biological threats. In addition, the study develops the Checklist RAMPA (CIR), considering a more comprehensive model for evaluating laboratory bioprotection, which incorporates cyberbioprotection and intersectoral measures in line with international best practices. The thesis also examines the need for more effective integration between the health, security and intelligence sectors, exploring the inclusion of laboratory biosecurity, health security and biodefense in national intelligence governance. It is argued that formalizing laboratory intelligence within the Brazilian Intelligence System (SISBIN) or other (sub)systems would strengthen the country's ability to anticipate and respond to biological threats, ensuring greater inter-institutional coordination. The results obtained show that laboratory security must evolve towards an integrated model that encompasses physical, human and digital factors, ensuring that emerging challenges, such as cyberattacks on laboratory infrastructures and unauthorized access to sensitive data, are addressed in an integrated manner. In this sense, the research reinforces the urgency of a transdisciplinary and technological approach to protect public health and national security. Thus, this thesis contributes significantly to the field of biosafety,

biosecurity, intelligence and biodefense, offering concrete tools for the mitigation of biological risks and a new paradigm for the governance of health security in Brazil and abroad.

Keywords: biosafety; biosecurity; biodefense; health intelligence; laboratory intelligence; cyberbioprotection; health security; pathofinder brazil; biorisk management

LISTA DE ILUSTRAÇÕES

página

LISTA DE TABELAS

página

LISTA DE SIGLAS E ABREVIATURAS

ABI	Agentes Biológicos de Interesse
ABIN	Agência Brasileira de Inteligência
ABNT	Associação Brasileira de Normas Técnicas
ABRE	Abordagem Baseada em Risco e Evidência
ABSA	*American Biological Safety Association*
ADM	Armas de Destruição em Massa
AI	Atividade de Inteligência
AME	Avaliação-Mitigação-Efetividade (AMP, na sigla em inglês)
AMP	*Assessment-Mitigation-Performance* (AME, na sigla em português)
AMS	Assembleia Mundial de Saúde (WHA, na sigla em inglês)
ANVISA	Agência Nacional de Vigilância Sanitária
ABTS	Agentes Biológicos e Toxinas Selecionados
B2L	Biossegurança e Bioproteção Laboratoriais
BMBL	*Biosafety in Microbiological and Biomedical Laboratories*
BMUC	Risco Moderado de Uso Criminoso (LMUR, na sigla em inglês)
BPL	Bioproteção laboratorial
BPPM	Boas Práticas e Procedimentos Microbiológicos (GMPP, na sigla em inglês)
BRM	*Biorisk Management*
BSL	*Biosafety Level* (NB, na sigla em português)
BTPU	*INTERPOL Bioterrorism Prevention Unit*
BWC	*Biological Weapons Convention*
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CBM	*Confidence Building Measures*
CCAI	Comissão de Controle da Atividade de Inteligência
CDC	*Centers for Disease Control and Prevention*
CE	Comissão de Estudo
CEN	Comitê Europeu de Normalização
CFTV	Circuito Fechado de Televisão
CG	Conselho de Governo
CGBS	Coordenação-Geral de Bens Sensíveis
CGIE	Coordenação-Geral de Inteligência Externa

CGPSE	Coordenação-Geral de Proteção e Setores Estratégicos
CIA	*Central Intelligence Agency*
CIR	*Checklist* RAMPA
CIN	Centro de Inteligência Nacional
CIEVS	Centro de Informações Estratégicas em Vigilância em Saúde
CME	Comitê de Monitoramento de Eventos de Saúde Pública
CN	Conhecimentos Necessários
COQBRN	Coordenação de Ameaças QBRN e Não Proliferação
CONSISBIN	Conselho Consultivo do Sistema Brasileiro de Inteligência
COTESB	Coordenação de Tecnologias Sensíveis e Biodefesa
CR	*Core Requirements*
CS	Conhecimentos Selecionados
CSNU	Conselho de Segurança da Organização das Nações Unidas
CNPq	Conselho Nacional de Desenvolvimento Científico e Tecnológico
CPAB	Convenção para a Proibição do Desenvolvimento, Produção, e Estocagem de Armas Bacteriológicas (Biológicas) e Toxínicas e para a sua Destruição
CPAQ	Convenção sobre a Proibição de Armas Químicas
CREDEN	Câmara de Relações Exteriores e Defesa Nacional
CWA	CEN *Workshop Agreement*
DCI	Departamento de Contrainteligência
DCN	Desdobramentos de Conhecimentos Necessários
DCT	Departamento de Contraterrorismo
DDHH	Direitos Humanos
DF	Distrito Federal
DIE	Departamento de Inteligência Estratégica
DIEX	Departamento de Inteligência Externa
DINT	Departamento de Inteligência Interna
DoD	*United States Department of Defense*
DOI	Departamento de Operações de Inteligência
Dstl	*Defence Science and Tecnology Laboratory*
DTRA	*Defense Threat Reduction Agency*
DURC	*Dual Use Research of Concern* (PUD, na sigla em português)
DVA	*Detection, Verification and Risk Assessment*

EMS	*Event Management System*
EMUR	*Extreme Malicious Use Risk* (REUC, na sigla em português)
ENINT	Estratégia Nacional de Inteligência
EPI	Equipamento de Proteção Individual (PPE, na sigla em inglês)
ESINT	Escola de Inteligência da ABIN
ESPII	Emergência em Saúde Pública de Importância Internacional (PHEIC, na sigla em inglês)
ESPIN	Emergência em Saúde Pública de Importância Nacional
EUA	Estados Unidos da América
FAO	*Food and Agriculture Organization of the United Nations*
FAPESP	Fundação de Amparo à Pesquisa do Estado de São Paulo
FEM	Fórum Econômico Mundial
FFAA	Forças Armadas
FLONA	Floresta Nacional
FSAP	*Federal Select Agent Program*
GB	Guerra Biológica
GBL	Guia de Bioproteção Laboratorial da OMS – 1ª edição
GBL2	Guia de Bioproteção Laboratorial da OMS – 2ª edição
GHSA	*Global Health Security Agenda*
GMPP	*Good Microbiological Practice and Procedure* (BPPM, na sigla em português)
GSI	Gabinete de Segurança Institucional
GSN	Grupo de Supridores Nucleares (GSN – NSG na sigla em inglês)
HIM	*Health Emergency Information and Risk Assessment*
HMUR	*Moderate Malicious Use Risk* (RAUC, na sigla em português)
HCF	*High-Containment Facility*
HCBL	*High-Cointainment Biological Laboratory*
HCL	*High-Cointainment Laboratory* (LAC, na sigla em português)
HCM	*Heightened Control Measures*
HCR	*High-Consequence Research* (PAI ou PGD, na sigla em português)
HND	História Natural da Doença
HRF	*High-Risk Facility*
IA	Inteligência Artificial
IBAMA	Instituto Brasileiro do Meio Ambiente

IBC	*Institutional Bisafety Committee*
IBTR	*International Biological Threat Reduction*
IE	Inteligência Epidemiológica
IFBA	*International Federation of Biosafety Associations*
IHR	*International Health Regulations* (RSI, na sigla em português)
ILS	Instalação Laboratorial Selecionada (HRF, na sigla em inglês)
IM	Inteligência Médica
INTERPOL	*International Criminal Police Organization*
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
IS	Inteligência em Saúde
ISO	*International Organization for Standardization*
ISU	*BWC Implementation Support Unit*
ITS	Individualistas Tendendo ao Selvagem
JEE	*IHR Joint external Evaluations*
LAC	Laboratórios de Alta Contenção
LACON	*Large Area Concept*
LAI	Lei de Acesso à Informação
LANAGRO	Laboratório Nacional Agropecuário
LBM	*Laboratory Biosafety Manual/*OMS
LBM3	*Laboratory Biosafety Manual, 3th Edition/*OMS
LBM4	*Laboratory Biosafety Manual, 4th Edition/*OMS
LFDA	Laboratório Federal de Defesa Agropecuária
LMUR	*Low Malicious Use Risk* (RBUC, na sigla em português)
MAPA	Ministério da Agricultura e Pecuária
MBI	Material Biológico de Interesse
MBGC	Material Biológico de Grande Consequência
MC&A	*Material, Control and Accountability* (MC&A)
MCE	Medidas de Controle de Risco Essenciais (CR, na sigla em inglês)
MCM	Medidas de Controle de Risco Máximas ou *Maximum Containment Measures*
MCR	Medidas de Controle de Riscos Reforçadas (HCM, na sigla em inglês)
MCTI	Ministério da Ciência, Tecnologia e Inovação
MMA	Ministério do Meio Ambiente
MMUR	*Moderate Malicious Use Risk* (RMUC, na sigla em português)

MRE	Ministério das Relações Exteriores do Brasil
MRE	*Microbiological Research Establishment*
MS	Ministério da Saúde
MTCR	*Missile Technology Control Regime* (RCTM, na sigla em português)
NB	Nível de Biossegurança (BSL – na sigla em inglês)
NBBC	*National Biosafety and Biosecurity Committee*
NBBF	*National Biosafety and Biosecurity Regulatory Framework*
NBR	Norma Brasileira da Associação Brasileira de Normas Técnicas
NIH	*National Insititutes of Health*
NSABB	*National Science Advisory Board for Biosecurity*
NSG	*Nuclear Suppliers Group* (GSN, na sigla em português)
NUPI	Núcleo de Pesquisa em Inteligência da ESINT/ABIN
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
OECD	*Organisation for Economic Co-operation and Development*
OGM	Organismos Geneticamente Modificados
OI	Objetivos de Inteligência
OMS	Organização Mundial da Saúde (WHO, na sigla em inglês)
ONU	Organização das Nações Unidas
OPAS	Organização Pan-Americana de Saúde (PAHO, na sigla em inglês)
P2R2	Prevenção, Preparo, Resposta e Reconstrução
P3	*Predict, Prevent, Prepare*
PAHO	*Pan-American Health Organization* (OPAS, na sigla em português)
PAI	Pesquisa de Grande Impacto (HCR, na sigla em inglês)
PANGEIA	Programa de Articulação Nacional entre Governo, Empresas e Instituições Acadêmicas para a Prevenção e Mitigação do Risco de Eventos Químicos, Biológicos, Radiológicos e Nucleares Selecionados da ABIN
PCDF	Polícia Civil do Distrito Federal
PDCA	*Plan-Do-Check-Act* (PFCA, na sigla em português)
PGB	Programa de Guerra Biológica
PF	Polícia Federal
PFCA	Planejar-Fazer-Checar-Agir (PDCA, na sigla em inglês)
PGC	Pesquisa de Grandes Consequências (HCR, na sigla em inglês)
PHE	*PAHO Health Emergencies*

PHEIC	*Public Health Emergencies of International Concern* (ESPII, na sigla em português)
PI-ABIN	Plano de Inteligência da ABIN
PLANINT	Plano Nacional de Inteligência
PNI	Política Nacional de Inteligência
PNPC	Programa Nacional de Proteção do Conhecimento
POP	Procedimento Operacional Padrão (SOP, na sigla em inglês)
PP	Pesquisa de Preocupação
PPE	*Personal Protective Equipment* (EPI, na sigla em inglês)
PR	Presidência da República do Brasil
PS	Pesquisa Selecionada
PROCAD	Programa de Cooperação Acadêmica em Defesa Nacional da CAPES
Pronabens	Programa Nacional de Integração Estado-Empresa na Área de Bens Sensíveis
PTS	Patógenos e Toxinas Selecionados
PUD	Pesquisa de Uso Dual (DURC, na sigla em inglês)
QBRN	Químicas, Biológicas, Radiológicas e Nucleares
RAUC	Risco Alto de Uso Criminoso (HMUR, na sigla em inglês)
RBUC	Risco Baixo de Uso Criminoso (LMUR, na sigla em inglês)
RCTM	Regime de Controle de Tecnologia de Mísseis (MTCR, na sigla em inglês)
RELASP	Relatório de Avaliação dos Sistemas de Proteção Laboratorial
REUC	Risco Elevado de Uso Criminoso (EMUR, na sigla em inglês)
RMUC	Risco Moderado de Uso Criminoso (MMUR, na sigla em inglês)
RSI	Regulamento Sanitário Internacional (IHR, na sigla em inglês)
SB3	Sociedade Brasileira de Biossegurança e Bioproteção
SCF	Sistema Ciberfísico
SEPE	Superintendência Pernambuco da Agência Brasileira de Inteligência
SEPB	Superintendência Paraíba da Agência Brasileira de Inteligência
SINDE	Sistema de Inteligência de Defesa
SISBIN	Sistema Brasileiro de Inteligência
SISP	Subsistema de Inteligência de Segurança Pública
SNL	*Sandia National Laboratories*
SOP	*Standard Operating Procedures* (POP, na sigla em português)

SPAR	*IHR* State Party Self-Assessment Report
SSBA	*Security Sensitive Biological Agents*
SSS	Sociedade Secreta Silvestre
SVS	Secretaria de Vigilância em Saúde do Ministério da Saúde
TAG-B	*WHO Techinical Advisory Group on Biosafety*
TUD	Tecnologia de Uso Dual
TS	Tecnologia Selecionada
UFGD	Universidade Federal da Grande Dourados
UFPE	Universidade Federal de Pernambuco
UFV	Universidade Federal de Viçosa
URSS	União das Repúblicas Socialistas Soviéticas
USP	Universidade de São Paulo
WHA	*World Health Assembly* (AMS, na sigla em português)
WHO	*World Health Organization* (OMS, na sigla em português)

LISTA DE SÍMBOLOS

®	Registro de patente ou de programa de computador

SUMÁRIO

1. INTRODUÇÃO

Entende-se que a bioproteção laboratorial (*laboratorial biosecurity*) é um termo amplamente descrito como o "conjunto de ações que visam a minimizar o risco do uso indevido, roubo e/ou a liberação intencional de material com potencial risco à saúde humana, animal e vegetal"[1, p. 17].

A gestão da bioproteção laboratorial (*laboratorial biosecurity management*), por sua vez, guia e supervisiona a implementação de programas de bioproteção laboratorial, normalmente em conjunto com programas de biossegurança laboratorial. Deve-se garantir que cada componente do sistema de bioproteção laboratorial funcione de maneira efetiva[2, p. 61].

Há necessidade urgente de aprimoramento das medidas de controle de biossegurança e bioproteção laboratorial (B2L) no Brasil. É recomendável enfatizar a importância da avaliação de risco na gestão de biorriscos e a adoção de diretrizes internacionais, a exemplo da ISO 35001:2019, como padrão[3, p. 251].

Essa tese é sobre a gestão da bioproteção laboratorial (BPL) na perspectiva da inteligência em saúde (*health intelligence*). Foca-se em laboratórios com agentes biológicos selecionados que infectam ou causam dano direto e primordialmente a humanos, sejam eles agentes zoonóticos ou não; e com a realização de pesquisas de potencial uso dual.

É extensa a literatura científica que aponta para um crescimento de risco associado a cenários de possibilidade de disseminação intencional de agentes biológicos de alto risco e de pesquisas de grandes consequências (PGC)[1,4]. No contexto pós-emergência de saúde pública de interesse internacional (ESPII) pela COVID-19, a segurança da saúde humana (*health security*, em livre tradução)[1] ganhou relevância.

Na pesquisa anual do Fórum Econômico Mundial (FEM) sobre a situação do risco global corrente (*current risk landscape*) para 2024, a disseminação acidental ou intencional de agentes biológicos figura em 17º lugar entre os vinte riscos globais mais prováveis[5, p.13].

A percepção do risco potencial associado a agentes biológicos ficou mais evidente para a população em geral, após a morte de cerca de 27 milhões de pessoas no mundo pelo agente biológico Sars-CoV-2, entre janeiro de 2020 e novembro de 2023[6], estimada pelo excesso de mortalidade (*excess mortality*) no mundo. Tal impacto esteve associado a uma significativa, embora temporária - e

posteriormente revertida -, queda na expectativa de vida da humanidade, a maior no século XXI, até o momento.

Além de uma percepção de risco pós-pandêmica mais apurada, o número de “laboratórios de contenção biológica alta (NB-3) e máxima (NB-4) e suas variações, seja para apoiar ações de saúde e defesa humana, animal ou vegetal, ou para o desenvolvimento de pesquisas, cresceram consideravelmente, no século XXI, em todo o mundo”[4, p.15].

Por conseguinte, o planejamento e implementação de boas práticas de biossegurança e bioproteção laboratoriais ou, mais *lato sensu*, a gestão adequada da biossegurança e bioproteção laboratoriais se torna primordial. Com isto, busca-se garantir a segurança da saúde (*health security*) em um mundo com número crescente de unidades laboratoriais voltadas para pesquisas com agentes biológicos cujo risco de disseminação, intencional ou não, é significativo para atuação preventiva e responsiva do Estado. Tais agentes biológicos, ditos selecionados, são custodiados em estruturas laboratoriais, ditas, por isso, selecionadas[1,2,7].

A atividade de Inteligência, na sua busca por antecipação de fatos e situações que possam impactar a sociedade e na sua vocação institucional por caracterizar ameaças prioritárias à segurança humana, é elemento importante na gestão de bioproteção[1, 8-10].

Em apoio à atuação de gestores de biossegurança e bioproteção, a inteligência pode caracterizar as ameaças e, por conseguinte, analisar esse elemento importante do risco biológico (o nível de ameaça), no qual se deve basear a implementação de medidas de bioproteção[11-14].

Padrões internacionais de gestão de biossegurança e bioproteção, como o ISO 35001:2019[15]; as recomendações do Manual de Biossegurança Laboratorial[16] (LBM, na sigla em inglês), da Organização Mundial da Saúde (OMS); e a prestigiosa publicação Biossegurança em Laboratórios Microbiológicos e Biomédicos[17] (BMBL, na sigla em inglês), dos Centros para Controle de Doenças nos Estados Unidos da América (CDC/EUA) trazem relativamente pouca informação sobre a implementação de programas de bioproteção efetivos.

O foco destas publicações, assim como da Norma Brasileira (NBR) da Associação Brasileira de Normas Técnicas (ABNT) 17069-1[18] (ABNT NBR 17069-1) sobre ”requisitos específicos para o nível de biossegurança (NB-1)” é a biossegurança laboratorial, com muitas lacunas e falhas na apresentação do tema da bioproteção laboratorial.

Se a falta de um arcabouço brasileiro adequado de normas e de instituições reguladoras, no que diz respeito à biossegurança, é evidente[1,2,4], na área de bioproteção as lacunas e desafios são ainda maiores. A integração saúde-segurança-inteligência, fundamental para o funcionamento de medidas de bioproteção, ainda é escassa, apesar de alguns avanços pontuais na última década[19-23]. Neste tripé, em processo de integração interinstitucional, o papel do Estado é central, porque as ações de segurança exigidas, bem como as de inteligência, são muitas vezes atividades específicas de carreiras de Estado, isto é, são ações típicas de Estado[24].

A gestão moderna de biossegurança e bioproteção laboratorial exige um arcabouço robusto que integre inteligência laboratorial, bioproteção física e ciberbioproteção. A proteção digital de dados sensíveis e o monitoramento de ameaças cibernéticas em laboratórios críticos são elementos indispensáveis para a biodefesa e a segurança da saúde. Neste sentido, a ciberbioproteção deve ser compreendida como uma dimensão fundamental da bioproteção, uma vez que ataques cibernéticos podem comprometer dados de patógenos de alto risco, afetando a infraestrutura laboratorial e facilitando acessos indevidos a informações estratégicas sobre agentes biológicos.

O Brasil é um país com histórico de eventos de intrusões laboratoriais, sabotagem biológica e ameaças expressas de disseminação de agentes biológicos para consecução de crimes[25-27], embora não frequentes. O aprofundamento da cultura e de medidas efetivas de bioproteção é fundamental para a segurança da saúde brasileira, e ultrapassa os limites do espaço físico dos laboratórios.

A bioproteção necessária também deveria chegar aos locais de possível disseminação de agentes biológicos selecionados: i. em pastos e lavouras do terceiro maior[d] país exportador de produtos agropecuários do mundo[28]; em espaços de grande circulação da sexta maior população humana do planeta[29]; e em estruturas estratégicas da oitava maior economia mundial[29].

Neste caso, trata-se de lançar mão de um conceito de bioproteção extendida, que considera não apenas os locais de custódia de agentes, mas também pontos de sua disseminação intencional. Entretanto, a abordagem deste conceito e seus desdobramentos excede o foco da presente tese.

[d] Em 2023, o Brasil foi o maior produtor mundial de soja, café, suco de laranja e açúcar. E o segundo maior produtor mundial de carne de frango e carne bovina[28].

Optou-se por direcionar o esforço científico na revisão e análise de elementos da bioproteção laboratorial, percebida como a parte mais carente de abordagens acadêmicas no binômio biossegurança-bioproteção laboratoriais.

Percebem-se diversas lacunas na produção científica brasileira – e também mundial – sobre o tema da bioproteção laboratorial e buscou-se sanar algumas delas, criando ferramentas para apoiar a práxis de gestores que desejam implementar programas de bioproteção mais robustos e coerentes com as ameaças biológicas presentes na contemporaneidade.

A pesquisa apresentada nesta tese, considera este panorama para:

a. Revisar a atuação integrada de órgãos de segurança-inteligência e saúde no gerenciamento do risco biológico selecionado, principalmente dos riscos de bioproteção laboratorial;

b. Discutir as obrigações internacionais do Brasil, na área de capacidades laboratoriais;

c. Analisar nos principais documentos recomendatórios internacionais de biossegurança e bioproteção laboratoriais lacunas e desafios para a implementação de gerenciamento de risco de bioproteção laboratorial;

d. Compreeender criticamente a importância da gestão de risco baseada em ameaças e o papel dos órgãos de segurança e inteligência nesse gerenciamento integrado;

e. Apresentar e discutir os conceitos de “inteligência em saúde” e “inteligência laboratorial”;

f. Registrar e analisar a atuação da inteligência brasileira, mais especificamente da Abin e seu programa PANGEIA, nos primeiros anos de atividade, apontando para desafios presentes;

g. Discutir a análise de risco de evento biológico selecionado intencional no Brasil, a partir da apresentação de ameaças reais à bioproteção laboratorial;

h. Desenvolver uma ferramenta de avaliação de risco (*PathoFinder Brazil®),* com a finalidade de identificar possíveis pesquisas de alto impacto e laboratórios que custodiam material biológico de grandes consequências, auxiliando na ação da segurança-inteligência;

i. Apresentar e discutir um modelo de avaliação de riscos (*Risk Assessment*) baseado em Medidas de Proteção Ampliada (*Checklist*

RAMPA – CIR), adaptado à realidade brasileira, e focado em ciberbioproteção e intersetorialidade.

São aproveitadas informações primárias a partir da vivência do autor da tese, na condição de seu idealizador e primeiro coordenador, para o registro histórico da atuação inicial do PANGEIA/ABIN, entre 2018, ano de sua criação, e 2020, primeiro ano da pandemia de COVID-19, que resultou em significativas mudanças para atuação da ABIN na área de ameaças biológicas.

O relato de vivência é complementado, por meio de informações sobre as atividades da ABIN na área da segurança da saúde dadas como resposta ao pedido de informações realizado junto ao Sistema Eletrônico do Serviço de Informação ao Cidadão (https://esic.cgu.gov.br/sistema/site/index.aspx), segundo a Lei de Acesso à Informação (LAI), sob número de protocolo 0007700074720172.

Vislumbrou-se realizar o registro histórico da atuação da ABIN, a partir da análise dos documentos orientadores da atividade de inteligência (AI) e das competências do PANGEIA como forma de avaliar o papel da inteligência na área da saúde, da epidemiologia e da gestão de biorrisco no tocante a laboratórios biomédicos.

A percepção da importância do desenvolvimento de ferramentas para tornar mais robusta a governança de gestão de biossegurança e bioproteção laboratoriais resultou em uma proposta transdisciplinar de análise dos componentes de um sistema de bioproteção laboratorial segundo as principais fontes internacionais, a exemplo dos dois manuais produzidos pelos Sandia National Laboratories (SNL)[2,13]; bem como dos dois Guias de Bioproteção Laboratorial (GBL e GBL2) da OMS[22,23], editados em 2009 e 2024, respectivamente.

Estas quatro referências se tornaram o fundamento do CIR. A partir de análise minuciosa das recomendações destes quatro documentos-base para a implementação dos componentes dos sistemas de bioproteção, elaboraram-se os quesitos de avaliação de sistemas de bioproteção laboratorial na forma de um *checklist*.

A leitura crítica destes quatro documentos-base para implementação de sistemas de bioproteção laboratorial foi realizada em diálogo analítico com os três principais documentos-padronizadores da gestão de biossegurança e bioproteção *lato sensu,* igualmente supracitados (ISO 35001:2019[15]; LBM4[16]; e BMBL[17]); mas também com a tríade de documentos multilaterais que expandem a importância do

tema: o Regulamento Sanitário Internacional[53] (RSI); a Convenção de Armas Biológicas[36] (BWC, na sigla em inglês); e a Resolução 1540 do Conselho de Segurança da Organização das Nações Unidas[59] (CS/ONU).

Optou-se por realizar a análise minuciosa dos componentes do sistema de bioproteção, em que se baseou o ClR, no capítulo 6 (subcapitulo *6.3*), deixando para o capítulo 2 (subcapítulo 2.1) unicamente a menção dos componentes clássicos dos sistemas de bioproteção. Concluiu-se, para justificar essa decisão, que, sendo o ClR um aspecto central da pesquisa – e original também, na medida em que um novo componente e a atualização de aspectos dos componentes clássicos são propostos -, as recomendações em se baseiam o questionário deveriam constar dos resultados e discussão e não da mera revisão bibliográfica.

A divisão didática dos riscos de bioproteção de furto/roubo como riscos de bioproteção laboratorial persistentes e os novos riscos, mormente relacionados a pesquisas de uso dual, chamados de riscos emergentes, apesar de uma inovação teórica da tese, foi propositadamente descrita no capítulo 2 (tópicos 2.1.4.2 e 2.1.4.3), em razão de ser "conceitos-menores", no sentido de originalidade e impacto potencial do uso. Deixaram-se os "conceitos-maiores" de *inteligência em saúde* e de *inteligência laboratorial* para uma discussão mais ampla nos capítulos dos resultados e conclusões (subcapítulos 6.1 e 7.1, respectivamente).

É mister esclarecer que a atividade de inteligência (AI) desempenhada por órgãos centrados nessa finalidade, como a ABIN, é considerada não como parte do setor segurança, mas do setor inteligência. O enfoque da inteligência na presente pesquisa justifica que a AI seja referida como um setor próprio de atividade de Estado. O setor de segurança, por sua vez, engloba mormente as polícias estaduais e federais, que possuem frações de inteligência, embora a atividade central não seja a inteligência em si[e].

O conteúdo desta tese não reflete a opinião da ABIN ou do Governo da República Federativa do Brasil, mas unicamente a convicção individual do autor, obtida mediante o resultado da pesquisa científica empreendida.

---

[e] Sobre esta relação da inteligência policial com a atividade policial, vale recordar o recente debate interno na Polícia Federal brasileira se a inteligência ali desenvolvida seria uma atividade-meio ou atividade-fim. Na ABIN, é óbvio afirmar que este debate nunca teria lugar. Por isso, cabe a distinção entre setor inteligência (cujos órgãos ou frações possuem a finalidade de produzir conhecimentos de inteligência) e setor de segurança (cujos órgãos ou frações realizariam ações de inteligência como um meio para o efetivo desempenho de outra atividade finalística).

Em tempo pós-pandemia da COVID-19 (ou será apenas o início de uma nova era pandêmica?), a discussão sobre biodefesa, segurança da saúde (*health security*)[f] e inteligência am saúde, na sua interconectividade com a biossegurança e bioproteção laboratoriais (B2L) e a ciberbioproteção é extremamente oportuna:

> "*...a pandemia [de COVID-19] terá impactos duradouros em como percebemos a bioproteção, por meio de uma convergência de especialidades, das implicações para a segurança da saúde em nível individual e coletivo, de um limiar reduzido para atos de bioterrorismo e de um papel crítico que a ciberbioproteção irá desempenhar em proteger a crescente bioeconomia* [tradução e grifo nossos]."[20, p.vi].

[f] O termo segurança da saúde implica que a saúde de um indivíduo é um componente do senso geral de segurança do indivíduo[20, p. 79].

2. REVISÃO DE LITERATURA

2.1 Bioproteção Laboratorial (*laboratorial biosecurity*)

2.1.1 Conceitos de *biosecurity*

Na língua portuguesa, o termo *biosecurity* pode ser encontrado na literatura especializada em três traduções mais comuns:

a. biossegurança;
b. bioproteção; e
c. biosseguridade[21] ou biocustódia[15, p.5].

Esta multiplicidade de traduções está relacionada à variedade de significados tanto do termo em inglês *security* e, consequentemente, do termo *biosecurity*[1], além do uso de um termo assim abrangente por diferentes atores que lidam com diferentes atividades, competências e riscos biológicos.

Koblentz, um dos pesquisadores pioneiros na temática da segurança da saúde global (*global health security*) e professor associado do Instituto de Inovação em Biossaúde (*Institute for Biohealth Innovation*) da Universidade George Mason, em Washington DC/EUA[31], defendeu que o termo *biosecurity* possui quatro acepções na língua inglesa[32].

A variação semântica e a dificuldade de tradução do termo já fizeram com que especialistas em fóruns multilaterais recomendassem a manutenção do termo em inglês, sem traduzi-lo, em documentos oficiais de tais fóruns.

2.1.1.1 *Biosecurity* na perspectiva da proteção da agricultura e do meio ambiente

As áreas da agricultura e do meio-ambiente foram as primeiras a usar o conceito de *biosecurity*, originalmente para se referir à ação de prevenir ou diminuir a transmissão de doenças, naturalmente presentes, para rebanhos; e a transmissão de pragas para a lavoura. O conceito foi posteriormente ampliado para incluir ameaças à economia e ao meio-ambiente por organismos exóticos invasores[32].

Esta definição de *biosecurity* foi adotada pela Organização para a Alimentação e Agricultura (FAO, na sigla em inglês), “em relação a medidas sanitárias, fitossanitárias e zoosanitárias aplicadas nos sistemas regulatórios de alimentos e da agricultura[33]”. Para a FAO, o termo significa

> “uma abordagem estratégica e integrada que engloba a política e arcabouços regulatórios (incluindo instrumentos e atividades) de análise e gerenciamento de riscos relevantes para a vida e saúde humana, animal e vegetal, assim como os riscos associados ao meio ambiente.”[34]

Desde o início dos anos 2000, a *biosecurity*, na visão da FAO, "descreve de maneira ampla o processo e o objetivo de manejar riscos biológicos associados à alimentação e à agricultura”, abrangendo a introdução de pragas agrícolas, pestes e doenças animais e de zoonoses, a introdução e disseminação de Organismos Geneticamente Modificados (OGM) e seus produtos e a introdução e manejo de espécies e genes exóticos invasores. Seria um importante conceito para a sustentabilidade da agricultura e do meio-ambiente, incluindo a biodiversidade[33].

Hoje, a FAO vincula as ações de *biosecurity* ao paradigma da Saúde Única (*One Health*, em inglês), afirmando que ambos os conceitos “convergem como uma via única para um gereciamento de risco biológico aprimorado, em sistemas agroalimentares”. E prioriza ações de *biosecurity*, com o objetivo de: i. proteger a produção de alimentos; ii. promover a saúde humana, animal e vegetal e a biodiversidade; e iii. reduzir os impactos econômicos[34].

2.1.1.2 *Biosecurity* na perspectiva da proteção laboratorial

A segunda definição apontada por Koblentz "surgiu no final dos anos 1990, em resposta à ameaça do terrorismo biológico” e se refere a medidas para proteger agentes microbiológicos laboratoriais de "perda, roubo, utilização indevida, desvio ou escape intencional" de agentes patogênicos e toxinas[32].

É o conceito adotado pela OMS e pela Convenção de Armas Biológicas[36]. Normalmente, este conceito é utilizado mediante uso da expressão “*laboratorial biosecurity*”[16, 32, 35, 36].

Ressalte-se que a Convenção para a Proibição do Desenvolvimento, Produção, e Estocagem de Armas Bacteriológicas (Biológicas) e Toxínicas e para a sua Destruição (CPAB) adota o entendimento de *biosecurity* como "medidas de

proteção, controle e transparência implementadas para prevenir a perda, roubo, utilização indevida, desvio ou disseminação intencional de agentes biológicos toxinas e recursos relacionados assim como o acesso não autorizado, a retenção ou transferência deste material", em consonância com a OMS. Entretanto, há nota expressa da CPAB de que este entendimento não se trata de uma definição, tampouco tem caráter vinculante aos Estados-Parte da Convenção[36].

Após as investigações do Federal Bureau of Investigation (FBI) que apontaram para uma falha de *biosecurity* como causa dos atentados de bioterrorismo utilizando correspondências com antraz em 2001 nos EUA, esta conceituação ganhou maior relevância internacional[32].

2.1.1.3 *Biosecurity* na perspectiva da proteção contra o mal-uso de tecnologias de uso dual

A terceira definição de *biosecurity*, por outro lado, refere-se às técnicas e tecnologias que podem ser utilizadas para criar organismos patogênicos, para aumentar o impacto de organismos já existentes (ex. pesquisas de ganho de função - *gain of function*) ou criar componentes com atividade biológica. O foco muda de agentes biológicos em si ou as populações a serem protegidas, para se dirigir às técnicas e tecnologias utilizadas em sua criação[10].

Este conceito é utilizado pelo Comitê de Assessoramento Científico para Biosecurity (*National Science Advisory Board for Biosecurity* – NSABB), criado nos EUA em 2004, com competência principal de realizar o assessoramento governamental com respeito ao *biosecurity oversight* da pesquisa de uso-dual - definida como a pesquisa com propósito científico legítimo que pode ser desviada para servir de ameaça à saúde pública e/ou à segurança nacional[37-39]. Trata-se de um comitê federal no âmbito do equivalente ao Ministério da Saúde estadunidense (*National Institutes of Health* - NIH).

O conceito de *biosecurity* do NSABB não estaria dissociado da segunda definição, ao contrário do que afirma Koblentz, tanto que há relatórios específicos do órgão com recomendações para aumentar a confiabilidade dos pesquisadores (*personnel relialibility*) que lidam diretamente com agentes selecionados, a fim de diminuir o risco de uso mal-intencionado - em acordo com a segunda definição apresentada[38, 39].

O uso feito pelo NSABB do termo *biosecurity* é, portanto, uma ratificação do segundo conceito, mas o ampliando para considerar novas tecnologias com potencial de uso dual na área microbiológica e biomédica como ameaça[38, 39].

Sabe-se que a tecnologia de uso dual a ser protegida, caso seja mal-utilizada, ensejará a criação de material biológico de preocupação que pode ser usado contra populações. Assim, a consequência final a ser prevenida nessas duas últimas definições de *biosecurity* também se equivalem, uma vez que se trata de evitar a disseminação não intencional de agentes biológicos com potencial de causar grande impacto para a sociedade.

2.1.1.4 *Biosecurity lato sensu*

A quarta e última definição é a semanticamente significativamente mais ampla. Pode ser chamada de definição *lato sensu* de *biosecurity*.

Elaborada pelas Academias Nacionais de Ciência (*National Academies of Science*) dos EUA, esta definição se configura como uma síntese das demais definições. Segundo ela, *biosecurity* é a "segurança contra o uso inadvertido, inapropriado ou intencionalmente malicioso ou malévolo de agentes biológicos ou de biotecnologia potencialmente perigosos, incluindo o desenvolvimento, produção, estocagem; ou contra o uso de armas biológicas; assim como contra surtos de doenças emergentes e epidêmicas"[32].

Esta definição *lato sensu* inclui as ameaças biológicas que acontecem naturalmente, mas também as ameaças ditas acidentais e as intencionais[32].

Das quatro definições discutidas de *biosecurity*, considera-se que as três primeiras estejam em processo consolidado de significado - e, por conseguinte, de traduções - no Brasil, mesmo que falte consenso entre os pesquisadores que estudam estes conceitos no país[1].

Por outro lado, não há tradução adequada para o português deste conceito de *biosecurity* mais amplo ("*comprehensive definition of biosecurity*[32]"), de modo que seja mais prudente o uso do termo em inglês quando se quiser referir ao sentido lato.

Segundo o proposto por COELHO (2017), esta definição se confunde com a própria ideia da segurança da saúde (*health security*), podendo-se afirmar que se trata de praticamente sinônimos[1].

2.1.1.5 *Biosecurity* traduzida como biosseguridade ou biocustódia

Wunder[40] e Cardoso[41], ambos se referem ao conceito de *biosecurity* como "biosseguridade", o que deve ser explicado pela principal referência bibliográfica de ambos, Chaimovich, que, apesar de professor emérito do Instituto de Química Universidade de São Paulo (USP) e ex-presidente do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), é pesquisador de origem chilena e provavelmente foi influenciado, em seu artigo "Biosseguridade"[21], pela sua língua natal, uma vez que, na língua espanhola, *biosecurity* foi traduzido pelo autor como como *bioseguridad*.

Esta tradução, entretanto, contraria a tradução oficial da ISO 35001:2019 para o espanhol, segundo a qual "*bioseguridad*" é biossegurança:

> *"práticas e controle que reduzem o risco de disseminação ou liberação não intencionada de materiais biológicos. [tradução nossa]."*[15, p. 5]

Já o uso do termo biocustódia como sinônimo de bioproteção laboratorial seria uma tradução literal do termo "*biocustodia*" que, segundo a norma ISO 35001:2019[15, p.5], é um sinônimo para "*bioprotección*" no sentido de bioproteção laboratorial:

> *"práticas e controle que reduzem o risco de perda, roubo, mal-uso, extravio ou liberação intencional não autorizada de materiais biológicos [*tradução nossa*]."*[15, p. 5]

2.1.2 Conceito de bioproteção laboratorial

2.1.2.1 Bioproteção laboratorial conforme a OMS e os CDC

Segundo o glossário da OMS constante da quarta e última edição do seu Manual de Biossegurança Laboratorial (LBM4, na sigla em inglês), bioproteção laboratorial (*laboratory biosecurity*) são

> *"Princípios, tecnologias e práticas que são implementadas para a proteção, controle e conformidade [*accountability*] de materiais biológicos e/ou do equipamento, habilidades e informações relacionados ao seu manuseio. A bioproteção busca prevenir seu acesso não autorizado, a perda, furto, mal-uso, extravio ou disseminação* [tradução nossa]*"* [1, p.xi]

Na mesma publicação da OMS, que é a edição vigente, biossegurança laboratorial (*laboratorial biosafety*) está descrita como

> "*Princípios, tecnologias e práticas de contenção (*containment*) que são implementadas para prevenir a exposição não intencional a agentes biológicos e toxinas ou à sua disseminação acidental* [tradução nossa]" [1, p.x]

Estas definições são idênticas com as da última e vigente edição do manual BMBL/CDC, de 2020, em que a mesma terminologia para os dois conceitos está presente. Verifica-se, portanto, que as definições internacionais dos dois termos (biossegurança e bioproteção laboratoriais) são amplamente aceitas pelas duas principais normas recomendatórias mundiais.

Ambos os conceitos são praticamente os mesmos desde que surgiram as primeiras recomendações sistematizadas e públicas para a implementação de ações e medidas de biossegurança laboratorial, nos anos 1980; e as primeiras recomendações sistematizadas e públicas para a implementação de ações e medidas de bioproteção laboratorial, na primeira década do novo século XXI.

2.1.2.2 Avanço nas recomendações de bioproteção laboratorial pela OMS

Em 2004, na terceira e penúltima edição do Manual de Biossegurança Laboratorial (LBM3, na sigla em inglês), a OMS atribuíra à bioproteção uma parte com um único capítulo de duas páginas sobre "Conceitos de bioproteção laboratorial" (*Part II - Laboratory biosecurity, Chapter 9 - Laboratory biosecurity concepts*) contendo um detalhamento mínimo (mais conceitual) do tema, em um único tópico[35, p. 45].

Em 2020, todavia, na quarta e vigente edição do LBM, a OMS detalhou elementos-chave para um programa de bioproteção laboratorial em uma seção com o quádruplo de páginas (*Section 8 – Laboratory biosecurity*), em relação às do LBM3, e nove capítulos[16, pp.83-90].

Nas duas páginas dedicadas à BPL, a OMS define-a como

> "*medidas de proteção pessoal e institucional planejadas para prevenir a perda, furto/roubo, mal-uso, extravio ou disseminação intencional de patógenos e toxinas* [tradução nossa]."[35, p.47]

As práticas de biossegurança são descritas como a base das ações de BPL. E a OMS afirma que

> "*um programa específico de bioproteção deve ser (*must be*) planejado e implementado para cada instalação (...) e deve incluir* inputs *de (...) agências de segurança (*law enforcement*)* [tradução nossa]"[35, pp.47-48]

O documento introduz inicialmente o conceito mais atual de bioproteção laboratorial, sem mudanças significativas em relação ao conceito dezesseis anos anterior constante do LBM3:

> "*Bioproteção laboratorial se refere a medidas de proteção pessoal e institucional planejadas para prevenir a perda, furto/roubo, mal-uso, extravio ou disseminação intencional de agentes biológicos custodiados em laboratório* [tradução nossa]."[16, p.83]

O lançamento das últimas edições coincide com o primeiro e mais temeroso ano da pandemia da COVID-19. Nesta década e meia, em média, entre as duas últimas edições do LBM/OMS, a ampliação do tema da bioproteção nos documentos refletiu a maior preocupação em sistematizar recomendações de bioproteção para o conjunto de laboratórios.

Dois anos depois do lançamento do LBM3, a OMS lança, em 2006, seu primeiro Guia de Bioproteção Laboratorial (*Laboratory Biosecurity Guidance* - GBL)[23]. Posteriormente, quatro anos depois do lançamento do LBM4, a OMS lança, em 2024, a segunda edição do seu Guia de Bioproteção Laboratorial (GBL2), a partir do engajamento de especialistas internacionais e do Grupo de Assessoramento Técnico em Biossegurança da OMS (TAG-B, na sigla em inglês)[22], no âmbito do Programa de Biossegurança e Bioproteção Laboratorial da OMS.

O documento foi financiado pelo Departamento de Defesa (DoD) dos EUA, por meio da sua Agência de Redução de Ameaças (DTRA, na sigla em inglês), tendo como revisores organizacionais a Associação Americana de Segurança Biológica (ABSA, na sigla e inglês); o Governo do Canadá; a Sociedade Mexicana de Biossegurança e o Governo dos EUA[22, p.x].

> "*Essa edição do Guia de Bioproteção Laboratorial é uma revisão completa da primeira edição, publicada em 2006. Os maiores avanços são: a adaptação do LBM4 para a aplicação da abordagem baseada em risco e evidência também à bioproteção laboratorial; a ênfase na compreensão da biossegurança e bioproteção laboratoriais como um* continuum*; e inclusão de novos desenvolvimentos na ciência e tecnologia; e o enfoque da*

> *bioproteção laboratorial em todos os três níveis (o laboratório, a instituição e o corpo regulatório nacional)"*[22, p.1].

Para a OMS, a bioproteção laboratorial é inseparável da biossegurança laboratorial[g] (**Figura** 1), e as duas áreas mutuamente se complementam na garantia de operação segura e protegida de laboratórios[22, p.1].

Ressalte-se, entretanto, que, desde o LBM3, há recomendação de treinamentos e programas específicos para a bioproteção laboratorial, distintos daqueles de biossegurança[35, p.37].

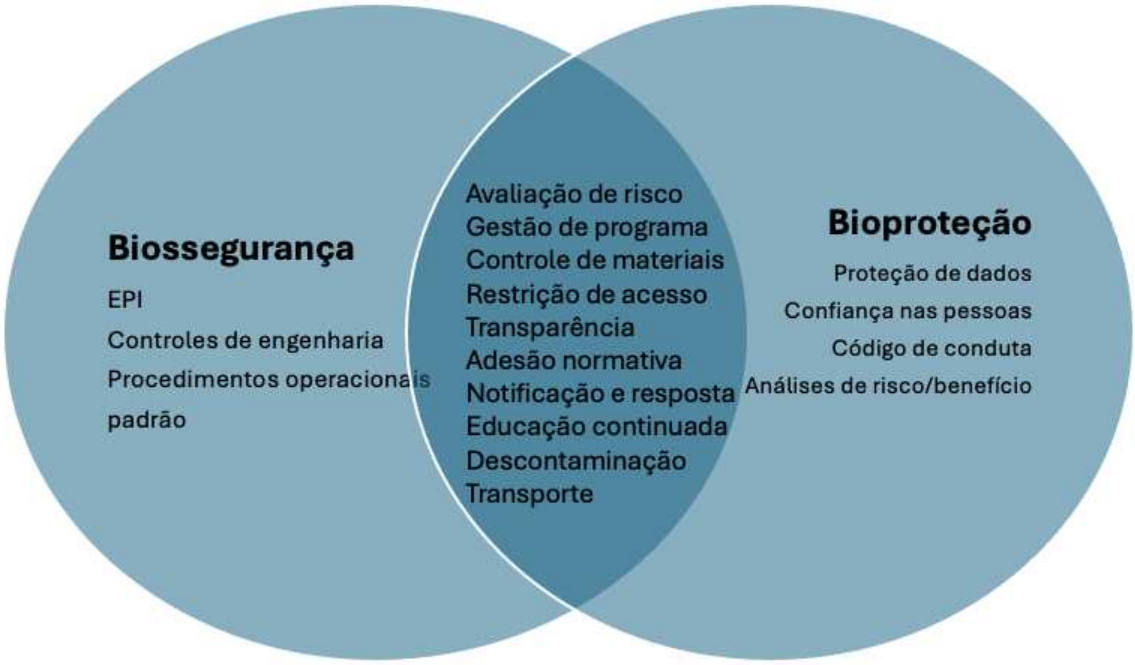


Figura 1 *– Espectro da gestão de risco biológico: exemplos de elementos específicos e comuns da biossegurança e bioproteção laboratoriais* (adaptado da OMS[22, p. 2] pelo autor)

Nos 20 anos que separam o LBM3 do GBL2, houve uma ampliação das ameaças à bioproteção, em razão do maior conhecimento acerca do impacto do uso de tecnologias emergentes.

Do enfoque restrito aos próprios patógenos como ameaças potenciais de disseminação intencional, tendo o furto e roubo da ABTS como principais cenários

[g] Há afirmação da OMS de que "práticas efetivas de biossegurança formam as fundações da bioproteção laboratorial"[123, p.36].

de risco, passa-se a considerar a pesquisa de alto impacto/grandes consequências (*high-consequence research - HCR*) potencial como ameaças igualmente importantes[22, p.4].

> *"Para enfatizar a importância de avaliar os riscos de biossegurança e bioproteção relacionados à pesquisa com material biológico que podem causar consequências graves ou catastróficas à vida, o Guia de Bioproteção Laboratorial usa o termo pesquisa de alto-impacto/grandes-consequências para descrever esses experimentos. Outros termos são usados como pesquisa de uso dual de preocupação, pesquisa de uso dual ou pesquisa de preocupação."*[35, p.4]

A pesquisa de alto impacto (PAI) ou pesquisa de grandes consequências (PGD) ou pesquisa de uso dual (PUD) ou pesquisa de preocupação (PP) ou ainda pesquisa selecionada (PS), se usarmos a analogia do termo ABTS, podem ser considerados sinônimos, para fins de gestão de bioproteção laboratorial. Enfatiza-se que o impacto ou consequência das pesquisas supracitadas são potenciais.

Cabe mencionar uma mudança de perspectiva conceitual entre o GBL e o GBL2, na medida em que o primeiro é focado no conceito de material biológico de interesse (MBI) e o segundo, em material biológico de grande consequência (MBGC).

O conceito de MBI, segundo o GBL da OMS é:

> *"todo material biológico que requer monitoramento administrativo, controle e responsabilização, além de medidas específicas de proteção e monitoramento nos laboratórios, a fim de proteger seu valor econômico e histórico e de proteger a população de seu potencial de dano. Pode incluir patógenos e toxinas, além de organismos não patogênicos, cepas vacinais, alimentos, OGMs, componentes celulares, elementos genéticos e amostras extraterrestres* [tradução nossa]*."*[23]

O conceito de MBI foi importante porque criou uma categoria de classificação dos agentes e materiais biológicos, ratificando a ideia de que todo material biológico é classificável quanto ao seu risco, mas só alguns são considerados estratégicos (ou de interesse), porque possuem valor econômico e histórico e são propícios a servir como ameaça grave à saúde e segurança públicas[1, p. 97].

O problema do conceito de "interesse" é que ele é subjetivo. Na época, para a OMS, cabia aos órgãos e instalações que custodiassem agentes biológicos

para fazer juízo de valor quanto a importância econômica e histórica de cada agente custodiado[1, p.97].

No GBL2, por outro lado, o conceito não aparece, mas é substituído por material biológico de grande consequência (MBGC)[22]. Percebe-se, portanto, que se chega a uma denominação mais objetiva, uma vez que a análise do impacto/consequência potencial do mal uso deste material é algo objetivamente definido.

Junto com o conceito de MBGC, surge o de PAI/PGC, para se referir a ameaças de bioproteção emergentes, conforme supracitado. Ressalte-se, então, que os termos mais amplos para se referir a materiais e pesquisas que exigem avaliação de risco de biossegurança e bioproteção laboratoriais são esses.

Entre os MBCG e as PGC, podemos ter os materiais biológicos e pesquisas selecionados e também podemos encontrar os materiais biológicos e pesquisas de uso dual. Deste modo, todos os ATBS e PS são MBCG e PGC, respectivamente, todavia nem todos os MBCG e PGC são selecionados, conforme será detalhado *a posteriori*.

2.1.2.3 Avanço nas recomendações de bioproteção laboratorial pelos CDC

Quanto aos CDC, referência mundial em biossegurança e bioproteção laboratoriais, a última edição do seu manual *Biosafety in Microbiological and Biomedical Laboratories (BMBL)*, de junho de 2020, significou avanço e atualização de recomendações de bioproteção, na medida em que ampliou e detalhou o assunto[17].

Em 2009, na quinta e penúltima edição do BMBL, a bioproteção, pela primeira vez nesta publicação, fora objeto de uma seção específica "Seção 6 - Princípios de Bioproteção Laboratorial"[19, pp.104-113].

Em 2020, na sexta edição, a seção foi ampliada e discutiu o desenvolvimento de um “Programa de Bioproteção Laboratorial”, com base em Avaliação de Risco de Bioproteção[17, pp.119-129].

2.1.2.4 Bioproteção laboratorial nas normas CEN CWA 15793:2011 e ISO 35001:2019

O Consenso de *Workshop* do Comitê Europeu de Normalização[h] (CEN CWA, na sigla em inglês) é uma norma europeia equivalente, para a União Europeia, às normas do Instituto Nacional de Metrologia, Qualidade e Tecnologia (INMETRO) para o Brasil.

A Organização Internacional para Padronização (ISO, na siga em inglês), com sede na Suíça, por sua vez, congrega os órgãos nacionais de normalização, como o INMETRO, para facilitar e coordenar a unificação de normas técnicas, normas de procedimento e classificações.

A norma CWA 15793:2011[65] e a ISO 35001:2019[15] são específicas sobre "gestão de risco biológico em laboratórios ou outras organizações relacionadas". Elas não são impositivas, mas referenciais recomendatórios aos laboratórios (públicos e privados) e aos órgãos e estruturas aos quais se subordinam, no caso de laboratórios públicos[105].

A norma CWA supracitada se baseia no LBM3 e no GBL – de maneira compatível com as normas ISO 9001:2000 (sobre qualidade) e ISO 14001:2004 (sobre meio ambiente) e OHSAS 18001:2007 (sobre saúde ocupacional e segurança) - de modo que deverá ser atualizada com base nos LBM4 e GBL2, mais recentes. Por sua vez, a norma ISO supracitada, mais do que a CWA, baseia-se na própria CWA 15793:2011 e no LBM3, entre outros documentos, mas sem menção ao GBL ou GBL2 como referenciais teóricos.

O tópico 2.1.3 (*Gestão de risco em bioproteção laboratorial*) tratará da análise comparativa destas normas, sob o ponto de vista de seus conteúdos de recomendação.

Quanto às definições de termos-chave, verfica-se que, em ambas as normas, o significado de bioproteção laboratorial é equivalente ao conceito da OMS supracitado.

A bioproteção é descrita na ISO como uma área complementar à biossegurança laboratorial, dentro do contexto de gestão de risco biológico e que devem ter medidas de controles de risco integradas[15, p.15].

Especificamente, a ISO traz o assunto da bioproteção dentro do tópico 7.2.2 (*medidas de confiabilidade de pessoal*), que também aborda o controle de acesso[15, p.16-17], mas também nos tópicos de segurança da informação (7.5.4)

[h] Órgão com sede em Bruxelas/Bélgica.

segurança de pessoal (7.7), segurança física (8.4), inventário de materais biológicos (8.5) e transporte de material biológico (8.10).

Há menção na norma sobre a necessária integração do laboratório com órgãos de segurança-inteligência no tópico 8.9 (*resposta a emergência e plano de contingência*), quando a ISO afirma:

> "A organização deve assegurar a adequada coordenação com grupos de resposta de emergência externos quando lhes delegar a tarefa. [tradução nossa]"[15, p.22].

Entretanto, na identificação de ameaças e caracterização de riscos, não há menção à importância da troca de informações com os setores de segurança-inteligência, focando a tarefa como se completamente interna ao laboratório (*organización*).

Considerando, por sua vez, a CWA, apesar de mais detalhada na descrição da estratégia de avaliação de risco, a identificação de perigos é igualmente um processo tido como precipuamente restrito ao ambiente interno organizacional:

> "*O primeiro passo no processo de gerenciamento de risco é identificar todos os perigos*[i] *que são relevantes para o biorrisco. É útil envolver toda a equipe de trabalho nesse processo e usar* inputs *de especialistas em segurança [*safety*] e gerenciamento de risco. [*tradução e grifos nossos*]"*[65, p.17].

Há breve menção sobre a utilização de "expertise externa ou especializada não encontradas na instalação"[65, p. 18], entretanto não se mencionam qual seria e como esta expertise externa poderia contribuir com o processo.

De forma análoga à ISO, mas de maneira um pouco mais extensa e detalhada, o documento traz recomendações focada em biossegurança laboratorial, embora aborde algums áreas de importância conjunta também para a bioproteção.

No tópico sobre gerenciamento operacional e de infraestrutura, são realizadas sugestões nas áreas de: proteção (*security*) física; proteção de dados; controle de estoques; transporte; e proteção de pessoal[65, pp.34-39].

[i] Perigo (*hazard*), na CWA 15793:2011, é "fonte, situação ou ato com o potencial de causa um dano. E dano (harm) é "efeito adverso na saúde das pessoas, animais, plantas, meio-ambiente e propriedades[65, p.12]. Neste sentido, toda ameaça à bioproteção, por exemplo um grupo bioterrorista, é também um perigo, à luz desta norma.

2.1.2.5 Bioproteção laboratorial na ABNT NBR 17069-1:2023

A Associação Brasileira de Normas Técnicas (ABNT) é o foro nacional de normatização. As normas técnicas, como a 17069-1, de 30 de maio de 2023, foram elaboradas por uma Comissão de Estudo (CE) da ABNT[18].

As normas publicadas pela ABNT, assim como as normas internacionais ISO, são voluntárias e não suprem requisitos legais, isto é, são respectivamente de aplicação facultativa e de regulamentam nenhum dispositivo legal[18].

Sob o título geral Biossegurança e bioproteção – infraestrutura laboratorial", a norma tem a previsão de conter as seguintes partes:

1. Parte I: Requisitos específicos para o nível de biossegurança 1 (NB-1);
2. Parte II: Requisitos específicos para o NB- 2; e
3. Parte III: Requisitos específicos para o NB-3[18, p. v].

Ela traz na seção de termos e definições, conceitos de biossegurança e bioproteção laboratoriais compatíveis com os da OMS e dos CDC.

Define a "classe de risco 1" como "agentes biológicos conhecidos por não causarem doenças em humanos, animais vegetais e ao meio ambiente"[18, p.3]. E o NB-1 como o nível básico de biocontenção, indicado para o trabalho com agentes biológicos da classe de risco 1[18, p.4].

A Norma Brasileira (NBR) 17069-1:2023 foi desenvolvida

> *"com o objetivo de promover a confiança e a segurança na operação de laboratórios de nível de biossegurança (NB-1), no que se refere especificamente à infraestrutura laboratorial adequada para este nível de biossegurança (...)*
> *Embora esta parte da ABNT NBR 17069 aborde os temas da biossegurança e bioproteção, não existem elementos de bioproteção significativos relacionados à infraestrutura, como utilidades e/ou equipamentos a serem destacados para o nível de biossegurança-1 (NB-1)."*[18, pp.v-vi]

De fato, com exceção do título e do último parágrafo acima, não existe nenhuma menção no documento de 26 páginas à bioproteção laboratorial. Entre as 24 referências bibliográficas, não há nenhuma que trate especificamente de bioproteção laboratorial, nem mesmo o GBL da OMS.

Na introdução da norma, “as utilidades e/ou equipamentos a serem destacads para o nível de biossegurança 1 (NB-1)”, com a finalidade de servirem de medida de controle de riscos específicos de bioproteção laboratorial, “serão apresentados em normas posteriores que abordarão procedimentos relacionados ao tema *[bioproteção] [grifo nosso]*”[18, p. vi].

Causa estranheza que a norma afirme que “não existem elementos de bioproteção significativos (...) para o NB-1” sem referenciar. Conforme veremos adiante, esta afirmação não tem cabimento teórico, à luz das principais diretrizes de bioproteção laboratoriais existentes.

Melhor seria a norma ter restrito o seu título e escopo ao tema de biosserguança laboratorial unicamente, para não induzir que a bioproteção laboratorial estaria sendo contemplada, em seu componente de infraestrutura, ao não se adotarem medidas de controle de riscos essenciais (MCE) para a bioproteção.

2.1.2.5 Bioproteção laboratorial e governança multilateral

Nas últimas décadas, ênfase foi dada no trabalho laboratorial seguro (*safe*) com agentes biológicos, particularmente com a publicação do LBM4 e do BMBL6. Mas este não foi o caso da bioproteção laboratorial, cuja ênfase dos países para a criação de arcabouços de governança se situa muito atrás daquela da biossegurança[22, p.45].

No caso brasileiro, cuja implementação e supervisão (*oversight*) de biossegurança em LAC prescinde de regulamentação adequada[3], há uma dupla omissão regulatória. A revisão do regulamento e da legislação internacional sobre bioproteção laboratorial ajudariam o país a moldar a sua governança.

Independente da existência ou não de normativa nacional sobre gestão de biossegurança e bioproteção laboratoriais, é responsabilidade de todas as organizações que trabalham com agentes e toxinas biológicas garantir que a operação seja segura (*safe*) e protegida (*secure*)[13, p.31].

Em 2021, na 74ª Assembleia Mundial de Saúde (AMS), a importância da bioproteção laboratorial foi reconhecida pelos Estados-Parte da Organização Mundial de Saúde (OMS). Esse reconhecimento da AMS serviu de base para a Organização elaborar o GBL[22, p.2].

De fato, o guia da OMS foi escrito com a finalidade de propor uma estrutura de governança para identificar, gerir e supervisionar riscos de bioproteção em atividades laboratoriais[22, p.2].

Em conjunto com outros manuais de biossegurança de grande repercussão internacional (LBM4, BMBL), mas que cada vez mais abordam, conforme revisado, aspectos de bioproteção laboratorial, o GBL constitui um ponto de partida para a organização de modelos de gestão de bioproteção laboratorial.

Ressalte-se que a obrigação dos laboratórios e instalações com material biológico de operarem de maneira segura e protegida é decorrente da responsabilidade dos Estados, mediante compromissos internacionais, em garantir um monitoramento de biorriscos efetiva.

Os três principais compromissos internacionais vinculantes são a Convenção de Armas Biológicas, a Resolução 1.540 e o Regulamento Sanitário Internacional.

Estes três instrumentos, em conjunto com outras estruturas e compromissos menos abrangentes, mas igualmente importantes, como o Protocolo de Cartagena[j] e Biossegurança e os regimes multilaterais de controle de exportação de bens e tecnologias duais, entre outros, constituem o arcabouço internacional para legislação sobre biorriscos (*international framework for biological risk legislation*)[22].

2.1.2.5.1 Bioproteção laboratorial e a Convenção de Armas Biológicas

A Conveção sobre a Proibição do Desenvolvimento, Produção e Estoque de Armas Bacteriológcas (Biológicas) e Toxínicas e sobre sua Destruição (CPAB, na sigla em português; e BWC, na sigla em inglês)[48] foi a primeira Convenção a proibir o uso de toda uma categoria de arma de destruição em massa (ADM), as armas biológicas. Ela foi assinada em 10 de abril de 1972 e entrou em vigor em 16 de março de 1975.

[j] O Protocolo de Cartagena em Biossegurança entrou em vigor em 11 de setembro de 2003, com 103 países signatários. Ele complementa a Convenção sobre a Diversidade Biológica, no sentido de lidar com riscos biotecnológicos emergentes, principalmente que resultam em organismos geneticamente modificados (OGM). O Protocolo de Cartagena trata da necessidade de segurança, precaução e equilíbrio entre os benefícios econômicos potenciais e a saúde pública[93].

Em seu artigo primeiro, a CPAB define que nenhum Estado-Parte[k] deve, em nenhumas circustância, desenvolver, produzir, estocar, adquirir ou reter: i. "agentes microbiológicos ou outros agentes biológicos ou toxinas, quaisquer que sejam sua origem ou método de produção, de tipos e em quantidades que não se justifiquem para fins profiláticos, de proteção ou outros fins pacíficos"; e ii. "armas, equipamentos ou vetores destinados à utilização destes agentes ou toxinas para fins hostis ou em conflitos armados"[48].

Depreende-se da CPAB que armas biológicas teriam uma conceituação finalística, uma vez que todo material biológico utilizado para fins ofensivos, com ou sem equipamentos e/ou vetores associados poderia ser considerado uma arma biológica[1, p. 89].

Os artigos terceiro e quarto formam a cerne da Convenção ao determinar, respectivamente, que todos os Estados-Parte devem:

> "em hipótese alguma ajudar, encorajar ou induzir qualquer Estado, grupo de Estados ou organizações internacionais a produzir ou adquirir qualquer agente, toxina, arma, equipamento ou meios de disseminação previstos no Artigo primeiro da Convenção.
> (...)
> tomar qualquer medida necessária para proibir e prevenir o desenvolvimento, produção, estoque, aquisição ou retenção de agentes, toxinas, armas, equipamentos e meios de disseminação (...) dentro do seu Estado, dentro de sua jurisdição ou em qualquer lugar sob seu controle [tradução nossa]."[48]

Trata-se, portanto, de uma norma multilateral que obriga Estados. Entretanto, a depender da ação ou omissão do Estado, um MBGC, por exemplo, utilizado de maneira lícita por um laboratório – para pesquisa, por exemplo – pode se transformar em arma biológica nas mãos de atores estatais estrangeiros.

Portanto, se um material biológico for extraviado de um laboratório biomédico e for usado num ataque biológico por um ator estatal, haverá um incidente que a CPAB busca prevenir. Esse cenário obriga a CPAB a se preocupar com as capacidades laboratoriais e o gerenciamento de risco biológico de biossegurança e bioproteção

Neste sentido, a custódia de MBGC e a realização de PAI/PGC se constituem em objetos de interesse da Convenção, que publicou, em 2008,

[k] Em 2024, havia 187 Estados-Parte e quatro signatários da CPAB[120].

documento específico sobre biossegurança e bioproteção, utilizando os conceitos[l] segundo a OMS[118].

Neste documento, resta clara a percepção dos Estados-parte de que tanto a biossegurança quanto a bioproteção laboratoriais estão concatenadas com os propósitos e objetivos da Convenção.

Sobre a relação específica entre BPL e a CPAB, está expressamente reconhecido que os conceitos de bioproteção laboratorial estão incluídos nos artigos III e IV, supracitados[118].

Além disso, é lembrado que as Segunda (1986), Terceira (1991) e Quarta (1996) Conferências de Revisão[m] da CPAB mencionaram: "a importância de (...) legislação sobre proteção física de laboratórios e instalações para prevenir acesso não autorizado e a remoção de material patogênico ou tóxico [tradução nossa]."[118]

No Encontro dos Estados-Parte da CPAB em 2003 alguns países (e grupos de países) expressamente demonstraram interesse em promover assistência em biossegurança e bioproteção laboratoriais: Austrália, Canadá, União Europeia, Alemanha, Rússia, Suiça, Reino Unido, Irlanda e os EUA. Na ocasião, circulou um documento informal de propostas na área que incluía sugestões de tópicos que acordos de bioproteção laboratorial deveriam considerar:

1. Boas práticas científicas;
2. Listas de controle nacionais flexíveis;
3. Regras de embalagem e rotulagem;
4. Controle de acesso e sistemas de supervisão em instituições selecionadas;
5. Análise de antecedentes de pessoal;
6. Atividades de monitoramento abrangente e integrada;
7. Identificação e registro de instalações selecionadas, sistemas de transporte e pessoal;
8. Mecanismo para criar e manter dados detalhados e precisos de custódia, transporte, estoque, uso, pessoal com aprovação de trabalho e recursos selecionados [tradução nossa].[118]

[l] O documento cita que nas reuniões da CPAB em 2003, um delegado usou uma explicação didática para ajudar os participantes a entender a diferença entre os dois termos: "Biossegurança protege as pessoas dos germes; bioproteção protege os germes das pessoas"[118, p.3].

[mm] As conferências ocorrem a cada 5 anos, em média, para revisarem e emendarem a CPAB estabelecerem metas e diretrizes para os cinco anos seguintes.

Além disso, o documento trazia cinco propostas para o fortalecimento da cooperação interna:

1. Identificar uma agência coordenadora nacional ou criar uma nova autoridade central de supervisão;
2. Desenvolver um plano de implementação da bioproteção nacional;
3. Usar organismos de supervisão ética governamentais e não-governamentais para criar uma cultura nacional de bioproteção;
4. Implementar programas de alerta e treinamento coordenados; e
5. Incorporar medidas de bioproteção em guias de boas práticas ou outras normas não vinculantes.

A Sexta Conferência de Revisão da CPAB (2006) exortou, por fim, os Estados-Parte a: "garantirem que agentes biológicos e toxinas relevantes para a Convenção sejam protegidos e salvaguardados, inclusive por meio de medidas no controle de acesso e na manipulação de tais agentes e toxinas".[118]

Ressalte-se que, em 1987, a CPAB introduziu medidas de construção de confiança (*confidence building measures* – CBM, na sigla em inglês). Desde então, o s Etados-Parte precisam submeter relatórios anuais à Unidade de Apoio de Implementação (ISU, na sigla em inglês) – que é a estrutura física e secretarial da CPAB – descrevendo seis CBM implementadas nacionalmente:

1. Troca de informações sobre: i. centros de pesquisa e laboratórios; e ii. programas de biodefesa;
2. Troca de informaçnoes sobre epidemias de doenças infecciosas ou ocorrências similares causadas por toxinas;
3. Encorajamento da publicação de resultados e promoção do uso do conhecimento obtido [*com programas de biodefesa*];
4. Declaração da legislação, regulamentação e outras medidas;
5. Declaraçnao de atividades passadas em pesquisa biológica ofensiva ou defensiva e programas de desenvovlimento; e
6. Declaração de instalação para a produção de vacinas [*tradução e grifos nossos*].[22, p. 51-52]

2.1.2.5.2 Bioproteção laboratorial e a Resolução 1540

O Conselho de Segurança da Organização das Nações Unidas (CSNU) aprova a sua Resolução 1540[59], em 18 de abril de 2004, pouco após os ataques de bioterrorismo com antraz nos EUA, em 2001; e da promulgação da lei do bioterrorismo (*Public Health Security and Bioterrorism Preparedness and Response Act*) pelos EUA, em 2002[1, pp. 47-48].

Internalizada no Brasil por meio do Decreto nº 7722, de 20 de abril de 2012[60], a resolução onusiana afirma que a proliferação de armas biológicas (além de químicas e nucleares) é uma ameaça à paz e à segurança internacionais; e manifesta grave preocupação com as ameaças do terrorismo e do tráfico criminoso de armas biológicas (entre outras armas QBRN)[59].

Ela serve como uma complementação, de certo modo, à CPAB, na medida em que está focada em prevenir a obtenção, por atores não estatais[n], de armas biológicas e materiais correlatos. Por sua vez, a Convenção se volta precipuamente para vincular Estados contra a proliferação de armas biológicas e contra eventual apoio para que outros Estados obtenham acesso a elas.

Em seus doze artigos, o CSNU se utiliza do Capítulo VII da Carta das Nações Unidas ("Ação relativa a ameaças à paz, ruptura de paz e atos de agressão") para:

> "1. Decidir que todos os Estados devem se abster de prover qualquer forma de apoio a atores não estatais que tentem desenvolver, adquirir, produzir, possuir, transportar, transferir ou utilizar armas nucleares, químicas e biológicas e seus meios de disseminação.
> 2. Decidir também que todos os Estados, de acordo com seus procedimentos nacionais, devem **adotar e reforçar leis apropriadas e efetivas que proíbam atores não estatais a produzir, adquirir, possuir, desenvolver, transportar, transferir ou utilizar** armas nucleares, químicas e biológicas e seus meios de disseminação, em particular para razões terroristas (...)
> 3. Decidir também que todos os Estados devem tomar e **reforçar medidas para estabelecer controles domésticos para prevenir a proliferação de armas** nucleares, químicas ou biológicas e seus meios de disseminação, incluindo estalebecer os controles apropriados sobre materiais relacionados e para esse fim devem:
> a. Desenvolver e manter **medidas apropriadas e efetivas para prestar contas e proteger tais itens em produção**, uso, estoque ou transporte;
> b. Desenvolver e manter medidas apropriadas e efetivas de proteção física; (...) [tradução e grifos nossos] "[59]

Resta claro, portanto, que o sistema ONU impõe ao Estados que implementem medidas de bioproteção laboratorial adequadas, a fim de proteger

[n] Pessoas ou grupos que atuam independentes de uma autoridade oficial governamental[22, p. 51].

materiais biológicos que, se utilizados de maneira intencional e ofensiva, caracterizam o uso de armas biológicas por atores não estatais.

Com a Resolução 1540, o CSNU estabeleceu um comitê, conhecido como o Comitê 1540, que funciona como uma estrutura física e secretarial com vistas a apoiar e monitorar a implementação da resolução e permitir a troca de informações sobre as medidas tomadas pelos países-membros da ONU (https://www.un.org/en/sc/1540/), entre outras competências[59, 61].

Em 30 nov. 2022, o CSNU instituiu a Resolução 2663[61] que reiterou a importância de todos os Estados implementarem a Resolução 1540 de maneira integral e extendeu o mandato do Comitê 1540 por mais dez anos, até 2032.

2.1.2.5.3 Bioproteção laboratorial e o Regulamento Sanitário Internacional

O Regulamento Sanitário Internacional (RSI) está em sua terceira edição, aprovada em 2005 e vigente desde 15 de junho de 2007. Tem por objetivo auxiliar a comunidade internacional para prevenir e responder a riscos iminentes à segurança da saúde pública global[52, 53].

Segundo o RSI, que gera vinculação legal dos 194 Estados-Parte da OMS, cabe aos países-membros o compromisso de avaliar, desenvolver e manter capacidades essenciais (*core capacities*) de vigilância, avaliação e resposta a eventos de saúde[o]. E, entre as capacidades essenciais, listadas em seu Anexo 1A.6[52, p.41], estão as adequadas capacidades laboratoriais.

As "adequadas capacidades laboratoriais" pressupõem o adequado gerenciamento de risco biológico nessas instalações. Por sua vez, o gerenciamento de risco biológico depende da implementação de medidas efetivas de controle de risco de biossegurança e de bioproteção laboratoriais[54].

Com base na adesão brasileira ao RSI, portanto, ratifica-se a ideia de que organizações que trabalham com agentes biológicos e toxinas têm a responsabilidade de operar segura (*safely*) e protegidamente (*securely*). Esta é uma exigência obrigatória em nível multilateral. Cabe ao Estado brasileiro regulamentar e supervisionar esta obrigação perante o RSI, a OMS e a comunidade internacional.

---

[o] Evento, segundo o RSI, "significa uma manifestação de doença ou uma ocorrência que cria potencial para doença."[52, p. 7]

Na estrutura (*framework*) de monitoramento e avaliação do RSI, a gestão de biossegurança e bioproteção laboratoriais é um dos aspectos que deve ser detalhado pelos Estados-Parte no relatório de autoavaliação (SPAR, na sigla em inglês). Além disso, é uma das dezenove áreas avaliadas pelas Avaliações Externas Conjuntas do RSI/OMS (JEE, na sigla em inglês)[22, p. 2].

Em maio de 2020, na vigência da pandemia da COVID-19, a Assembléia Mundial da Saúde (WHA, na sigla em inglês) adotou a Resolução WHA73.8, intitulada “Fortalecendo a Preparação para Emergências em Saúde: Implementação do Regulamento Sanitário Internacional (2005)”, que lembra os

> *“compromissos feitos por meio das Metas de Desenvolvimento Sustentável, incluindo o fortalecimento de capacidade de todos os países ... para alerta precoce, redução de risco e gestão de riscos em saúde globais e nacionais. (*tradução nossa*).”*[64]

E urge os estados membros da OMS, incluindo o Brasil, a

> “*continuar a construir capacidades-chave para detectar, avaliar, notificar e responder a eventos de saúde pública conforme definido no Regulamento Sanitário Internacional [*tradução nossa*]”*[64].

Em primeiro lugar, portanto, existe uma relação direta da necessidade de o Estado garantir a implementação de medidas adequadas de monitoramento de biorrisco de biossegurança e de bioproteção laboratoriais para fins de atender às capacidades essenciais (e obrigatórias, isto é, vinculantes) exigidas pelo RSI/OMS. E este monitoramento de risco (*risk assessment*) é contínuo e pressupõe medidas de medição e controle destes riscos.

Em segundo lugar, ressalte-se que acidentes ou incidentes de biossegurança e bioproteção laboratoriais devem ser caracterizados como eventos de interesse do RSI. Alguns deles são de notificação obrigatória para a OMS, inclusive.

Para ser caracterizado como um evento de saúde pública que precisa ser notificado para a OMS, o RSI traz um “instrumento de decisão para avaliação e notificação de eventos” em que há quatro perguntas-base.

Caso um evento seja vinculado a respostas afirmativas a, no mínimo, duas das quatro perguntas-base, esse evento deve ser obrigatoriamente notificado para a OMS (via ponto focal do RSI)[1, p.169; 52]:

1. O impacto do evento contra a saúde pública é grave?

2. O evento é incomum ou inesperado?
3. Há um risco significativo de disseminação internacional?
4. Há um risco significativo de restrições de viagem e comércio?

Relacionado à segunda pergunta do instrumento (“o evento é incomum ou inesperado[p]?”), percebe-se que um ataque biológico, *per si*, seria um evento de saúde incomum ou com chances de ser inesperado.

De modo que, se o agente disseminado tiver impacto grave sobre a população (pergunta 1) ou risco de propagação internacional (pergunta 3) ou risco significativo de restrições ao comércio ou viagens internacionais (pergunta 4), o evento de ataque biológico deve ser notificado[1, 52].

Na prática, um ataque biológico tenderá sempre a ser notificado, porque dificilmente seu impacto não será grave o suficiente para ser desprezível à luz do RSI. Os ataques biológicos são eventos historicamente de grande comoção e terror social, com impactos sociopsicológicos graves. Além disso, o número de casos e mortes para esse tipo de evento costuma ser grande para os locais em que ocorrem.

Segundo o RSI, a notificação de um evento se fundamenta na ideia de detecção e alerta precoce de emergência em saúde de interesse nacional ou internacional (ESPIN ou ESPII) potenciais. Desta forma, o risco de disseminação intencional (ou não) de ABTS/MBGC, são de interesse da OMS e de seu RSI, porque estão normalmente associados a patógenos que apresentam potencial de causar ESPIN ou ESPII.

2.1.2.5.4 Modelos de Governanças Nacionais

O LBM4 da OMS traz três abordagens para o desenvolvimento de regulamentações de biossegurança nacionais como parte de um arcabouço legislativo para a biossegurança laboratorial[16, p.93].

[p] Exemplos de eventos incomuns são os causados por um agente desconhecido; ou quando a evolução é mais grave do que o esperado ou os sintomas são raros; ou quando a ocorrência do caso é rara para a região, estação do ano ou população afetada. Exemplos de eventos inesperados são os causados por doença ou agente que já tenha sido eliminado ou erradicado naquele Estado ou que nunca tenha sido notificado anteriormente[1,55].

Em que pese a menção exclusiva ao termo biossegurança laboratorial, as abordagens podem se estender igualmente para a BPL[16, p.93]:

1. Abordagem baseada em atividades – o método dess abordagem consiste no desenvolvimento de regulamentação que se aplica ao tipo de trabalho/pesquisa que é realizada em um agente biológico (ao invés de no agente biológico em si). Por exemplo, regulamentação instituída para todo o trabalho que envolva DNA recombinante.
2. Abordagem baseada em listas – o método dessa abordagem consiste em desenvolver um ou mais conjuntos de regulamentações nacionais vinculadas a listagem de agentes biológicos aos quais as regulamentações se aplicam.
3. Abodagem de grupos de perigo/risco – o método dessa abordagem consiste em classificar os agentes biológicos em grupos de perigo ou risco baseados nas características e perfil epidemiológico de cada agente. Regulamentações são, em seguida, instituídas para aplicar a cada grupo de perigo/risco, que pode variar de 1 a 4[q].

A abordagem ABRE de monitoramento de risco pode ser considerada também uma forma de abordagem de governança, na medida em que a legislação se baseie em estipular requisitos de controle de risco baseados nas evidências (informações coletadas) e nos riscos quantificados.

Tanto que o GBL2 defende que poderia ser uma solução viável (*feasible solution*) para os países a utilização, para o arcabouço normativo de B2L, de uma abordagem híbrida com elementos baseados em risco e evidência (abordagem ABRE) e uma abordagem baseada em lista regularmente atualizada[22, p.46].

[q] A definição clássica dos grupos de risco sugere que o Grupo de Risco 1 (risco individual e comunitário inexistente ou baixo) – um microorganismo que improvavelmente causa doença humana ou animal. Grupo de Risco 2 (risco individual moderado, risco comunitário baixo) – um patógeno que pode causar doença humana ou animal, mas é improvável que seja um perigo grave ao pessoal do laboratório, à comunidade, aos rebanhos e ao meio ambiente; exposição laboratorial pode causar infecção séria, mas com tratamento e medidas preventvas efetivas disponíveis e risco associado de disseminação limitado. Grupo de Risco 3 (risco individual alto, risco comunitário baixo) – um patógeno que normalmente causa doença grave humana ou animal, mas não se dissemina usualmente de um indivíduo infectado para outro; tratamento e medidas preventivas estão disponíveis. E Grupo de Risco 4 (risco individual e comunitário alto) – um patógeno que usualmente causa doença humana ou animal grave e que pode facilmente ser transmitido de um indivíduo para outro, direta ou indiretamente. Tratamento e medidas preventivas não estão normalmente disponíveis[16, 35].

Uma autoridade nacional determinaria uma lista de materiais biológicos de grandes consequências (MBGC) - como patógenos, toxinas, sequências nucleicas (sequências de preocupação – *sequences of concern*) e fenótipos desenvolvidos - que podem ser utilizadas em ou serem o resultado de pesquisas de grandes consequências (PGC). Definir quais MBGC e PGC requerem regulamentação de B2L deve ser baseado em avaliação de risco e conhecimento científico[22, p.46].

A OMS propõe que uma autoridade nacional crie um comitê de especialistas independentes em B2L para realizar o monitoramento de risco e/ou regularmente revisá-lo, a fim de identificar MBGC que precisam de regulamentação. Desta forma, estabelecer-se-ia um sistema de dois níveis (*two-tier system*) para a regulação nacional de MBGC e PGC (**Figura 2**):

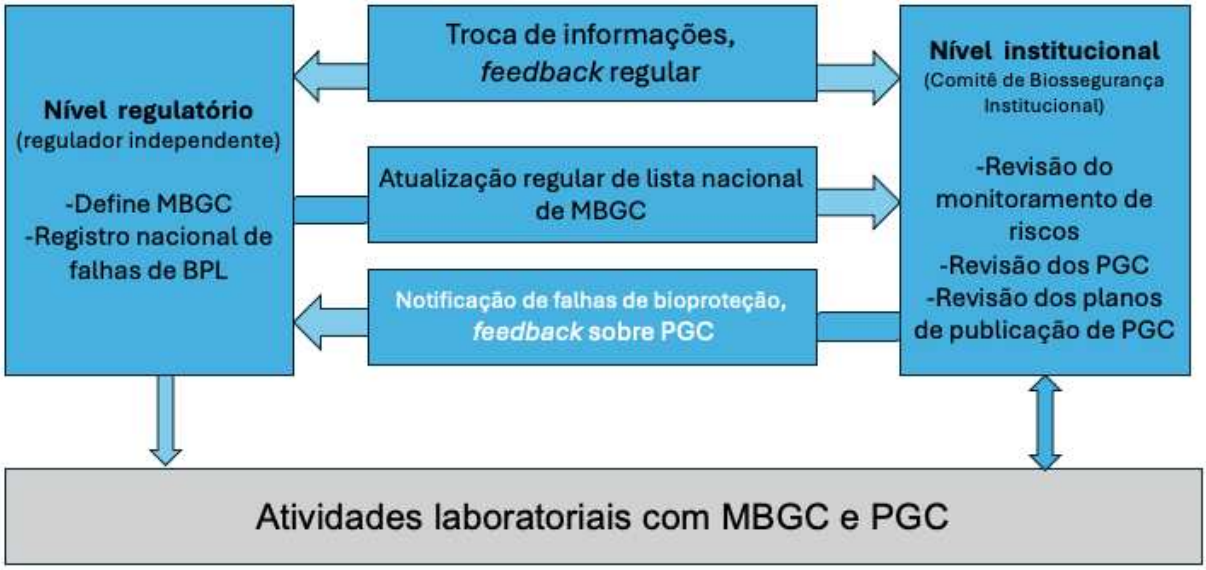


Figura 2 – *Visualização esquemática do sistema de dois níveis para a governança nacional de MBGC e PGC* (adaptado de OMS[22, p. 47] pelo autor)

A ideia central do sistema de dois níveis é a existência, em nível laboratorial/institucional, de um Comitê de Biossegurança Institucional (CBI), também responsável por questões de BPL; e, no nível regulatório, seja nacional ou estadual – a depender do grau de federalização de um Esatdo -, uma autoridade independente do laboratório e seus órgãos que defina os MBGC e realize a

supervisão adequada, com troca de informações regulares sobre falhas, MBGC e PGC[22].

2.1.2.5.4.2 O Guia para a Implementação de Requisitos Regulatórios da OMS e a Bioproteção Laboratorial

Em 2020, quatro anos antes do GBL2, a OMS publicou um *Guia para a implementação de requisitos regulatórios de biossegurança e bioproteção em laboratórios biomédicos* [tradução nossa][123] em que buscou

> "informar e apoiar autoridades legislativas e executivas nacionais, planejadores de políticas públicas (*policy-makers*) e reguladores, em criar, aprimoram e implementar um arcabouço regulatório para garantir o mais alto padrão de biossegurança e bioproteção laboratoriais".[123, p. 2]

O Guia se baseia em sete passos para a implementação das medidas:

> 1. "Mobilizar compromisso e recursos nacionais;
> 2. Conduir uma avaliação nacional;
> 3. Estabelecer mecanismos operacionais e institucionais, em nível nacional, e desenvolver regulações mais bem adaptadas;
> 4. Fortalecer o conhecimento regulatório;
> 5. Implementar e reforçar regulamentações;
> 6. Estabelecer redes de troca de informação nacionais e parcerias internacionais; e
> 7. Revisar performance e adaptabilidade [tradução nossa]"[123, p. 16].

Ao se revisarem passo-a-passo as recomendações da OMS na perspectiva da BPL, percebem-se algumas dignas de nota. No passo 1 (*Mobilizar compromisso e recursos nacionais*), é sugerido que uma política nacional de B2L seja única ou parte de uma outra política (ex. política de segurança da saúde – *health security policy*)[123, p.18].

A OMS também explicita quais grupos podem compor um comitê nacional de B2L (NBBC, na sigla em inglês), órgão fortemente recomendado, citando expressamente os "representantes da segurança nacional" (*national security representatives*)[123, p.18].

Quanto ao passo dois (*Conduzir uma avaliação nacional*), é destacada a necessidade de mapear infraestrutura e recursos laboratoriais e a governança existente, antes de planejar novo arcabouço. Entre os aspectos a serem mapeados está "o estado atual da custódia de agentes biológicos e de biotecnologias"[123, p.21].

Quanto ao passo três (*Estabelecer mecanismos operacionais e institucionais, em nível nacional, e desenvolver regulações mais bem adaptadas*), o

Guia cita explicitamente que um arcabouço regulatório nacional de biossegurança e bioproteção (NBBF, na sigla em inglês) deve constar, entre seus elementos, um "programa de bioproteção" e "monitoramento de risco"[123, p. 25].

Além disso, afirma ser vital para o NBBF abordar elementos que regulem a posse, uso e acesso a materiais biológicos, com objetivo primário de prevenir acesso não autorizado. Neste sentido, o documento exemplifica que, em países com sistemas regulatórios de BPL bem definidos, leis exigem que os laboratórios possuam licenças e/ou autorização de segurança (*security clearance*), além de requisitos específicos para a gestão de bioproteção laboratorial, como treinamentos, gestão de estoque/inventário e de informações e procedimentos de proteção no transporte[123, p.36].

O Guia da OMS é taxativo em afirmar que a busca de uma legislação integrada de biossegurança e de bioproteção laboratoriais pode ser problemática, de modo que muitos países regulamentam as duas áreas separadamente. É recomendado, por fim, que o NBBF promova avaliação regular e abrangente do monitoramento de potencial de uso dual das atividades laboratoriais no país.[123, p.36]

Quanto ao passo quatro (*Fortalecer o conhecimento regulatório*), há expressa preocupação da OMS em garantir um processo de tomada de decisão que considere assessoramento científico adequado. Para tanto, o Guia propõe a criação de um comitê de assessoramento científico independente e/ou desenvolva competências de assessoramento internamente em órgãos ou agências governamentais[123, p.52].

Quanto ao passo cinco (*Implementar e reforçar regulamentações*), a OMS cita diversos desafios potenciais, mas quase todos focados na implementação de aspectos de biossegurança laboratorial.[123, pp.43-50]

Quanto ao passo seis (*Estabelecer redes de troca de informação nacionais e parcerias internacionais*), são especificadas possíveis canais interinstitucionais em nível nacional: entre autoridades regulatórias (ex. saúde humana, saúde animal, proteção ambiental, defesa); organizações científicas; organizações de pesquisa; indústria. Verifica-se, portanto, pouca preocupação com a interação do setor saúde com segurança-inteligência[123, p.51].

Quanto ao sétimo e último passo (*Revisar performance e adaptabilidade*), considera-se a necessidade de revisão e avaliação regulares do NBBF com o fito de verificar a efetividade e o melhoramento contínuo[123, pp. 52-53].

2.1.2.6 Componentes da bioproteção laboratorial

Apesar de o termo proteção (*security*) *tout court* estar normalmente associado à proteção física das instalações[2], um programa efetivo e completo de bioproteção costuma ser descrito como dividido em cinco componentes[2]:

1. Bioproteção das instalações;
2. Bioproteção de pessoal;
3. Bioproteção de materiais;
4. Bioproteção do transporte; e
5. Bioproteção de dados.

O conjunto destes cinco componentes, que interagem entre si e se complementam, formam o conceito de sistema de proteção ou, mais especificamente, sistema de bioproteção laboratorial. As medidas executadas em cada componente, isoladamente, em tese, configuram as partes de um sistema de medidas de controle de risco de bioproteção.

Na prática, entretanto, há dificuldade na separação entre as medidas tomadas por cada um dos componentes, pois podem ser medidas de intesecção, isto é, comuns a dois ou mais componentes (**Figura 3**).

Figura 3 – *Rosa clássica de medidas de controles de risco de bioproteção laboratorial* (adaptado de SALERNO & GAUDIOSO[2, p. 38] pelo autor)

2.1.3 Gestão de risco em bioproteção laboratorial

De maneira geral, o risco é o "efeito da incerteza", considerado o efeito como "um desvio do esperado" e a incerteza como "o estado, inclusive parcial, da deficiência da informação relacionada com a compreensão ou com o conheciemtno de um evento, seu impacto ou sua probabilidade".[15, p. 4]

O risco de biossegurança e de bioproteção, tal qual um risco qualquer, é função da chance (*likelihood*) e da gravidade dos impactos ou consequências (*consequences*) potenciais de um evento[2, p. 13] (**Figura 4**).

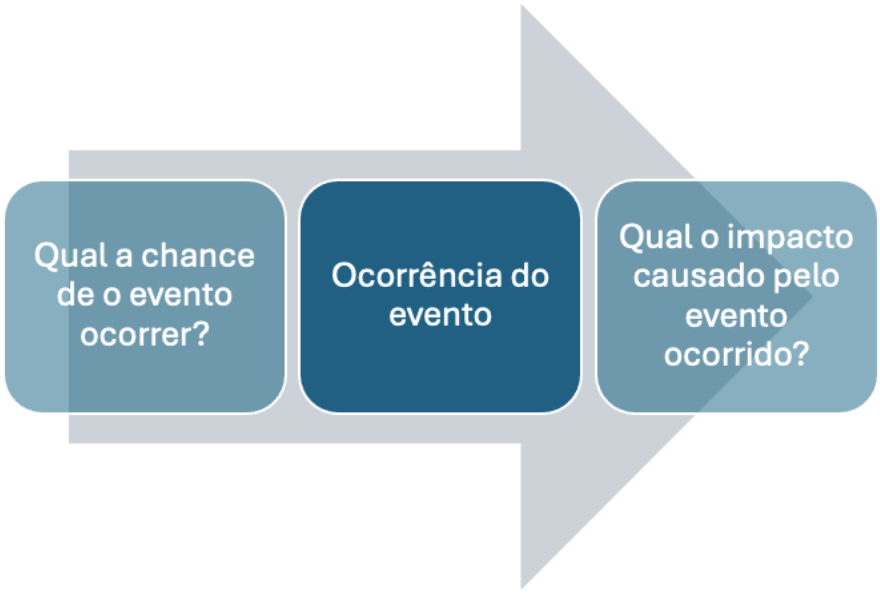


Figura 4 – *Relação entre o tempo, a chance (likelihood) e o impacto (consequence) de um evento biológico* (adaptado de SALERNO & GAUDIOSO[13, p. 49] pelo autor)

A gestão de risco de bioproteção laboratorial é uma combinação da avaliação de risco ("qual o risco?") com medidas de redução de risco (*risk reduction*). A gestão de risco (*risk management*) define e prioriza os riscos que existem no laboratório ou derivados do que existe no laboratório, enquanto a redução de risco determina como tais riscos serão mitigados[2, p. 15].

Com a finalidade de responder sobre qual o risco, é necessário conhecer quais os eventos potenciais ("o que pode dar errado?"); qual a chance deste evento ocorrer e qual o impacto potencial deste evento (caso o evento ocorra)[45].

> "Uma *avaliação de risco é um processo sistemático e estruturado para analisar e determinar o risco, e a avaliação de risco deve servir de base para a gestão de risco* (tradução nossa)." [2, p.13]

Considerando que os objetivos da biossegurança e da bioproteção laboratoriais são diferentes, o conceito de risco biológico será diferente para as duas avaliações de risco[13, p.48] (**Figura 5**):

Figura 5 – *Três passos gerais para a avaliação de risco (risk assessment), incluindo definição de eventos (situações), identificação (definição) dos riscos e medição (evaluation) dos riscos* (elaborado pelo autor).

O processo de identificação de riscos *lato sensu*, por muitos usado como sinônimo de avaliação de risco (*risk assessment*) pode ser descrito por esse tripé de ações:

1. Definir as situações
2. Definir os riscos associados
3. Medir os riscos (*risk evaluation*)

A nomenclatura associada à gestão de risco varia conforme os autores. A OMS detalha que só se pode falar em risco após a sua medição em termos de chance e impacto[22]. Entretanto, Salerno & Gaudioso colocam a definição (enquanto identificação) dos riscos antes de sua medição em termos de chance e impacto[13, p. 49] no tripé de ações supracitado.

Vale frisar, entretanto, que as determinações do GBL2 são as mais recentes sobre bioproteção laboratorial e conseguem sistematizar com significativa

organização e rigor técnicos as abordagens sobre o tema publicadas nas décadas anteriores[22].

Segundo o CWA 15793:2011, a gestão de biorrisco (*biorisk management* – BRM, na sigla em inglês) é definida como

> *"um sistema ou processo para controlar riscos de segurança e de proteção associados ao manuseio ou estocagem e descarte de agentes biológicos e toxinas em laboratórios e instalações."*[65]

Gestão de biorriscos, portanto, objetiva o controle dos riscos biológicos, por meio de ferramentas e ações que permitem prevenção (zerá-lo) e mitigação (diminui-lo a níveis aceitáveis) em monitoramento contínuo[2, 13, 16, 22].

A gestão de biorrisco laboratorial é descrita como um novo campo, de origem formal que remonta aos primeiros anos da década de 2000. Seu advento é marcado pela ocorrência de incidentes laboratoriais graves como os ataques com antraz, nos EUA, em 2001; e as infecções adquiridas em laboratório por SARS-CoV-1, na Ásia, em 2003 e 2004[13, p.31].

Em resposta, a comunidade científica e de gestores de políticas públicas internacional buscou criar uma abordagem de gestão de risco biológico harmonizada globalmente, a fim de aumentar a percepção e alerta sobre os riscos biológicos e para estabelecer padrões de conformidade para atividades de biossegurança e bioproteção em todo o mundo[13, p.31].

Os dois componentes mais antigos e fundamentais da gestão de risco (*risk management*) são a identificação de riscos e o monitoramento de riscos (*risk assessment)*. Eles só seriam formalmente descritos na década de 1980, com os estudos de Kaplan e Garrick[45, 66].

Desde então, os campos da análise de risco (*risk analysis*) e do monitoramento de risco (*risk assessment*) se expandiram, tornando-se parte de vários processos administrativos e industriais[13, p.32].

Um exemplo das consequências benéficas para a sociedade decorrentes da aplicação sistemática de modelos de gestão de risco é o da aviação comercial. Historicamente, a segurança da aviação foi construída sobre análises reativas de acidentes passados. Nas últimas décadas, com a introdução da análise de risco e a identificação e monitoramento de todas as áreas de risco, a indústria da aviação atingiu níveis altos de segurança[67].

2.1.3.1 O modelo AME

A OMS adotou em 2010 um modelo de gestão de biorrisco chamado AME (*tradução nossa*) para se referir a avaliação-mitigação-efetividade (AMP - *assessment-mitigation-performance -,* em inglês), que foi amplamente utilizado na formação de multiplicadores de gestão de biorrisco nos anos 2010-2016[13, 68].

A ideia central do modelo AME é considerar três elementos críticos "avaliação" (*assessment*), "mitigação" e "efetividade" coletivamente, de modo que não sejam tratados individualmente. A gestão de biorrisco somente acontece quando se apoia concomitantemente nesses três alicerces, como um banco que só se sustenta de pé se houver três pés simultaneamente presentes (**Figura 6**).

Figura 6 – Tripé dos elementos críticos do Modelo AME de gestão de biorrisco (adaptado de SALERNO & GAUDIOSO[13, p. 33] pelo autor)

2.1.3.1.1 Avaliação de risco no modelo AME

O entendimento (*understanding*) do risco é o objetivo central da avaliação de riscos no modelo AME de gestão de biorrisco[13, p.45]. A avaliação de risco (*risk assessment)* nesse modelo é um processo fundamental para compreender os riscos e servir de guia para a mitigação (segundo alicerce do modelo AME)[13, p.33].

O resultado de uma avaliação de risco é a seleção apropriada de medidas de controle de riscos de biossegurança; controle de riscos de bioproteçãs; e outras medidas de salvaguarda, a fim de mitigar os riscos até um nível consderado aceitável[13, p.33].

A avaliação dos riscos de um laboratório biomédico deve ser realizada e revista ao menos anualmente, mas sempre que pesquisas, processos, materiais (incluindo MBGC ou não) e tecnologias mudam. A mudanças destes elements implicam em mudança de risco e na obrigação de nova avaliação[13, p.34].

Uma avaliação de risco efetiva é específica e única para determinado laboratório ou instalação. Ressalte-se que a qualidade do resultado da avaliação depende inteiramente da qualidade das informações coletadas[13, p.34].

Deste modo, as pessoas que participam da avaliação precisam ser intimamente familiarizadas com os agentes custodiados pelo laboratório, pelos procedimentos realizados, pelo próprio pessoal dos diversos setores laboratoriais e com o modo como tudo isso pode significar perigos, ameaças e, eventualmente, riscos[13, p.34].

Uma avaliação de risco ou classificação de risco específica para um agente biológico que apenas considere as características biológicas deste agente não serve para uma avaliação de biorrisco adequada[13, p.34].

2.1.3.1.1 O ciclo PFCA no modelo AME

Nos anos 1950, Edwards Deming propôs o que ficou conhecido como "ciclo de *Deming*" ou "roda de *Deming*" ou ainda "ciclo PFCA" (PDCA, na sigla e inglês). Segundo DEMING (1950), processos de trabalho importantes deveriam ser geridos como um *loop* contínuo de feedback com quatro passos[13, p.40] (**Figura 7**):

Figura 7 – O ciclo PFCA (adaptado de SALERNO & GAUDIOSO[13, p. 41] pelo autor)

1. Planejar uma mudança e determinar objetivos;
2. Fazer – implementar o planejamento, executar o processo e testar a mudança desejada;
3. Checar os resultados obtidos com a implementação e comparar com as metas planejadas; medir a efetividade das ações empreendidas e identificar o aprendizado; avaliar como os riscos estão sendo controlados; e
4. Agir – realizar ações corretivas para resolver as diferenças entre os resultados obtidos e as metas planejadas; analisar as causas da discrepência; tomas as ações com base no que foi aprendido.

As duas normas CWA 15793:2011[65] e a ISO 35001[15] utilizam o ciclo PFCA - o que na primeira é chamada de “princípio PFCA” (*tradução nossa*)[65, p. 5] e, na segunda, é esquematizada com uma “pirâmide descendente com um modelo de gestão de risco biológico” (tradução nossa)[15, p. viii] – como base para a abordagem de

sistema de gerenciamento, construído no conceito de melhora contínua por meio deste ciclo de planejamento, implementação, revisão e melhoramento[65].

2.1.3.2 Monitoramento de risco (*risk assessment*)

O *risk assessment,* traduzido na perspectiva do modelo AME como "análise de risco"[13], ganha outra conotação nos documentos mais recentes da OMS, seja o LBM4[16] ou o GBL2[22].

De uma ideia de definição de ações/situações de perigo/ameaças e medida de controle de riscos associadas a tais ações/situações, como parte de um tripé de elementos constituintes do processo de gestão de biorrisco, chega-se à ideia do *risk assessment* como monitoramento de risco[16].

O LBM4 trouxe uma seção sobre o tema de monitoramento de risco de biossegurança e de bioproteção laboratoriais[16, pp.5-26]. No mesmo ano, em 2020, publicou documento específico sobre monitoramento de risco, como uma monografia associado (*associated monograph*) ao LBM4[63].

O documento mais específico da OMS sobre o tema, a monografia, dialogando com o seu documento de referência, o LBM4, traz a seguinte definição para monitoramento de risco (*risk assessment*):

> *"Um processo sistemático de coleta de informações; de avaliação das chances e impactos (*consequences*) da exposição a ou disseminação de um perigo (*hazard*); e de determinação das medidas de controle de risco apropriadas para reduzir o nível risco para aceitável [*tradução e grifos nossos*]."*[63, p.ix]

Vale enfatizar que a OMS utiliza o termo *assessment* para se referir ao processo do que se pode traduzir por "monitoramento de risco". Trata-se de um vocábulo em inglês sem tradução precisa no português, mas que objetiva oferecer *feedback* para melhoria contínua (questão central: como podemos melhorar o controle contínuo dos riscos?).

Na nova abordagem, o *assessment* passa a ser mais totalizante, no sentido de um acompanhamento sistêmico e sistemático, abordando não apenas a coleta de informações para identificação de perigos/ameaças e definição/medição

dos riscos, mas também inclui o processo de planejamento, implementação e revisão das medidas de controle de riscos, de maneira cíclica[16, 22].

De um modelo de representação estática, como um banco alicerçado por um tripé, chega-se a uma abordagem cíclica. O controle de riscos biológicos - seja em nível laboratorial ou nacional – passa a ser descrito como baseado na realização de um monitoramento de risco (*risk assessment*)[16, p.6].

Em outras palavras, o monitoramento de risco de biopoteção (*biosecurity risk assessment*) é visto como necessário para prevenir incidentes (*incidents*) de bioproteção laboratorial com MBGC e PGC, por meio da implementação de medidas de controle de risco (*risk control measures*)[22, p. 19].

Para a caracterização das abordagens de monitoramento de biorrisco laboratorial, vale conceituar alguns termos-chave, segundo o GBL2:

> *"**Acidente** [accident] – Uma ocorrência não intencional causada por inadvertência ou negligência que resulta em: dano real, como uma infecção, doença, dano em humanos, animais ou plantas, ou contaminação do meio ambiente; acesso não autorizado; perda; furto/roubo; ou mal uso, extravio ou disseminação ou weaponização de material, tecnologia ou dados relevantes sob o ponto de vista de bioproteção laboratorial.*
>
> *(...)*
>
> ***Perigo*** [hazard] – *Um objeto ou situação que pode potencialmente causar efeitos adversos quando um organismo, sistema ou (sub) população lhe é exposta. No caso da biossegurança laboratorial, o perigo é definido como agentes biológicos que têm o potencial de causar efeitos adversos em humanos, animais e a comunidade mais ampla e o ambiente. Um perigo não se torna um risco até que a chance e as consequências deste perigo causar dano sejam conhecidas. O termo bioperigo [*biohazard] *é especificamente usado no contexto de bioproteção laboratorial.*
>
> *(...)*
>
> ***Ameaça*** [threat] – *Uma intenção e habilidade maliciosa de causar um evento adverso, incluindo lesão* [injury], *perturbação, dano* [damage], *furto/roubo, extravio, maluso, acesso não autorizado, disseminação intencional de materiais e informação ou sabotagem.*
>
> ***(...)***
>
> ***Incidente** – Uma ação ou ocorrência que tem o potencial de, ou resulta em, exposição do pessoal do laboratório a agentes biológicos e/ou a disseminação intencional ou não que pode ou não causar dano real.* [tradução e grifo nossos]."[22, p. xiv-xv]

Em suma, tanto o termo acidente quanto incidente se referem a eventos de bioproteção e biossegurança, com a diferença de que o incidente não gera dano real, mas potencial de dano. Como exemplo, deixar uma porta aberta em área restrita seria um incidente. Porém, este incidente somente se torna um acidente, quando em decorrência dele efetivamente se concretizar um furto de MBGC, por exemplo.

Verifica-se que a definição de ameaça, mais ligada ao contexto da bioproteção, porque associada a uma “intenção” é um direcionamento do glossário da GBL2, em relação aos glossários da CWA 15793:2011 e da ISO 35001:2019, que se restrigem à noção de “perigo”[15, 65].

2.1.3.2.1 Abordagem baseada em risco e evidência (ABRE)

Em 2020, a OMS publicou o LBM4, que promove estruturadamente, pela primeira vez, uma abordagem baseada em risco e evidência (ABRE) para a biossegurança laboratorial[20] (**Figura 8**).

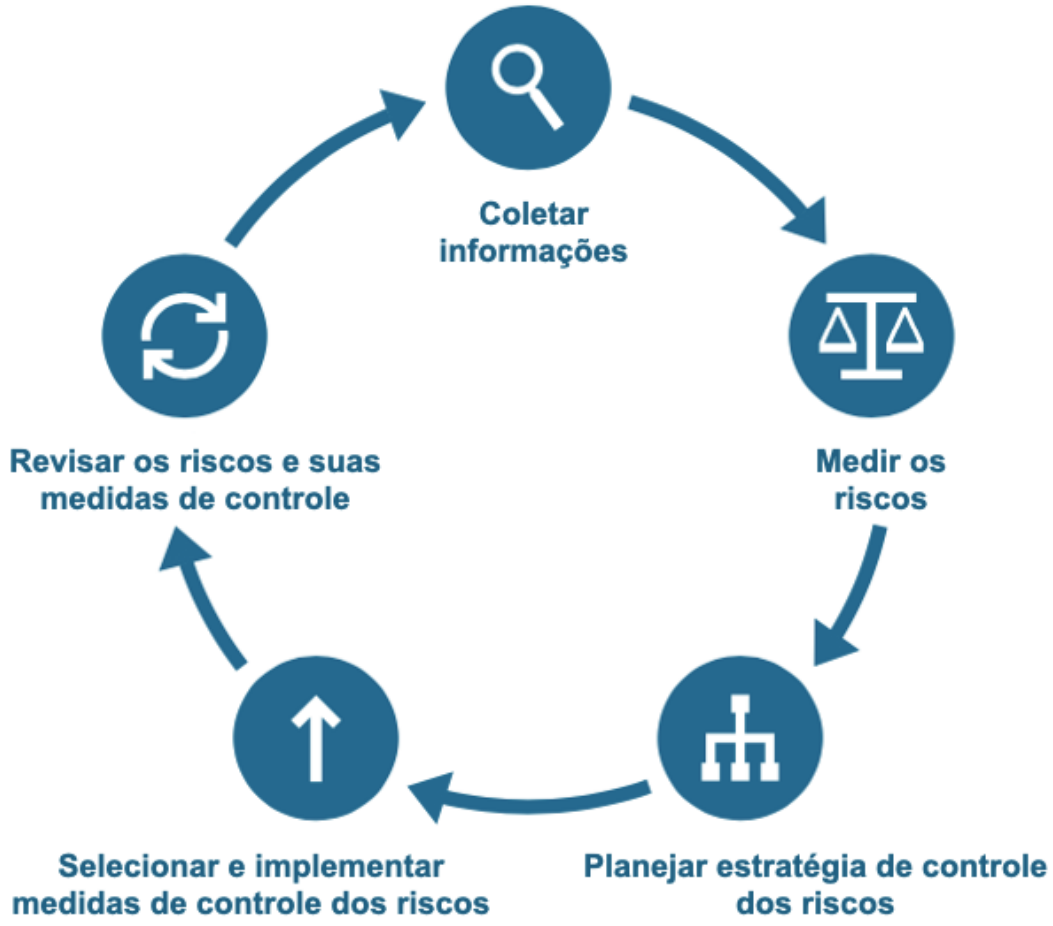


Figura 8 – *Framework* do monitoramento de risco (risk assessment) de biossegurança e bioproteção laboratoriais (adaptado da OMS pelo autor)[16, 22, 63].

A estruturação do monitoramento de risco (*risk assessment*) proposto no LBM4 busca permitir aos laboratórios planejarem e implementarem medidas de controle de risco que sejam importantes (relevantes), efetivas e sustentáveis – isto é, mantidas por um longo período ou permanentemente[16].

No GB2, a aplicação desta abordagem é igualmente recomendada para PAI/PGC e outras atividades com MBGC, tecnologias ou dados, na perspectiva da bioproteção laboratorial[22].

Apesar de organizado por passos, segundo a OMS, o processo de avaliação de risco pode acontecer de forma mais automática e simultânea no cotidiano de profissionais responsáveis pela biossegurança e bioproteção laboratoriais[63, p.3].

O *framework* é uma sugestão de processo que inclui todos os passos e considerações-chave necessárias para monitorar a chance (*likelihood*) e

consequência/impacto (*consequences*) de uma exposição ou disseminação a agentes biológicos. Ele não se propõe a ser a única forma de realizar um monitoramento de risco efetivo. De qualquer modo, um monitoramente de risco efetivo deve ser implementado de maneira transparente e rigorosa[63, p.3].

Enquanto primeiro passo, a coleta de informações é tratada como o ponto de partida para a toda a denição de risco posterior. Só há risco, se houver quantificação dos elementos do risco (chance e impacto potenciais de ocorrência de um evento). Desta forma, a coleta de informações efetiva deve ser suficiente para estimar os elementos do risco a ponto de caracterizá-lo em termos de chance e impacto potencial[63].

Entretanto, não há descrição específica nem no LBM4 nem no GBL2 nem na monografia de monitoramento de risco sobre o processo de coleta de informações seja do MBGC/PAI seja das ameaças à bioproteção.

No segundo passo do processo de monitoramento de risco, a OMS recomenda *evaluate the risk*, o que se traduz por “medir os riscos”. Neste caso, percebe-se que o termo *evaluate*, refere-se a identificar e quantificar os riscos, sendo um termo mais conclusivo e objetivo (questão central: quais os riscos?).

Uma vez definidos os perigos ou ameaças, deve-se qualificar (ou quantificar, a depender da metodologia) as chances e impactos. A OMS propõe uma matriz para definição de biorrisco, qualitativa, em cinco níveis para cada variável (**Figura 9**):

Consequências de exposição/ disseminação	Chance de exposição/disseminação				
	Rara	Improvável	Possível	Provável	Quase certa
Grave	Médio	Médio	Alto	Muito alto	Muito alto
Maior	Médio	Médio	Alto	Alto	Muito alto
Moderado	Baixo	Baixo	Médio	Alto	Alto
Menor	Muito baixo	Baixo	Baixo	Médio	Médio
Negligenciável	Muito baixo	Muito baixo	Baixo	Médio	Médio

Figura 9 – Matriz de medição qualitativa de biorrisco baseada na chance de exposição/disseminação e impacto (adaptado da OMS pelo autor)[63, p.13]

A OMS reconhece que

> *"Apesar de uma abordagem qualitativa para combinar parâmetros de chance e consequência numa matriz de risco ser apresentada como um método de quantificação de risco aqui, é importante frisar que métodos quantitativos (por exemplo, com* score *numérico simples ou modelos matemáticos complexos) ou híbridos (semiquantitativos) também podem ser utilizados.* [tradução e grifo nossos]"[63, p.11]

Embora a OMS disponibilize a matriz, não há exemplificações práticas de utilização da ferramenta a partir de cenários de ameaças de bioproteção laboratorial. A monografia da OMS traz entre seus anexos dois modelos de formulários de monitoramento de riscos divididos por passos (curto e longo), além de vários exemplos de preenchimento (Anexos 3 a 6), para diversas situações e agentes custodiados[63, pp.32-144].

2.1.3.2.3 Monitoramento de riscos de bioproteção laboratorial

O GBL2 traz uma lista de incidentes laboratoriais considerados de bioproteção, divididos didaticamente de acordo com os componentes de implementação de medidas de controle de risco[22, p. 41]. A lista é não exaustiva, mas exemplificativa para apoiar o processo de medição de riscos (*risk evaluation*):

1. Incidentes de bioproteção envolvendo diretamente agentes biológicos
    a. Perda deliberada ou acidental de agentes biológicos;
    b. Disseminação não autorizada de agentes biológicos;
    c. Furto/roubo de agentes biológicos de interesse;
    d. Extravio de agente biológico durante transporte;
    e. Mal-uso de MBGC.
2. Incidentes de proteção física
    a. Acesso não autorizado às áreas do laboratório;
    b. Sabotagem das atividades e/ou equipamentos do laboratório;
    c. Queda de energia;
    d. Uso ou manutenção inapropriada de equipamentos ou infraestrutura laboratorial;
    e. Arrombaento e intrusão;

f. Roubo ou furto de equipamentos.

3. Incidentes de proteção de pessoal
    a. Eventos causados por um infiltrado (ex. furtos);
    b. Riscos às pessoas;
    c. Não adesão às normas por pessoal interno ou visitantes.
4. Incidentes relacionados a proteção de dados e ciberbioproteção
    a. Acesso não autorizado a programas informáticos ou perda de informações (digitais ou impressas), como dados de pessoas, dados de pesquisa, dados de sequências genéticas ou procedimentos operacionais;
    b. Descontinuidade das operações devido a um ciberataque;
    c. Acesso digital não autorizado a equipamento laboratoria conectado a alguma rede;
    d. Interrupção remota de equipamento conectado (ex. sistema de proteção laboratorial);
    e. Furto/roubo, mal-uso ou sabotagem com dados e sistemas digitais de informações de interesse à bioproteção;
    f. Espionagem de informação de interesse.

Ressalte-se que terrorismo e extorsão são duas ameaças intencionais à bioproteção, que podem estar relacionados a quaisquer dos eventos supracitados contra MBGC ou PAI[22, p.22].

Podem ocorrer situações que facilitem ou aumentem o risco de eventos de bioproteção laboratorial e devem ser consideradas nos planos de bioproteção laboratorial, de acordo com o contexto em que o laboratório está inserido[22, p.22-23]:

1. Vandalismo, piquetes, ocupação e barricadas;
2. Disputas e insatisfações trabalhistas, incluindo episódios de violência no local de trabalho;
3. Greve;
4. Desordem civil ou guerra;
5. Falhas de contenção ou em algum processo de bioproteção devido a conflitos violentos ou desastres naturais (ex. inundações, furacões, deslizamento de terras etc.);
6. Falta de pessoal;
7. Cortes de recursos.

A OMS traz algumas estratégias-chave para mitigação de riscos no LBM4[16, p.18]:

1. Eliminação – eliminar o perigo
    a. Exemplo: usar um agente biológico inativado.
2. Redução e substituição – reduzir o risco
    a. Exemplos: reduzir o volume ou titulação do material biológico utilizado; substituir o agente biológico ativado por um atenuado ou por outro de menor infectividade/patogenicidade;
3. Isolamento – isolar o perigo
    a. Exemplo: manter o agente biológico em um dispositivo de contenção primária (como uma cabine de segurança);
4. Proteção – proteger o pessoal ou meio-ambiente
    a. Exemplos: vacinar o pessoal do laboratório; usar EPI;
5. Conformidade – dispor de controles normativos e manter a efetividade do programa de gerenciamento de riscos
    a. Exemplos: implementar boas práticas e procedimentos microbiológicos (BPPM – GMPP na sigla em inglês); dispor de procedimentos operacionais padrão (POP) claros; estimular cultura de segurança e proteção; educar e treinar o pessoal continuadamente.

Segundo a CWA 15793:2011 e a ISO 35001:2019, deve-se estabelecer um comitê de gestão de risco biológico para dar suporte ao sistema de gestão de risco biológico. Sempre que possível, este comitê deve ser composto por membros que sejam independentes das atividades que se está supervisionando sob o ponto de vista do risco biológico[16. 65].

2.1.3.3 Requisitos essenciais (*core requirements*) de bioproteção laboratorial

Segundo o LBM4, para a maioria das atividades laboratoriais, a chance de exposição e/ou disseminação é improvável; e o impacto potencial associado varia de negligenciável a moderado. Isto significa que o risco inicial é muito baixo ou baixo

e está próximo ou abaixo do limite de risco aceitável antes mesmo de que medidas de controle sejam implementadas[16].

Apesar disso, são recomendadas pela OMS a adoção de medidas, consideradas essenciais de biossegurança laboratorial, independente do risco:

> *"Diretrizes internacionais e boas práticas aceitas para a biossegurança recomendam a adoção de um conjunto básico de princípios, tecnologias e práticas como medidas para controle de risco de biossegurança garantindo que todo o trabalho se mantenha abaixo dos limites de risco aceitável.*
> *Por esta razão, este manual dispõe um conjunto mínimo de medidas de controle de risco para ser implementado durante qualquer travalho com agentes biológicos. Esta combinação de medidas de controle é conhecida coletivamente como os requisitos essenciais* [core requirements] [tradução e grifo nossos]."[16, p.19]

Os requisitos essenciais (*core requirements*) sugeridos pela OMS no LBM4 são medidas de controle de risco consideradas a fundação (*foundation*) e uma parte integrante da biossegurança laboratorial[16, p.27]. Elas buscam refletir os padrões internacionais e as melhores práticas de biossegurança.

Destaque-se que há uma seção inteira no Manual sobre os requisitos, praticamente exclusivos para o controle de riscos de biossegurança laboratorial[16, pp.27-48], e não de bioproteção laboratorial.

A título de exemplificação, algumas das medidas constantes dos requisitos essenciais são:

> "*Lavar as mãos minuciosamente, preferencialmente com água corrente morna e sabão, depois de manusear material biológico e/ou animais; antes de sair do laboratório; ou quando as mãos estão (ou supostamente estão) contaminadas.*
> *(...)*
> *Usar luvas descartáveis todo o tempo em que estiver manuseando materiais que contenham (ou supostamente contenham) agentes biológicos. As luvas descartáveis não devem ser reutilizadas* [tradução nossa]"[16, pp.28 e 30].

As diretrizes da OMS seguem com informações práticas para a implementação de medidas de controle de riscos de biossegurança reforçadas (Seção 4 - *Heightened Control Measures*[16, pp.49-58]) e medidas de controle de riscos de biossegurança máximas (Seção 5- *Maximum Containment Measures*[16, pp.59-64]), quando a implementação de medidas de controle de risco essenciais não é suficiente para mitigar o nível de risco para abaixo do limite do aceitável.

A relação das medidas de controle de risco essenciais (MCE), reforçadas (MCR) e máximas (MCM) e os elementos do risco são demonstradas por um modelo gráfico (**Figura 10**):

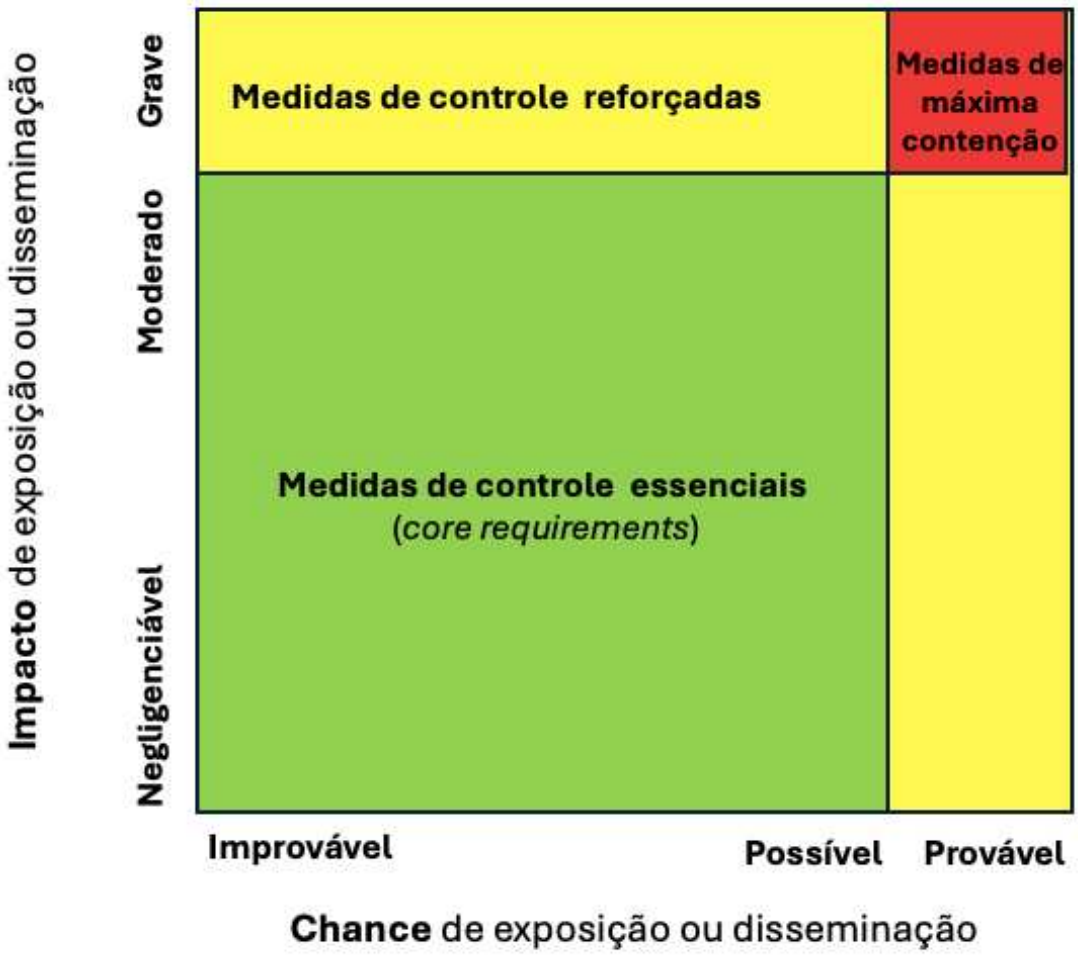


Figura 10 *– Medidas necessárias de controle do risco de biossegurança e bioproteção laboratoriais baseadas na chance e impacto de eventos de biorrisco* (elaborado pelo autor).

2.1.4 Riscos de bioproteção laboratorial

2.1.4.1 Riscos biológicos globais

O programa de guerra biológica britânico, que será melhor detalhado posteriormente (tópico 2.2.2), chegara à conclusão, desde os anos 1950, de que o impacto de um ataque biológico poderia ser superior a de um ataque nuclear[7].

A pesquisa militar britânica tratou do conceito de “Large Area Concept” (LACON), que foi pesquisado nas estruturas militares do Reino Unido até os anos 1960. Segundo o LACON, no lugar de usar uma bomba contendo MBGC, uma aeronave dispersaria aerossol com patógenos por toda uma região ou país[7, p.51].

O LACON foi testado em 1957. Utilizou-se uma partícula traçadora fluorescente (*tracer particle*), que simularia o agente biológico. O material foi dispersado em uma linha de 300 milhas ao longo de grandes áreas do Reino Unido por aeronaves militares[7].

Cientistas estimaram que, se o teste utilizasse agente patogênico como a bactéria *Francisella tularensis*[r] ou a *Coxiella burnetii*[s], aproximadamente 28 milhões de pessoas teria recebido uma dose suficiente para infecção. A conclusão do teste era de que o Reino Unido poderia ser totalmente infectado por um patógeno em um único ataque biológico.

Percebe-se, portanto, que as consequências de um evento de ataque aéreo com MBGC pode chegar a ser catastrófico. Esta realidade científica, quando cotejada com as noções de risco biológico, apontam para um potencial de risco muito alto em alguns cenários de eventos de bioproteção labotarial.

A partir dos anos de 2010, o aprofundamento de estudos sobre análise de risco propôs uma nova categoria de risco, ao se debruçar sobre aqueles com potencial de causar impacto potencialmente infinito, isto é, impacto que resulte no fim da vida humana[14].

No relatório pioneiro *12 Riscos que Ameaçam a Civilização Humana*[14], pandemia global e biologia sintética são dois riscos de eventos biológicos selecionados descritos como de impacto potencial infinito.

Durante a segunda metade da década passada, o uso de armas de destruição em massa (ADM), entre elas as armas biológicas, foi visto como o principal risco global, em termos de impacto, superando eventos climáticos extremos e crises hídricas[5]

Ressalte-se que, para a ONU, ADM são sinônimo de armas químicas, biológicas e nucleares, bastando a utilização de um agente químico ou biológico de forma ofensiva, contra um indivíduo ou um país, para que ele seja considerado uma

[r] Causadora da tularemia[69].

[s] Causadora da Febre-Q, considerada a doença mais infecciosa do mundo (uma única bactéria pode ser suficiente para infectar um ser humano)[70].

arma, mesmo que não tenha passado por um processo de industrialização ou melhoramento técnico[1].

A percepção crescente de risco biológico por ação intencional resultou, em 2019, numa consulta da INTERPOL aos governos mundiais, com vistas à criação de uma “Unidade de Bioterrorismo”, descrita no documento de consulta como uma “Plataforma de Análise de Incidentes Biológicos”. Seu objetivo estratégico era:

> “...criar um sistema global de alerta precoce voltado para as necessidades da aplicação da lei em relação ao rastreio e avaliação de riscos biológicos em tempo real. Este sistema tem o objetivo de agilizar e contextualizar o fluxo de informações com a finalidade de apoiar os esforços de identificação, resposta e investigação de potenciais incidentes envolvendo material biológico."[119]

A Unidade de Prevenção ao Bioterrorismo (BTPU) da INTERPOL foi de fato craiada, em 2020, calcada em inteligência policial, por meio da ferramenta BioTracker, que permite análises antecipatórias de eventos biológicos potenciais, entre outras ferramentas de gerenciamento e análise de dados policiais[119].

Na década de 2020, com a piora da percepção do risco associada a eventos climáticos extremos e da mudança crítica de sistemas planetários, a percepção de risco de eventos biológicos (*biological hazards*) diminuiu em termos relativos[5, p. 37].

Entretanto, a percepção de risco biológico, por evento acidental ou intencional, continua entre os vinte maiores riscos globais para o FEM, em sua pesquisa de percepção de 2023-2024, com impacto potencial (gravidade – *severity*) na próxima década de aproximadamente 4,5 (quatro e meio) de um máximo de 7 (sete)[5, p. 37].

O relatório anual de riscos globais expõe a conexão deste risco (disseminação de agentes biológicos) com o risco de doenças infecciosas, considerado de média influência de risco global. As doenças infecciosas, por sua vez, possuem interconexão com riscos sociais, tecnológicos e econômicos de maior influência como: polarização social; desinformação; crises econômicas; e uso de inteligência artificia (IA)[5, p.44].

A interconexão destes riscos evidencia a importância destes eventos em uma rede de riscos globais, que necessitariam de medidas preventivas e mitigadoras transversais[46]. É evidente, por exemplo, a possibilidade de que, sem a devida regulação e medidas de bioproteção de PAI/PGC, ferramentas de IA signifiquem

ultrapassar a barreira de conhecimento que antes dificultava ações com agentes biológicos[46].

2.1.4.2 Riscos clássicos ou persistentes de bioproteção laboratorial

Quando da publicação das primeiras normas sobre bioproteção laboratorial, a exemplo do LBM3, em 2004, e o GBL, em 2009, o foco das ameaças a bioproteção laboratorial era o extravio, furto (obtenção de maneira criminosa sem grave ameaça nem emprego de violência contra terceiros) e roubo (obtenção de maneira criminosa mediante grave ameaça ou emprego de violência contra terceiros) de ABI/ABTS/MBGC.

Ressalte-se que o extravio, em si, é um perigo, mas não uma ameaça, na medida em que não caracteriza uma ação intencional. De qualquer modo, aumenta o risco de o MBGC ser furtado e, neste sentido, a ameaça, a partir do extravio, seria concretizada após o ato de furto, contemplado de maneira evidente entre as ameaças persistentes à bioproteção laboratorial.

Neste sentido, a organização esquemática do risco de bioproteção laboratorial, em comparação com o risco da biossegurança laboratorial era restrito (**Figura 11**):

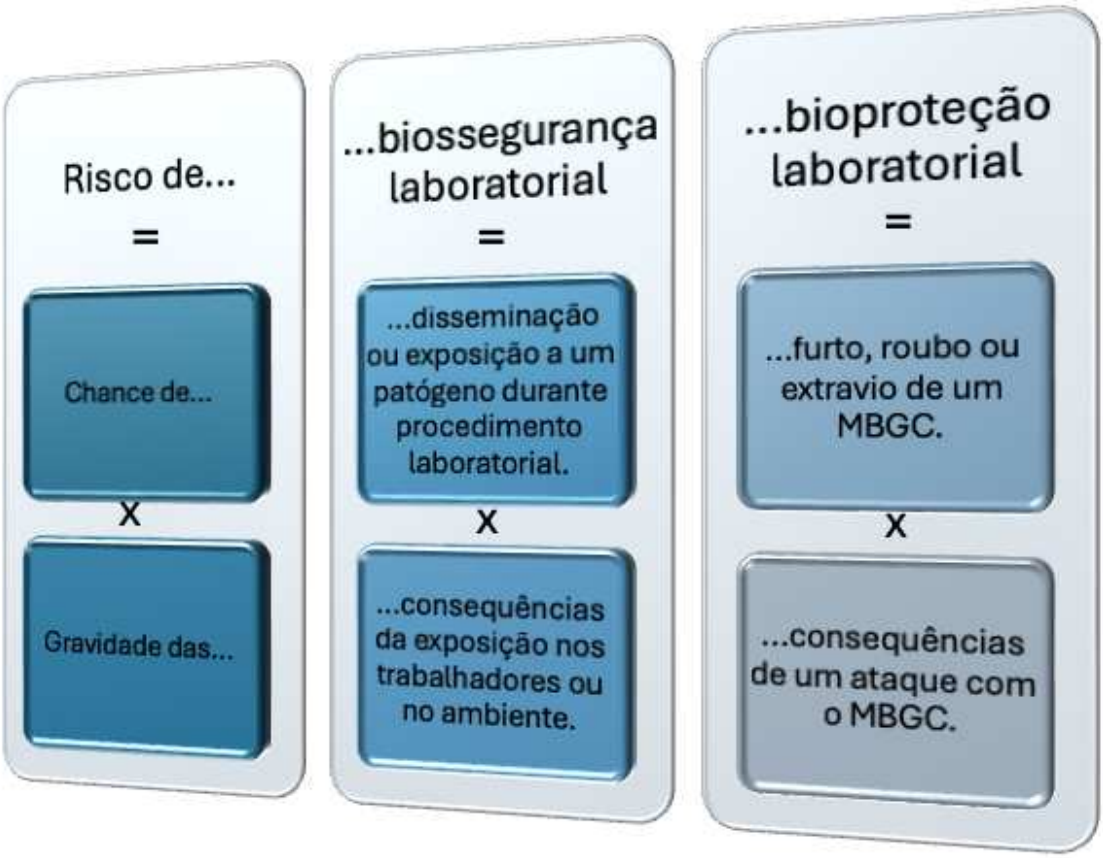


Figura 11 *– Elementos clássicos ou persistentes do risco de bioproteção laboratorial (*adaptado de SALERNO & GAUDIOSO[2, p. 14] pelo autor)

Em se tratando dos primeiros riscos de bioproteção percebidos e analisados pela comunidade científica, é possível chamá-los de riscos persistentes, utilizando, por analogia, a nomenclatura da bioética de proteção para dividir os problemas da bioética em persistentes ou emergentes[62].

É importante esta distinção didática, a fim de realizar um recorte temporal dos diferentes enfoques dados para as ameaças vinculadas à bioproteção. Na pespectiva dos riscos persistentes, a avaliação das chances de um indivíduo ou grupo de pessoas intencionamente furtar ou roubar um ABI/ABTS/MBGC é chamada de ameça potencial (*potential threat*)[2, p. 14] **(Figura 12)**:

Figura 12 – *Elementos de riscos clássicos ou persistentes de bioproteção laboratorial* (adaptado de GAUDIOSO & SALERNO[2, p.14] pelo autor)

A maior parte dos agentes e toxinas biológicos não são bons candidatos para uso em eventos de disseminação deliberada, como em ataques bioterroristas ou biossabotagens[2]. Por isso, os riscos associados a materiais biológicos precisam ser individualizados em cenários de risco únicos[2].

Cada cenário de risco possui, portanto, três componentes a serem considerados na análise[2]:

1. O material biológico de interesse (MBI) ou material biológico de grande consequência (MBGC), que pode ser um agente ou toxina selecionados (ABTS), custodiado em uma instalação laboratorial selecionada (ILS) ou não;
2. Um indivíduo ou grupo de indivíduos que querem disseminar criminalmente o MBI/MBGC; e
3. Uma ação a ser perpetrada pelo(s) criminoso(s) para obter o MBI/MBGC (ex. roubo de um ABTS em uma ILS).

Na termiologia de segurança, é comum chamar de adversários (*adversaries*) os indivíduos que intencionam obter um item criminosamente para causar um mal[2, p.14].

2.1.4.3 Riscos emergentes de bioproteção laboratorial

A percepção do risco de bioproteção laboratorial mudou nas últimas três décadas, passando do foco em furto e roubo[22, 23] para novas situações e tecnologias que surgem a partir dos anos 2010[35].

Didaticamente, cabe chamar os novos riscos de bioproteção laboratoriais de riscos emergentes, em contraposição aos riscos persistentes supracitados. Para o GBL2 da OMS[35], os riscos emergentes estão associados a tecnologias emergentes e ameaças de bioproteção potenciais como a:

1. Engenharia genética
    a. Edição genômica;
    b. Drives gênicos (*gene drives*); e
    c. Manipulação epigenética.
2. Biologia sintética;
3. Inteligência artificial;
4. Biologia de uso individual (*do-it-yourself biology*); e
5. Publicação de pesquisa de alto impacto.

A rigor, seguindo a terminologia da própria OMS[16,22,63], estes "riscos" arrolados serias perigos (*hazards*) emergentes, mas que se tornam riscos quando analisados à luz das chances e impactos potenciais em cenários de mal uso intencional associado.

A fim de conhecer se um laboratório apresenta esses riscos potenciais, isto é, se o laboratório desenvolve pesquisa de alto impacto (PAI), o próprio GBL2 sugere que sejam realizadas as seguintes perguntas:

> *1. O laboratório planeja usar ou produzir (ou usa ou produz) material biológico que possui uma das características abaixo (assinale todas as características que se aplicam):*
>
> *a. Habilidade de interferir, evardir-se (*bypass*) de ou reduzir a efetividade de tratamento ou profilaxia (incluindo vacinação);*
>
> *b. Virulência, transmissibilidade (intrínseca e extrínseca[t]) ou letalidade aprimoradas;*
>
> *c. Patogenicidade aumentada;*
>
> *d. Alcance modificado quanto a hospedeiros e tropismo, incluindo potencial seleção inadvertida (*inadvertent selection*) por passagem seriada (*serial passage*) em células de humanos ou de outras espécies hospedeiras;*
>
> *e. Habilidade de se evadir (*bypass*) de métodos de detecção e diagnóstico*

[t] Transmissibilidade intrínseca (*transmissibility*) é a capacidade de transmissão enquanto propriedade intrínseca do patógeno, relacionada à sua biologia. A transmissibilidade extrínseca (*communicability*) é a capacidade observada de transmissão, considerando o contexto externo e medidas de controle ou a capacidade de transmissão em condições específicas. Exemplo: a transmissibilidade extrínseca da tuberculose é reduzida em ambientes bem ventilados e com acesso ao tratamento adequado.

> *f. Potencial de uso como um material biológico gravemente danoso ou até mesmo uma arma biológica;*
> *g. Produção de toxinas (ou produção aumentada de toxinas) ou aprimoramento de toxicidade de toxina existente;*
> *h. Estabilidade e resistência aumentada à descontaminação;*
> *i. Absorção, toxicocinética ou suscetibilidade pelo hospedeiro alteradas;*
> *j. Habilidade de se evadir (*bypass*) da imunidade natural;*
> *k. Capacidade aprimorada de disseminar-se ou de facilitar a disseminação.*
>
> *2. O conhecimento (dados, metodologia ou resultados), tecnologias e produtos intermediários ou finais (ex. toxinas ou ácidos nucleicos) das pesquisas empreendidas podem ser mal utilizados para causar dano?*
> *3. O agente/material biológico custodiado ou conhecimento pesquisado no laboratório colocam em risco alguma das populações abaixo, se disseminado? [tradução nossa].”* [35, pp. 4-5]

Se a resposta for sim para quaisquer das três perguntas, o laboratório efetua PAI e, portanto, apresenta riscos emergentes de bioproteção laboratorial. Portanto, precisaria ser submetido a uma avaliação de risco de biossegurança e bioproteção laboratoriais[35, p.5].

Na perspectiva dos riscos emergentes, portanto, tem-se a seguinte representação gráfica dos elementos do risco (**Figura 13**):

Figura 13 – *Elementos de risco emergentes de bioproteção laboratorial* (elaborado pelo autor)

Em suma, o risco de bioproteção na atualidade é aquele decorrente de ameaças tanto persistentes (extravio, furto e roubo) quanto emergentes. As ameaças emergentes são um conceito presente nas normas da década de 2020, porque decorrem da evolução da percepção de riscos.

Com o advento de novas tecnologias bioquímicas, novas ameaças emergentes tendem a surgir, assim como novos meios de implementar medidas de bioproteção específicas contras a novas ameaças. Assim, a gestão de risco de bioproteção varia com novas ameaças e precisa de constante atualização.

2.2 Biodefesa na perspectiva da bioproteção laboratorial

Para definir biodefesa, observam-se dois aspectos integrantes do conceito: o primeiro é o sujeito, o componente “quem” executa as ações de biodefesa; o segundo é o objeto finalístico, o componente “contra o quê” tais ações são executadas.

Segundo Koblentz e Lentzos, o termo biodefesa (*biodefense* ou *biodefence*, em inglês) tem sido usado para descrever os programas militares de armas biológicas[11]. Seria, portanto, *stricto sensu,* uma área militar voltada para a realização de um ataque biológico contra o inimigo externo ou para a defesa destes ataques.

Este uso remonta à primeira geração de tais programas, no período entreguerras (1919-1938), quando a França, o Japão e a então União das Repúblicas Socialistas Soviéticas (URSS) organizaram programas estatais pioneiros de pesquisas ofensivas e defensivas com agentes biológicos[12].

O vínculo militar do termo biodefesa pode ser encontrado no trabalho das brasileiras Rambauske, Cardoso e Navarro, ao defender que "o bioterrorismo ultrapassa as áreas do campo militar (biodefesa) e torna-se um tema de relevância para os profissionais da área da saúde (biossegurança)”[42].

Elas citam Isla, autor que, na verdade, reconhece o caráter misto da biodefesa, utilizando o qualificador “biodefesa civil” (*civilian biodefense*) para se referir à participação de atores não-militares nas ações de defesa biológica[47].

Koblentz e Lentzos reconhecem, entretanto, que uma definição mais ampla tem sido adotada, considerando biodefesa como o conjunto das atividades de prevenção, preparo e resposta a ameaças biológicas, em larga escala, tanto contra populações civis quanto militares[11].

A necessidade de explicitar, na conceituação *lato sensu* de Klobentz e Lentzos, que a biodefesa lida com ameaças “tanto contra populações civis quanto militares” justifica-se face ao reconhecimento pelos autores da ampliação do escopo do termo “defesa”, tradicionalmente restrito à esfera militar[11].

Trata-se, portanto, da apropriação de um termo tradicionalmente vinculado à área de defesa, isto é, de proteção da soberania do Estado, por meio das FFAA, para conferir significado mais amplo, resultado da percepção de que o tema outrora restrito ganha importância acadêmica e não prescinde de políticas e estudos que transcendam a área militar.

Em consonância com esta definição, Wunder conceitua o termo como conjunto de ações políticas e estratégicas a serem executadas pelo Estado, com o objetivo de proteger a população contra infecções causadas por surtos epidêmicos de ocorrência natural e por armas biológicas provenientes do terrorismo ou guerra biológica[40].

2.2.1 Análise comparativa de conceitos e práticas estrangeiros de biodefesa

Após os ataques biológicos com antraz nos EUA em outubro de 2001, o entendimento do termo biodefesa "mudou significativamente... como o processo utilizado para proteger tanto populações civis quanto militares", afastando-se da associação tradicional com assuntos exclusivamente militares[49].

O sujeito de biodefesa deixa de ser militar para incluir atores civis, governamentais ou não, e o objeto finalístico deixa de ser os programas de armas biológicas para ser as ameaças biológicas contra populações militares e civis[1, 49].

A noção de intersetorialidade - ou integração interagências, para citar uma expressão análoga comumente empregada por militares - torna-se dominante, porque se percebe que a ação isolada de órgãos de cada área - saúde e segurança - compromete a efetiva proteção do indivíduo. Por conseguinte, a segurança dos indivíduos deixa de ser atribuição dos órgãos securitários - polícia, inteligência e FFAA - para ser de atribuição conjunta[1].

O aumento da percepção internacional do risco de eventos QBRN perpetrados por autores não estatais leva à elaboração de políticas mais eficientes para a diminuição do impacto e da probabilidade de ocorrência destes eventos[56].

Esta ideia resta clara na estadunidense Diretriz Presidencial para a Segurança Interna (*Homeland Security Presidencial Directive*, HSPD-10), de 2004, em que o presidente George W. Bush defende que "estamos continuamente adaptando as FFAA dos EUA para enfrentar o desafio das armas biológicas", enfatizando que "a capacidade privada, local e estadual serão ampliadas e coordenadas por recursos federais para proporcionar níveis de defesa contra-ataques biológicos"[56].

Dois ministérios não militares, o de Segurança Interna (*Department of Homeland Security*) e o de Estado (*Department of State*) se tornam expressamente

responsáveis por coordenar o preparo e resposta a eventos QBRN nacionais e internacionais, respectivamente[56].

Apesar da tendência internacional - acadêmica e governamental - de transmilitarização das políticas estatais de biodefesa - e aqui se utiliza o termo defendido por COELHO (2017) para se referir à ampliação do estabelecimento legal de competências a atores não militares[1] -, a Portaria Normativa no 585 do Ministério da Defesa (MD) do Brasil, de 07 de março de 2013, traz em seu artigo segundo a conceituação de defesa biológica, sinônimo de biodefesa, como "conjunto de medidas estruturadas a serem implementadas pelas Forças Armadas para prevenir e enfrentar ataques por agentes biológicos ou toxínicos"[57].

Verifica-se que, para as FFAA brasileiras, segundo esta norma, a biodefesa se restringia a ações estritamente militares contra-ataques com agentes biológicos, contrariamente à tendência vigente de ampliação dos atores envolvidos na prevenção, preparo, resposta aos eventos QBRN.

Além da normativa do MD, o termo biodefesa é encontrado no regimento interno da Agência Brasileira de Inteligência (ABIN), órgão não militar - apesar de integrante da estrutura do Gabinete de Segurança Institucional (GSI), consuetudinariamente uma estrutura com status ministerial comandada por um general do Exército[1].

A reestruturação da ABIN ocorrida após a instituição da PNI - normatizada no Decreto nº 8.905, de 17 de novembro de 2016, e detalhada no mais novo Regimento Interno da ABIN - criou uma Coordenação de Análise de Tecnologias Sensíveis e Biodefesa (COTESB). A inteligência estratégica utiliza o termo biodefesa em consonância com a definição transmilitarizada, defendida pela maioria dos autores supracitados[1, 40, 47, 49, 56].

A utilização do termo biodefesa, neste caso, demonstra o interesse institucional de a ABIN se colocar como parte da biodefesa civil brasileira ou, para ser mais preciso com as definições referenciadas, como parte da biodefesa brasileira *tout court*, utilizando-se o conceito estadunidense ampliado de biodefesa[1].

Percebe-se, em suma, quase um consenso, entre os autores e as legislações estudados, sobre a tendência de transmilitarização e intersetorialização dos atores da biodefesa. Esta conclusão nos ajuda a consolidar a ideia de "quem" executa as ações de biodefesa[1].

Mas o segundo componente importante do conceito o "contra o quê", finalístico, não parece tão consensual. Alguns acadêmicos ampliam o objeto da

ações de biodefesa para as ameaças biológicas como um todo, inclusive os eventos não intencionais (ex. as pandemias, isto é, evento natural)[1,40].

O próprio termo "defesa" se contrapõe à ideia de “ataque”, que é um evento precipuamente intencional, de modo que soa mais evidente restringir o escopo da biodefesa à defesa contra o uso intencional de agentes biológicos. Ressalte-se, entretanto, conforme citado, que alguns autores preferem se referir ao termo de maneira mais ampla para abranger contramedidas que fazem frente a ameaças biológicas naturais ou eventos não intencionais envolvendo agentes biológicos[1,40].

Longe de diminuir a importância dos militares nas atribuições da biodefesa, a transmilitarização do termo confere maior importância a todos os seus atores estatais, inclusive as FFAA, na medida em que valoriza as ações de biodefesa como estratégicas - também porque ratificam-nas como dependentes de uma resposta supraministerial - para a nação[1].

Percebemos como a evolução do termo biodefesa, do início do século XX, quando foi engendrado, ao início do XXI, quando ganha uma acepção mais ampla, transmilitarizada, deveu-se ao modo como os Estados reagiram à necessidade de proteger seus cidadãos, sobretudo do uso intencional de agentes biológicos por atores estatais e não-estatais (subnacionais ou transnacionais). As ameaças potenciais e reais, à medida que se modificam, também mudam a resposta estatal e, por conseguinte, alteram a maneira de defini-la conceitualmente[1].

Os EUA foram os maiores mobilizadores de recursos - humanos e financeiros, inclusive por meio de cooperação internacional -, desde o início dos anos 2000, para a formulação e implementação de ações na área de contramedidas às ameaças biológicas. Assim, a maneira como os formadores de políticas e de opinião dos EUA - que interferem nas ações de seu governo - lidam com tais conceitos é fundamental para a consolidação da ideia de biodefesa em todo o mundo[1].

2.2.2 O advento da biodefesa e a governança internacional de agentes biológicos selecionados e de tecnologias de uso dual

Nos EUA, a grande capacidade de preparo e resposta, aliada à robusta infraestrutura laboratorial derivada, inclusive, de programas de produção de armas

biológicas e defesa contra elas, tornou a participação militar fundamental na construção da governança de agentes biológicos selecionados[59, 60].

Como se pode observar, revisando a pesquisa histórica sobre programas de biodefesa de BALMER & MOON (apud LENTZOS, 2016), a custódia laboratorial de MBGC ganha especial relevância a partir de programas de guerra biológica (PGB)[7, pp. 43-53].

Neste sentido, pode-se afirmar que os riscos biológicos de biossegurança e bioproteção laboratorial se ampliaram na humanidade em razão de programas de armas biológicas, que seriam posteriormente, e com algumas mudanças de enfoque, chamados de programas de biodefesa[1, 7].

De fato, três dos maiores PGB do século XX, que cooperavam entre si, foram o do Reino Unido, EUA e Canadá. Os três países consideravam que o uso de guerra biológica (GB) tinha enorme potencial militar, mesmo na vigência do Protocolo de Genebra de 1925, uma vez que o Protocolo, na prática, permitia que um país atacado com armas biológicas pudesse revidar com a mesma arma[7, p.45].

O Departamento de Biologia de Porton, sediado em um compexo de laboratórios militar na cidade de Porton Down/Reino Unido, foi criado secretamente em 1940, tinha como prioridade produzir arma biológica para uso em retaliação. Na década de 1940, no Reino Unido, autoridades militares defendiam que a pesquisa sobre GB era de nível tão importante quanto a pesquisa nuclear[7, p.47].

Após a Segunda Guerra Mundial, a estrutura laboratorial militar de Porton Down, então ampliada e chamada pelo novo nome de Instituição de Pesquisa Microbiológica (MRE, na sigla em inglês) ainda trabalhava com a expectativa de desenvolver até 1957 uma arma biológica com impacto comparável a uma bomba atômica[7, p. 48].

Durante os anos 1970, o foco das pesquisas no complexo laboratorial foi crescentemente em doenças com maior implicação para a saúde pública, e o Reino Unido muda oficialmente seu PGB para unicamente defensivo[7, p.53].

Atualmente, o complexo de laboratórios em Porton Down possui unidade NB-4 e recebe o nome de Laboratório de Tecnologia e Ciência de Defesa (Dstl, na sigla em inglês)[7, p. 48].

O advento e posterior abandono dos programas ofensivos legou questionamentos reiterados por pesquisadores da área de biodefesa:

> *"Por que esses países empreenderam programas de armas biológicas? Que tipos de armas biológicas foram buscadas? Dada a ambição inicial dos*

> *programas de armas biológicas, que progressos foram obtidos quando do fechamento dos programas e como isto pode ser explciado? Por que o governo britânico e estadunidense abandonaram a política de retaliação e adotaram o desarmamento contra armas biológicas e pesquisa defensiva* **[**tradução nossa**]***?"*[7 p. 44]

De qualquer modo, o investimento militar em estruturas de pesquisa e produção de bioarmas, seja no Reino Unidos e nos EUA, seja na antiga União das Repúblicas Socialistas Soviéticas (URSS), com concomitante aumento substancial de biorrisco, levou ao desenvolvimento de importantes práticas de B2L[1, 7].

Tais práticas e expertises militares serviram de material de referência para a constituição dos primeiros guias de biossegurança laboratorial.

A importante criação de capacidades militares (e de cultura militar) para lidar com ameaças biológicas persistiu com a ampliação dos programas de biodefesa, nas últimas décadas, de modo que as estruturas nacionais de P2R2 contra eventos biológicos não pode prescindir destas capacidades, seja no treinamento de capacidades civis, seja no compartilhamento de estruturas e troca de informações diversas[1].

Além disso, foi sobretudo a preocupação da biodefesa com ataques biológicos que levou a criação de parte importante do arcabouço multilateral de B2L, incluindo a BWC, a Resolução 1.540 e os regimes de controle de exportação de bens e tecnologias duais.

Em suma, a revisão da história dos PGB e de sua transformação em programas de biodefesa apontam para a importância da inclusão da biodefesa no planejamento e implementação de uma governança robusta, nacional e internacional, de biossegurança e bioproteção laboratoriais.

2.3 Inteligência na perspectiva da bioproteção laboratorial

Não é fácil definir a atividade de inteligência (AI) ou seu sinônimo, inteligência *tout court*. Porque não existe uma teoria da inteligência[9, p.6]. O mais próximo de uma teoria brasileira de inteligência seria a Doutrina de Inteligência da ABIN, principal e exclusivo órgão federal de inteligência civil brasileira[8].

Historicamente, quando se analisam as definições de inteligência de vários gestores da inteligência estadunidense, associa-se a AI principalmente à ameaça externa. Segundo Vernon Walters, por exemplo, que foi Diretor-Adjunto da Agência Central de Inteligência dos EUA (CIA, na sigla em inglês), entre 1985-89 (Governo Reagan) e adido militar (*military attaché*) dos EUA no Brasil nos anos 1960:

> "*Inteligência é informação, nem sempre disponível no domínio público, relacionada à força, recursos, capacidades e intenções de um país estrangeiro, que pode afetar nossas vidas e a segurança de nosso povo* [tradução nossa]"[9, p.6].

Nos anos 1996, entretanto, o Conselho de Relações Externas dos EUA, propôs a definição de que:

> "*Inteligência é informação não publicamente disponível ou análise baseada, ao menos em parte, em tal informação, preparada para decisores ou outros atores governamentais* [tradução nossa]"[9, p.6].

Estas concepções mostram a importância da guerra fria e da visão adversarial externa, a de que há adversários e ameaças externas a serem combatidos, servindo a inteligência como ferramenta de enfrentamento em prol da defesa da segurança nacional. Neste sentido, Michal Warner, historiador da inteligência estadunidense e professor da Universidade Johns Hopkins, em Washington D.C., resume:

> *"Inteligência é uma atividade secreta de Estado para compreender e influenciar entidades estrangeiras*"[9, p.10].

Esta concepção de inteligência, proveniente precipuamente de pessoas ligadas à CIA, relaciona-se com o que a Doutrina de Inteligência da ABIN define como um ramo da AI: a inteligência externa (*foreign intelligence*).

> *"A inteligência externa trata de temas sobre os quais o Estado tem pouco ou nenhum poder de decisão ou intervenção unilateral e que exigem estratégias de posicionamento internacional para nego- ciação e consecução dos interesses nacionais. O foco dessa inteligência é reunir dados, informações e conhecimentos para entender e contextualizar fatos,*

> *eventos, situações e fenômenos que ocorrem no contexto global, bem como seu impacto à atuação do Brasil na arena internacional"*[8, 54].

A CIA ou o Serviço Secreto de Inteligência (SIS, na sigla em inglês), serviços de inteligência externos dos EUA e do Reino Unido, respectivamente, são órgãos voltados para a inteligência externa. É missão da CIA:

> *"Antecipar ameaças e ajudar os objetivos de segurança nacional por meio de:*
> *-Coleta de inteligência externa útil;*
> *-Produção de análise objetiva a partir de qualquer tipo de fonte;*
> *-Conduzir ações secretas efetivas conforme decisão presidencial;*
> *-Salvaguardar os segredos que ajudam a manter nossa Nação segura.* [tradução nossa]*"*[94]

Esta linguagem explícita de que a inteligência destes países é associada ao secretismo, inclusive no nome do SIS, e à ação externa para defesa da segurança nacional contra inimigos externos se coaduna com o divulgado abertamente pelo Reino Unido:

> *"Nós somos o SIS – o Serviço de Inteligência Secreto do Reino Unido – também conhecido como MI6*[u]*. Nosso pessoal trabalha secretamente em todo o mundo para fazer o Reino Unido mais seguro e mais próspero. Por mais de 100 anos SIS garantiu o Reino Unido e nossos aliados um passo à frente de nossos adversários. Nós somos criativos e determinados – usando tecnologia de ponta e espionagem.*
> *Nós temos três principais objetivos: parar o terrorismo, desorganizar a atividade de estados hostis e dar ao Reino Unido vantagem cibernética."*[95]

É importante iniciar as considerações sobre a inteligência e a B2L com a descrição da inteligência de alguns países ocidentais que ainda mantêm uma AI externa baseada em premissas de defesa contra inimigos externos, para destacar, em primeiro lugar, que a postura de qualquer Estado com serviços secretos abertamente espiões, são em si uma ameaça de bioproteção a laboratórios brasileiros que realizam pesquisas de alto impacto (PAI) consideradas pesquisas biológicas de ponta.

Além disso, serve para comparar o paradigma da AI em países que construíram a sua inteligência com grande influência militar e precipuamente voltada para a defesa externa, com o paradigma da AI no Brasil, que construiu a sua inteligência moldada sobretudo na defesa contra o inimigo interno, fortalecendo a inteligência interna em detrimento da inteligência externa[1, 97].

---

[u] *Military Intelligence* – Seção 6. Em contraposição à *Military Intelligence* – Seção 5 (MI-5), hoje conhecido como *Securtiy Service*, voltado para a inteligência e contrainteligência interna[96].

Trata-se de um paradigma voltado para o externo e militarizado *versus* um outro voltado para o interno e policialesco. No segundo caso, como o brasileiro, com a substituição do Serviço Nacional de Informações (SNI) pela ABIN, em 1999, surge uma tendência de modernização transmilitarizada e transecuritizada da inteligência de Estado.

> "Atuar de maneira transecuritizada não significa desconsiderar a relevância da temática de segurança estrita - até porque a Inteligência é órgão tradicionalmente de segurança e tem muito a contribuir na área -, mas tornar igualmente relevantes os demais setores.
> O conceito de transecuritização engloba as mudanças na doutrina e na produção da Inteligência, sob o paradigma da se- gurança humana, e implica na ideia de que os temas e diretrizes da atividade se tornam transdisciplinares."[97, p.86]

Para aprofundamento sobre a visão brasileira acerca da AI, vale destacar a auto-refexão da própria ABIN sobre a atividade. A ABIN é um órgão que, por sua origem militar, e cultura ainda militarizada, trata a AI de maneira a guardar muita influência da segurança e das Forças Armadas[1]. Deste modo, sua doutrina espelha a realidade da AI brasileira e merece ser considerada na discussão contemporânea do papel da inteligência na B2L e no P2R2 a eventos de biorrisco[8].

A Doutrina de Inteligência da ABIN foi atualizada em novembro de 2023 e se trata de documento oficial do Estado brasileiro sobre a AI. Segundo essa nova Doutrina de Inteligência da ABIN:

> "A atividade de inteligência produz conhecimentos e realiza ações visando à redução de vulnerabilidades e à neutralização de ameaças contra a segurança das pessoas e das instituições brasileiras. Também visa a proteger informações, pessoas, áreas, instalações e meios sensíveis, prevenindo, detectando, identificando, obstruindo e neutralizando ações de inteligência adversas."[8, p.12]

A atividade de inteligência, portanto, tal como descrita na doutrina, possui dois ramos: a inteligência (definida na primeira sentença do parágrafo transcrito imediatamente acima); e a contrainteligência (definida na segunda e última sentença).

Segue a Doutrina sobre o primeiro ramo da AI:

> "*A inteligência é o ramo da atividade voltado para a produção e a difusão de conhecimentos relativos a fatos, eventos, situações ou fenômenos que ocorram dentro e fora do território nacional, de imediata ou potencial influência sobre o processo decisório e a ação governamental, que se constituam ou indiquem oportunidades e ameaças aos objetivos fundamentais do Estado*."[8, p.14]

Considerando estas definições dos ramos da AI, pode-se concluir que entre as ameaças sob escopo da inteligência, podem-se arrolar as ameaças biológicas, assim como, entre as áreas e instalações a serem protegidas pela contrainteligência, podem estar os laboratórios de interesse, que custodiam MBGC e PAI/PGC.

O artigo terceiro da Constituição Federal de 1988 traz os quatro objetivos fundamentais da República Federativa do Brasil:

> "I - construir uma sociedade livre, justa e solidária;
> II - garantir o desenvolvimento nacional;
> III - erradicar a pobreza e a marginalização e reduzir as desigualdades sociais e regionais;
> IV - promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação."[24]

Se "promover o bem de todos" é um objetivo fundamental do Estado brasileiro, considerando que as ameaças à bioproteção laboratorial afetam o bem de todos e possuem influência imediata sobre o processo decisório, então é necessário que a inteligência se debruce sobre questões relativas à bioproteção laboratorial, seguindo o disposto na própria Doutrina da ABIN.

Diferentemente do paradigma estadunidense-britânico – que não é diferente, neste aspecto, dos paradigmas de inteligência da Rússia ou China[1] -, a doutrina de inteligência brasileira não coloca a espionagem estrangeira como objetivo de atuação da ABIN e ainda pressupõe a possibilidade de se fazer inteligência de Estado sem operações secretas no estrangeiro[8], algo que dificilmente seria institucionalmente aceito pela política externa brasileira.

2.3.1 Documentos orientadores da atividade de inteligência no Brasil

Se, por um lado, a dissociação da política externa brasileira com uma inteligência externa nos moldes da CIA e do SIS legou uma inteligência brasileira focada na atuação interna. Por outro lado, levou a AI do SNI a uma aproximação com a inteligência militar e policial e à priorização de temas policiais no trabalho da inteligência[97].

A “falta de vocação externa” da AI no Brasil também gerou outra consequência importante: a generalização extrema do escopo da atividade de inteligência, institucionalizada na lei que cria a ABIN.

Segundo a Lei nº 9.883, de 07 de dezembro de 1999, que também institui o Sistema Brasileiro de Inteligência (SISBIN), entende-se como

> *“...inteligência a atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado. (...) Entende-se como contrainteligência a atividade que objetiva neutralizar a inteligência adversa."*[72]

Ora, “fatos e situações de imediata ou potencial influência sobre o processo decisório” podem ser aqueles relacionados a, na prática, qualquer assunto, uma vez que o processo decisório do poder executivo federal delibera sobre absolutamente todas as matérias sob responsabilidade do Estado, de educação à macroeconomia, de saúde à defesa nacional[97].

A inespecificidade do escopo de atuação da inteligência federal e civil brasileira, tal como disposto na lei de criação do SISBIN e da ABIN, reflete-se na atual missão da ABIN:

> “*Antecipar fatos e situações que possam impactar a segurança da sociedade e do Estado brasieiros, de modo a assessorar o mais alto nível decisório do País, bem como salvaguardar conhecimentos sensíveis e aprimirar a Atividade de Inteligência de Estado.”*[73]

2.3.1.1 Política Nacional de Inteligência (PNI)

A amplitude ilimitada e inespecífica de atuação potencial do SISBIN e da ABIN é delimitada pela ideia de uma Política Nacional de Inteligência (PNI)[v] balizadora, constante do artigo quinto da lei:

> “*Art. 5º - A execução da Política Nacional de Inteligência, fixada pelo Presidente da República, será levada a efeito pela ABIN, sob a supervisão da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo.*
>
> *Parágrafo único. Antes de ser fixada pelo Presidente da República, a Política Nacional de Inteligência será remetida ao exame e sugestões do competente órgão de controle externo da atividade de inteligência.*
>
> *Art. 6º - O controle e fiscalização externos da atividade de inteligência serão exercidos pelo Poder Legislativo..."*[72]

[v] Documento não classificado.

Entre a criação da ABIN, em 1999, e 2016, ano de criação da PNI, fixada pelo Decreto no 8.793 de 29 de junho de 2016 e vigente até hoje, a lacuna das diretrizes de inteligência foram supridas por outras normas infralegais que mantiveram um escopo quase ilimitado[1, 74].

Este período e escopo são bem descritos e analisados por COELHO (2017), que revelou o conteúdo da Resolução da Câmara de Relações Externas e Defesa Nacional (CREDEN) Nº 02/2009[w].

A norma, integralmente disposta no Anexo A, arrola 26 (vinte e seis) áreas de atuação do SISBIN e ABIN e, até o presente momento, não teria sido revogada, estando vigente, a despeito da fixação da PNI.

> "Por outro lado, a abrangência pouco limitada pode contribuir para a falta de foco de trabalho na ABIN, que diferentemente dos demais órgãos do SISBIN, costuma tratar de todos os temas listados, com maior ou menor enfoque, de acordo com o interesse de seu corpo gerencial e das demandas presidenciais" [1, p.81]

São três os itens que mencionam diretamente ATBS/MBGC e CS/PAI/PGC:

1. Item "d" - "biodefesa da população e dos recursos naturais e agropecuários";
2. Item "q" - "existência, acesso, posse e uso de armas de destruição em massa e seus sistemas vetores que possa ocasionar reflexos para o Brasil; e
3. Item "r" – tráfico de armas, munições, explosivos, materiais radioativos, tecnologias sensíveis e bens de uso dual.

A PNI, por sua vez, "define parâmetros e limites da atuação da atividade de inteligência e de seus executores", "para balizamento das atividades dos diversos órgãos" que integram o SISBIN[75]. Considera 11 (onze) ameaças como principais ou priorizadas[69]. São elas:

1. Espionagem – ação que visa à obtenção de conhecimentos ou dados sigilosos;

[w] Esta norma infralegal, classificada como Reservada, foi desclassificada em 2014, mas somente foi tornada parcialmente pública em 2017, na referida pesquisa. Ela foi incorporada a esta tese no seu Anexo A.

2. Sabotagem – ação deliberada que visa a danificar dados, materiais ou instalações;
3. Interferência Externa – atuação deliberada de governos ou pessoas que possam influenciar os rumos políticos do país, em detrimentos ds interesses nacionais;
4. Ações contrárias à Soberania Nacional – atentam contra a autodeterminação, a não-ingerência e o respeito à Constituição e às leis;
5. Ataques cibernéticos;
6. Terrorismo;
7. Atividades ilegais envolvendo bens de uso dual e tecnologias sensíveis;
8. Armas de Destruição em Massa;
9. Criminalidade Organizada;
10. Corrupção; e
11. Ações Contrárias ao Estado Democrático de Direito – atentam contra o pacto federativo, os direitos e garantias fundamentais, o bem-estar e a saúde da população, entre outras[75].

Em suma, a Política definiu os parâmetros e limites da atuação da atividade de inteligência, identificando as principais ameaças, ou seja, aquelas que apresentam potencial capacidade de colocar em risco a segurança da sociedade e do Estado[75, p. 8].

Cabe refletir sobre uma das conclusões e as consequentes recomendações apresentadas por COELHO (2017), para aprofundar a integração saúde-segurança e a transecuritização da inteligência de Estado:

> *"CONCLUSÃO 5: O SISBIN e o CONSISBIN foram concebidos para lidar prioritariamente com ameaças securitárias tradicionais e suas estruturas dificultam o aprofundamento da transecuritização da inteligência estratégica.*
> *o RECOMENDAÇÃO 5a: O SISBIN pode exercer importante papel na aproximação do setor de segurança com o da saúde, inclusive mediante a criação de um subsistema de segurança da saúde (*health security*). Esta aproximação poderia partir tanto da ABIN, órgão central do SISBIN, quanto dos órgãos de saúde (MS, MAPA e MMA). Na falta de iniciativa de uma das partes, a outra deveria servir de incentivadora de protagonismo.*
> *o RECOMENDAÇÃO 5b: O CONSISBIN deveria ser integrado por órgãos não-securitários e contar com a participação do MS, MAPA e MMA, dada a relevância estratégica destes três ministérios e dos temas abordados pelas suas respectivas "inteligências".*
> *o RECOMENDAÇÃO 5c: O SISBIN poderia focar não apenas na integração de órgãos, mas de sistemas, como o SIPRON, SINPDEC, entre outros."* [1,p.246]

As recomendações continuam atuais, na medida em que não houve alteração dos documentos orientadores da AI, desde a aprovação de suas primeiras versões, até o momento.

2.3.1.2 Estratégia Nacional de Inteligência (ENINT)

A ENINT é um documento não classificado de orientação estratégica decorrente da PNI, fixada por meio do Decreto nº 8.793, de 29 de junho de 2016. A partir das ameaças priorizadas na Política, a Estratégia define eixos estruturantes e objetivos estratégicos de atuação dos órgãos de inteligência[78].

O documento foi discutido pelo CONSISBIN e aprovado por todos os órgãos do Sistema. O ENINT com a PNI "são elos aglutinadores dos órgãos que compõem o SISBIN e os direcionadores para a formulação das iniciativas estratégicas referentes à Atividade de Inteligência"[78, p. 7].

A ENINT define a missão do SISBIN como "desenvolver a AI, de forma integrada, para promover e defender os interesses do Estado e da sociedade brasileira."[78, p. 11].

A ENINT identifica eixos estruturantes (ou eixos de sustentação) como resultado da análise do ambiente estratégico e da análise de desafios. Os quatro eixos organizam os desafios, alinhando-os com o fito de impulsionar o funcionamento do SISBIN:

1. Atuação em rede – preconiza o trabalho coordenado, integrado e sinérgico entre os participantes do Sistema. Está correlacionada com dois desafios:
    a. Fortalecimento da atuação integrada e coodenada da AI; e
    b. Fortalecimento de cultura de proteção do conhecimento e de preservação do sigilo.
2. Tecnologia e capacitação – sustenta a necessidade de capacitação de alto nível para os profissionais de inteligência e de investimento em tecnologias de ponta, incluindo tecnologias para tratamento e análise de dados. Está correlacionada com três desafios:
    a. Maior utilização de tecnologias de ponta especialmente no campo cibernético;

b. Intensificação do uso de tecnologias de tratamento e análise de grandes volumes de dados (*Big Data* e *Analytics*); e

c. Ampliação e aperfeiçoamento do processo de capacitação oara atuação na área de inteligência.

3. Projeção internacional – o Brasil necessita estar inserido na ordem internacional com protagonismo. Está correlacionado com dois desafios:

a. Ampliação da internacionalização da AI brasileira; e

b. Apoio ao fortalecimento da inserção do país no cenário internacional.

4. Segurança do Estado e da sociedade – a antecipação de fatos e situações que se caracterizam como ameaças à integridade da sociedade é essencial para que o processo de assessoria ao mais alto nível decisório seja efetivo. Está correlacionado com três desafios:

a. Apoio ao combate à corrupção, ao crime organizado, aos ilícitos transnacionais e ao terrorismo.

b. Monitoramento e enfrentamento eficaz de ações adversas contra interesses nacionais; e

c. Aprimoramento da legislação para a AI[78, p. 10].

Por sua vez, com base nos desafios estratégicos e nos eixos de sustentação, foram definidos trinta e três objetivos para o desempenho eficaz da AI, considerando o horizonte temporal de cinco anos (2018-2023).

Cada desafio foi vinculado a de dois a quatro objetivos estratégicos, sem ordem de prioridade, conforme as figuras abaixo, que mostram as correlações entre os eixos estruturantes, os desafios e os objetivos estratégicos da ENINT[78, pp.29 e 30] (**Tabela 1 e Tabela 2**):

EIXOS ESTRUTURANTES	DESAFIOS	OBJETIVOS ESTRATÉGICOS
1. Atuação em rede	1.1 Fortalecimento da atuação integrada e coordenada da Atividade de Inteligência	○ Aprimorar os processos e protocolos para comunicação e compartilhamento de informações ○ Mapear e gerenciar os principais processos a serem realizados no SISBIN ○ Definir e regular critérios para atuação conjunta e coordenada no âmbito do SISBIN
	1.2 Fortalecimento de cultura de proteção do conhecimento e de preservação do sigilo	○ Criar protocolos conjuntos para proteção de conhecimentos sensíveis ○ Aperfeiçoar o processo de gestão de riscos ○ Fomentar a cultura de proteção do conhecimento na sociedade
2. Tecnologia e Capacitação	2.1 Maior utilização de tecnologias de ponta, especialmente no campo cibernético	○ Ampliar a capacidade do Estado na obtenção de dados por meio da Inteligência cibernética ○ Fortalecer a capacidade de pesquisa e desenvolvimento em tecnologia da informação e comunicação (TIC) ○ Aprimorar a capacidade de desenvolver e implementar criptografia de Estado ○ Modernizar a infraestrutura de tecnologia da informação e comunicação (TIC)
	2.2 Intensificação do uso de tecnologias de tratamento e análise de grandes volumes de dados (*Big Data e Analytics)*	○ Ampliar a capacidade de obtenção e análise de grandes volumes de dados estruturados e não estruturados ○ Aprimorar a estruturação e o compartilhamento de bases de dados de Inteligência ○ Promover a interoperabilidade de bases de dados de interesse em nível nacional
	2.3 Ampliação e aperfeiçoamento do processo de capacitação para atuação na área de Inteligência	○ Promover a integração entre as Escolas de Governo para ampliar a oferta de cursos relacionados à Inteligência e estruturar capacitações conjuntas ○ Estabelecer processo de gestão por competências para capacitação em Inteligência ○ Fortalecer a educação a distância (EAD) ○ Promover a qualificação técnica para proteção e exploração do campo cibernético

Tabela 1 – *Eixos estruturante, desafios e objetivos estratégicos da ENINT* [78]

3. Projeção internacional	3.1 Ampliação da internacionalização da Atividade de Inteligência brasileira	○ Aumentar a representação da Atividade de Inteligência no exterior ○ Incrementar a interação do SISBIN com os demais sistemas de inteligência em temas de interesse ○ Aperfeiçoar a qualificação de adidos e demais agentes diplomáticos ○ Aumentar a participação em fóruns, eventos e encontros internacionais
	3.2 Apoio ao fortalecimento da inserção do País no cenário internacional	○ Ampliar as redes de parcerias e incrementar os acordos de cooperação internacional ○ Apoiar as instituições brasileiras em sua atuação no exterior ○ Ampliar o intercâmbio de informações entre os órgãos brasileiros com atuação no exterior ○ Consolidar a Atividade de Inteligência em questões externas estratégicas
4. Segurança do Estado e da sociedade	4.1 Apoio ao combate à corrupção, ao crime organizado, aos ilícitos transnacionais e ao terrorismo	○ Estabelecer temas prioritários para produção de conhecimentos referentes às seguintes ameaças: corrupção, crime organizado, ilícitos transnacionais e terrorismo ○ Aprimorar os meios de compartilhamento de informações sobre as seguintes ameaças: corrupção, crime organizado, ilícitos transnacionais e terrorismo ○ Criar protocolos específicos para atuação integrada do SISBIN em relação às seguintes ameaças: corrupção, crime organizado, ilícitos transnacionais e terrorismo
	4.2 Monitoramento e enfrentamento eficaz de ações adversas contra interesses nacionais	○ Identificar os principais temas de interesse nacional para defesa contra ações adversas externas ○ Estabelecer sistema de alerta para prevenção de potenciais ações adversas ○ Criar protocolos específicos para atuação integrada visando a neutralização de ações adversas
	4.3 Aprimoramento da legislação para a Atividade de Inteligência	○ Acompanhar e apoiar o processo legislativo nos temas de interesse da Atividade de Inteligência ○ Aperfeiçoar o marco legal da Atividade de Inteligência

Tabela 2 – *Eixos estruturante, desafios e objetivos estratégicos da ENINT (continuação)*[78]

Destacam-se alguns objetivos estratégicos que são importantes para a revisão do papel da AI brasileira na área da inteligência laboratorial:

1. Aprimorar os processos e protocolos para comunicação e compartilhamento de informações;
2. Definir e regular critérios conjuntos para atuação conjunta e coordenada no âmbito do SISBIN;
3. Criar protocolos conjuntos para proteção de conhecimentos sensíveis;
4. Aperfeiçoar o processo de gestão de riscos;
5. Fomentar a cultura de proteção do conhecimento na sociedade;
6. Ampliar a capacidade do Estado na obtenção de dados por meio da inteligência cibernética;
7. Aumentar a representação da atividade de inteligência no exterior;
8. Aumentar a participaçnao em fóruns, eventos e encontros internacionais;
9. Apoiar as instituições brasileiras em sua atuação no exterior;
10. Consolidar a atividade de inteligência em questões externas estratégicas;
11. Estabelecer temas prioritários para produção de conhecimentos referentes às seguintes ameaças: (...) ilícitos transnacionais e terrorismo;
12. Ampliar os meios de compartilhamento de informações sobre as seguintes ameaças: (...) ilícitos transnacionais e terrorismo;
13. Criar protocolos específicos para atuação integrada do SISBIN em relação às seguintes ameaças: (...) ilícitos transnacionais e terrorismo;
14. Identificar os principais temas de interesse nacional para defesa contra ações advseras externas;
15. Estabelecer sistemas de alerta para prevenção de potenciais ações adversas; e
16. Criar protocolos específicos para atuação integrada visando à neutralização de ações adversas.

Todos esses dezesseis objetivos estratégicos da AI brasileira se coadunam com o papel da inteligência laboratorial, no sentido de mitigar e antecipar riscos de BPL.

2.3.1.3 Plano Nacional de Inteligência (PLANINT)

O Plano Nacional de Inteligência (PLANINT) foi instituído por meio da Portaria 40 do Gabinete de Segurança Institucional da Presidência da República do Brasil (GSI/PR). Ela foi assinada em 03 de maio de 2018 durante reunião do CONSISBIN[79].

Assim como a PNI e a ENINT, o PLANINT é um documento orientador da atividade de inteligência voltado para todos os órgãos do SISBIN, tendo sido elaborado pelo Sistema.

Se a PNI identificou as ameaças prioritárias a serem prevenidas e analisadas[75]; e se a ENINT identifica os desafios à AI e elenca eixos estrutrurantes de atuação[76], coube ao PLANINT estabelecer:

> "*as ações a serem planejadas e executadas pelas instituições integrantes do Sistema Brasileiro de Inteligência (SISBIN), com vistas à consecução dos objetivos estratégicos fixados pela Estratégia Nacional de Inteligência (ENINT).*"[77]

Como se trata de um documento classificado, e que não está focado na atuação apenas da ABIN, mas de todo o SISBIN, optou-se por não o analisar pormenorizadamente na presente pesquisa, focada na inteligência laboratorial, evitando questionamentos sobre levantamento de sigilo abrangente e desnecessário.

2.3.1.4 Plano de Inteligência da Agência Brasileira de Inteligência (PI–ABIN)

Consderando que o PLANINT é uma construção coletiva do SISBIN para nortear as ações de todos os integrantes do Sistema, os Planos de Inteligência (PI) são a orientação interna de cada órgão para as suas atividades específicas.

A ABIN institui o seu PI, chamado de PI-ABIN, por meio de documento do Gabinete de Segurança Intitucional (GSI), a Portaria 373/GSIPR[x], de 03 de outubro de 2018, explicitando objetivos de inteligência voltados para cada ameaça priorizada pelo PNI e julgada de competência de atuação da ABIN[80].

[x] Documento classificado.

"Módulo" é como o PI-ABIN denomina as áreas de atuação da ABIN para obtenção de conhecimentos. Na explicação do contexto ("Situação") do "Módulo Ameaças Químicas, Biológicas, Radiológicas e Nucleares (QBRN) e Tecnologias de Uso Dual":

> *"...o foco de atuação da ABIN na área de ameaças QBRN é restrito aos agentes químicos, biológicos, radiológicos e nucleares considerados estratégicos – por isso, selecionados -, assim como às pesquisas de uso dual relacionadas à disseminação destes agentes selecionados.*
>
> *Na falta de uma lista oficial dos agentes selecionados, a ABIN coordena, por meio do SISBIN, esforços institucionais para a elaboração de uma lista adaptada à realidade nacional. Enquanto a lista não existe, tem utilizado como referência listas estrangeiras, como a do* Federal Select Agent Program *(FSAP), programa governamental dos Estados Unidos da América*" [80]

Correlacionados às duas ameaças QBRN e tecnologias de uso dual, são definidos cinco objetivos de inteligência (OI) pela ABIN para sua atividade na produção de conhecimento e assessoramento presidencial sobre o assunto[80]:

1. Conhecer a ocorrência de agentes QBRN selecionados no Brasil e os riscos associados;
2. Conhecer a ocorrência de agentes QBRN selecionados na América Latina;
3. Conhecer a capacidade de prevenção, preparo e resposta a eventos QBRN selecionados no Brasil;
4. Conhecer os temas discutidos nos principais fóruns multilaterais de não-proliferação de armas de destruição em massa (ADM);
5. Conhecer políticas públicas estrangeiras para prevenção e mitigação do risco de eventos QBRN selecionados[80].

Cada OI é, por fim, associado a conhecimentos necessários (CN), que configuram o detalhamento daquilo que a ABIN precisa conhecer para cumprir com o preconizado para PI-ABIN, com base na ENINT e PNI.

Para o OI 1 ("Conhecer a ocorrência de agentes QBRN selecionados no Brasil e os riscos associados") estão listados cinco CN:

3.1 – Laboratórios públicos e privados NB3 e NB4 ou com agentes biológicos selecionados;

3.2 – Instalações que estocam, transportam, pesquisam, produzem e desenvolvem agentes químicos selecionados;

3.3 – Instalações nucleares com fontes radiológicas selecionadas;

3.4 – Empresas brasileiras que importam ou exportam bens controlados pelos regimes de não proliferação; e

3.5 – Pesquisas estratégicas e de uso dual nas áreas QBRN e relacionadas, como a missilística e a aeroespacial[80].

Para o OI 2 (“Conhecer a ocorrência de agentes QBRN selecionados na América Latina”) estão listados quatro CN:

2.1 - Laboratórios públicos e privados NB3 e NB4 ou com agentes biológicos selecionados;

2.2 – Instalações que estocam, transportam, pesquisam, produzem e desenvolvem agentes químicos selecionados;

2.3 – Instalações nucleares com fontes radiológicas selecionadas; e

2.4 – Pesquisas estratégicas e de uso dual nas áreas QBRN e relacionadas, como a missilística e a aeroespacial[80].

Para o OI 3 (“Conhecer a capacidade de prevenção, preparo e resposta a eventos QBRN selecionados no Brasil”) estão listados três CN:

3.1 – Recursos humanos e materiais na resposta a eventos QBRN nos estados;

3.2 – Planos de contingência ou resposta a emergências por eventos QBRN selecionados; e

3.3 – Casos de disseminação de agentes QBRN selecionados[80].

Para o OI 4 (“Conhecer os temas estratégicos discutidos nos principais fóruns multilaterais de não proliferação de ADM”) está listado um único CN, mas com quatro desdobramentos de conhecimentos necessários (DCN):

1.1 – Discussões estratégicas no âmbito da Convenção sobre a Proibição de Armas Químicas (CPAQ); da Convenção para a Proibição do Desenvolvimento, Produção, e Estocagem de Armas Bacteriológicas (Biológicas) e Toxínicas e para a sua Destruição (CPAB); do Regime de Controle de Tecnologia de Mísseis (RCTM - MTCR, na sigla em inglês); e do Grupo de Fornecedores Nucleares (GFN – NSG, na sigla em inglês):

1.1.1 – Posicionamento dos diferentes atores brasileiros (Ministério das Relações Exteriores, Forças Armadas, setor privado e organizações sociais);

1.1.2 – Principais posicionamentos estrangeiros (favoráveis e contrários ao brasileiro) e formas de pressão sobre o Brasil;

1.1.3 – Reflexos das decisões nestes foros sobre os setores estratégicos e a sociedade brasileira; e

1.1.4 – Programas (redes) de proliferação de ADM; *modus operandi* de redes de proliferação de ADM; e transferência intangíveis de tecnologias de uso dual[80].

Para o OI 5 ("Conhecer políticas públicas estrangeiras para prevenção e mitigação do risco de eventos QBRN selecionados") estão listados dois CN:

5.1 – Políticas públicas estrangeiras; e

5.2 – Casos de disseminação de agentes QBRN selecionados[80].

Os CN foram atribuídos pelo PI-ABIN para as diversas frações da Agência, no sentido de distribuir as comeptências de busca destes conhecimentos.

Com este arrolamento de conhecimentos necessários para o desempenho da AI pela ABIN, as Superintendências estaduais passam a ser responsáveis pela obtenção de informações e processamento de conhecimentos sobre, por exemplo, "laboratórios públicos e privados NB3 e NB4 ou com agentes biológicos selecionados" (CN 2.1), em nível estadual.

De maneira análoga, as adidâncias de inteligência[y] no exterior passam a ser responsáveis pela obtenção de conhecimentos sobre, por exemplo, "políticas públicas estrangeiras para prevenção e mitigação do risco de eventos QBRN selecionados" (CN 5.1), em nível nacional do(s) país(es) sob responsabilidade de cada adidância.

A pormenorização do trabalho de inteligência do PI-ABIN define também a regularidade com que cada fração deverá enviar conhecimentos sobre os assuntos

[y] Apesar de não constarem na estrutura regimental da ABIN[81], a Agência possui representações em 18 países da América, África, Ásia, Europa e Oceania. Tais representações são chamadas de adidâncias de inteligência. Oficiais de inteligência atuam nesses países, lotados nas embaixadas respectivas brasileiras, exercendo a função de adidos civis. Eles fazem o intercâmbio de informações e produzem conhecimentos sobre temas de interesse do Estado brasileiro[82].

atribuídos à sua competência para a sede, de modo a atender as necessidades de produção de conhecimento para os órgãos parceiros do SISBIN e para o mais alto nível decisório do país.

Ressalte-se que este rol de dados, a ser regularmente monitorado, e de conhecimentos, a ser regularmente produzido, não é exaustivo, na medida em que outros temas, mormente temas emergentes, podem surgir e requerer acompanhamento oportuno.

Deste modo, o PI-ABIN é entendido como um conjunto mínimo de conhecimentos requeridos para atender às necessidades priorizadas pela PNI e adaptadas à competência institucional da ABIN.

2.3.2 PANGEIA

O Programa de Articulação Nacional entre Governo, Empresas e Instituições Acadêmicas para a Prevenção e Mitigação de Eventos Químicos, Biológicos, Radiológicos e Nucleares Selecionados da Agência Brasileira de Inteligência (PANGEIA/ABIN) foi instituído pela Portaria nº 112/GSI/PR, de 17 de dezembro de 2018[106], com um nome e símbolo que remetem à união de continentes (**Figura 14**).

Figura 14 – Símbolo do programa PANGEIA/ABIN[83].

O planejamento do PANGEIA foi partiu de uma iniciativa da Direção Geral da ABIN para substituir o Programa Nacional de Intemnistégração Estado-Empresa na Área de Bens Sensíveis (PRONABENS), que tinha escopo restrito a apenas um

dos aspectos das ameaças químicas, biológicas, radiológicas e nucleares (QBRN)[84, 86].

Concebido e executado, conjuntamente pela então Coodenação-Geral de Bens Sensíveis (CGBS) do Ministério da Ciência, Tecnologia e Inovação (MCTI), o PRONABENS nunca existiu formalmente. Desde sua criação, até a escrita desta tese, nunca houve portaria ou norma que o instituísse e regulamentasse[86].

O PANGEIA foi criado pela então recém instituída Coordenação de Análise de Tecnologias Sensíveis e Biodefesa (COTESB)[85], para formalizar e ampliar as ações do PRONABENS, cujas atividades de *outreach* na área de bens sensíveis passou a ser uma das atividades do novo programa.

Apesar da criação da COTESB como fração de biodefesa da ABIN, a doutrina de inteligência e o regimento interno do órgão não definiram biodefesa. A ABIN utilizou o termo em consonância com a ideia transmilitarizada de biodefesa, demonstrando interesse institucional de a ABIN se colocar como parte da biodefesa civil brasileira ou, para ser mais preciso com as definições referenciadas, como parte da biodefesa brasileira *tout court*[1, p.4].

A portaria que institui o PANGEIA/ABIN[83] prevê a implementação de sete ações não exaustivas, isto é, ações que não estão listadas em detrimento da realização de outras ações no escopo do programa mas que não estão arroladas :

> "*I - Mapeamento de instalações que comercializam, custodiam, desenvolvem, estocam, produzem, transportam ou utilizam agentes selecionados e que pesquisam tecnologias com uso dual selecionadas, doravante chamadas instalações selecionadas, e dos riscos associados;*
> *II - Desenvolvimento e aplicação de ferramentas de avaliação de múltiplas ameaças à proteção dos agentes selecionados;*
> *III - Desenvolvimento e aplicação de ferramentas de avaliação dos sistemas de proteção das instalações selecionadas;*
> *IV - Sistematização de recomendações aos sistemas de proteção das instalações selecionadas, na forma de Relatórios de Avaliação de Ameaças e de Sistemas de Proteção (RELASP) e de Pareceres de Inteligência;*
> *V - Sensibilização e treinamento para fomentar a cultura de proteção dos agentes selecionados e das pesquisas de uso dual selecionadas;*
> *VI - Avaliação prévia (*security clearance*) e contínua de pessoas com acesso a agentes selecionados e pesquisas de uso dual selecionadas; e*
> *VII - Assessoramento no controle de comércio de agentes selecionados e outros bens de uso dual, em parceria com os órgãos nacionais competentes."*[83] (**Figura 15**)

Figura 15 – As sete ações de competência normativa do PANGEIA/ABIN[83,89].

Durante o planejamento do Programa, percebeu-se que as ameaças de disseminação intencional ou não de agentes QBRN eram tratadas de maneira fragmentada por diversas frações do órgão de inteligência civil brasileiro. Desta forma, havia várias equipes trabalhando temas correlatos com compartimentação entre elas e perda de efetividade.

Em 2018, ano de criação do PANGEIA, as áreas finalísticas da ABIN eram divididas em três departamentos:

1. Departamento de Inteligência Estratégica (DIE);
2. Departamento de Contrainteligência (DCI); e
3. Departamento de Contraterrorismo (DCT)[83].

O DIE, por um lado, se dividia em coordenações-gerais e estas, em coordenações. Havia coordenações que lidavam com acompanhamento e produção de conhecimentos sobre:

1. Países proliferadores de ADM e regimes de não proliferação;
2. Ameaças “naturais” (surtos e epidemias) e conjuntura internacional associada; e
3. Ameaças QBRN não intencionais e não naturais (ex. acidentes)[89-92].

O DCI, por outro lado, de maneira análoga ao DIE, seguindo a regras da administração do Executivo federal se dividia em coordenações-gerais e estas, em coordenações[83]. Havia coordenações que lidavam com acompanhamento e produção de conhecimentos sobre:

1. Sabotagem;
2. Espionagem;
3. Avaliação dos sistemas de proteção de instalações selecionadas; e
4. Setores estratégicos (ex. setor nuclear, aeroespacial e biotecnológico).

O DCT, por fim, se dividia em coordenações-gerais e coordenações que lidavam com acompanhamento e produção de conhecimento sobre:

1. Terrorismo;
2. Extremismo;
3. Crime organizado.

Não foram disponbilizadas as normas de formalização da então estrutura das coordenações citadas e suas competências de análise, constantes do Regimento Interno da ABIN, que é documento classificado e que detalha a estrutura subdepartamental[z].

Estes dados de pesquisa, portanto, são provenientes de fonte primária: o testemunho do autor enquanto ex-coordenador de área da ABIN, sem a respectiva norma que comprove a estrutura institucional.

[z] O decreto traz a estrutra até o nível de departamento, enquanto o Reguamento Interno detalhas a composição dos departamentos, bem como as competências de cada fração (coordenações e coordenações-gerais).

Entretanto, estas observações podem ser verificadas em *slides* de apresentações públicas do PANGEIA para órgãos parceiros do SISBIN, públicos e privados, a exemplo do mostrado na **Figura 16**:

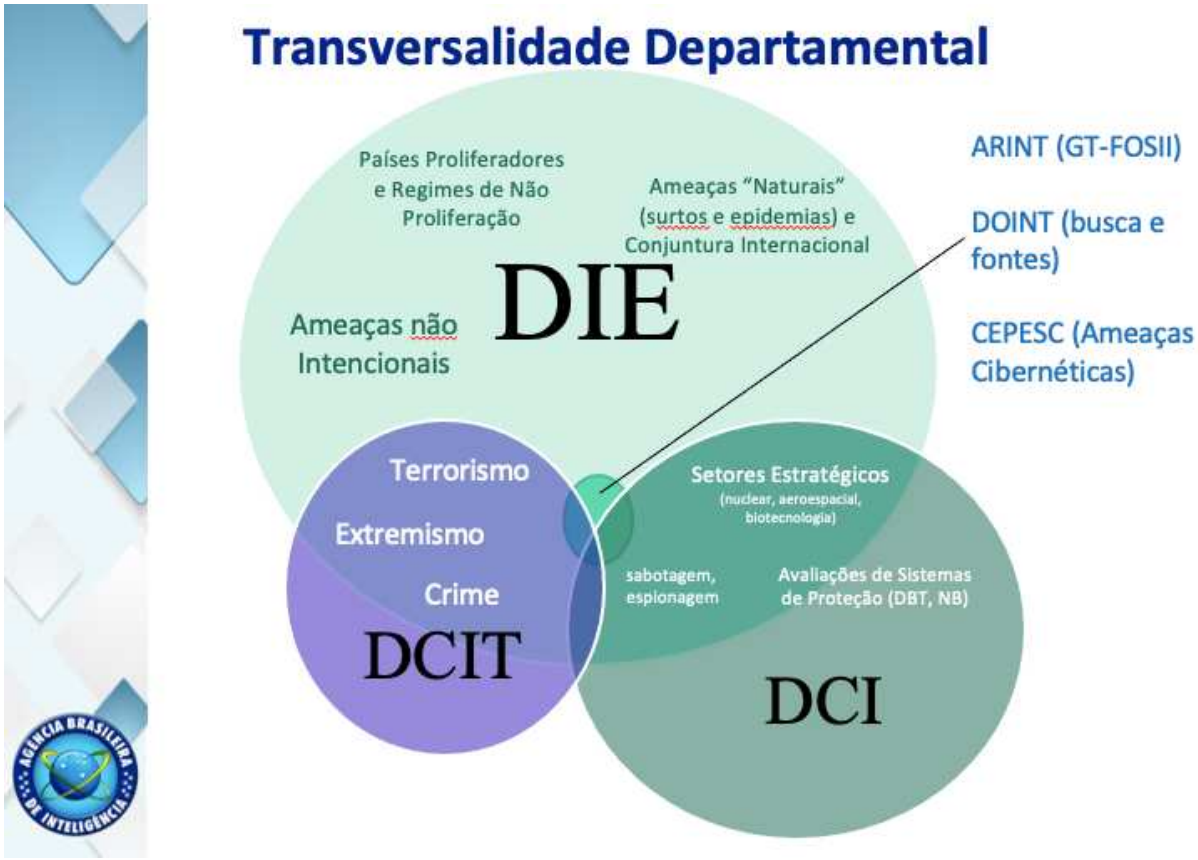


Figura 16 – Dispersão temática das ameaças QBRN e competências de algumas áreas finalísticas da ABIN, no ano de 2018[90].

Percebe-se, portanto, que o tema das ameaças biológicas envolvia, na percepção da inteligência brasileira e dos criadores do PANGEIA, pelo menos 12 áreas de atuação e acompanhamento da ABIN:

1. Infraestruturas críticas em setores estratégicos (ex. laboratórios);
2. Sabotagem;
3. Espionagem;
4. Avaliação de sistemas de proteção;
5. Crime organizado;
6. Crime comum ("não organizado");
7. Extremismo violento;

8. Terrorismo com armas de destruição em massa;
9. Disseminação “natural” de patógenos e toxinas (ex. epidemias não causadas intencionalmente);
10. Disseminação acidental de material biológico por falhas de biossegurança laboratorial;
11. Acompanhamento de países proliferadores de armas biológicas; e
12. Regimes de não proliferação de armas biológicas.

Tais áreas eram divididas em várias equipes de acompanhamento em diferentes coordenações de diferentes departamentos, apesar de serem assuntos transversais e com estreita ligação e complementaridade entre eles.

Havia, portanto, no tema transversal das ameaças biológicas, a compartimentação do acompanhamento, análise e produção de conhecimentos, prejudicando a atuação efetiva, por exemplo, na área de bioproteção laboratorial (**Figura 17**).

Figura 17 – Compartimentação de temas afins às ameaças QBRN na ABIN, sem o PANGEIA/ABIN[91].

Deste modo, a compartimentação entre as diferentes equipes e de diferentes departamentos criava situações indesejadas como esta situação hipotética: um analista que acompanha um regime de não proliferação de armas biológicas desconhecer os planos de um grupo terrorista internacional com atuação no Brasil em utilizar armas biológicas num atentado em território brasileiro.

Ou ainda: um analista que acompanha o tema de infraestruturas críticas laboratoriais desconhecer as ameaças de crime organizado que paira sobre este laboratório.

A criação da COTESB e do PANGEIA/ABIN serviram para reunir todas estas ameaças numa única coordenação e uma única equipe, que acompanhava de maneira transversal o tema das ameaças biológicas e atuava em um único programa da inteligência.

O PANGEIA parte da simbologia da junção dos continentes, isto é, da aproximação de frações (continentes) que estão normalmente separadas e compartimentadas, para propor, no âmbito da ABIN, o conceito inovador de abordagem transversal de ameaças e oportunidades (**Figura 18**):

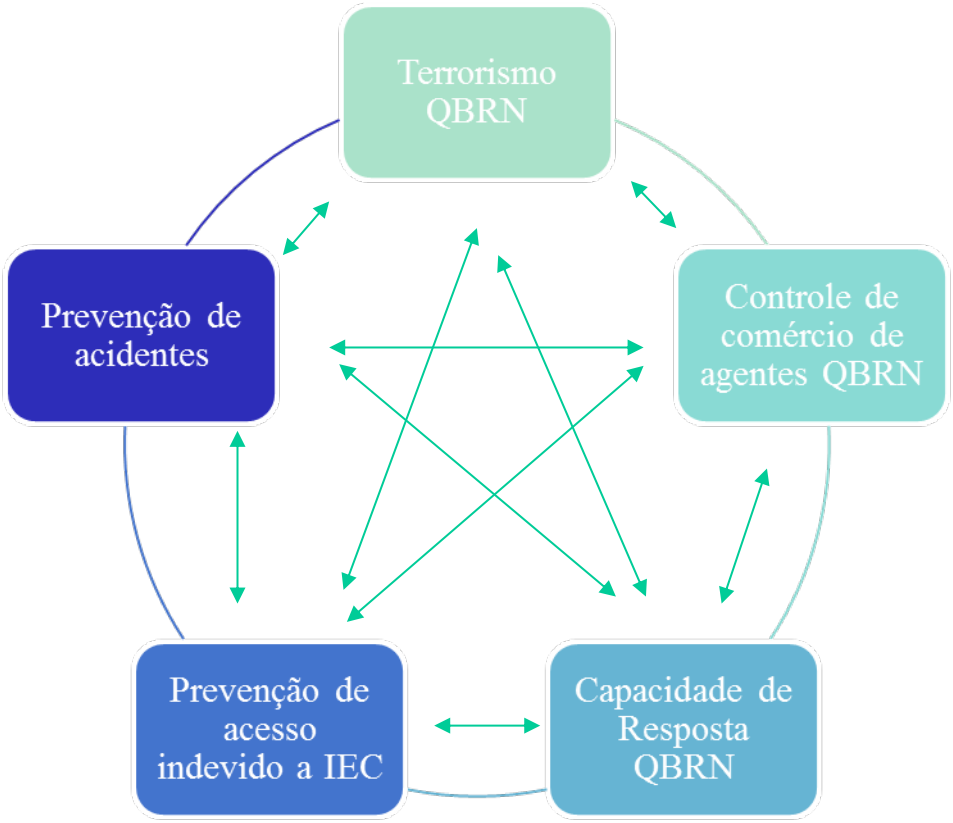


Figura 18 – Integração de temas afins às ameaças QBRN, integrados pelo PANGEIA/ABIN[91].

A criação da COTESB, de fato, tratou-se de transformar a percepção de um tema que estava situado no ramo da inteligência externa[aa] para que se tornasse um tema precipuamente transnacional, isto é, que transcende a dicotomia anacrônica do campo interno *versus* campo externo.

Da sua criação em 2017 à sua extinção em 2019, a COTESB foi uma das duas coordenações ligadas à então Coordenação-Geral de Inteligência Externa (CGIE)[bb]. A antecessora da COTESB, chamada de Coordenação de Análise de Não-Proliferação e Tecnologias Sensíveis (COATS), era focada no acompanhamento e

[bb] A outra era a então Coordenação de Análise de Assuntos Internacionais (COAAI), cuja enorme abrangência temática do nome nunca refletiu adequadamente as suas competências. Se pensarmos que os regimes de não proliferação, por exemplo, é um assunto internacional, poderemos querer atribuí-lo à COAAI, quando era tema da COATS.

assessoramento de regimes e fóruns multilaterais de não proliferação e em ações de sensibilização (*outreach*) de empresas sobre a governança de bens e tecnologias de uso dual. Era, portanto, uma coordenação com olhar voltado sobretudo para a segurança internacional, tanto que reproduzia em seu nome, fração análoga que existia no Ministério das Relações Exteriores (MRE), com quem deveras dialogava institucionalmente.

A COTESB foi planejada praticamente ao mesmo tempo do PANGEIA para juntos superarem a ideia de fragmentação e compartimentação dos temas relacionados a riscos e ameaças QBRN em um acompanhamento e análise integrados – a exemplo de um continente único e aglomerador, a PANGEIA.

Sob o ponto de vista de estrutura, o ideal, entretanto, seria o de localizar a COTESB fora do binarismo interno e externo, próprio do século XX e da emergência dos primeiros serviços secretos. Mas não havia estrutra semelhante na ABIN, como ainda não o há coordenações de análises temáticas que estejam situadas em estruturas supra-departamentais ou em departamento de inteligência transnacional.

Portanto, por uma questão de inércia estrutural, a COTESB se manteve vinculado à então CGIE.

A portaria do PANGEIA, ao determinar o escopo de atuação, assim o descreveu:

> "Trata-se de um programa da ABIN, implementado em parceria voluntária com instituições públicas e privadas, com a finalidade de antecipar fatos e situações relacionados à disseminação de agentes químicos, biológicos, radiológicos e nucleares (QBRN) selecionados, para assessoramento do processo decisório."[81]

Verifica-se que os fatos e situações relacionados à disseminação de agentes biológicos selecionados podem ser causados por quaisquer das ameaças vinculadas aos 12 temas de acompanhamento supracitados.

Por exemplo, para citar uma das ameaças vinculadas a tema de análise de inteligência da ABIN, os regimes de não proliferação estão relacionados com o risco de disseminação de ABTS, na medida em que dificultam a proliferação de armas biológicas.

Outro exemplo: o extremismo violento com ataques biológicos está relacionado com a disseminação de ABTS, na medida em que diretamente provoca esta disseminação.

Neste sentido, a atuação da inteligência na área de bioproteção laboratorial, por meio do PANGEIA, buscava igualmente atuar na antecipação de fatos e situações relacionados à disseminação de agentes biológicos selecionados.

Esta possibilidade de disseminação via falhas de bioproteção, por sua vez, está intimamente ligada à possibilidade de obtenção de ABTS para uso em atos de sabotagem, terrorismo, crime comum, crime organizado, extremismo violento e outras formas de ameaça.

Desde a extinção da COTESB, a principal fração da ABIN que lidava com riscos biológicos, cerca de dois meses antes do surgimento dos primeiros casos de COVID-19 (então n-SARS-CoV) – o principal evento biológico mundial desde a Gripe Espanhola em 1918 – a estrutura do PANGEIA foi assumida por outra coordenação, inicialmente, com competência de implementar outras ações e programas, além do PANGEIA.

Antes, na COTESB, ressalte-se que o PANGEIA era o único programa coordenado pela fração, permitindo uma atenção e recursos que não eram divididos por outros programas. O PANGEIA deixa, portanto, de ser prioritário na atuação da fração em que está inserido, até perder pessoal envolvido (e treinado) no tema, e ser transferido para uma divisão (fração menor administrativamente do que uma coordenação, na estrutura do Executivo Federal).

O contexto de tais mudanças ocorre em concomitância ao fortalecimento da inteligência interna com a criação de uma estrutura departamental maior do que qualquer outro Departamento da Abin, chamado de Centro de Inteligência Nacional (CIN)[cc], focado em inteligência interna, ramo que passa a ter uma relevância muito maior do que tivera até então na ABIN, desde a sua criação – pelo menos no que diz respeito à estrutura departamental.

A perda de importância de temas transnacionais e transecuritizados, como a B2L e o PANGEIA, e o paralelo fortalecimento de temáticas voltadas à “inteligência interna”, sob enfoque mais corrente e menos estratégico, demonstrou um retrocesso na tendência modernizante de trasecuritização e transilitarização, com abordagem mais estratégica pela inteligência de Estado civil brasileira.

O resultado concreto desta mudança, na perspectiva do PANGEIA e da prevenção e mitigação de biorriscos, sobretudo laboratoriais, pode ser avaliado com

a revisão atenta de dois documentos não classificados que são os Relatórios Anuais da ABIN, de 2023 e 2024[100, 101].

Nesses últimos relatórios de ações realizadas pela Agência nos dois últimos anos, as palavras *biossegurança*, *bioproteção*, *riscos biológicos*, *PANGEIA* e *laboratório*/*laboratorial* não aparecem nenhuma vez. De um programa com umas das maiores produtividades de ações e relatórios, em 2018 e 2019, as ações do PANGEIA desaparecem da Abin nos dois últimos anos[100, 101].

Apesar da manutenção, oficialmente, da vigência do PANGEIA, que consta em página atualizada em novembro de 2023 do sítio da ABIN[83], a instituição deixou de realizar ações sistemáticas do programa, e o assunto não é questionado pela Comissão de Controle da Atividade de Inteligência (CCAI) do Congresso Nacional, órgão de controle externo da AI no Brasil.

Apesar da criação, em 2024, de uma coordenação específica para lidar com as ameaças QBRN e para coordenar o PANGEIA, nos moldes da COTESB, a Coordenação de Ameaças QBRN e Não Proliferação (COQBRN), vinculada ao atual Departamento de Contrainteligência, vivencia um significativo retrocesso, comparado com a situação de pré-2019/2020, na perspectiva da B2L, em termos de número de servidores e recursos disponíveis.

Nos últimos anos, a sobrevalorização não apenas de ameaças securitárias “internas” se tornou um obstáculo à modernização da AI, no sentido de ampliar a temática para riscos transdisciplinares à segurança humana, a exemplo dos riscos laboratorias.

Há igualmente um movimento de valorização da inteligência corrente em detrimento da estratégica, e até mesmo em detrimento da inteligência operacional-tática em diversas áreas[8].

Esse reforço na importância da inteligência interna – e na enfatização de temas internos e externos, ao contrário de favorecer a transdisciplinarização temática – poderia ser descrito como um retrocesso, no sentido da modernização da inteligência:

> Ao criar e discutir o conceito da transecuritização da Inteligência Estratégica, buscou-se analisar sistematicamente um processo em curso e de fundamental importância para tornar a Inteligência mais eficiente na sua missão de antecipar fatos de impacto relevante contra a sociedade. Este processo não é inexorável, mas passível de retrocessos.
> A possibilidade de retrocessos está, em parte, associada a aspectos do sistema de Inteligência que tendem a sobrevalorizar as ameaças securitárias[97, p.88]

Tal movimento de fortalecimento institucional da inteligência interna, sob a égide da inteligência corrente, não é exclusivo, dado que há vetores concomitantes de fortalecimento de alguns temas de inteligência estratégica transdisciplinar, a exemplo da crise climática[dd].

Percebe-se, entretanto, que os temas transversais tendem a ganhar e perder relevância à mercê das mudanças de governo, tal como ocorrido com a B2L e a área de análise de meio ambiente. A constância de fortalecimento da inteligência menos estratégica e mais corrente, entretanto, tem sido uma realidade pelo menos nos últimos 15 anos.

Quanto à inteligência laboratorial, a criação da COQBRN pela ABIN, apesar de dispor de recursos humanos e materiais significativamente inferiores ao da antiga COTESB, pode apontar para um passo pequeno na direção de potencial de retomada das ações de B2L do PANGEIA[ee].

[dd] Em 2024, a Escola de Inteligência da ABIN (ESINT/ABIN) criou um Núcleo de Pesquisa em Inteligência (NUPI), com alguns grupos de pesquisa, entre eles um sobre "Inteligência, Segurança e Mudanças Climáticas" do qual o autor da presente tela faz parte. A criação deste grupo de pesquisa se baseia no fato de que transições globais e mudança climática se configuram como um tema de interesse prioritário para a ESINT[106, p.19].

[ee] Os dados de recursos humanos e orçamentários são sigilosos e foram obtidos diretamente pelo autor do presente estudo, por isso permanecerão classificados na presente pesquisa.

2.3.3 Ameaças de eventos biológicos selecionados no Brasil

Durante a atuação do PANGEIA, a atividade de coleta de informações e acompanhamento das ameaças biológicas, fases do ciclo de inteligência conforme supracitado, seguiram o determinado pelo PI-ABIN[80].

Apesar de os objetivos de conhecimento não mencionarem explicitamente as ameaças, o OI 1, ao mencionar "*Conhecer a ocorrência de agentes QBRN selecionados no Brasil e os riscos associados*", implicitamente considerava as ameaças de BPL como objetivo de inteligência da ABIN[80].

Ora, se não há risco de BPL sem ameaças, havia determinação expressa (fase 1 do ciclo de inteligência – "*objetivar*") para coletar informações (fase 2 do ciclo) e acompanhar o tema (fase 3 do ciclo)[8].

Entre 2017 e 2019, a título de exemplificação da gravidade das ameaças QBRN, com ênfase para as ameaças biológicas, foram acompanhadas as seguintes ameaças com potencial repercussão à BPL no Brasil:

1. Sociedade Secreta Silvestre (SSS) – organização criminosa que demonstrou, em 2019, intenção de de uso de toxina biológica, ao emitir um comunicado ameaçando de morte a então ministra dos Direitos Humanos (DDHH) e atual senadora da República Damares Alves. A autointitulada sociedade secreta mencionou, pela primeira vez, a possibilidade de uso de uma arma de destruição em massa: uma "toxina mortal", sem especificar qual seria.
    a. A Sociedade Secreta Silvestre é uma organização informal, representante no Brasil do ideário ecoextremista do grupo internacional Individualistas Tendendo ao Selvagem (ITS). Intitula-se um grupo terrorista, afirmando estarem "Em Tocaia Terrorística Contra o Progresso Humano!" (**Figura 19**).

Figura 19 – Página inicial do sítio "Maldição Ancestral", que foi tirada do ar pela Sociedade Secreta Silvestre[ff].

b. São objetivos da SSS no Brasil, segundo o próprio grupo[115]:
   I. Ataques indiscriminados contra alvos humanos e não-humanos para gerar terror e instabilidade político-social;
   II. Infiltração em protestos sociais para disseminar o caos por meio da violência;
   III. Repulsa às reclamações sociais das organizações civis. Repulsa à cidadania;
   IV. Fragilização das estruturas do sistema tecnoindustrial;
   V. Eliminação completa da civilização moderna com o combate indiscriminado contra a espécie humana;
   VI. Ações violentas para causar o máximo de danos possíveis com vistas a construir um cenário social catastrófico;
   VII. Combate à robotização humana (chamada pelo grupo de transhumanismo), onde tudo seria virtualizado, medido, observado, conectado, controlado e contido;

[ff] Com a finalidade de não serem identificados, o grupo migrava o sítio regularmente de endereço, até que ele deixou de ser publicado.

VIII. Destruição da realidade do *cybermundo*, que estaria erradicando a natureza selvagem e as liberdades individuais[115].

c. A organização publicou seu primeiro manifesto em agosto 2016, reinvidicando produção e colocação de artefato explosivo no estacionamento em frente ao Shopping Conjunto Nacional, em Brasília/DF[gg].

d. O último ataque do grupo, até então, foi em uma sede do Instituto Brasileiro do Meio Ambiente (IBAMA), na Floresta Nacional (FLONA) de Brasília, em 28 de abril de 2019[114].

e. Houve também ameaça ao então presidente Jair Bolsonaro, seus familiares e ao então Ministro do Meio Ambiente Ricardo Salles, em entrevista concedida à Revista Veja, por meio de um programa de troca de mensagens na rede de computadores profunda (*deep web*):

> "VEJA – Por que até hoje a Polícia Federal não descobriu a identidade de vocês?
>
> Anhangá[hh] – Porque são incompetentes e porque não somos meros amadores. Aqueles idiotas da Operação Hashtag foram presos enquanto preparávamos quase 10 quilos de explosivo. Não somos meros amadores, dominamos técnicas de segurança, de engenharia, de comportamento social. Pra falar a verdade discutimos internamente com membros de outros países e chegamos a conclusão que das polícias de cada país onde opera ITS a do Brasil é a mais avançada, mas ainda sim não foi capaz.
>
> Como costumamos dizer, caminhamos como uma lebre, silenciosamente."[114]

f. Em 01 de janeiro de 2019, a Polícia Civil do Distrito Federal (PCDF) e a Polícia Federal (PF) prenderam três pessoas suspeitas de integrarem a célula brasileira da SSS. Após nove

---

[gg] Com atuação predominante na capital federal até 2020, realizou e reivindicou seis ataques. A SSS reivindicou, por exemplo, a fabricação e colocação de um artefato explosivo próximo ao Santuário Menino Jesus, em Brazlândia/DF, em 24 de dezembro de 2018. Cerca de 1500 pessoas realizavam uma missa natalina no local, no momento programado para o atentado. Entretanto, o artefato não explodiu no tempo esperado, por falha técnica[115].

[hh] O suposto representante do grupo que concedeu a entrevista intitulou-se Anhangá, que é, na cultura tupi, um cervo branco com olhos vermelhos de fogo, reconhecido pelos povos originários da região do Vale do Anhangabaú como o protetor da caça e da pesca[114].

dias de prisão provisória, os três suspeitos foram soltos por ausência de provas[115].

g. Não se pode descartar, portanto, que seus integrantes estejam ativos e que busquem realizar alguma ação para produção ou obtenção de MBGC para fins de disseminação intencional em ato de bioterrorismo.

2. Operação *HASHTAG* (PF) – com importante apoio de inteligência da ABIN, a primeira célula terrorista brasileira foi identificada e presa em 2016. O planejamento de atuação da organização criminosa, ligada a Al-Qaeda, era possivelmente provocar um atentado terrorista bioquímico em estações de tratamento de água do Rio de Janeiro, durante a vigência dos Jogos Olímpicos[116] (**Figuras 21** e **22**):

Figura 20 – Imagem de apresentação da Operação *HASHTAG* da PF em *slide* da ABIN[121].

EXCELENTÍSSIMO SENHOR JUIZ FEDERAL DA 14ª VARA DA SUBSEÇÃO JUDICIÁRIA DE CURITIBA – SEÇÃO JUDICIÁRIA DO PARANÁ

Nas conversas, há, ainda, passagem extremamente grave, na qual ALISSON revela a sua intenção de promover um **EXTERMÍNIO EM MASSA** (POGROM[59]) durante a Olimpíada, com o uso de armas bioquímicas, contaminando os reservatórios de uma estação de abastecimento de água (p. 74/75 do arquivo "TL_POSTAGENS"). Na mensagem, ele ainda afirma que, "de fato, as Olimpíadas seria uma ótima chance", e que um ataque bioquímico "entraria para a história". No final ainda refere que "eu estaria disposto".

Figura 21 – Trecho da denúncia efetuada pelo Ministério Público Federal (MPF) para a Justiça Federal, após a Operação *HASHTAG* da PF[116].

3. Operação ALQUIMIA – com importante apoio de inteligência da ABIN, que foi responsável pela Operação ALQUIMIA[ii], a inteligência PF deu andamento ao caso; foram realizadas busca e apreensão e detenção de dois irmãos no interior paranaense que tentavam arrecadar fundos para realizar um ataque com armas químicas com discurso supremacista branco, racista e antissemita. Os irmãos divulgavam informações sobre síntese de armas químicas na rede mundial de computadores por meio de redes sociais e da *Wikipedia*.
4. Mercados Ilegais na rede mundial de computadores profunda (*deepweb ou darkweb*) – foi a primeira atuação na área de ciberbioproteção pela AI no Brasil; com ajuda de software de busca na *deepweb*, a COTESB iniciou o monitoramento de mercados de agentes biológicos e toxinas, que eram vendidos ilegalmente mediante pagamento por criptomoedas e cuja entrega era concretizada com a informação, pelo vendedor criminoso ao comprador criminoso, das

[ii] Nome informal atribuído às ações de inteligência, sem valor como inquérito policial, no âmbito da tentativa de identificar a ameaça representada pelas publicações sobre ataques químicos.

> coordenadas de GPS onde a encomenda seria colocada. A COTESB/ABIN conseguiu identificar oferta de ricina e de antraz, ambos considerados ABTS pelo FSAP estadunidense.

Em suma, apenas com uma amostragem de dois anos de acompanhamento, verifica-se a importância do envolvimento da inteligência na governança de biorriscos.

Além disso, enfatiza-se que o Brasil possui uma série de ameaças de uso de armas biológicas por grupos/indivíduos. À exceção das detenções realizadas em decorrência da Operacão *Hashtag* (PF) e Operação Alquimia (ABIN), a SSS e os mercados ilegais na *darkweb* continuariam ativos.

Em ambos, a obtenção de MBGC e de PAI/PGC são interessantes para os criminosos, aumentando o valor do ativo biológico e resultados de pesquisas disponíveis em laboratórios brasileiros, que passam a ser de interesse das ameaças e precisam de bioproteção efetiva.

Neste sentido, qualquer plano de BPL precisa levar em consideração estas e outras ameaças atuais, a fim de basear o planejamento e implementação de medidas de controle de risco (passos 3 em diante da abordgagem ABRE da OMS) em seu monitoramento de risco (*risk assessment*) de BPL.

2.3.4 Vulnerabilidades de biossegurança e bioproteção laboratoriais no Brasil

Há pouco mais de 10 anos, LINCOLN (2014) apresentou suas conclusões sobre lacunas do sistema de governança da saúde global no Brasil:

> "Considerando a característica de Cisne Negro que o fenômeno Terrorismo carrega em si, o potencial uso de organismos e toxinas biológicas para ataques extremistas não pode ser descartado. Assim, os exemplos de uso intencional de tais agentes demonstram não apenas a factibilidade de seu emprego, mas também a necessidade da construção de um sistema robusto em nossa sociedade para lidar com essa ameaça."[117, p. 96]

Um sistema robusto, segundo o autor, incluiria, entre outros fatores e recomendações:

1. Autoridade central nacional para coordenar biorriscos;
2. Protocolo nacional de P2R2 na área biológica, a exemplo de uma Política Nacional para a Prevenção e Resposta a Incidentes Biológicos;
3. Falta de compromissos formais sobre o ameaças biológicas entre os membros do SISBIN;
4. Vigilância epidemiológica integrada com a segurança-inteligência;
5. Educação continuada na área de biorriscos para o setor da saúde;
6. Cooperação internacional no âmbito de estruturas multilaterais para intercâmbio técnico;
7. Criação de um laboratório NB-4 estratégico para o Brasil; e
8. Acompanhamento dos novos biorriscos (ex. engenharia genética e biologia sintética)[117].

Apesar de as lacunas supracitadas não serem focadas apenas em B2L, elas constituem carências de um hipotético arcabouço institucional necessário para enfrentamento de biorriscos em geral. E os riscos de B2L são importantes biorriscos.

Mais focados em biorriscos laboratoriais, MENDONÇA & MAFRA (2023)[122] ressaltaram lacunas observadas na governança brasileira de biossegurança e bioproteção, com base nas recomendações do documento *Guidance on implementing regulatory requirements for biosafety and biosecurity in biomedical laboratories – a stepwise approach*, da OMS[123]:

1. Ausência de um modelo de fomento do ensino, pesquisa, desenvolvimento tecnólgico e inovação;

2. Carência de um arcabouço normativo abrangente e adequado à complexidade do tema;
3. Ausência de um “Programa Nacional de Capacitação” em B2L;
4. Falta de uma “Rede Nacional de Laboratórios de Alta Contenção”;
5. Carência de um planejamento estratégico que inclua a definição da infraestrutura desejável para o país no tocante ao quantitativo e aos níveis de biossegurança dos laboratórios;
6. Falta de mecanismos para a certificação de laboratórios de alta contenção biológica; e
7. Necessidade de coordenar ações de colaboração nos níveis nacional e internacional, envolvendo B2L.

MENDONÇA (2024) empreendeu uma análise da implementação brasileira dos sete passos[3, pp.229-235]. Conclui, com extensa fundamentação teórica, que são deficiências no arcabouço regulatório de B2L:

> “a. A falta de uma autoridade nacional centralizada responsável pela supervisão e coordenação de assuntos de biossegurança e bioproteção no Governo Federal do Brasil, determinando critérios para a certificação de LAC e conduzindo inspeções de instalações;
> b. A falta de critérios padronizados de análise de risco;
> c. A falta de modelos para notificação de acidentes e incidentes;
> d. A deficiência em criar requisitos voltados para LAC; e
> e. A ausência de sistema de classificação de patógenos baseado em grupos de risco [tradução nossa].”[3, p.230]

Tais seis deficiências fundamentam o que seria publicado posteriormente, em 2024[123], em conjunto com MAFRA.

Sob o ponto de vista da bioproteção laboratorial, MENDONÇA (2024) enfatiza a importância das auditorias em B2L “englobarem aspectos de bioproteção” [tradução nossa].” Neste sentido, o autor elogia a iniciativa do MAPA em incluir representantes da ABIN na sua comissão de biossegurança laboratorial[3, p.216].

A partir da experiência brasileira, o autor amplia as recomendações da OMS para uma autoridade central, mencionando que há especialistas em B2L em órgãos de segurança brasileiros (ex. Polícia Federal) e de inteligência (ex. ABIN)[3, p.224]. A dispersão de expertises, inclusive, é mencionada pelo autor e por POMPEU (2014)[117] como justificativas para uma autoridade com poder supreministerial ou interministerial.

Há pelo menos mais de 10 anos, portanto, sabe-se pormenorizadamente as lacunas normativas para a implementação de capacidades laboratoriais no Brasil que signifiquem adequado *compliance* às normas internacionais.

A título de aprofundamento na análise de vulnerabilidades de B2L no Brasil, em 2018, o PANGEIA/ABIN empreendeu coleta de informações sobre laboratórios considerados NB-3 e NB-4 pelo MAPA e MS. Utilizou-se o questionário constante no ANEXO B desta pesquisa.

O objetivo era identificar vulnerabilidades e biorriscos laboratoriais, buscando, entre outros aspectos, se havia adequação dos laboratórios para a custódia de patógenos selecionados.

Como um dos resultados, produziu-se um mapa que demonstra a então gravidade da situação de custódia foi apresentado para autoridades laboratoriais do MAPA e do MS, a fim de, conjuntamente com a ABIN e demais órgãos parceiros, houvesse adequado planejamento de medidas de redução de risco[jj].

Obteve-se, na época, o conhecimento de que pelo menos nove estados possuíam laboratórios biomédicos que custodiavam agentes biológicos ou toxinas análogas à ricina incompatíveis com o NB laboratorial (**Figura 22**).

[jj] Sistema Eletrônico do Serviço de Informação ao Cidadão (https://esic.cgu.gov.br/sistema/site/index.aspx), segundo a Lei de Acesso à Informação (LAI), sob número de protocolo 0007700074720172.

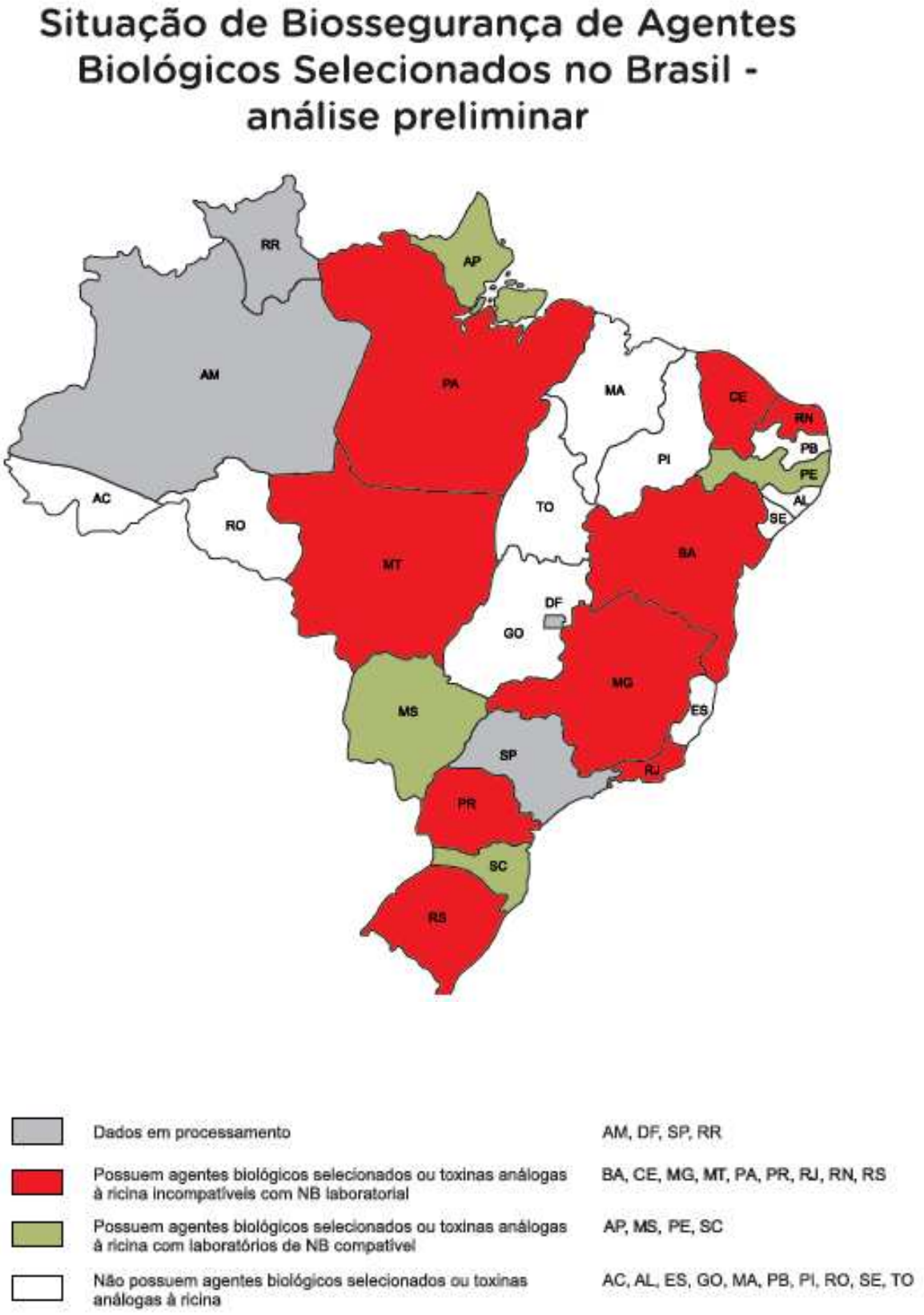


Figura 22 – Mapeamento de biorriscos em laboratórios do MAPA e do MS nos estados brasileiros[kk]

[kk] Sistema Eletrônico do Serviço de Informação ao Cidadão (https://esic.cgu.gov.br/sistema/site/index.aspx), segundo a Lei de Acesso à Informação (LAI), sob número de protocolo 0007700074720172.

As informações do mapeamento foram prestadas voluntariamente pelos laboratórios sem fiscalização ou auditoria posterior, de modo que há limitação na interpretação dos resultados.

Em sua pesquisa doutoral, MENDONÇA (2024) analisou questionário sobre B2L em 54 instituições respondedoras entre os noventa e dois laboratórios[II] biomédicos de alta conteção[3].

Em seu questionário de trezentas e oitenta e duas questões sobre biossegurança e bioproteção laboratoriais, há uma seção de perguntas sobre BPL com vinte e três questões (perguntas 291 a 313); e sete perguntas (264 a 269) na seção de *recursos humanos e treinamento* específicas sobre existência e capacitação de um *biosecurity officer*. No total as 29 perguntas sobre BPL, perfazem 7,6% do questionário[3, pp.387-391].

A revisão das questões permite identificar pelo menos sete delas que estão mais relacionadas à análise de risco de bioproteção. As demais dezesseis tratam de medidas de controle de riscos de BPL e abordam: iluminação pública; serviço de guarda; guardas em fins-de-semana e feriados; tipo de barreiras físicas; termo de cooperação com órgãos de segurança; controle de acesso em áreas restritas; inventário de transporte; pessoal externo; análise de antecedentes; procedimento padrão para transporte; adesão de procedimentos; frequência de transporte de ABTS; certificação para transporte; e percepção de segurança de dados[3, pp. 389-391].

Quanto às respostas, verificou-se que apenas 16,7% dos laboratórios respondedores possuem acordo de cooperação com autoridades de segurança e 25% possuem protocolo para análise de antecedentes de pessoal com acesso ao laboratório NB-3[3, p.241].

Tão baixa porcentagem de adesão a dois requisitos essenciais de controle de riscos de bioproteção demonstram a rara adequação de laboratórios brasileiros à BPL, ainda menor do que a adequação à maioria dos requisitos de biossegurança laboratorial.

Essa realidade pôde ser em parte constatada *in loco* em alguns laboratórios avaliados voluntariamente pelo PANGEIA/ABIN. Em razão do sigilo da documentação, o Relatório dos Sistemas de Proteção 0001/2018 (RELASP),

[II] Para o autor, este número é equivalente ao do Canadá; superior ao da Argentina , que possui menos de dez laboratórios NB-3; e muito menos do que os EUA e o Reino Unidos, que possuem respectivamente 1300 e 600 laboratórios de alta contenção (NB-3 e NB-4)[3, p.93].

elaborado para uma instalação brasileira NB-3, será apenas ilustrado com duas imagens. O documento mostrou falhas de barreiras de proteção (**Figura 23**) e de controle de acesso na portaria principal (**Figura 24**), entre outras dezenas de vulnerabilidades de bioproteção laboratorial.

Figura 23 – Recomendação do PANGEIA/ABIN de garantir três níveis de barreiras de proteção (Azul, amarelo e verde) em instalação NB-3 brasileira[mm].

[mm] Excerto do RELASP 0001/2018 foi obtido por meio do Sistema Eletrônico do Serviço de Informação ao Cidadão (https://esic.cgu.gov.br/sistema/site/index.aspx), segundo a Lei de Acesso à Informação (LAI), sob número de protocolo 0007700074720172.

Figura 23 – Duas vulnerabilidades apontadas pelo PANGEIA/ABIN (V6 e V7) e três medidas de redução de risco recomendadas (R14-16) em instalação NB-3 brasileira[nn].

Apesar do planejamento de acompanhamento contínuo, entretanto, o PANGEIA/ABIN realizou apenas outro RELASP em um segundo laboratório NB-3 brasileiro (RELASP 0002/2018) repetindo o resultado de dezenas de vulnerabilidade de proteção.

2.3.5 Conceito de inteligência epidemiológica

Desde a pandemia da COVID-19, com seus impactos sociais e econômicos sem precedentes no século XXI, houve o reconhecimento de que a inteligência epidemiológica era estratégica para a resposta efetiva a uma emergência em saúde[64].

[nn] Excerto do RELASP 0001/2018 foi obtido por meio do Sistema Eletrônico do Serviço de Informação ao Cidadão (https://esic.cgu.gov.br/sistema/site/index.aspx), segundo a Lei de Acesso à Informação (LAI), sob número de protocolo 0007700074720172.

Em agosto de 2020, a OPAS adotou a Resolucão CD58R9, propondo o fortalecimento da inteligência epidemiológica como uma das quatros linhas estratégicas de ação da política (*policy*) de resposta à pandemia da COVID-19:

> *"a importância de expandir o uso de diferentes fontes de informação e a necessidade de rápida verificação de sinais de ameaças potenciais à saúde pública, gestão efetiva de volumes significativos de informação e rápida adaptação e inovação contínuas para auxiliar o alerta e resposta precoces."*[55]

Inteligência epidemiológica é tradução livre para o termo *epidemic intelligence*, utilizado pela Organização Pan-Americana de Saúde (OPAS) e pela OMS:

> *"O que é conhecido como Inteligência Epidemiológica (IE) é o ciclo de coleta organizada e sistemática, análise e interpretação de informações de todas as fontes para detectar, verificar e investigar riscos à saúde potenciais (...) Inteligência Epidemiológica é uma atividade intensiva em recursos, ininterrupta (24/7/365) e que requer equipe altamente qualificada e dedicada para implementar um sistema e uma rede de alerta global precoce e eficiente (*tradução nossa*)."*[10]

Neste sentido, a OPAS reconhece que as autoridades de saúde pública nacionais, a OMS e a própria OPAS realizam inteligência epidemiológica com a finalidade de detectar riscos à saúde, em uma articulação mediante responsabilidade compartilhada[50]. O Sistema de Gestão de Eventos (EMS, na sigla em inglês) da OMS é o sistema eletrônico central para registrar, acessar e gerir informações sobre todos os eventos potenciais.

Na OPAS, a inteligência epidemiológica é conduzida no Departamento de Emergências em Saúde (PHE, na sigla em inglês), na Unidade de Informações e Avaliação de Riscos de Emergências em Saúde (*Health Emergency Information and Risk Assessment Unit* - HIM, na sigla em inglês). A HIM possui três equipes:

i. Equipe de mapeamento (*Mapping team*);

ii. Equipe de detecção, verificação e avaliação de risco (*Detection, Verification and Risk Assessment team* - DVA, na sigla em inglês); e

iii. Equipe de análise epidemiológica (*Epidemiological analytics team*)[10].

2.3.5.1 O fortalecimento da capacidade multilateral de inteligência epidemiológica

Em 05 de maio de 2021, a Organização Mundial da Saúde (OMS) anunciou o lançamento de um polo (*hub*) para inteligência pandêmica e epidêmica (*Pandemic and Epidemic Intelligence*) em colaboração com a Alemanha e sede em Berlim. A iniciativa tem o objetivo de rastrear, coletar, analisar e usar dados de surtos, epidemias e pandemias para melhor preparo, predição e gestão destes eventos[50].

Originalmente proposto pelo Diretor-Geral da OMS durante a pandemia da COVID-19, Tedros Adhanom Ghebreyesus, para a então chanceler da Alemanha, Angela Merkel, o polo funcionará como um centro de inteligência epidemiológica para a OMS, a partir de um investimento inicial previsto de 30 milhões de euros[50].

Os objetivos do polo são de:

> *"encorajar pesquisadores, representantes governamentais e parceiros privados a criarem bancos de dados integrados com diversas fontes de informação: saúde pública; dados sociais e de comportamento; mídias sociais e convencionais; mobilidade e viagens; e dados ambientais. Estes bancos de dados permitiriam colaboração multidisciplinar para o desenvolvimento de ferramentas e modelos preditivos de análise de risco, por meio do uso do estado da arte tecnológico, como: inteligência artificial; monitoramento de medidas de controle de doenças; fluxo de informações; e produção de conhecimentos efetivos para decisores de países-membros da OMS (*tradução nossa*."*[50]

Apesar de críticas de que o conceito de sistemas de detecção precoce, com foco em análise preditiva, poderia criar a percepção de que é possível controlar a disseminação de uma pandemia e afastar os esforços de ações de preparo, como o fortalecimento de sistemas de saúde de países menos desenvolvidos[11], por exemplo, a estrutura do polo da OMS permite entender a ideia e a importância da inteligência epidemiológica, no contexto da prevenção de eventos de risco biológico globais.

A OPAS, na esteira da implementação do polo de inteligência epidemiológica da OMS em Berlim, lançou, em outubro de 2024, uma estratégia de inteligência epidemiológica, com a finalidade de fortalecer a detecção precoce de emergências em saúde entre 2024 e 2029. Com esta iniciativa, as Américas tornar-

se-ão a primeira região da OMS a implementar uma estratégia em inteligência epidemiológica[51].

Na estratégia, a organização de saúde reconhece que:

> "*Ameaças de saúde pública são onipresentes e têm o potencial de crescimento na próxima década devido a fatores como as rápidas mudanças de contextos sociais, demográficos, epidemiológicos e ambientais; ao aumento das viagens e do comércio internacional; e à emergência de novos patógenos, tudo contribuindo para o acionamento de novos riscos que precisam de inteligência epidemiológica efetiva para a detecção oportuna e alerta precoce de emergências em saúde.*"[51, p. 1]

O objetivo da estratégia é nortear e apoiar os Estados-Membros no fortalecimento da inteligência epidemiológica na região para o alerta precoce de emergências em saúde. Ela se baseia em quatro linhas estratégicas de ação:

> 1. Fortalecer a coordenação e liderança da inteligência epidemiológica para o alerta precoce e o monitoramento de eventos agudos em saúde pública e emergências;
> 2. Fortalecer a capacidade técnica para a implementação efetiva e sustentável da inteligência epidemiológica;
> 3. Melhorar a integração e interoperabilidade de sistemas e ferramentas para fortalecer a inteligência epidemiológica; e
> 4. Incentivar a colaboração entre instituições de vigilância para compartilharem melhores práticas, promoverem engajamento ativo, fortalecerem a troca de informações e otimizarem a rápida verificação de sinais de saúde pública."[51, pp. 6-7].

Verifica-se, portanto, uma tendência pós-2020 de fortalecimento das capacidades de produção de conhecimentos de inteligência voltados para a área de saúde.

2.4 Ciberbioproteção: conceito emergente

A ciberbioproteção se preocupa com os riscos da pesquisa biológica, particularmente aqueles amplificados pela digitalização da informação biológica e da automação biotecnológica[71, p.11].

O termo foi citado primeiramente em PECCOUD *et al* (2018) para se referir aos novos riscos emergentes na fronteira entre o ciberespaço e a biologia[72].

> "*Assim como a emergência da rede mundiais de computadores algumas deécadas atrás resultou em uma grande revolução, e, por necessidade, foi complementada pelo campo da ciberproteção, estamos diante da era da ciberbioproteção com suas próprias vulnerabilidades de proteção* [tradução nossa] "[71]

DITTRICH et al. (apud BURNETTE, 2020) afirmam que "uma área emergente que conecta os princípios da ciberproteção e a necessidade de proteger a economia de indústrias biológicas (*bioeconomia*) é chamada de ciberbioproteção" [tradução nossa][70, p. 83].

A ciberbioproteção, enquanto uma nova disciplina, não visa apenas a prevenir e mitigar os riscos de ciberataques tradicionais, mas também os riscos relacionados com sistemas ciberfísicos[oo] (SCF) e suas vulnerabilidades. De fato, cada vez mais, os campos da biocência dependem de SCF, que geram potencial para falhas de segurança e proteção em cada ponto onde os processos ou serviços participam da interface entre os domínios cibernéticos e físicos[71, 72].

Apesar de o termo "ciberbioproteção", analisado dentro do campo da B2L, estar ligado a eventos intencionais, de maneira análoga à ideia de bioproteção laboratorial[71], muitos autores utilizam o termo *cyberbiosecurity* para incluir tanto biossegurança (medidas para prevenir eventos não intencionais) quanto bioproteção (medidas para prevenir eventos intencionais)[72].

> "*Vale mencionar que os SCF possuem limites pouco precisos entre a segurança (*safety*) e a proteção (*security*), e, mesmo nos campos de estudos cibernéticos, os dois termos são utilizados intercambiavelmente*[pp]*. Do mesmo modo, o termo ciberbioproteção utiliza essa ideia* [de limites pocuo precisos] *para se referir a todo o espectro de vulnerabilidades* [tradução e grifo nossos]"[71, p.12].

[oo] Trata-se de sistemas com estruturas físicas vinculadas ou controladas por sistemas informáticos[71].

[pp] Como exemplo da intercambialidade dos termos na área cibernética, vale citar a própria definição de ciberproteção (*cybersecurity*) constante do glossário do GBL2 da OMS: ""prevenção de dano e proteção e restauro de computadores, sistemas de comunicação eletrônica, serviços de comunicação eletrônica, comunicações com fio e comunicações eletrônicas, incluindo informação aí contida, de modo a garantir a disponibilidade, integridade, autenticação e confidencialidade das informações"[22].

Portanto, prevalece a ideia do termo tal como concebido inicialmente, de ciberbioproteção relacionada aos novos riscos que surgem na fronteira entre o ciberespaço e a biologia[72], sejam eles riscos de segurança (*safety*) ou de proteção (*security*).

Em 2019, REED & DUNAWAY introduzem o termo ciberbiossegurança como “cibervulnerabilidades (...) que podem resultar em contaminação ambiental ou ameaçar a saúde de humanos, animais e plantas”, sem especificar se se trata de uma exposição não intencional ou disseminação intencional[73].

Desta feita, encontra-se na literatura especializada tanto o termo ciberbioproteção (*ciberbiosecurity*)[71,72] quanto o termo ciberbiossegurança (*ciberbiosafety*)[73] para se referir precípua e simultaneamente aos mesmos riscos: de segurança e de proteção, de maneira intercambiável.

2.4.1 Riscos de ciberbioproteção

As ameaças de ciberproteção (*cybersecurity threats*) são alguns dos atos criminosos que mais crescem no mundo atual, com perdas econômicas devidas a cibercrimes que devem superar U$10 trilhões em todo o mundo, em 2025[108]. A pandemia da COVID-19 resultou em um ambiente digital mais lucrativo para cibercriminosos, em parte porque tornou os hábitos e a economia mais digitalizados[20, p.83].

Há histórico de danos cibernéticos de SCF, pelo menos desde 2008, como ato de ciberterrorismo/ciberssabotagem, a exemplo da explosão do gasoduto Baku-Tbilisi-Ceyhan, na Turquia, fazendo analistas de segurança mencionarem uma suposta nova era de ciberguerras[109].

No contexto hospitalar, em setembro de 2020, ocorreu a primeira morte atribuída a um ciber-homicídio, no Hospital Universitário de *Düsseldorf*, quando um ataque *hacker* desligou todos os sistemas de computadores e não foi possível, pelo desligamento, transferir uma paciente grave oportunamente para outro hospital. O ciberataque levou ao óbito da paciente e a uma investigação criminal por homicídio[111].

De fato, hospitais têm sido um alvo crescente de cibercriminosos, desde a pandemia da COVID-19. Ataques com extorsão para liberação de dados cresceu

350% em empresas de saúde em 2019, em comparação com 2018. Em 2020, mais de 5 milhões de prontuários de pacientes foram vazados e comprometidos como resultado de falhas de ciberproteção[70].

No contexto das ciências biológicas ou da biossaúde (*biohealth*)[110], o uso de SCF em laboratórios pode alterar propriedades biológicas de MBGC, por exemplo, ou alterar, sabotar e furtar PGC. Durante o desenvolvimento urgente de tecnologias vacinais contra o SARS-CoV-2, teria havido o envolvimento de grupos hackers russos e chineses com ciberataques a empresas como a Novavax, Moderna e outras.

> "*O comprometimento de SCF pode levar a situações como a síntese errada ou até mesmo perigosa de biomateriais ou à interferência em sistemas de contenção* [tradução nossa]."[70, p.12].

Além disso, no ambiente laboratorial conectado a sistemas informáticos, conforme supracitado no tópico 2.1.3.2.3 (*Monitoramento de riscos de bioproteção laboratorial*), no GBL2, a OMS lista incidentes de BPL. Entre eles, estão arrolados[22, p.41]:

1. Acesso não autorizado a programas computacionais ou perda de informações (digitais ou impressas), como dados de pessoas, dados de pesquisa, dados de sequências genéticas ou procedimentos operacionais;
2. Descontinuidade das operações devido a um ciberataque;
3. Acesso digital não autorizado a equipamento laboratoria conectado a alguma rede;
4. Interrupção remota de equipamento conectado (ex. sistema de proteção laboratorial); e
5. Furto/roubo, mal-uso ou sabotagem com dados e sistemas digitais de informações de interesse à bioproteção.

Trata-se todos de incidentes de uso não autorizado ou intencional, descritos como de bioproteção laboratorial, mesmo que se reconheça amplamente que tenham repercussão sobre aspectos de biossegurança laboratorial.

Isto ocorre porque, no contexto laboratorial, o papel crítico da ciberbioproteção é, segundo a OMS, o de proteger o acesso cibernético aos equipamentos laboratoriais e aos sistemas prediais de ataques, o que concentra o

foco da ciberbioproteção laboratorial no monitoramento de riscos de eventos intencionais[22, p. xiv].

A chance destes ataques não é negligenciável. Durante os últimos anos, a indústria de biotecnologia sofreu ataques graves, apesar de não haver percepção generalizada da população e do pessoal de laboratórios sobre este aspecto do risco de ciberbioproteção[71, p.12].

Em parte, esta subpercepção de risco está relacionada com o fato de que cientistas e seus gestores não costumam ser treinados nem ter experiência em segurança-inteligência[71, p.12], ainda menos se houver a conexão da ameaça entre segurança-interligência-cibernética.

É fundamental perceber que biorriscos estão em constante transformação. Enquanto sistemas tradicionais baseados em patógenos (*pathogen-based*) são úteis na avaliação de riscos de B2L, a endemicidade dos patógenos custodiados varia conforme a região e pode estar associada a um risco relativo mais baixo em certas regiões do planeta[112, p.8].

Ademais, novas ferramentas de *biodesign,* aprimoradas por tecnologias de inteligência artificial (IA), tornariam os modelos de avaliação de risco baseados em patógenos obsoletos, na medida em que as ferramentas conseguem, de maneira cada vez mais efetiva, desenvolver moléculas com funções específicas que são codificadas em sequências não encontradas na natureza[112].

Neste sentido, coloca-se a questão da necessidade de um futuro cujo paradigma será a identicação e monitoramento de riscos baseados na função da pesquisa[112], o que compexifica o processo de gerencimanto de riscos de biossegurança e bioproteção laboratoriais.

3. HIPÓTESE

A ausência de um arcabouço normativo abrangente e de ferramentas analíticas robustas prejudica a gestão integrada de biossegurança e bioproteção laboratoriais e biodefesa no Brasil. A implementação de um modelo transdisciplinar que integre inteligência e práticas de bioproteção, com foco na ciberbioproteção e na intersetorialidade, pode melhorar significativamente a cultura de bioproteção laboratorial e a capacidade de prevenção, mitigação e resposta a biorriscos laboratoriais.

4. OBJETIVOS

4.1 Objetivo geral

Desenvolver ferramentas (*Checklist RAMPA* e *PathoFinder Brazil*®) para uso em um modelo integrado de gestão de biorriscos, com foco em bioproteção laboratorial, considerando a ciberbioproteção, a biossegurança, a biodefesa e a inteligência.

4.2 Objetivos específicos

a. Analisar lacunas normativas e estruturais no Brasil e nas diretrizes internacionais quanto à gestão de biossegurança e bioproteção laboratoriais;
b. Propor elementos para um arcabouço teórico-metodológico para integração intersetorial na área de biossegurança e bioproteção laboratoriais;
c. Discutir as obrigações internacionais do Brasil, na área de capacidades laboratoriais;
d. Analisar nos principais documentos recomendatórios internacionais de biossegurança e bioproteção laboratoriais lacunas e desafios para a implementação de gerenciamento de risco de bioproteção laboratorial;
e. Compreeender criticamente a importância da gestão de risco baseada em ameaças e o papel dos órgãos de segurança e inteligência nesse gerenciamento integrado;
f. Apresentar e discutir os conceitos de “inteligência em saúde” e “inteligência laboratorial”;
g. Registrar e analisar a atuação da inteligência brasileira, mais especificamente da Abin e seu programa PANGEIA, nos primeiros anos de atividade, apontando para desafios presentes;
h. Discutir a análise de risco de evento biológico selecionado intencional no Brasil, a partir da apresentação de ameaças reais à bioproteção laboratorial;
i. Desenvolver uma ferramenta de identificação de ameaças (*PathoFinder Brazil®),* com a finalidade de identificar pesquisas de alto impacto e laboratórios ocultos que custodiam material biológico de grandes consequências, auxiliando no adequado monitoramento de riscos; e
j. Discutir um modelo de avaliação de sistemas de controles de riscos de bioproteção laboratorial (*Checklist RAMPA* – ClR), adaptado à realidade brasileira e focado em ciberbioproteção e intersetorialidade.

5. MATERIAIS E MÉTODOS

5.1 Apresentação, análise e aplicação de novos conceitos transdisciplinares na área de bioproteção laboratorial, segurança da saúde (*health security*) e biodefesa

A existência de vernáculos de cada área, por um lado, facilita a delimitação de objetos e competências próprios, mas, por outro, pode servir como obstáculo à integração destas áreas. A almejada transdiciplinaridade, no nível acadêmico, que reflete a complexidade do mundo real e que, eventualmente, no nível das ações públicas, é materializada na intersetorialidade, requer os conceitos-chave dialógicos[1].

A metodologia adotada para este ponto do desenvolvimento da tese utilizou a revisão bibliográfica transdisciplinar com textos e artigos de referência nas áreas da saúde, segurança, inteligência e defesa, para identificar a interconexão de conceitos e eventuais conflitos entre eles.

Problemáticas conceituais foram identificadas e propostas definições originais, com a finalidade de contribuir para o debate acadêmico dessas problemáticas.

Em se tratanto de uma área tão intersdisciplinar quanto incipiente, a gestão de bioproteção laboratorial beneficiar-se-à de conceitos provenientes de uma leitura não restrita a uma única disciplina. Esta dinâmica ocorreu na elaboração dos conceitos de inteligência em saúde; e de inteligência laboratorial.

Ressalte-se que, num trabalho que se propõe servir como ciência aplicada no sentido de analisar conceitos e situações para apresentar soluções de uso prático, a elaboração de novos conceitos pressupõe situá-los na governança atual de bioproteção.

Desta forma, o método utilizado discutiu as implicações da implementação de frações de inteligência em saúde e da inteligência laboratorial na governança da saúde pública global, tendo por base as disposições da OPAS, OMS e do RSI sobre as capacidades de inteligência epidemiológica e as capacidades laboratoriais dos Estados-parte, o que inclui o Brasil.

Além dos novos conceitos elaborados, foi possível revisar criticamente a situação dos conceitos de segurança da saúde, *biosecurity* e biodefesa à luz da

governança brasileira, permitindo concatená-los com os dois conceitos novos e com a situação de algumas governanças estrangeiras de referência.

5.2 Desenvolvimento da ferramenta de avaliação de risco PathoFinder Brazil®

A metodologia adotada para este desenvolvimento utilizou a coleta de dados de diferentes fontes, com foco em informações relevantes sobre bolsas, auxílios, grupos de pesquisa e currículos de pesquisadores.

As principais fontes utilizadas foram do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) e da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES).

5.2.1 Coleta de dados

a. CNPq - A coleta de dados no CNPq foi realizada na plataforma de Dados Abertos, abrangendo informações abrangentes sobre bolsas, auxílios, grupos de pesquisa e currículos registrados na Plataforma Lattes. Os dados obtidos, até 10 de setembro de 2023, englobaram 139.770 projetos, 217.621 pesquisadores distribuídos em 252 instituições.

b. FAPESP - Para os dados da FAPESP, foi acessada a Biblioteca Virtual com a finalidade de obter informações sobre bolsas e projetos de auxílio à pesquisa. A base de dados da FAPESP, acessada até 10 de setembro de 2023, continha detalhes de 180.044 projetos e 18.514 pesquisadores de 137 instituições.

c. CAPES - Utilizando-se da política de dados abertos da CAPES com a finalidade de obter informações sobre Produção Intelectual e Catálogo de Teses e Dissertações, foram obtidos dados que abrangeram o período de 2017 a 2020. Com eles, foi possível mapear 1.924.073 trabalhos, envolvendo 80.439 pesquisadores e 266 instituições.

d. PubMeD – A base PUBMED de artigos foi utilizada para acesso em aba específica do PathoFinder Brazil® para o aprofundamento da obtenção de dados de pesquisadores de interesse. Uma varredura na base de dados PubMed foi realizada para localizar artigos publicados pelos pesquisadores identificados no *dataset* final. A pesquisa bem-sucedida encontrou 2.201 pesquisadores, com um total de 57.128 artigos publicados em 4.847 jornais.

5.2.2 Criação dos *datasets*

Um conjunto de dados (*dataset*), que funciona como a base para a busca finalística, envolveu a fusão das informações provenientes das três plataformas de pesquisa supracitadas.

O *dataset* (*dataset* 1) final contém informações importantes para o proósito do programa, como a plataforma de busca utilizada; nome da instituição; cidade da instituição; nome do pesquisador; e título do trabalho. Uma pesquisa nos títulos dos trabalhos foi conduzida para a localização de termos específicos, produzindo um *dataset* com 6.844 linhas e 8 colunas.

Um segundo *dataset* (*dataset* 2) está associado à base PubMed e mostra os resumos (*abstracts*) dos trabalhos dos pesquisadores identificados nas buscas, permitindo a triagem mais detalhada das pesquisas de interesse. Nos termos de busca cadastrados até o momento, a busca no *dataset 2* resultou em 3.028 trabalhos, 2.900 pesquisadores e 359 instituições, distribuídas por 131 cidades.

5.2.3 Integração com aplicativo *Shiny* e aprimoramentos

Um aplicativo *Shiny* foi desenvolvido para permitir a exploração e visualização dos resultados de busca do programa por um usuário.

A ferramenta foi chamada de *PathoFinder Brazil®* como um programa de computador desenvolvido no âmbito do Programa de Cooperação Acadêmica em Defesa Nacional (Edital PROCAD-DEFESA 2019/PROCAD-DEF20191324749P) e registrado sob o Certificado de Registro de Programa de Computador (Processo Nº BR512024000746-6)[30].

O *PathoFinder Brazil®* está hospedado no endereço eletrônico: https://procaddefesa.shinyapps.io/AppDatasetAllExtra/, atualmente com acesso restrito mediante autorização de seus desenvolvedores.

Aprimoramentos futuros podem incluir também a vinculação de inteligência artificial para o aprofundamento das buscas e para a leitura e interpretação dos resumos, permitindo maior automatização das buscas e identificação mais rápida e efetiva de pesquisas e pesquisadores de maior interesse para ações de *outreach*.

Além disso, a vinculação com bases estrangeiras permitiria o uso do *PathoFinder Brazil*® como ferramenta de antecipação e análise preliminar de riscos em países estrangeiros, com ênfase para os países com maior proximidade física e com maior troca de pessoas e mercadorias com o país, por apresentarem maior biorrisco associado ao Brasil.

5.3 Aprimoramento e Adaptação de modelo de avaliação de sistemas de controles de riscos de bioproteção laboratorial (*Checklist RAMPA* - CIR)

A elaboração de um questionário para avaliação dos sistemas de bioproteção laboratorial partiu da revisão e análise dos Questionários de Avaliação de Vulnerabilidades ("*Vulnerability Assessment Questionnaires*") elaborados originalmente por Salerno & Gaudioso (2007)[2, p.107].

O trabalho dos autores na difusão da implementação de ações e medidas de bioproteção laboratorial tem sido importante desde a primeira década do século XXI, após a disseminação de Antrax nos EUA por falhas de bioproteção laboratorial.

Na época da elaboração dos questionários supracitados, ambos atuavam como membros do Programa de Redução de Ameaças Biológicas Globais Laboratórios Nacionais Sandia (SNL IBTR, na sigla em inglês), em colaboração com a Federação Internacional de Associações de Biossegurança (IFBA, na sigla em inglês).

Os *Sandia National Laboratories* (SNL, na sigla em inglês) são uma organização técnica multidisciplinar que atuava como assessora técnica para o governo federal dos EUA nos anos 2000.

A partir da análise dos questionários dos SNL, cotejou-se com a bibliografia especializada mais recente, como o LBM4, da OMS[16]; a 6ª edição do BMBL, dos CDC[17]; a ISO 35001:2019[15]; a NBR 17069-1/2023[18]; e a atualização das pesquisas de SALERNO & GAUDIOSO (2020)[13], para complementar o instrumento de avaliação.

O resultado foi adapatado para a realidade brasileira, a partir da experiência em atuar com as avaliações de sistemas de proteção laboratorial empreendidas pelo PANGEIA/ABIN, em 2019.

Neste ano, equipes da ABIN vinculadas ao PANGEIA foram deslocadas sob minha coordenação para realizar as avaliações em dois Laboratórios Federais de Defesa Agropecuária (LFDA), antigos Laboratórios Nacionais Agropecuários (Lanagros), do MAPA, em São Paulo e em Pernambuco. Além disso, houve visitas técnicas a outros LAC brasileiros.

Na ocasião das avaliações, houve uma aplicação de questionários utilizados no Programa Nacional de Proteção do Conhecimento (PNPC), que era utilizado em hotéis, estádios de futebol e outras estruturas críticas em Grande Eventos nacionais e internacionais, com sede no Brasil.

O resultado foi uma boa análise de vulnerabilidades com foco em elementos de proteção física, proteção de pessoal e proteção de dados, entretanto sem detalhamento necessário para certos aspectos laboratoriais, que um questionário de aplicação mais geral deixa de contemplar.

Percebeu-se, com os trabalhos, a necessidade de elaboração de um modelo original específico para a análise de vulnerabilidades de bioproteção laboratorial, o que se procurou sanar com a elaboração do presente *Checklist Risk-Assessment em Modelo de Proteção Ampliada - RAMPA* (ClR). A metodologia do ClR considera aspectos físicos, operacionais e digitais da bioproteção laboratorial.

6. RESULTADOS E DISCUSSÃO

6.1 Apresentação, análise e aplicação de novos conceitos transdisciplinares na área de bioproteção laboratorial, segurança da saúde (*health security*) e biodefesa

A definição *latu sensu* de *biosecurity*[32] se confunde com a definição transmilitarizada de biodefesa (*biodefense*)[11] e com a ideia de segurança da saúde (*health security*)[1].

O uso intercambiado entre os três conceitos é possível e, de fato, ocorre com frequência na literatura analisada sobre prevenção, preparo e resposta a eventos biológicos os mais diversos, assim como na literatura acadêmica.

Percebe-se que os órgãos ou profissionais da área de saúde tendem a escolher o termo segurança da saúde (*health security*), para se referir a área comum entre saúde pública e segurança púbica[125].

Por sua vez, profissionais da área de ciências, não restritos à saúde humana, a exemplo daqueles das ciências agrárias, preferem o uso do termo *biosecurity*, em sua significação *lato sensu*. Com a ressalva de que, ainda assim, os dois termos, por se referirem ao vocábulo segurança (*security*), tendem a ser conceitos mais vinculados aos setores de segurança pública.

Por último, militares tendem a usar mais o termo biodefesa para se referir ao mesmo significado dos dois termos anteriores. Desta forma, conclui-se que, apesar do vernáculo de cada área ou nicho, o significado é intercambiável, porque se refere, em geral, ao mesmo objeto, conforme analisado.

Para a realidade brasileira, considerando que os próprios militares definem a defesa, e por conseguinte biodefesa, como atividade típica das Forças Armadas[57], o uso do termo para se referir a atividades também civis poderia gerar confusão e até mesmo afastar autores civis de competências relevantes relacionadas ao assunto.

De maneira análoga, o uso dos termos *biosecurity* ou segurança da saúde, em documentos intersetoriais, merece as mesmas ressalvas, mormente em contexto de busca de transecuritização de atividades civis mais amplas, a exemplo da AI desempenhada pela ABIN e demais órgãos do SISBIN.

Neste sentido, conclui-se que, fora dos ambientes específicos da segurança – em que os termos *biosecurity* e *health security* podem e devem ser

empregados, porque tendem a ser mais bem compreendidos; e fora dos ambientes militares - em que o termo biodefesa pode e deve ser empregados, porque mais bem compreendido -, na confecção de normas estatais e intersetoriais, é preferível que estes três termos sejam evitados e substituídos pela sua significação literal.

No lugar de uma “Política Nacional de Biodefesa”, por exemplo, que seja aplicável a todos os órgãos civis e militares, preferir a nomenclatura “Política Nacional de Prevenção, Preparo e Resposta a Eventos Biológicos Selecionados”, por exemplo.

Esta ressalva não se aplicaria ao uso do termo bioproteção laboratorial (*laboratorial biosecurity*), entratento, tendo em vista que esta expressão é amplamente conhecida em quaisquer das áreas mencionadas, diferentemente do que ocorre com o termo lato sensu *biosecurity*.

Conforme os documentos revisados, a ampliação de programas de biodefesa, em substituição muitas vezes a antigos PGB, não significam maior segurança biológica, porque não necessariamente tais programas significam menos risco.

Oficialmente defensivas, as atividades realizadas nos últimos anos no Dstl, em Porton Down/Reino Único, para citar um exemplo, envolvem PAI e MBGC, como o vírus Ebola. São muitas vezes atividades que estão em uma estreita faixa limítrofe entre pesquisa defensiva e pesquisa ofensiva.

Em 08 nov. 2016, durante a Conferência de Revisão da CPAB, no Palácio das Nações em Genebra/Suiça, houve um evento paralelo (*side event*) de lançamento de um documentário da rede BBC, também apoiado pelo Dstl. No documentário, promovido pelo Governo Britânico, mostou-se que uma das pesquisas “de defesa” em Porton Down seria a aerolização do vírus Ebola[128].

Ora, pesquisar sobre a capacidade de o vírus Ebola ser transmitido em aerossóis pode nos remeter imediatamento ao LACON do MRE inglês. É difícil argumentar que se trata de pesquisa precipuamente defensiva.

Tanto esta exibição do documentário gerou inquietação, que a comitiva diplomática russa na Conferência de Revisão da CAB protestou expressamente no evento acusando o Reino Unido de contrariar, em admitir contrariar a CAB em evento da própria Convenção. O autor desta tese estava presente ao lançamento do filme e pôde testemunhar o episódio.

Se, por um lado, a realidade dos programas de biodefesa em expansão[1] significa riscos, isso traz a oportunidade de busca de melhor governança

internacional no sentido de criar mais mecanismos de cooperação ou de imposição de medidas de controle de risco biológico laboratorial.

Além disso, a relação dos programas de biodefesa com laboratórios de alta contenção permite que tais estabelecimentos planejem e implementem medidas efetivas de biossegurança e bioproteção laboratoriais e que os países que os detêm adotem normativas robustas sobre o tema.

De fato, são nesses países, que dispunham de PGB e LAC associados a eles pregressos - e atualmente programas robustos de “biodefesa” -, que se encontram boas práticas de biossegurança e bioproteção e normas passíveis de serem replicadas no Brasil de tão efetivas e inovadoras.

São esses países, também, a exemplo dos EUA, que oferecem possibilidades de cooperação e apoio a iniciativas brasileiras e internacionais em busca de uma melhor governança de biossegurança e de bioproteção laboratorial.
Se este incremento de políticas e práticas de bioproteção compensam os riscos biológicos ampliados com os programas de biodefesa aí tem-se um questionamento para outros trabalhos acadêmicos e para a comunidade de inteligência em saúde.

6.1.1 Inteligência laboratorial: atividade necessária

Inteligência pandêmica (*pandemic inteligence*), assim como inteligência epidêmica (*epidemic intelligence*) são termos usados pela OPAS e OMS para se referir igualmente a um conceito mais amplo e mais adequado, qual seja inteligência epidemiológica[11].

Se há preocupação com epidemias e pandemias e interesse pela detecção precoce de ameaças à saúde[12], não se poderia restringir a atividade de inteligência na área da saúde à coleta e análise de dados e conhecimentos unicamente epidemiológicos.

Ademais, de maneira análoga à definição de vigilância em saúde, com suas quatro áreas de atuação (vigilância sanitária, vigilância epidemiológica, vigilância ambiental e vigilância em saúde do trabalhador)[101, p. 6], a inteligência em saúde seria o termo mais adequado para abarcar a ideia de uma atividade de inteligência que englobe a antecipação de fatos e situações sanitárias, epidemiológicas e ambientais – e por que não de saúde do trabalhador? - que possam impactar a sociedade.

A inteligência em saúde, enquanto atividade antecipadora de riscos em saúde, com o propósito de assessoramento decisório, seguindo um método de coleta, síntese, análise e difusão de conhecimentos, é fundamental na gestão de biossegurança e bioproteção laboratoriais.

A produção e troca de conhecimentos sobre biossegurança e bioproteção laboratoriais deve ser executada de maneira integrada com estruturas de inteligência epidemiológica, mas requer a execução de atividades com escopo distinto da inteligência epidemiológica em si, a exemplo de visitas laboratoriais para avaliação de sistemas de medidas de controles de risco bioproteção laboratorial.

A diferença de escopo entre a vigilância epidemiológica e a gestão de biossegurança e bioproteção laboratoriais permite inferir que a especialização de uma estrutura governamental para tratar da inteligência laboratorial seria necessária, estando ligada à principal fração de um ministério (Ex. Ministério da Saúde ou MAPA ou ainda Ministério da Defesa) que trate de operacionalizar e garantir o cumprimento de normas de biossegurança e bioproteção laboratoriais.

Do ponto de vista didático, portanto, seria preferível pensar a inteligência laboratorial como uma área da inteligência em saúde diversa das quatro áreas supracitadas e constantes das normas de vigilância brasileiras. Tratar-se-ia de um quinto elemento da inteligência em saúde e que complementa a atuação das demais áreas e que com as demais interage em busca de maior efetividade mútua.

Em suma, dadas as características próprias e a importância da inteligência voltada para a biossegurança e, precipuamente, à bioproteção laboratorial, caberia considerar uma quinta área de inteligência em saúde: a inteligência laboratorial, com o objetivo de produzir e trocar conhecimentos de inteligência a serem utilizados no processo de gestão de biossegurança e bioproteção laboratoriais.

Segundo a Doutrina da Atividade de Inteligência da ABIN:

> "A atividade de inteligência (...) é exercida por organismos de inteligência. Vale reiterar, esses organismos podem ser classificados como serviços de inteligência, quando têm por finalidade a execução da atividade de inteligência, ou como frações de inteligência, quando integram órgãos que possuem outras finalidades."[24, p.23]

Neste sentido, como o "conjunto dos organismos de inteligência de um país constitui a sua comunidade de inteligência"[24, p. 23], ao se tratar de "fração" de inteligência laboratorial, vinculada ao Ministério da Saúde, por exemplo, refere-se a

um membro da comunidade de inteligência do Brasil perfeitamente inserido na doutrina de inteligência.

Não há, portanto, necessidade, perante tal doutrina, de que a atividade de inteligência laboratorial seja realizada exclusivamente por um serviço de inteligência, como a ABIN. Ela pode ser desempenhada por uma ou diversas frações de inteligência em um ou diversos ministérios ou órgãos públicos e privados que possuem interesse em produzir conhecimentos sobre ameaças e oportunidades que envolvam laboratórios.

Pode-se inferir que a coordenação em Brasília da Rede CIEVS é uma fração de inteligência do MS, em que pese seria ideal, para esta classificação, que um método de produção do conhecimento fosse formalizado, a fim de configurar uma das importantes características do ciclo definidor da atividade de inteligência, que é o ciclo de coleta, síntese, análise, produção e difusão de produtos de inteligência.

Nem mesmo a criação de sistemas (ou subsistemas) de inteligência, no Brasil, exigem aval da ABIN ou do SISBIN:

> "No Brasil, os órgãos federais de inteligência são organizados em um sistema próprio definido legalmente, o SISBIN. Também exis- tem subsistemas setoriais, como o Sistema de Inteligência de Defesa (SINDE)[qq], regulado por Portaria Normativa do Ministério da Defesa, ou o Subsistema de Inteligência de Segurança Pública (SISP), regulado por Decreto Federal. O importante é notar que a comunidade de inte- ligência do país é maior do que o Sisbin, incluindo também as insti- tuições estaduais e municipais, de outros poderes da República e entidades privadas de interesse para a atividade."[24, p.24]

Desta forma, até a organização de um sistema de inteligência laboratorial poderia ser instituído de maneira autônoma ao SISBIN, como o é o SINDE. Vale ressaltar que a própria Rede CIEVS funciona como um sistema de inteligência epidemiológica, a partir da integração de várias frações de inteligência (os CIEVS

[qq] O Subsistema de Inteligência de Segurança Pública (SISP) foi criado pelo Decreto Presidencial no 3.695, de 21 de dezembro de 2000. O Sistema de Inteligência de Defesa (SINDE), instituído pela Portaria Normativa no 295/MD, de 3 de junho de 2002, não é um sistema interministerial no âmbito do Sisbin, mas uma estrutura interna do MD, apesar de articulada com o Sisbin, para integrar os órgãos de Inteligência das Forças Armadas[97, p. 88].

estaduais e municipais) que foi instituído independente da comunidade de inteligência externa à esta Rede. [83,84]

Segundo a Doutrina de Inteligência da ABIN, o funcionamento da inteligência pode ser esquematizado em um ciclo composto por cinco fases, caracterizadas pelas ações de:

1. Objetificar – definição, normalmente pela alta gerência dos organismos e frações de inteligência, dos objetos de acompanhamento contínuo.
2. Acompanhar – processo contante de planejamento, reunião e processamento de dados; é fase permanente durante todo o ciclo, tão ou mais importante do que a coleta na medida que o acompanhamento traz a necessária longitudinalidade temporal e o acúmulo de dados necessários para a adequada informação.
3. Informar – formalização e difusão do conhecimento produzido *ex officio* ou por pedido da autoridade.
4. Decidir – definição pelo decisor sobre como proceder diante do que foi informado, deliberando sobre as medidas a serem implementadas para a consecução de um objetivo.
5. Agir – adoção de medidas e procedimentos para concretizar o que foi decidido[8].

Percebe-se um paralelismo interessante entre o ciclo de inteligência e o ciclo da abordagem ABRE de monitoramente de risco. Tal paralelismo não significa a correspondência de fases de ambos os ciclos – porque são ciclos de própositos diferentes e não permitiriam tal analogia. Porém, cabe analisar uma vinculação entre as fases dos dois ciclos, a fim de compreender como a inteligência laboratorial interagiria com a abordagem ABRE de monitoramento de riscos.

Na inteligência laboratorial, o “objetivar” (primeira fase) do ciclo de inteligência seria voltado para o planejamento da identificação e medição de riscos de bioproteção (os dois primeiros passos da abordagem ABRE).

O acompanhamento dos temas relativos às ameaças de BPL (“acompanhar” - segunda fase) e a informação (“informar” – terceira fase) serviriam para subsidiar a coleta de informações sobre perigos/ameaças (primeiro passo da abordagem ABRE) e a consequente caracaterização dos riscos associados (segundo passo da abordagem ABRE) [8, 16, 22].

É exatamente na fase de coleta de informações e de medição dos riscos, que se se dispõe de menos instruções sobre como realizá-las na práxis por profissionais de B2L[8, 16, 22].

A partir da medição de riscos, pode-se entrar no segundo conjunto de passos da abordagem ABRE, que seriam vinculados à implementação de medidas de controle dos riscos quantificados. Estas medidas coincidem, no ciclo da inteligência, com o “decidir” (quarta fase) e o “agir” (quinta e última fase do ciclo de inteligência) [8, 16, 22].

O *feedback* de ambos os ciclos é contínuo, de modo que a revisão dos riscos e suas medidas de controle (quinto e último passo da abordagem ABRE) influencia na nova coleta de informações (reinício do primeiro passo da abordagem ABRE) e no “objetivar” e no “acompanhar” do novo ciclo de inteligência[8, 16, 22].

Esta análise relacional está baseada na ideia de que o decisor ao qual se vincula a fração ou órgão de inteligência laboratorial é também gestor de B2L, isto é, quem determina – sozinho ou em conjunto com outros gestores - o planejamento e implementação das medidas de controle de rsicos.

A medição dos riscos, por sua vez, enquanto processo contínuo, dialoga e faz feedback com o “acompanhar” e o “informar” do ciclo de inteligência[8, 16, 22]. Este processo de interação entre os dois ciclos pode ser esquematizado para garantir melhor compreensão da íntima conexão dos dois trabalhos (**Figura 25**):

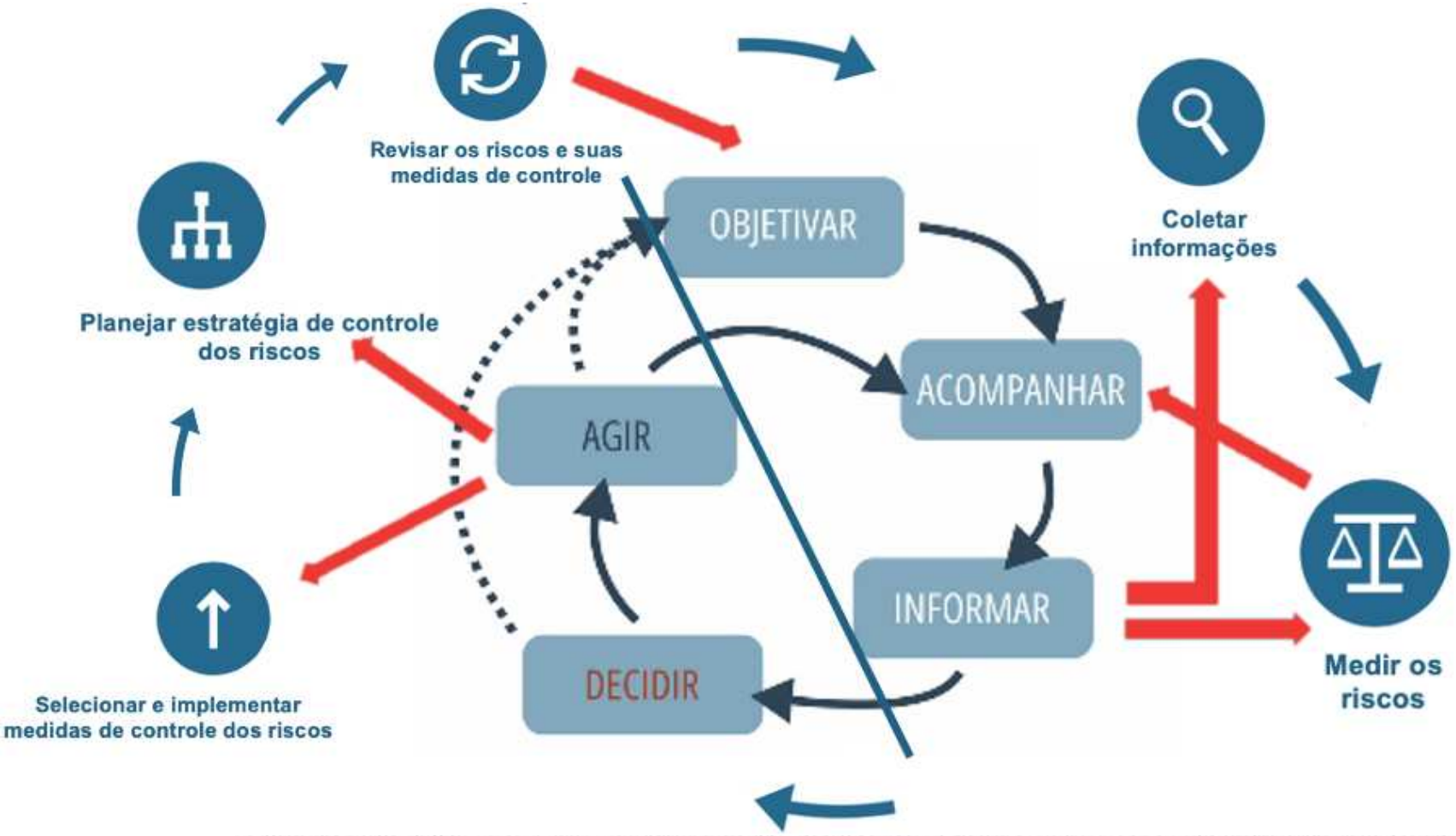


Figura 25 – *Paralelismo entre o ciclo de inteligência com o ciclo da abordagem ABRE (elaborado pelo autor).*

Por fim, a inteligência laboratorial seria uma fração ou órgão assim caracterizado por possuir algumas particularidades típicas da atividade de inteligência[8]:

1. Produzir conhecimentos de acordo com o ciclo de inteligência;
2. Produzir conhecimentos de acordo com a metodologia de produção do conhecimento (MPC)[8, p.107 e ss];
3. Difundir conhecimentos a um decisor, de acordo com objetivos de interesse do Estado; e
4. Possuir pessoal continuamente treinados para a realização das atividades de inteligência.

O escopo de análise e acompanhamento de uma fração de inteligência laboratorial seriam os fatos e situações relacionados à disseminação intencional de um MBGC ou ABTS custodiado em laboratório.

Na revisão de literatura sobre inteligência e biodefesa, foram abordados doze temas tratados pelo PANGEIA/ABIN porque relacionados com eventos biológicos selecionados:

1. Infraestruturas críticas laboratoriais;
2. Sabotagem;
3. Espionagem;
4. Avaliação de sistemas de proteção;
5. Crime organizado;
6. Crime comum (“não organizado”);
7. Extremismo violento;
8. Terrorismo com armas de destruição em massa;
9. Disseminação “natural” de patógenos e toxinas (ex. epidemias não causadas intencionalmente);
10. Disseminação acidental de material biológico por falhas de biossegurança laboratorial;
11. Acompanhamento de países proliferadores de armas biológicas; e
12. Regimes de não proliferação de armas biológicas.

São estes mesmos temas que uma estrutura de inteligência laboratorial deve acompanhar, a fim de conseguir analisar adequadamente riscos biológicos associados.

Na perspectiva da bioproteção laboratorial, entretanto, o rol de temas transversais cai para dez, uma vez que a disseminação “natural” e “acidental” sairiam do escopo.

1. Infraestruturas críticas laboratoriais;
2. Sabotagem;
3. Espionagem;
4. Avaliação de sistemas de proteção;
5. Crime organizado;
6. Crime comum (“não organizado”);
7. Extremismo violento;
8. Terrorismo com armas de destruição em massa;
9. Acompanhamento de países proliferadores de armas biológicas; e
10. Regimes de não proliferação de armas biológicas.

Resta claro que os objetivos de atuação da inteligência laboratorial são distintos da atuação da ABIN ou da inteligência da Polícia Federal, por exemplo. Enquanto à ABIN e à PF interessaria conhecer detalhes sobre eventual célula terrorista atuando no Brasil e com intenção de uso de uma toxina selecionada, a fim de identificar seus integrantes e detê-los, à fração de inteligência laboratorial à fração de inteligência laboratorial interessa conhecer o suficiente para caracterizar o grupo enquanto ameaça à bioproteção laboratorial, sem prescindir da troca de informações com outras frações e órgãos de inteligência.

Esta caracterização depende de conhecer se o grupo possui potencial de atacar um laboratório ou de se infiltrar em um, além dos meios potenciais de uso no ataque (ex. armas brancas ou armas de fogo de alta energia cinética, como fuzis?).

Por isso, mesmo que os objetivos sejam distintos, a análise de inteligência laboratorial, assim como as ações tomadas para prevenção e mitigação dos riscos de um evento de disseminação de ABTS por falha de bioproteção, não se pode prescindir de uma troca de informações efetiva entre analistas de inteligência que abordem transversalmente essas dez ameaças ou, neste contexto, bioameaças.

BURNETTE (2020), já percebera a avaliação de bioameaças (*biothreat assessment*) como um “*fundamento para a bioproteção*” [tradução nossa][20, pp.13-33]. Para ele:

> “Enquanto a sexta edição do BMBL informa ambos os paradigmas da avaliação de risco de biossegurança e de bioproteção, as conexões entre os aspectos de biossegurança e bioproteção permanecem indefinidos. Em

> outras palavras, a continuidade e direcionalidade de uma ameaça, vulnerabilidade e metodologia de avaliação de risco estão grandemente ausentes [tradução nossa].”[22. p. 31]

O reconhecimento destas lacunas, portanto, não é novo na literatura especializada em BPL, mas pode remontar a 2020 ou antes, mas não foram suficientes para alterar as diretrizes da OMS com o recém-publicado GBL2.

Por fim, é mister enfatizar que a efetiva sinergia entre a inteligência, com tais *inputs* sobre ameaças, em conjunto com os órgãos de segurança pública e as instituições laboratoriais apresentam grande interdependência. A segurança pública precisa entender os riscos laboratoriais para participar adequadamente dos planos de P2R2, assim como os laboratórios necessitam de entender o papel da segurança-inteligência na construção do processo de BPL.

6.1.1.1 Classificação da inteligência em saúde e da inteligência laboratorial por propósito

Uma das formas mais comuns de classificação da AI é a classificação por propósito:

> “A classificação por propósito diferencia os produtos de inteli- gência de acordo com o seu escopo e o emprego almejado para cada um deles. Nesse sentido, o conhecimento pode subsidiar a tomada de decisão sobre o delineamento de uma política pública (Inteligência Estratégica), sobre as ações propostas para sua consecução (Inteligência Tática), sobre a operacionalização dessas ações (Inteligência Operacional)“[8, p.42].

Ora, se a atividade de inteligência *lato sensu* pode ser classificada, enquanto o objeto de análise (escopo) e a finalidade (emprego almejado), em operacional, tática e estratégica, o mesmo se aplicaria à inteligência em saúde e à inteligência laboratorial.

Um exemplo de ação típica da inteligência em saúde operacional seria, na área epidemiológica, identificar um *cluster* de transmissão de uma epidemia em um bairro. Na área sanitária, por sua vez, uma ação de inteligência em saúde operacional seria identificar o comércio de lote fraudado de medicamento, objetivando neutralizar a venda deste lote.

Um exemplo de ação típica da inteligência em saúde tática seria o acompanhamento sistemático de rumores sobre disseminação de doenças, com o

fito de identificar e antecipar um surto ou uma epidemia. O monitoramento e análise de inteligência contínuos no *hub* da OMS em Berlim/Alemanha configura uma atividade de inteligência em saúde tática, portanto.

Por último, um exemplo de ação típica da inteligência em saúde estratégica seria a análise de conhecimentos operacionais e táticos para elaborar cenários de retração ou expansão de risco de acidentes laboratoriais no Brasil.

No âmbito do MS, a Rede CIEVS, apesar do termo “estratégico” em sua nomenclatura, é precipuamente um conjunto de frações que produzem conhecimentos operacionais e táticos.

A rigor, a suposta falta de vinculacão da Rede CIEVS com a doutrina de inteligência brasileira e com o SISBIN, decorrente da legítima autonomia dessa estrutura de inteligência epidemiológica, assim como a decorrente falta de treinamento dos analistas da rede na linguagem de produção do conhecimento de inteligência, isto é, na metodologia de produção do conhecimento (MPC) – tão própria da comunidade de inteligência no Brasil – impediria a priori que o CIEVS fosse considerado uma fração de inteligência.

Ressalte-se, entretanto, que não existe normativa que sustente esta exigência caracterizadora. Não há previsão legal nem normativa infralegal, no Brasil, para quais seriam os requisitos que consideram uma fração ou órgão como de inteligência.

Não há sequer impedimento legal ou normativo para que frações e órgãos de inteligência em saúde elaborem doutrina própria e técnica de produção do conhecimento original e distinta do que hoje a ABIN, como órgão central do SISBIN, cria e difunde aos seus parceiros.

Neste sentido, a atuação objetiva do CIEVS ou de qualquer outra fração existente ou a ser criada no âmbito do MS ou de qualquer órgão de saúde, em nível municipal, estadual ou federal, para efetuar ações e medidas de inteligência, permite a sua classificação como fração ou órgão de inteligência em saúde.

O foco deste órgão ou fração em produzir conhecimentos operacionais, táticos ou estratégicos não tem relação com o nível municipal, estadual ou federal. Pode-se vislumbrar o cenário de que uma fração de inteligência municipal produza conhecimento estratégico para o decisor do município, mesmo que, para um decisor estadual ou federal, este conhecimento não seja estratégico.

Seguem-se alguns exemplos de situações de análise operacional, tática e estratégica na área de inteligência em saúde (e mais especificamente no conceito de inteligência laboratorial) em diferentes níveis federativos, para exemplificação:

1. Inteligência em saúde operacional
    a. Produto de inteligência epidemiológica operacional - identificação dos dados (nome, endereço, etc.) de uma pessoa infectada por Monkeypox, a partir de rumores que circularam numa rede social de que havia um infectado em um determinado bairro.
    b. Produto de inteligência laboratorial operacional – conclusão de que um estudante estrangeiro no laboratório de antrax faz parte de um grupo supremacista no seu país de origem; monitoramento de acessos a redes de laboratórios estratégicos; detecção de tentativas de intrusão digital em laboratórios; proteção contra ataques *ransomware* em laboratórios.
2. Inteligência em saúde tática
    a. Produto de inteligência epidemiológica tática – modelagem com padrão dispersivo de uma doença infectocontagiosa epidêmica no Brasil para os próximos 30 dias.
    b. Produto de inteligência laboratorial tática – avaliação de que todos os laboratórios biomédicos que custodiam ABTS de uma determinada instituição acadêmica possuem falhas graves de bioproteção física; análise de padrões de ciberataques a infraestruturas laboratoriais e desenvolvimento de ações de prevenção e de respostas rápidas a tais ataques.
3. Inteligência em saúde estratégica
    a. Produto de inteligência epidemiológica estratégica – analisar a tendência de queda ou aumento da cobertra vacinal no país e apontar os principais determinantes.
    b. Produto de inteligência laboratorial estratégica – analisar a tendência de ameaças expressas de uso ABTS por organizações extremistas e conhecer as capacidades de acesso a esses ABTS por tais organizações; assessorar o desenvolvimento de políticas públicas nacionais para a proteção digital de laboratórios estratégicos; integrar a segurança cibernética com estratégias nacionais de B2L, segurança da saúde e biodefesa.

É importante frisar que a estruturação de uma rede de inteligência laboratorial pode se especializar na produção de conhecimentos operacionais, táticos ou estratégicos, de maneira independente, de acordo com o interesse e possibilidades do gestor.

A criação das capacidades de produzir inteligência tática e estratégica, por exemplo, pode ser ganha com o tempo, iniciando a rede de inteligência laboratorial pelo foco em inteligência operacional, por exemplo.

Outra possibilidade é a de uma fração de inteligência se especializar em produzir um dos tipos de inteligência (operacional, tática ou estratégica) e lançar mão de parcerias com outros órgãos ou frações de inteligência laboratorial para a produção dos tipos de inteligência laboratorial que não poderão de realizados.

Ou ainda dividir competências entre diferentes esferas: por exemplo possuindo frações de inteligência laboratorial descentralizadas nos laboratórios selecionados, com foco em inteligência operacional; estas frações podem ser subordinadas ou vinculadas a frações regionais de inteligência tática; e, por fim, todas se reportarem a uma fração central (na sede do órgão gestor), que produziria inteligência estratégica.

Independente da habilidade de uma fração de inteligência da saúde utilizar um método próprio ou comum – utilizado também por outros órgãos - de produção do conhecimento, os analistas que trabalham com dados de saúde (ex. sanitários e epidemiológicos) precisam de conhecimento especializado na área laboratorial.

Não é possível vislumbrar a produção de conhecimento estratégico, tático e nem operacional, na área de saúde e na área laboratorial, sem conhecimentos técnicos especializados.

6.1.1.2 Área de atuação da inteligência em saúde e da inteligência laboratorial

Segundo a Doutrina de Inteligência da ABIN (2023), a inteligência acompanha diversos tema e produz conhecimentos sobre eles. São descritas quatro conjuntos de temas de acompanhamento pela inteligência:

1. Inteligência externa – “trata sobre temas sobre os quais o Estado tem pouco ou nenhum poder de decisão ou intervenção unilateral e que

exigem estratégias de posicionamento internacional para negociação e consecução dos interesses nacionais."[8, p. 52]

2. Inteligênca interna – "trata de temas que estão integralmente sob a competência de intervenção do Esatdo."[8, p.52]
3. Inteligência transnacional – "trata de temas transfronteiriços, parcialmente sob capacidade de intervenção do Estado, mas que exigem negociaçnoes e parcerias internacionais para adoção de políticas efetivas para concretização dos objetivos do Estado."[8, p.53]
4. Inteligência cibernética – "trata de temas voltados ao espaço cibernético, cuja natureza ubíqua, distribuída e descentralizada implica capacidade limitada de intervenção do Estado."[8, p 53]

A doutrina da ABIN cita como exemplos de temas de acompanhamento de inteligência externa: os fóruns multilaterais e a questão armamentista; de inteligência interna: implementação de políticas públicas; de inteligência transnacional: extremismos internacionais; e de inteligência cibernética: incidentes cibernéticos contra infraestruturas críticas[8].

Na perspectiva da B2L, podemos concluir que esta divisão não faz sentido e não seria própria para os desafios e ameaças do século XXI: dificilmente uma ameaça prioritária de acompanhamento no rasil é um tema exclusivamente interno ou externo.

Por exemplo, na segurança pública, a implementação de políticas públicas de combate às drogas (acompanhamento da inteligência interna, *a priori*) não depende unicamente de ações brasileiras, porque elas devem se basear em acordos e documentos multilaterais (acompanhamento da inteligência externa, *a priori*).

Além disso, as principais organizações criminosas de tráfico de entorpecentes são transacionais (acompanhamento da inteligência transnacional, a *priori*). E muito da lavagem de dinheiro empreendida por elas acontecem no ambiente cibernético (acompanhamento da inteligência cibernética, *a priori*).

Destarte, como classificar a área da inteligência que acompanharia o tráfico de drogas no Brasi entre as quatro mencionadas na Doutrina da ABIN? Não seria possível fazê-lo, porque é um tema que transpassa estas classificações. Poderíamos dizer que se trata de um tema transnacional, se considerarmos tais

temas com de abrangência interna e externa, sobrepujando a classificação dual de inteligência interna e externa.

Considerando que a divisão de temas entre interno e externo dificilmente se encaiXaria em algum tema de ameaça prioritária moderna, não faria mais sentido dividir os acompanhamentos temáticos desta forma. Neste sentido, todos os principais temas supracitados pela PNI como relacionados a ameaças prioritárias, seriam temas transnacionais.

Meio ambiente, que ganha relevância crescente como tema de acompanhamento nas últimas décadas, de maneira análoga ao raciocínio feito com o tráfico de entorpecentes, não poderia ser tema de inteligência interna, como a Doutrina da ABIN quer fazer crer.

Na perspectiva da B2L, temos outro exemplo de temática que não se encaixa na anacrônica divisão de áreas interna *versus* externa, uma vez que a autonomia do Brasil em planejar e implementar medidas de controle de biorriscos laboratoriais precisa dialogar com obrigações multilaterais, conforme supracitado. E a ciberbioproteção coloca a B2P em um plano de inteligência cibernética também.

Tem-se, em suma, que a inteligência laboratorial é tema transversal de acompanhamento de inteligência e, por envolver a contrainteligência em diversas medidas de controle de riscos, é uma temática que transcende a própria divisão clássica da AI entre os ramos da inteligência e da contrainteligência.

Na perspectiva da abordagem baseada em risco e evidência (abordagem ABRE), propagada pelo LBM4 e GBL2 e analisada no tópico 2.1.3.2.1, o *framework* de monitoramento de risco de B2L (FIGURA 7) pode ser interpretado por anaogia como forma de demonstrar o quanto a divisão da AI em dois ramos, inteligência e contrainteligência, não faz sentido na inteligência laboratorial e na maioria dos temas hodiernos[16, 22, 63].

Entre os quatro passos da abordagem ABRE, os dois primeiros (coletar informações; e medir os riscos) estariam vinculados ao ramo da inteligência, na medida em que são voltados “para a função informacional”[8, p.42].

A inteligência em saúde e sua componente inteligência laboratorial servem como exemplificação de como a doutrina de inteligência, em muitos documentos atuais – como na revisão recentíssima da própria ABIN, mas que está em consonância com o que é produzido e praticado por muitos dos serviços de inteligência estrangeiros[8, 94, 95, 96] - persiste no erro de dividir temas em ações e

serviços erroneamente distintos e compartimentados, comprometendo a efetividade de suas ações.

O apego anacrônico à dupla dicotomia *inteligência versus contrainteligência* e *inteligência externa versus inteligência interna* não faz mais sentido teórico nem prático, sobretudo desde o pós-1945, quando os principais temas de ameaças globais (e, por serem globais, são também ameaças nacionais – ex. uso de armas de destruição em massa, terrorismo, criminalidade organizada, ameaças ao meio ambiente, violação de direitos humanos, mudanças climáticas etc.) se tornam objeto de tratados e outras ações multilaterais. As capacidades laboratorias e as ameaças biológicas associadas não poderiam estar de fora deste processo de multilateralização e transnacionalização.

6.1.1.3 Desafios para integração da Inteligência em saúde (inclusive a inteligência laboratorial) com a PNI e o SISBIN

Apesar de o surgimento da PNI, em 2016, ter significado um foco e, portanto, possibilidade de maior efetividade na atuação da inteligência brasileira, quando comparada com as diretrizes da CREDEN, o documento é restritivo para a área de saúde, ao manter a inteligência securitizada em alguns aspectos, e ignorar temas importantes de áreas tradicionalmente menos securitárias, como a saúde.

Um dos eixos da AI não abordados pela PNI é a atuação da inteligência em saúde *lato sensu*. Se a inteligência em saúde, por exemplo na sua vertente de inteligência epidemiológica, tem competência e interesse em eventos biológicos não selecionados, ela não está contemplada pela PNI, apesar de o Ministério da Saúde fazer parte do SISBIN e potencialmente poder utilizar o sistema para troca de informações destes assuntos.

Trata-se de exemplo de assunto que claramente pode ser de interesse de outros órgãos igual ou potencialmente membros, inclusive ógãos estaduais da área de saúde.

A evidente restrição acontece, porque o foco da transecuritização da PNI na área de ameaças biológicas se restringe a eventos selecionados, que são corretamente aqueles de interesse da ABIN, um órgão que precisa se especializar para se tornar mais efetivo.

Verfica-se, então, que a transecuritização da inteligência[1] é limitada na área de saúde, na medida em que não reconhece áreas de atuação tática, operacional e estratégica na saúde que não sejam, *a priori*, de competência da ABIN e de outros órgãos de segurança-inteligência.

Esta falta de reconhecimento pode afastar a integração dos órgãos de saúde com os órgãos de segurança-inteligência. Afasta-se porque não considera como parte da atividade de inteligência nacional temas externos às competências dos órgãos mais tradicionalmente ligados à atividade como a ABIN e os órgãos policiais e militares.

Neste sentido, é mister repensar a PNI, para que possibilite maior autonomia de definição de atuações transecuritizadas da inteligência, sem necessidade de interferência dos órgãos tradicionais de segurança-inteligência.

Para atuar como órgão central do SISBIN, não é necessário que a ABIN produza conhecimento de inteligência sobre todos os temas (ou ameaças) elencados(as) como prioritários.

Esta possibilidade já é praticada, no tocante ao tema da corrupção, que está entre as ameaças prioritárias da PNI, mas não é escopo de atuação da ABIN, por entendimento interno e externo – na medida em que os decisores tendem a não demandar a ABIN sobre este tema - de que não cabe ao órgão produzir conhecimentos sobre o assunto.

Outra possibilidade de modernização transecuritizada para incluir na AI a inteligência em saúde é a ampliação de subsistemas de inteligência, cada qual com temas priorizados próprios, sem que a ABIN seja o órgão central dos susbsistemas, mas se mantendo como órgão coordenador do sistema como um todo.

A ampliação do escopo do sistema de inteligência nacional, reconhecendo que existem temas de inteligência importantes para o Estado, apesar de não contemplados na PNI, caso não se concretize, tende a afastar a segurança-inteligência das áreas não contempladas, como a saúde.

Independentemente do SISBIN, a inteligência em saúde existirá enquanto trabalho e produção do MS, com o enfoque epidemiológico – sem se esgotar neste tema -, e enquanto trabalho e produção da ANVISA.

Se os órgãos não forem adequadamente incorporados ao SISBIN, representados por suas frações que de fato produzem ou consomem conhecimentos de inteligência epidemiológica (ex. Secretaria de Vigilância em Sáude – SVS) e de inteligência sanitária, haverá perda de efetividade do sistema.

Se a SVS, ou fração equivalente que coordene a REDE CIEVS, tem a competência de gerir a principal rede de inteligência epidemiológica brasileira, é preciso identificar que fração teria vocação de gerir a troca de conhecimentos sobre a biossegurança e bioproteção laboratoriais.

Para os órgãos da área de saúde integrantes do SISBIN, como o MS e a ANVISA, a falta de priorização de temas de inteligência em saúde, como a área epidemiológica e sanitária, em razão da base securitizada e militarizada do Sistema, diminuem o interesse destes dois membros em se aproximar do SISBIN e implementar o PLANINT e seus documentos precursores, a PNI e a ENINT.

Ora, se os documentos não dialogam com a inteligência em saúde e seus temas prioritários e de maior interesse pelo MS e ANVISA, não há estímulo institucional para o planejamento destas áreas com base nos documentos norteadores da AI no Brasil.

Neste sentido, consolidam-se sistemas paralelos de inteligência em saúde, como o da REDE CIEVS, rede de inteligência epidemiológica, que dialoga pouco com os demais órgãos do SISBIN.

Chama-se paralelo, sob o ponto de vista do SISBIN, mas sem menosprezar obviamente a condição autônoma e legítima do MS de estruturar rede semelhante para atender às políticas de integralidade do SUS e também o disposto no RSI.

O PANGEIA/ABIN buscou aproximar a ABIN da inteligência epidemiológica, desde sua criação, ao aceitar o convite do MS de se manter como membro observador do Comitê de Monitoramento de Eventos de Saúde Pública (CME), coordenado pelo Centro Nacional de Informações Estratégicas em Vigilância em Saúde (CIEVS Nacional)[88].

Também estimulou a presença de frações de inteligência epidemiológica do então Ministério da Pecuária e Agricultura (MAPA), no mesmo Comitê. Entretanto, o arranjo destas participações era frágil, porque desprovido de arcabouço normativo que estruturasse um sistema (ou subsistema, se vinculado ao SISBIN) efetivo de troca de informações de inteligência epidemiológica, que fosse reconhecido e fortalecido legalmente.

Dada a importância de planejamento e estruturação de sistema intersetorial semelhante ao da REDE CIEVS, incluindo o elemento de inteligência laboratorial na estrutura, não é prudente que o MS, enquanto órgão autônomo e

vocacionado para coordená-lo, aguarde a tomada de consciência institucional da ABIN ou do SISBIN para criá-lo.

O MS poderia, ao contrário, fortalecê-lo, diante da excessiva secutirização da AI brasileira, buscando normatizá-lo enquanto sistema, independente do SISBIN, se for o caso, em um primeiro momento, dada a necessidade urgente de o Brasil instituir padrões efetivos de biossegurança e de bioproteção laboratoriais.

Desde 2018, o PI-ABIN determina necessidade de a ABIN conhecer sobre a ocorrência de ABTS no Brasil e os riscos associados a esta ocorrência (OI 1). Este objetivo de inteligência descreve, portanto, a atuação interessada em mapear os riscos de eventos de bioproteção, entre outros, uma vez que o risco de furto e roubo de ABTS é um risco associado à ocorrência de ABTS no território brasileiro.

Ademais, laboratórios de alta-contenção (LAC) e ILS no Brasil e na América Latina (CN 2.1), assim como recursos de resposta a eventos biológicos (CN 3.1); planos de contingência ou resposta a eventos biológicos (CN 3.2); e casos de disseminação de ABTS (CN3.3) são assuntos de monitoramento regular da ABIN, segundo o PI-ABIN.

Estes conhecimentos são fundamentais para a avaliação do risco eventos de bioproteção e para o adequado assessoramento a decisores sobre a gestão de biossegurança e bioproteção laboratoriais no Brasil.

Nestes quatro itens de CN, estão descritas atividades evidentes de inteligência em saúde, mais precisamente de inteligência laboratorial, na medida em que objetivam entender vulnerabilidades e oportunidades para a efetiva gestão de biossegurança e bioproteção laboratoriais.

Sem a colaboração dos gestores laboratoriais e seus superiores, é impossível à ABIN desempenhar as atividades previstas no PI-ABIN em seu módulo de Ameaças QBRN.

Esta dependência estruturante permite refletir se tais objetivos de inteligência seriam melhor atribuídos não à ABIN em si, mas aos órgãos que são responsáveis pela gestão de bioproteção laboratorial.

Sem uma relação de subordinação ou sem mandato legal para tornar obrigatório o repasse de informações e a possibilidade de visitas laboratoriais, a obtenção de informações sobre as LAC e ILS fica condicionada à boa vontade dos gestores laboratoriais e ao bom relacionamento entre a ABIN e tais gestores.

Se se opta por uma construção de inteligência laboratorial fora da ABIN, a estrutura do SISBIN pode ser aproveitada para integrar a fração responsável pela

obtenção e análise dos dados, na medida em que os eixos estruturantes e os objetivos estratégicos da ENINT permitem dialogar com uma inteligência em saúde voltada para a biossegurança e bioproteção laboratoriais.

A atuação em rede (eixo estruturante 1); a busca de maior tecnologia e capacitação (eixo estruturante 2); a projeção internacional (eixo estruturante 3); e a segurança da sociedade (eixo estruturante 4) são igualmente estratégicos para qualquer atividade de inteligência laboratorial, seja ela exercida por ministérios gestores de redes laboratoriais seja ela exercida por órgãos autônomos, criados para este fim específico.

Considerando que o PLANINT e o PI-ABIN se baseiam nos objetivos estratégicos da ENINT para delimitar suas ações, e que a ENINT definiu estes objetivos para o quinquenio 2018-2023, desde o início de 2024, portanto, haveria necessidade de atualização dos documentos orientadores da AI.

Entretanto, os documentos não foram revisados até o momento e continuam em vigor. De modo que, a rigor, os CN e seus DCN previsto no PI-ABN continuam válidos e sob competências das frações de inteligência a que foram atribuídos.

Surge, portanto, uma oportunidade de revisão na perspectiva defendida nesta tese, com a transecurituzação dos temas e inclusão, por exemplo, do escopo da inteligência em saúde como parte do SISBIN, desde que seja do interesse do MS tratar de eventuais benefícios desta inclusão.

A abordagem da inteligência laboratorial deve estar considerada neste novo escopo, voltada precipuamente às necessidades de gestão de bioproteção, tendo em vista que a bioproteção laboratorial é a área da inteligência laboratorial que mais se beneficia da integração saúde-segurança.

Ao MS e à ANVISA cabem participar do processo de renovação do PLANINT e dos Planos de Inteligência orgânicos de cada membro do SISBIN, a fim de garantir a priorização de temas de seu interesse fora do escopo securitizado-militarizado.

Ao CONSISBIN e à ABIN, por sua vez, cabe perceber a necessidade de pensar novos temas e sistemas de inteligência consdeirando a segurança da saúde (*health security*) e da inteligência em saúde, chamando o MS e a ANVISA para discutirem em conjunto uma visão transecuritizada e transmilitarizada da AI, na busca de sua modernização e integração.

Ressalte-se que a transmilitarização da AI, na perspectiva da bioproteção laboratorial não significa excluir a biodefesa e as estruturas de defesa QBRN ou P2R2 militares do processo de construção de um sistema de inteligência laboratorial.

Considerando a importância das estruturas e conhecimentos militares para a construção da biodefesa, inclusive na sua relação com a B2L[rr], integrar as FFAA neste campo é ampliar a efetividade da atuação integrada em um tema grandemente transmilitarizado em si, porque excede em muito a temática militar.

No Brasil, o número de laboratórios civis, incuindo instalações da área de saúde e da área de educação/pesquisa excede em muito o número de laboratórios estritamente militares. Deste modo, uma governança robusta de B2L é de interesse de toda a sociedade civil. Por isso, o tema da gestão de biossegurança e bioproteção laboratoriais é precipuamente um tema de interesse civil, com com importante e necessária participação de biodefesa estritamente militar.

Considerando a cultura histórico-institucional da ABIN de ser um órgão que atende demandas de órgãos diversos, é razoável discutir a alta probabilidade de que, mediante a demanda de Ministérios afetos à necessidade de troca de informações sobre inteligência laboratorial, a exemplo do MAPA e do MS, a ABIN possa aumentar seu esforço de produzir inteligência laboratorial e entregar o que for demandado institucionalmente.

Nesse sentido, o aprofundamento institucional da gestão de B2L por ministérios interessados nos conhecimentos de inteligência laboratorial deve levar em consideração a tarefa de demandar à ABIN e ao SISBIN sobre o tema, permitindo direcionar a AI brasileira para o assunto.

6.1.1.4 Inteligência laboratorial e monitoramento de risco (*risk assessment*) de bioproteção laboratorial: modelo tridimensional de governança de B2L

Conforme o LBM4 da OMS, o processo de monitoramento de risco, considerando os cinco passos da abordagem ABRE, possui considerações-chave a serem levadas em consideração em cada passo do processo[16, pp.7-8].

[rr] Dadas as especificidades de lidar com a B2L na perspectiva da biodefesa, caberia até pensarmos em um ramo da biodefesa que poderia ser intitulado *biodefesa laboratorial*.

No passo dois (“medir os riscos”), são considerações-chave os questionamentos abaixo:

1. Como pode acontecer uma disseminação [*intencional do MBGC custodiado*]*?*
2. Qual a chance de uma disseminação [*idem*]*?*
3. Qual o impacto de uma disseminação [*idem*]*?*
4. O que seria um risco aceitável [*de disseminação intencional de um MBGC*]*?*
5. Quais riscos são inaceitáveis [*de disseminação intencional de um MBGC*]*?* [*tradução e grifos nossos*][16, p.7]

Ora, apesar de o LBM4 e da monografia de monitoramento de risco da OMS[63] preconizarem estes questionamentos no processo de medição de riscos (passo dois da abordagem ABRE), verifica-se que é difícil para o “oficial de biossegurança laboratorial” e/ou o “Comitê Institucional de Biossegurança” (IBC, na sigla inglês), obterem estas respostas sobre ameaças como o crime organizado ou organizações terroristas, se não houver treinamento específico de segurança-inteligência e canais de troca de informações com órgãos ou sistemas de segurança-inteligência.

Destaca-se que os manuais de bioproteção são loquazes na defesa de que o monitoramento de risco (*risk assessment*) deve ser um trabalho de vários profissionais ligados ao laboratório, porque depende da coleta de informações técnicas as mais arangentes possíveis[13, 22].

Todavia, os mesmos manuais são discretos ao enfatizar a necessidade de envolvimento de órgãos de segurança-inteligência externos ao laboratório, assim como se omitem para ratificar a importância fundamental desta participação.

É muito provável que qualquer monitoramento de risco de bioproteção laboratorial que se se baseie unicamente nas recomendações do SNL, da OMS e dos CDC seja pouco efetivo.

No manual dos *Sandia National Laboratories* (SNL), de SALERNO & GAUDIOSO (2020), há uma única menção sobre a participação de órgãos de segurança externos ao laboratório no processo de avaliação de risco:

> “*uma avaliação de risco de qualidade é a culminância de contribuições de numerosas pessoas no laboratório ou instalação.*
> *(...)*
> *-Pessoal de segurança e resposta: esses indivíduos podem fornecer valiosas informações nas avaliações de risco. Por exemplo, órgãos*

> *externos, como as forças policiais, podem ter conhecimento sobre ameaças potenciais presentes na comunidade local*. [tradução nossa]"[13, p.60]

Observa-se que é uma menção modesta e aquém da importância da troca de informações sobre riscos de bioproteção com órgãos de segurança-inteligência. Sabe-se que as ameaças criminosas comuns e terroristas, por exemplo, raramente são ameaças da "comunidade local". Muitas vezes são ameaças nacionais ou internacionais acompanhadas por órgãos de segurança e inteligência com intercâmbio internacional de conhecimentos.

Destarte, a construção de frações de inteligência laboratorial integradas a uma rede de outros órgãos de inteligência, locais e nacionais, são fundamentais para a caracterização/medição de riscos (*risk evaluation*).

Ressalte-se ainda que o processo de coleta e análise de informações por frações ou órgãos de inteligência laboratorial poderia suprir mais adequadamente os requisitos dos passos 1 (coleta de informações) e 2 (medir os riscos) na abordagem ABRE sugerida pela OMS; ou avaliar os riscos mais efetivamente segundo o modelo AME dos SNL.

Não se pode, portanto, prescindir de troca de informações sobre fenômenos externos aos laboratórios com órgãos também externos ao laboratório, a fim de realizar identificação e medição de riscos e, consequentemente, avaliação/monitoramento de riscos efetivos.

Diferentemente de um modelo de monitoramento de riscos de biossegurança laboratorial, os questionamentos de bioproteção superam a capacidade interna a um laboratório e seus gestores de obter todas as respostas necessárias para a adequada implementação de um sistema de controle de riscos laboratoriais.

Merece destaque a indagação "o que seria um risco aceitável?". Ora, se se trata da possibilidade do risco de um ataque bioterrorista com antraz, por exemplo, a partir do roubo de MBGC de um laboratório que manipula estes bacilos não caberia ao laboratório poder definir a aceitabilidade de um risco.

Situações de alto impacto potencial colocam em risco a coletividade de tal modo que não deveria ser delegável pelo Estado a prerrogativa de dizer o que se aceita ou não em termos de medidas de controle de risco.

Deste modo, a pergunta colocada pelos documentos da OMS da forma como estão, parece induzirem a ideia errônea de que os níveis de risco aceitáveis ou não seriam definidos por gestores laboratoriais, quando, em matéria de

bioproteção laboratorial, o ideal é que tais definições sejam realizadas pelo Estado e materializada na forma de normas de garantia de bioproteção laboratorial e proteção biológica da sociedade.

Neste sentido, o assessoramento decisório por estruturas de inteligência laboratorial deveria incluir no seu escopo de objetivos também a definição, com o olhar estatal, de níveis de aceitabilidade de risco, para fins de planejamento de normas locais e nacionais.

Para evitar conflitos de interesse, é recomendável que os órgãos ou frações que definam tais níveis de aceitabilidade de risco sejam o mais dissociados possível dos gestores diretos dos laboratórios, que estarão sujeitos a tais normas regulamentadoras da gestão de biossegurança e bioproteção laboratoriais.

Neste sentido, pode-se vislumbrar uma estrutura em três níveis (*three-tier*) que seja mais robusta e voltada para a realidade da BPL do que a estrutura de dois níveis proposta pela OMS no GBL2[22] e revisada no tópico 2.1.2.5.4 (*Modelo de Governanças Nacionais*) acima.

Nesta estrutura de governança, que também poderia ser chamada de tridimensional – considerando que cada nível pode ser tratado como uma dimensão - tanto o nível regulatório quanto o nível institucional disporiam de uma fração de inteligência laboratorial ou, no caso do nível institucional, pontos focais de inteligência dentro do Comitê de B2L.

Outras inovações do modelo tridimensional, ao ser cotejado com o bidimensional do GBL2/OMS[22]:

1. Estabelecer a necessária triangulação da troca de informações/conhecimentos e do feedback regular sobre a governança de riscos de B2L;
2. Retificar que o Comitê Institucional não é apenas de biossegurança laboratorial, mas de B2L;
3. Explicitar, em nível regulatório, que são competências desse nível o registro nacional de MBGC e PGC, além das falhas de BPL – já inseridas no modelo do GBL2/OMS;
4. Instituir um registro nacional de boas práticas de B2L, na dimensão regulatória;
5. Atribuir à dimensão da inteligência laboratorial a competência de identificar e acompanhar as ameaças laboratoriais e apoiar o

monitoramento de risco (*risk assessment*), realizado em nível institucional;

a. Neste aspecto, vale ressaltar que a inteligência participaria do ciclo de monitoramento de risco, considerando a aboradagem ABRE da OMS, de acordo com o pararelismo supracitado no tópico 6.1.1 (*Inteligência laboratorial: conceito e práticas necessários*); e

6. Considerar o nível regulatório como nível de supervisão e de organização do preparo (*preparedness*) para resposta a um evento biológico por falha de B2L;
7. Integrar a dimensão da inteligência laboratorial em sistemas/subsistemas de inteligência, consequenteente integrando a governança e a gestão de B2L com uma rede de inteligência; e
8. Proporcionar a formação de uma rede de troca de informações de inteligência laboratorial entre o nível regulatório (ou os níveis regulatórios - a depender do país) nacional e as diversas instituições laboratoriais, de modo que se estabeleça um sistema de inteligência laboratorial no país.

Procura-se com essa estrutura de três níveis situar em um modelo transdisciplinar de governança o papel do nível inteligência, mediante a inclusão do que seriam as frações e/ou órgãos de inteligência no processo sistemático de monitoramento de riscos, definição de listas de MBGC, análise de PAI/PGC e P2R2 de eventos de bioproteção (**Figura 26**):

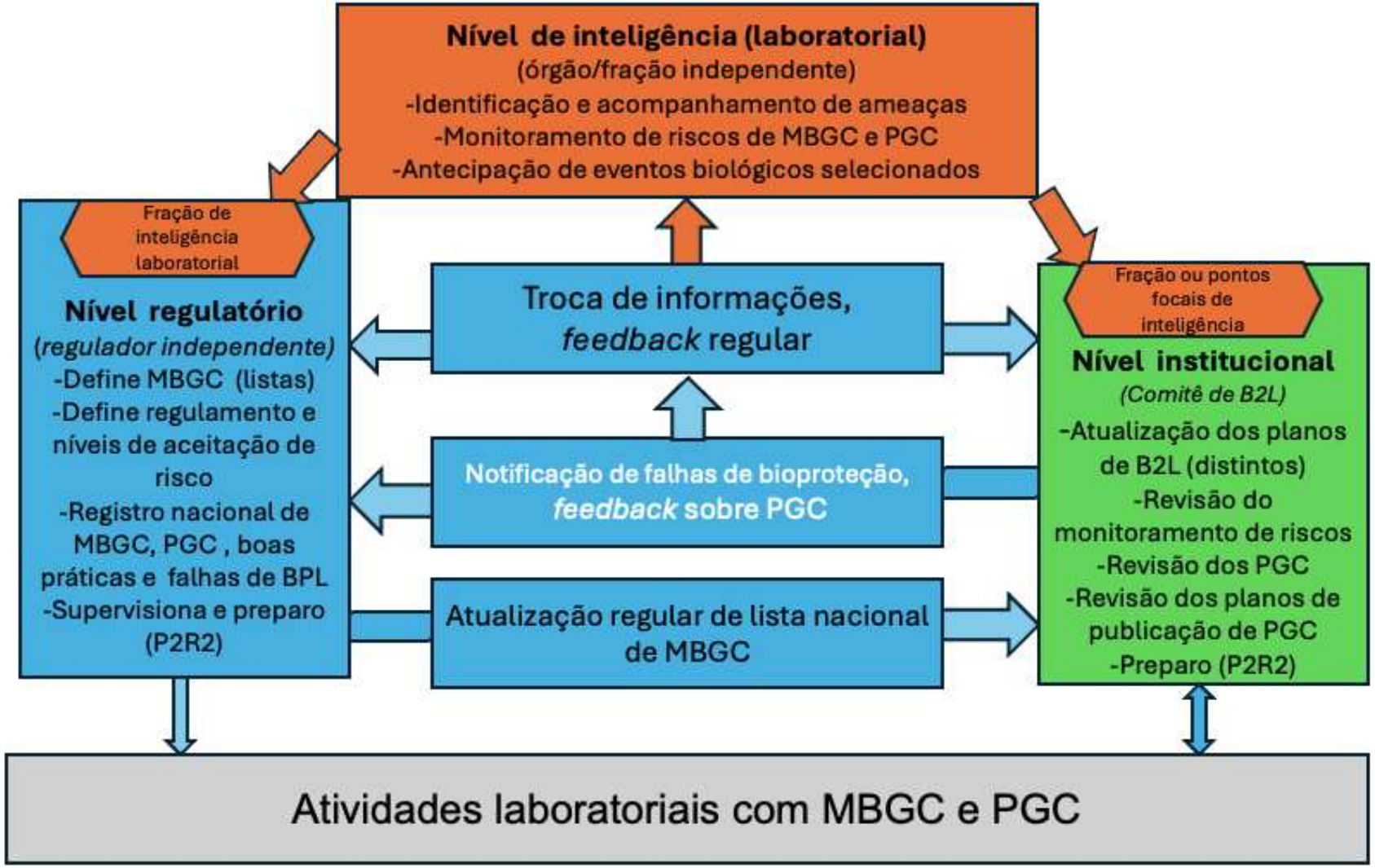


Figura 26 – *Sistema de três níveis de governança nacional de MBGC (elaborado pelo autor).*

Dessa forma, a inclusão de mecanismos como o *Checklist* RAMPA e o *PathoFinder Brazil®,* e o concomitante aprimoramento da colaboração intersetorial, poderiam ajudar na superação da lacuna na integração inteligência-segurança-gestão laboratorial, fortalecendo o arcabouço normativo da inteligência laboratorial na gestão de bioproteção e biodefesa no Brasil.

6.1.1.4 Inteligência laboratorial e integração multissetorial

Desde a pandemia da COVID-19, ampliaram-se os esforços internacionais de planejar e implementar mecanismos preventivos e de antecipação de emergências em saúde. Neste sentido, foi anunciado, em 2021, o polo de inteligência epidemiológica da OMS[50], e, em outubro de 2024, anunciada a Estratégia de Inteligência Epidemiológica da OPAS[51].

Há percepção de que são crescentes os riscos de ameaças em saúde pública. E os riscos laboratoriais e as ameaças de disseminação intencional de patógenos selecionados obedecem a essa tendência internacional e persistem entre os riscos globais mais importantes[1, 5, 7, 71].

Um evento de furto ou roubo de ABTS/MBGC é uma ameça potencial de evento de saúde pública, associado ao risco de provocar uma emergência em saúde de interesse nacional ou até internacional, a depender do patógeno disseminado criminosamente e das circunstâncias de sua disseminação[52,53].

Deste modo, a gestão de bioproteção dialoga com as obrigações internacionais brasileiras, mormente o RSI, preocupadas com a prevenção, preparo e resposta efetivos para uma emergência em saúde[52, 53].

Há de se considerar que, antes mesmo da disseminação de um ABTS/MBGC furtado ou roubado, o mero ato de furto ou roubo consumados de ABTS/MGBC é uma ameça potencial de evento de saúde pública, associado ao risco de provocar uma emergência em saúde de interesse nacional ou até internacional, a depender do patógeno disseminado criminosamente e das circunstâncias de sua disseminação.

Neste sentido, há de se avaliar que o furto ou roubo de agentes e toxinas biológicos deveriam ser notificados para a OMS à luz do RSI, tanto quanto a existência de casos de doenças e agravos em decorrência deste evento.

A notificação do furto ou roubo, antes de sua disseminação, permitiria questionamento sobre o fato de que há limitações para a integração saúde (OPAS, OMS e RSI) com órgãos de segurança (INTERPOL, EUROPOL, Conselho de Segurança das Nações Unidas etc.) também na esfera multilateral das Nações Unidas.

O Brasil é vinculado, perante o RSI e a OMS, a desenvolver capacidades de gestão de risco biológico de biossegurança e bioproteção laboratoriais efetivas. O país também é sujeito a seguir as normas e estratégias da OPAS para, no fortalecimento de suas capacidades-chaves em saúde, implementar inteligência epidemiológica efetiva[51,52].

A operacionalização de capacidades de gestão de biossegurança e bioproteção laboratoriais depende de conhecimentos de inteligência sobre ameaças potenciais que podem ser analisadas de maneira especializada por estruturas/equipes de inteligência laboratorial, enquanto elemento da inteligência em saúde.

A fração (ou frações) de inteligência laboratorial, portanto, pode servir como elo dos sistemas de biossegurança e bioproteção laboratoriais com os sistemas nacionais de inteligência, a exemplo do SISBIN, assim como com os sistemas de inteligência epidemiológica internacionais como o existente na OPAS e, mais recentemente, no polo (*hub*) da OMS, em Berlim/Alemanha.

A despeito da ausência de arcabouço brasileiro robusto sobre a monitorização de sistemas de biossegurança e bioproteção nos laboratórios brasileiros, a revisão dos documentos orientadores da AI permite concluir que houve iniciativas recentes de órgãos e programas, como o PANGEIA/ABIN, para criar mecanismos de monitorização específicos e com escopo próprio.

Percebe-se a preocupação de o SISBIN e a ABIN delimitarem o foco de atuação na área biológica para ameaças consideradas de maior risco, isto é, ameaças selecionadas, excluindo eventos biológicos de menor impacto.

De fato, é compreensível entender que não interessa ao único órgão federal exclusivamente voltado para a produção de conhecimento de inteligência, com sua limitação de recursos, materiais e humanos, preocupar-se com eventos biológicos de menor impacto, a exemplo de um derramamento de óleo diesel em uma estrada qualquer.

O SISBIN, portanto, reconheceu a necessidade de priorizar riscos e definir monitorização e assessoramento de inteligência laboratorial, na área de

inteligência em saúde, antes da definição brasileira sobre a eventual adoção de um sistema de agentes selecionados (similar ao estadunidense ou australiano ou de um arcabouço mais abrangente (similar ao canadense).

Estas duas opções, todavia, não são excludentes. É inclusive recomendável que o Brasil tenha uma regulação mais exigente para ABTS, mas disponha de um arcabouço de garantia de implementação de medidas efetivas de biossegurança e bioproteção que inclua outros laboratórios não selecionados.

Assim, haverá exigências crescentes que consideram primeiramente, de maneira mais cuidadosa, agentes e toxinas de alto e muito alto risco para eventos de disseminação intencional; e, em segundo lugar, mas não menos importante, um arcaboço regulatório e fiscalizador para laboratórios associados a riscos de biossegurança e bioproteção de riscos baixo e médio.

Entretanto, as iniciativas isoladas de monitorização de sistemas de biossegurança e bioproteção, enquanto não se tornam política robusta de Estado, tendem a ser mais facimente descartadas ou enfraquecidas em trocas regulares de gestão, como ocorreu a partir de 2019 com o PANGEIA/ABIN, que perdeu protagonismo com a mudança de gestão presidencial e gestão da ABIN.

Com a necessidade de revisão do PLANINT e, consequentemente, dos Planos de Inteligência orgânicos dos membros do SISBIN, há oportunidade de a ABIN ou restabelecer programas como o PANGEIA e aprofundar seus objetivos de inteligência em saúde; ou abrir mão destas suas atribuições (objetivos de inteligência) em nome do fortalecimento da inteligência laboratorial sob outra coordenação institucional.

Juntamente com a definição do arcabouço normativo que garanta a efetividade da gestão de biossegurança e bioproteção laboratoriais, é imprescindível discutir como se dará a obtenção de conhecimentos de inteligência laboratorial. E como deve ser garantida a troca de informações entre a área de saúde e segurança, para fins de definir riscos de bioproteção e a respectiva robustez, específica a cada ILS, de cada sistema de bioproteção laboratorial no Brasil.

Ressalte-se que a bioproteção laboratorial é um elemento central da segurança biológica (ou segurança da saúde) e deve ser integrada a ações e estratégias de biodefesa militar e a sistemas (ou subsistemas) de inteligência, a exemplo do SISBIN.

Esta integração com a defesa biológica pode se dar por meio de um sistema de inteligência que inclua setores das Forças Armadas que possuam ILS.

Neste sentido, a ideia de robustecer a inteligência laboratorial enquanto subsistema vinculado à inteligência da saúde, mediante integração também civil-militar, torna-se um cenário interessante para uma ação estatal efetiva na prevenção de riscos biológicos.

Por outro lado, há formas de pensar a estrutura de biodefesa como parte do processo de prevenção e resposta a eventos biológicos selecionados em território brasileiro e, diante desta competência ampliada para a atuação militar, o planejamento de planos de contigência ou protocolos multissetoriais de preparo e resposta deveriam levar estas competências em consideração.

A integração com os sistemas (ou subsistemas) de inteligência pode ocorrer sob coordenação ou não da ABIN, órgão central do SISBIN. Para que não haja perda de oportunidade, ministérios que supervisionam laboratórios direta ou indiretamente, como o Ministério da Saúde, Ministério da Agricultura e Pecuária e o Ministério da Educação (gestor indireto de laboratórios de universidades), podem se articular, independente do SIBSIN, para o estabelecimento de uma rede de inteligência laboratorial própria e que, posteriormente, poderia ser integrada ao SISBIN.

Esses três ministérios, em conjunto, possuem estrutura e orçamento muito superiores ao da ABIN e a de todos os demais membros da administração direta no SISBIN, de modo que não deveriam depender destes para iniciar uma estruturação de inteligência laboratorial[104, 105].

As frações de inteligência laboratorial não precisam, *a priori*, de enormes estruturas de pessoal e de recursos tecnológicos, seja em nível institucional seja em nível regulatório (estadual ou federal), mas requerem capacidade essencial de:

1. Coletar dados de fontes abertas e trocar conhecimentos de inteligência com outros órgãos que analisam ameaças biológicas no Brasil ou no exterior com repercussão no Brasil;
2. Produzir conhecimentos sobre as ameaças potenciais aos laboratórios, no contexto brasileiro;
3. Produzir conhecimentos para o monitoramento de risco (*risk assessment*);
4. Realizar análise de antecedentes de pessoal interno e externo (bioproteção de pessoas);
5. Realizar contrainteligência laboratorial (proteção de pessoas e proteção de dados e ciberproteção);

6. Articular P2R2 a eventos biológicos selecionados, de maneira integrada com órgãos de segurança e defesa (bioproteção intersetorial);
7. Aplicar avaliações de sistemas de redução de riscos de biossegurança e de bioproteção laboratorial (a exemplo do CIR); e
8. Produzir recomendações de bioproteção laboratorial, com base nas ameaças.

A contrainteligência laboratorial se faz necessária face a ameaças de espionagem e de recrutamento de pessoas, por exemplo. Restou evidente que a prática de espionagem é uma função expressa entre órgãos de inteligência estratégica estrangeiros, como a CIA e o SIS/MI-6[94, 95].

Desta forma, a contrainteligência laboratorial é uma medida de mitigação de riscos de bioproteção laboratorial e deveria fazer compor, com planejamento adequado, o conjunto de MRE de um laboratório estratégico.

Quanto à avaliação de antecedentes do pessoal de um laboratório, indivíduos estrangeiros ou nacionais residentes no exterior, a serem avaliados, podem não possuir um histórico documentado no Brasil e, em razão disto, o acionamento de órgão de inteligência estrangeiro ou de oficiais de inteligência estrangeiros podem ser necessários, de modo que as pessoas responsáveis por avaliação de antecedentes de estrangeiros deveriam estar, de algum modo, inseridas no SISBIN ou em sistema de troca de informações de inteligência de caráter similar ao SISBIN, a exemplo de frações específicas de inteligência laboratorial, em contato com oficiais de inteligência estrangeiros oficialmente acreditados no Brasil.

6.1.1.7 Inteligência laboratorial e o fortalecimento da cultura de BPL

A necessidade de criar frações voltadas para a produção de conhecimento de inteligência para, entre outras ações, subsidiar decisões associadas ao processo de monitoramento de biorriscolaboratorial aproximaria a gestão de B2L de profissionais ligados à segurança-inteligência.

Este fato é importante não apenas para o ganho de efetividade supracitado em várias análises apresentadas, mas para modificar o tratamento da

cultura de bioproteção laboratorial, que ainda é colocada em segundo plano quando comparada à centralidade da biossegurança laboratorial nas normas vigentes.

O exemplo da ABNT NBR 17069-1:2023, que conclui não existirem “elementos de bioproteção significativos” relacionados ao componente de infraestrutura laboratorial para o nível de biossegurança 1 (NB-1) reflete um grande desconhecimento do tema e a provável ausência de profissionais da área de segurança-inteligência nas discussões da CE responsável pela autoria da norma[18].

Assim pode-se deduzir em razão de a norma não referenciar nenhum documento sobre bioproteção, nem considerar a ideia de MCE (*core requirements*) na área de bioproteção.

Alem disso, ao afirmar que não há requisitos de BPL para um NB-1, contraria-se um princípio básico da B2L, que é a de interdependência entre as duas áreas, de segurança (*safety*) e de proteção (*security*), conforme revisado no tópico 2.1.2.2 e visualizado na FIGURA 1, a partir de considerações do LBM4 da OMS[22].

A falta de entendimento transdisciplinar sobre a relação entre bioproteção e biossegurança laboratoriais é tamanha que, mesmo citada entre as referências da ABNT NBR 17069-1:2023, as diretrizes do LBM4 são desprezadas no que tange à seção de bioproteção laboratorial deste importante manual.

Uma das áreas de interseção entre biossegurança laboratorial e BPL é o controle de acesso, que está incluso no componente de segurança/proteção física, que é o escopo principal da norma da ABNT citada.

Se ocorre um incidente de bioproteção em consequência de um acesso indevido a alguma área do laboratório NB-1, pode haver, por exemplo, um acidente laboratorial, porque o intruso poderia assustar, por exemplo, algum pesquisador e este se furar com uma matreial cortante.

Ou ainda poder-se-ia imaginar em um furto de materiais de limpeza no laboratório, que é um incidente de bioproteção, mas que compremete a esterilização adequada de superfícies laboratoriais.

Verifica-se, portanto, que uma infraestrutura mínima ou essencial quanto à proteção ao acesso indevido é fundamental para o efetivo controle de riscos de biossegurança, mesmo que estas MCE sejam descritas como medidas de bioproteção.

Ora, na norma, quando se afirma não existirem “elementos de bioproteção significativos” relacionados ao componente de infraestrutura laboratorial para o nível de biossegurança 1 (NB-1), ignora-se a ideia básica da

interconectividade e interdependência da bioproteção com a biossegurança laboratoriais.

Neste sentido, a norma da ABNT deveria ser revista completamente à luz transdisciplinar, com a participação de especialistas em segurança-inteligência laboratorial, com o fito de ganhar mais propriedade perante as diretrizes internacional de B2L.

O fortalecimento da cultura de bioproteção, portanto, e a própria necessidade de revisão de normas no sentido do promover a real integração das duas áreas, tal como preconizado pela OMS e pelos CDC, dependem da transdisciplinarização dos modelos de gestão de risco em B2L.

6.1.1.7 Análise de inteligência em saúde: risco de evento biológico de alto impacto no Brasil

A análise de percepção de risco global, segundo o FEM, aponta para um risco médio de evento biológico global, acidental ou intencional, em um horizonte de uma década a partir de 2024[5].

Tal medição de risco (*risk evaluation*) é obtida mediante a análise de chance de ocorrência – em que 9% dos especialistas entrevistados mencionam o risco como provável – e de uma avaliação média de impacto potencial – gradação de gravidade de 4,5 (quatro e meio) em um máximo de 7 (sete).

Inserida na dinâmica global, a medição de risco específica para o Brasil precisa considerar as chances e impactos próprios do país, bem como as características das ameaças locais (identificação de ameaças).

O Brasil tem histórico recente de ameaça expressa por indivíduos e grupos no sentido de provocar a disseminação intencional de agentes biológicos contra a sociedade brasileira. Considerando esta ameaça, não se pode afirmar que a probabilidade de ocorrência de um evento biológico selecionado no Brasil é muito baixa ou inexistente.

O histórico de ameaças expressas de ataque biológico por indivíduos e grupos, associado à média ou alta vulnerabilidade de biossegurança e bioproteção[ss]

[ss] A falta de coleta de informações de vulnerabilidades detalhadas nos laboratórios não permite precisar um nível correto e individualizado, mas, dada a ausência de requisitos essenciais na maior dos laboratóriosvisitados pelo PANGEIA/ABIN e analisados por MENDONÇA (2024)[3], depreende-se que o dificilmente o nível será inferior

– com ênfase para as vulnerabilidades de BPL - dos laboratórios selecionados brasileiros, resulta em probabilidade média para eventos biológicos selecionados.

Por sua vez, a probabilidade média associada a um impacto potencial que varia de baixo a muito alto resulta em risco variável de médio a alto – a depender do agente patogênico ou toxina - para um evento intencional, seja decorrente de uma ação de bioterrorismo, do crime organizado ou de ação criminosa individual.

Pode-se depreender dessa discussão que o nível de vulnerabilidades de B2L, com ênfase nas de bioproteção laboratorial, associado a um risco geral médio a alto de evento de bioproteção no Brasil permite afirmar que o país não realiza *compliance* adequada das principais normas multilaterais vinculantes, como a CPAB, a Resolução 1540/CSNU e o RSI.

Assim, o conceito de inteligência laboratorial proposto não apenas vem a complementar a inteligência em saúde, para garantir *compliance* efetivo das obrigações internacionais, mas também pode-se materializar na prática por meio do *PathoFinder Brazil®,* conforme detalhamento na discussão do próximo tópico, permitindo mapear laboratórios e pesquisas potencialmente sensíveis no contexto da B2L, segurança da saúde e biodefesa.

---

a médio. Avaliações de inteligência laboratorial mais pormenorizadas e individualizadas precisam ser empreendidas.

6.2 Desenvolvimento da ferramenta *PathoFinder Brazil®*

Com a finalidade de apoiar a necessária atuação preventiva/antecipatória da inteligência de Estado, face ao risco médio a alto, de um evento biológico selecionado intencional no Brasil, segundo critérios expostos nesta pesquisa, realizou-se a elaboração de um programa de computador que busca apontar pesquisadores e laboratórios precipuamente nacionais com pesquisas vinculadas a MBGC.

A OMS, por meio do *Guia para a implementação de requisitos regulatórios de biossegurança e bioproteção em laboratórios biomédicos* [tradução nossa][123] recomenda que, antes da implementação de medidas regulatórias, os países realizem uma avaliação nacional para conhecimento da infraestrutura laboratorial disponível e os materiais biológicos custodiados.

Por sua vez, o acompanhamento de bioameaças, tal como preconizado pela CPAB, pela Resolução 1540 e pelo RSI, pressupõe a identificação precoce de riscos e prevenção de eventos de acesso não autorizado a possíveis bioarmas, o que exige mapeamento adequado de laboratórios e instalações pelo Estado.

Com a ausência de regulamento de bioproteção que institua lista de notificação compulsória de manipulação/custódia de patógenos de grandes consequências e/ou de pesquisas de uso dual e de grande impacto, uma enorme quantidade de laboratórios e instalações tende a permanecer oculta para as autoridades brasileiras.

Trata-se de laboratórios ocultos, que, na verdade, podem ser um problema também para países que regulamentam tais aspectos, mas podem conviver com instalações que fogem às obrigações legais.

A identificação desses laboratórios é um trabalho de inteligência em saúde, mais especificamente de inteligência laboratorial. Para contribuir com esse trabalho, procurou-se desenvolver uma ferramenta que aglutinasse bancos de dados de acesso livre na rede mundial sobre pesquisas e pesquisadores, a fim de buscar possíveis laboratórios e pesquisas ocultas das autoridades.

Os resultados do uso dessa ferramenta, um programa de computador, serão tanto mais efetivaos quanto mais robusto o arcabouço regulatório de laboratórios biomédicos e pesquisas de uso dual.

6.2.1. Modo de funcionamento do *PathoFinder Brazil*®

O programa *PathoFinder Brazil*® é um programa de inteligência laboratorial[tt]. Em caráter experimental, está em sua primeira versão pós-registro. O uso é restrito a pessoas autorizadas mediante contato com os desenvolvedores.

Possui a tela inicial mostrada na **Figura 27.** No menu da esquerda, há alguns agentes biológicos passíveis de seleção e outros usados para exemplificação de pesquisa com a ferramenta. É possível marcar as caixas de um ou mais destes agentes[uu].

Abaixo, há duas réguas: a de principais pesquisadores (*top researchers)* e a de principais locais de pesquisa (*top institutions)*. Permitem escolher o número de pesquisadores e institutos/locais de pesquisa, em número de 1 a 10. A escolha será mostrada nas duas colunas da direta, omo resultados da busca.

Por último, no canto inferior esquerdo, há a opção de marcar o tipo de laboratório (*lab type*) entre NB-3 (BSL-3), NB-3A (ABSL-3) ou "Desconhecido" (*Unkonw*).

A alteração em qualquer parâmetro do buscador gera automaticamente a nova busca, alterando os resultados nas colunas da direita.

A primeira coluna – da esquerda para a direita -, com uma caixa laranja em sua borda superior, mostra o número total de pesquisadores que publicaram artigo ou obtiveram verba para pesquisa citando no resumo de seu artigo ou no projeto de pesquisa o patógeno que foi selecionado no buscador. Na coluna abaixo, é mostrado o ranqueamento dos pesquisadores com mais associações nas bases de pesquisa vinculadas com o patógeno selecionado.

A segunda coluna, mais à direita, possui uma caixa azul em sua borda superior, mostrando o número total de instituições ou outros locais de trabalho (ex. fundações, universidades, centros universitários etc.) mais associados ao termo de busca (**Figura 27**).

[tt] O *PathoFinder Brazil*® está temporariamente instalado no endereço eletrônico: https://procaddefesa.shinyapps.io/AppDatasetAllExtra/.

[uu] A adição de novos termos é possível e se dá mediante contato com o Prof. Elias Medeiros (eliasmedeiros@ufgd.edu.br).

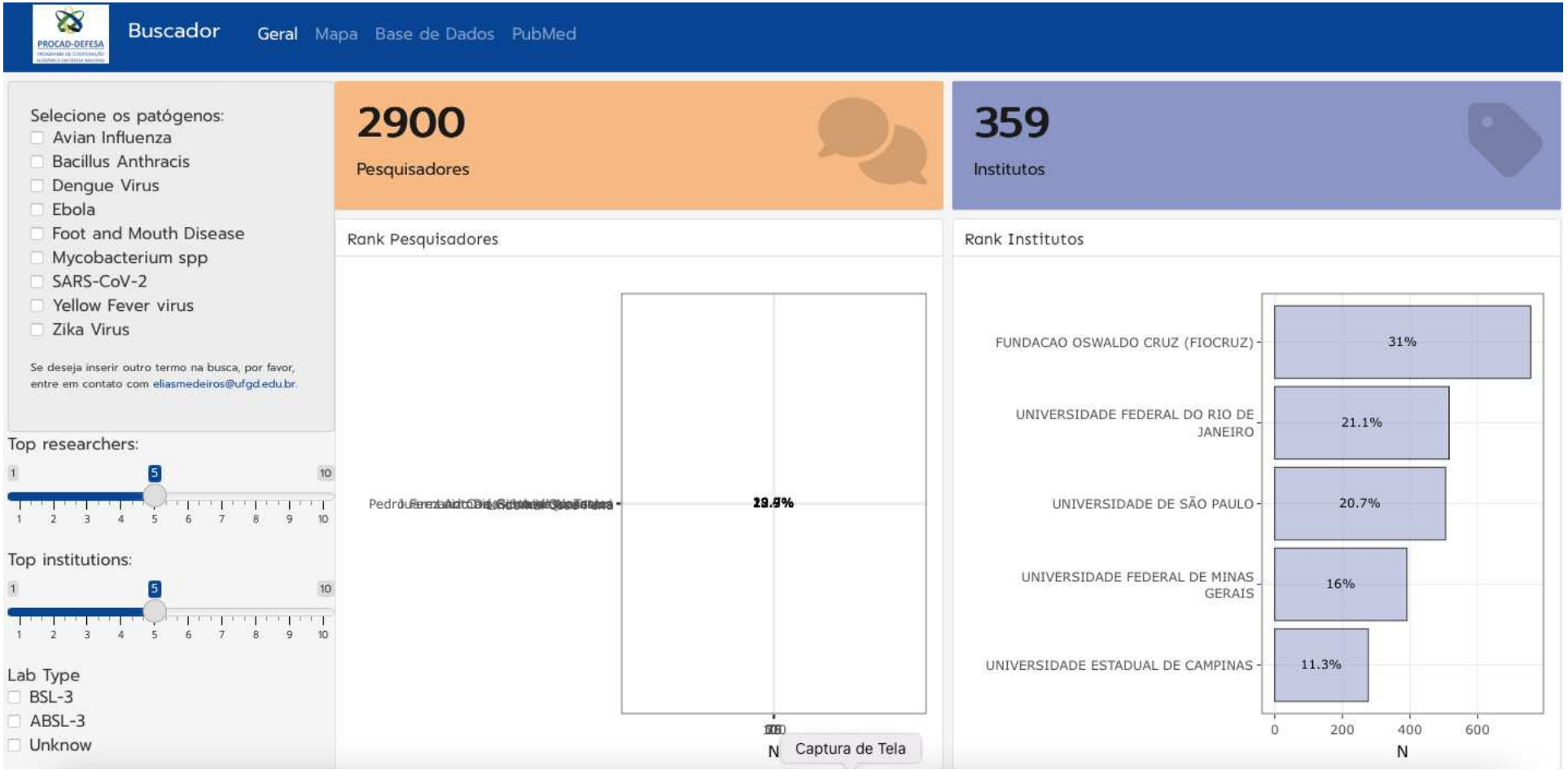


Figura 27 – *Tela inicial do programa PathoFinder Brazil. Disponível em: https://procaddefesa.shinyapps.io/AppDatasetAllExtra/ . Acesso em: 26 jan. 2025.*

Quando não houver seleção de patógeno, como no exemplo da **Figura 27**, as colunas mostram o total de pesquisadores nas bases utilizadas (dois mil e novecentos, em 26 jan. 2025); e o total de locais de pesquisa (359, em 26 jan. 2025).

A seleção exemplificativa de um patógeno, como o SARS-CoV-2, automaticamente modifica a quantidade de pesquisadores e de locais de pesquisa identificados para mil oitocentos e setenta e trezentos e dezesseis respectivamente (**Figura 28**).

Figura 28 – Exemplo de resultado de busca com a seleção do patógeno SARS-CoV-2 na versão experimental do *PathoFinder Brazil*®. Acesso em 26 jan. 2025.

O menu superior mostra as possibilidades de apresentação dos resultados, sendo a opção “Geral” a *default* (**Figura 29**).

Figura 29 – Opções do menu superior do *PathoFinder Brazil*. Acesso em 26 jan. 2025.

O submenu de seleção de patógenos foi programado para conter as nove entradas na versão inicial do programa. As escolhas foram aleatórias e contendo alguns patógenos selecionados para o FSAP, como vírs Ebola, e outros de menor risco de uso em ataques biológicos, como o vírus da Dengue (**Figura 30**).

Figura 30 – Opções de seleção de patógenos na versão experimental do *PathoFinder Brazil*®. Acesso em 26 jan. 2025.

Em versões futuras, não experimentais, seria possível programar um buscador em que o próprio usuário insira o termo de busca, não se restringindo a patógenos, mas com possibilidade de procurar resultados por “pesquisador” por “laboratórios” e por “pesquisas empreendidas” (ex. *gene editing*).

A visualização do ranqueamento de pesquisadores, baseado na escolha do número de ranqueados na tela inicial (opção Geral), dá-se em ordem decrescente do percentual de menções nas bases do *PathoFinder Brazil*® em relação a todas as menções obtidas para todos os pesquisadores (**Figuras 31 e 32**).

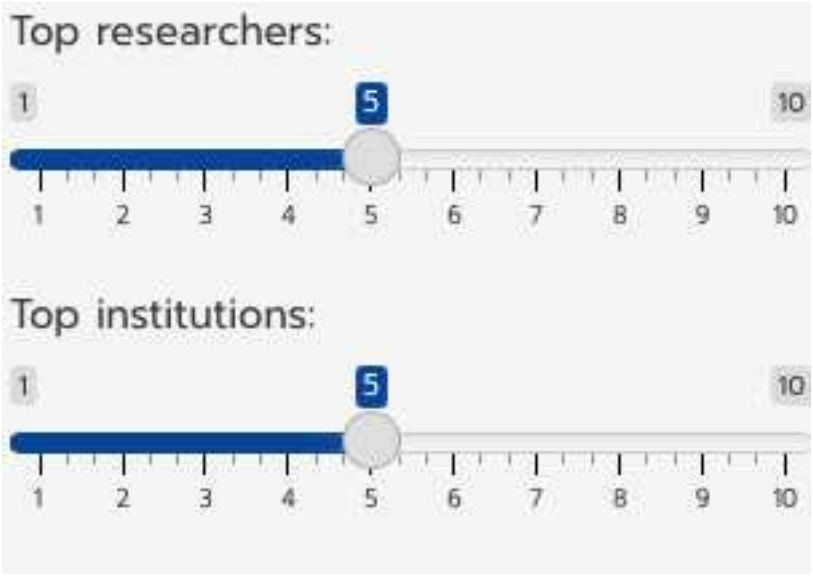


Figura 31 – Opções de seleção do número de pesquisadores e locais de pesquisa na versão experimental do *PathoFinder Brazil*®. Acesso em 26 jan. 2025.

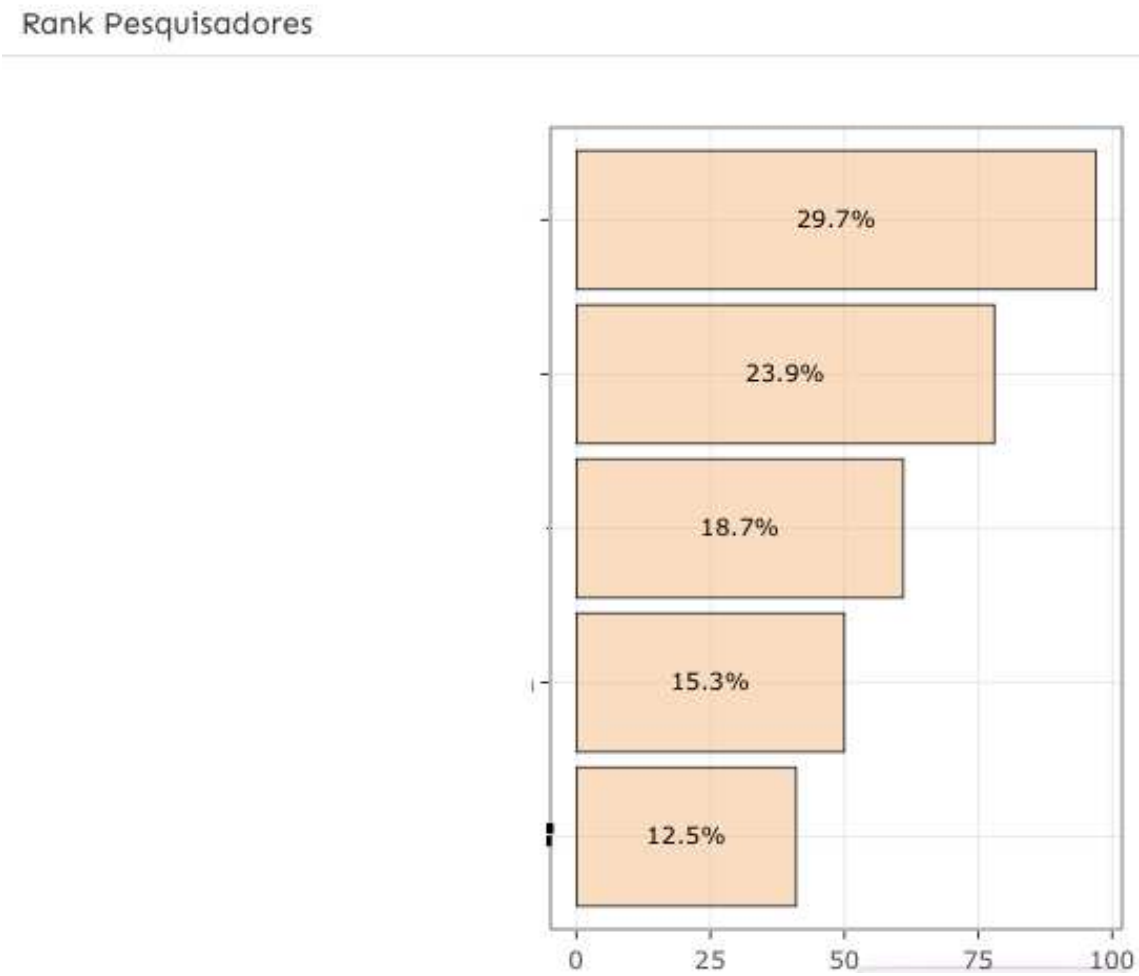


Figura 32 – Exemplo de ranqueamento de pesquisadores na versão experimental do PathoFinder Brazil®. Acesso em 26 jan. 2025.

A visualização do ranqueamento de locais de pesquisa, baseado na escolha do número de ranqueados na tela inicial (**Figura 31**), dá-se em ordem decrescente do percentual de menções nas bases do PathoFinder Brazil® em relação a todas as menções obtidas para todos os locais de pesquisa (**Figura 33**).

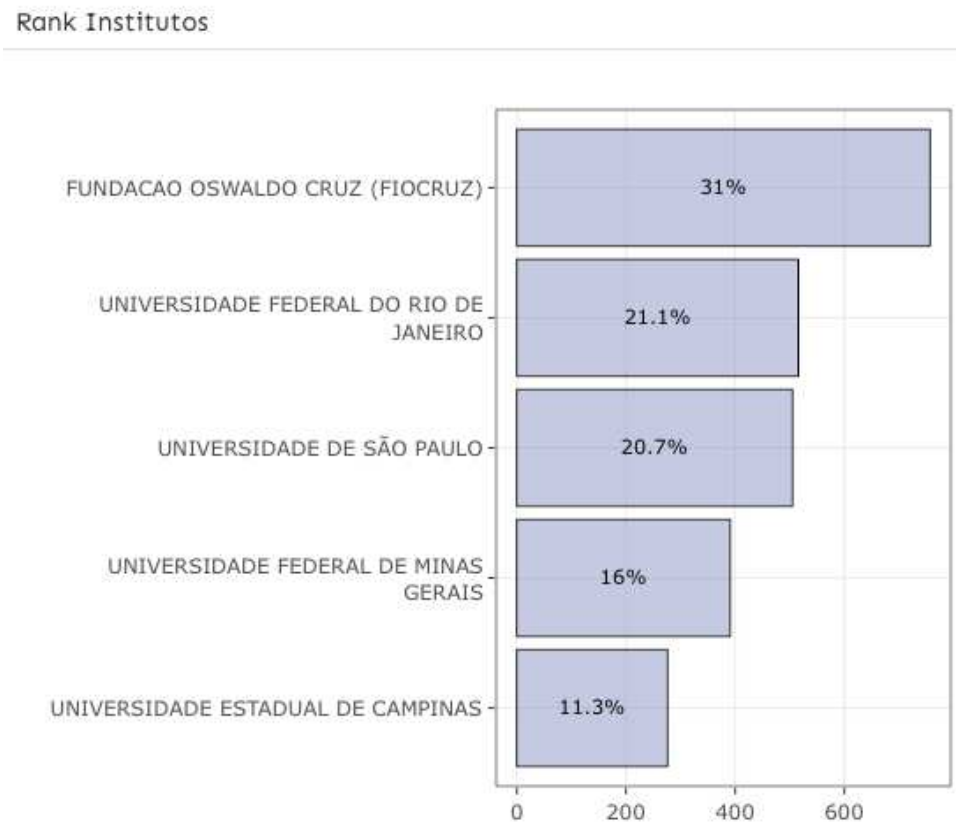


Figura 33 – Exemplo de ranqueamento de locais de pesquisa na versão experimental do *PathoFinder Brazil*®. Acesso em 26 jan. 2025.

Caso o usuário deseje visualizar a localização desses locais de pesquisa, pode clicar sobre a opção *Mapa* no menu superior. A tela automaticamente mostrará a localização dos laboratórios NB-3 e NB-3A (setas pretas com ilustração de casa vermelha ao centro das setas) registrados no PathoFinder Brazil®, associada à localização dos locais de pesquisa mencionados nos resultados da busca. Em um *zoom* menor, os resultados serão mostrados em aglomerado (**Figura 34**).

Figura 34 – Exemplo de visualização de mapa com os resultados de pesquisa. Em preto, os laboratórios NB-3 e NB-3A cadastrados. Em amarelo e verde, aglomerados dos locais de pesquisa referetes aos resultados de pesquisa. Versão experimental do *PathoFinder Brazil*®. Acesso em 26 jan. 2025.

Diminuindo-se a escala do mapa, por meio da aproximação do *zoom*, a localização dos locais de pesquisa será apresentada com precisão (setas azuis com ponto branco), em relação aos laboratórios NB-3 e NB3-A previamente resgitrados no programa (**Figura 35**).

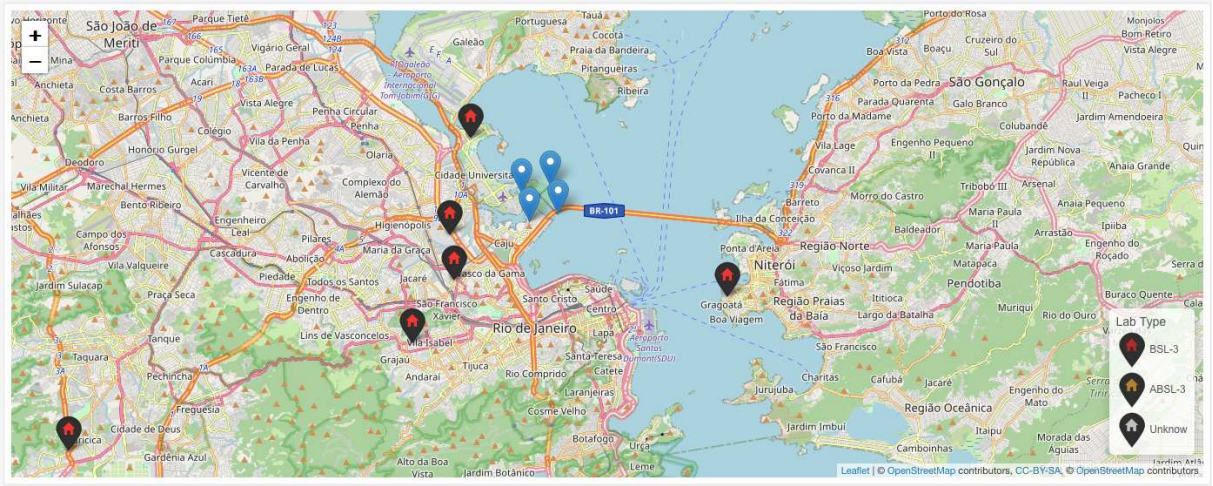
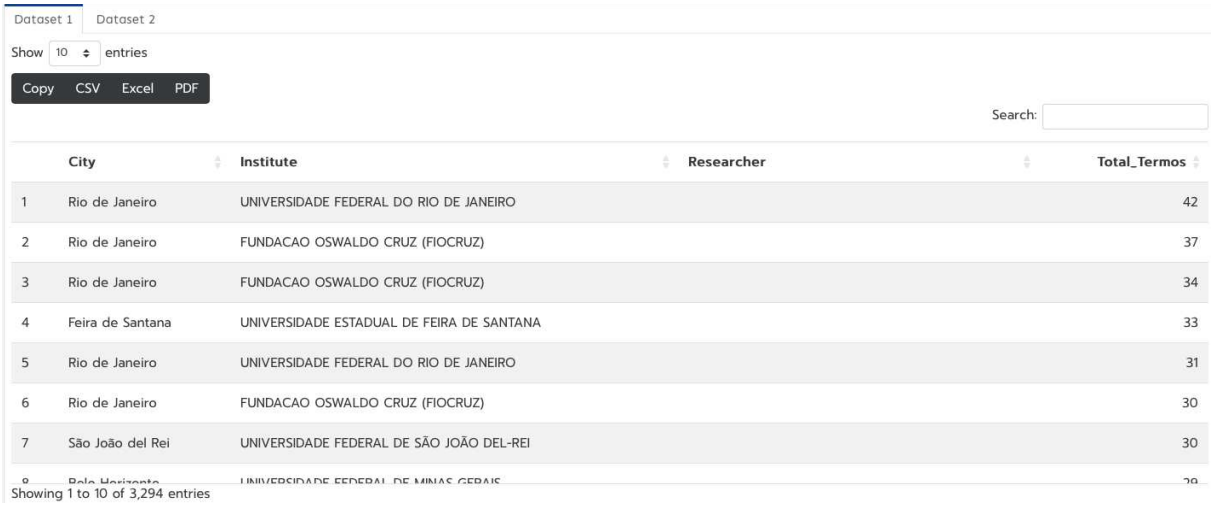


Figura 35 – Exemplo de visualização de mapa com os resultados de pesquisa. Em preto, os laboratórios NB-3 e NB-3A cadastrados. Em azul, os locais de pesquisa referentes aos resultados de pesquisa. Versão experimental do *PathoFinder Brazil*®. Acesso em 26 jan. 2025.

Se o usuário desejar fazer uma busca mais detalhada com os dados do resultado, pode-se clicar na opção *Base de Dados*. A tabela que será automaticamente apresentada (aba *Dataset 1*) mostra, em ordem decrescente, o total de menções (*Total_Termos*) de cada pesquisador em cada local de pesquisa. Se o mesmo pesquisador tiver associação com mais de um local de pesquisa, ele estará em tantas linhas diferentes quanto associações pesquisador-local de pesquisa (**Figura 36**).


Dataset 1 Dataset 2

Show 10 entries

Copy CSV Excel PDF

Search:

	City	Institute	Researcher	Total_Termos
1	Rio de Janeiro	UNIVERSIDADE FEDERAL DO RIO DE JANEIRO		42
2	Rio de Janeiro	FUNDACAO OSWALDO CRUZ (FIOCRUZ)		37
3	Rio de Janeiro	FUNDACAO OSWALDO CRUZ (FIOCRUZ)		34
4	Feira de Santana	UNIVERSIDADE ESTADUAL DE FEIRA DE SANTANA		33
5	Rio de Janeiro	UNIVERSIDADE FEDERAL DO RIO DE JANEIRO		31
6	Rio de Janeiro	FUNDACAO OSWALDO CRUZ (FIOCRUZ)		30
7	São João del Rei	UNIVERSIDADE FEDERAL DE SÃO JOÃO DEL-REI		30

Showing 1 to 10 of 3,294 entries

Figura 36 – Exemplo de ranqueamento de pesquisadores por locais de pesquisa (*Dataset* 1) na versão experimental do *PathoFinder Brazil*®. Os nomes dos pesquisadores foram apagados propositadamente. Acesso em 26 jan. 2025.

Nesta visualização, os dados podem ser copiados para a área de transferência (*copy*) ou exportados em formatos .CSV, .PDF ou .XLSX. E a busca pode ser refinada por meio do buscador (*Search*) no canot superior direito, em que se pode digitar qualquer nome de pesquisador.

Essa função de busca é importante, porque um pesquisador pode estar em primeiro lugar no ranqueamento da página inicial. Porém, se as menções forem vinculadas a vários locais de pesquisa, haverá uma fragmentação no número de menções, e o pesquisador estará em várias linhas em posição baixa na tabela *Dataset* 1. Fazendo-se busca do nome dele, mostra-se-ão todos os locais de pesquisa a que o pesquisador está vinculado.

Na aba *Dataset 2*, estará o detalhamento das menções por pesquisador. O usuário pode digitar o nome do pesquisador no campo *Search* e terá acesso ao título de cada artigo ou pesquisa em que foi encontrada menção ao patógeno buscado (**Figura 37**).

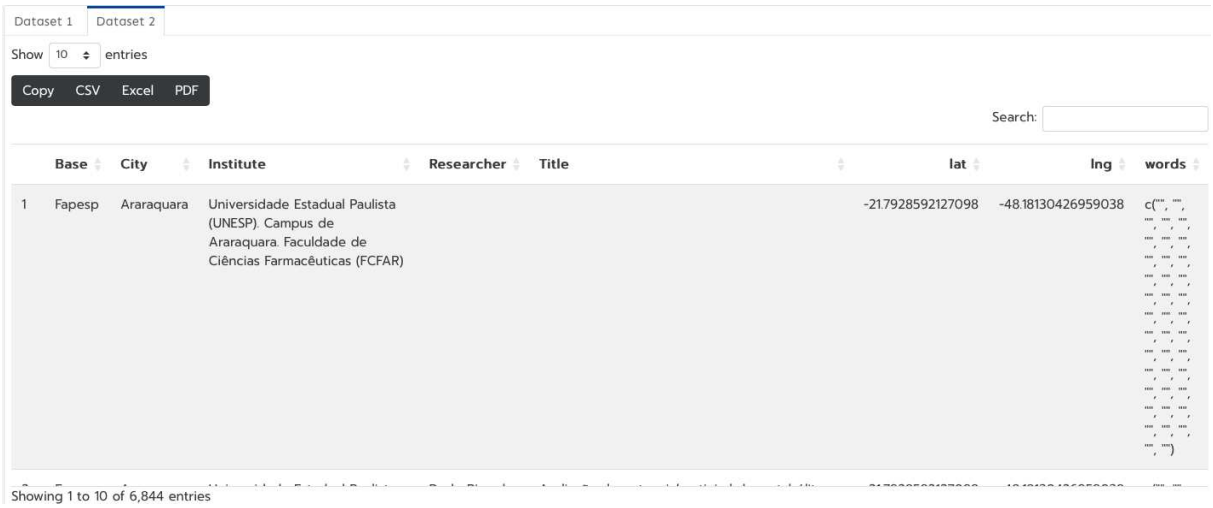


Figura 37 – Exemplo de detalhamento de menções (*Dataset* 2) na versão experimental do *PathoFinder Brazil*®. Os nomes dos pesquisadores e do título da pesquisa foram apagados propositadamente. Acesso em 26 jan. 2025.

Por fim, no campo *PubMed* no menu superior da tela incial, o usuário poderá escolher um nome de pesquisador (coluna da esquerda) e aparecerá o número de artigos publicados e indexados na base *PubMed* por ano e, de acordo com a presença ou não de menção ao patógeno selecionado (coluna do centro). Na coluna da direita, será apresentada uma *word cloud* das principais palavras-chave dos artigos do pesquisador (**Figura 38**).

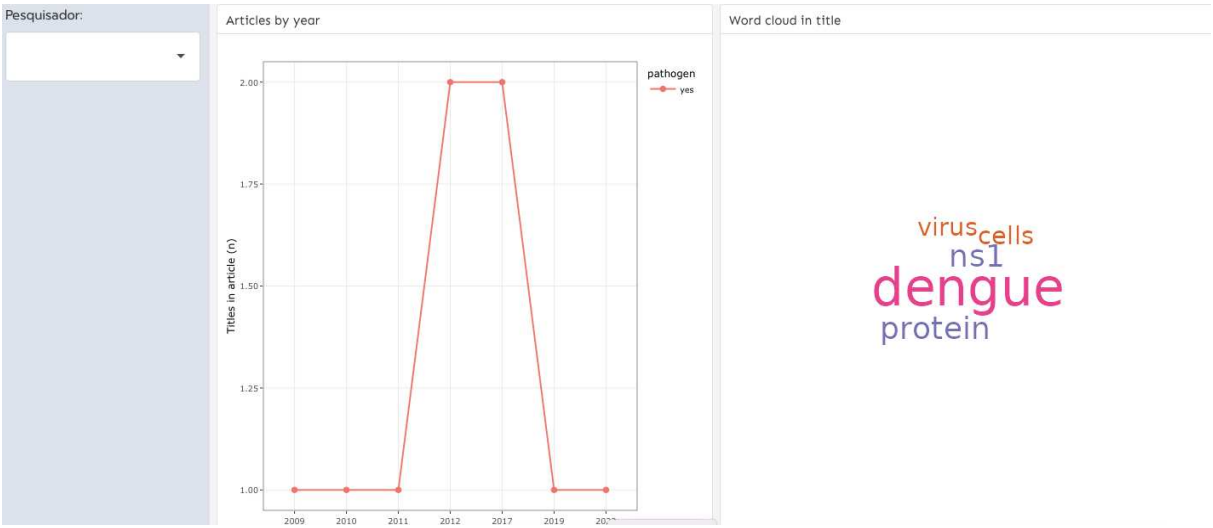


Figura 38 – Exemplo de busca no campo *Pubmed* da versão experimental do *PathoFinder Brazil*®. Os nomes dos pesquisadores foram apagados propositadamente. Acesso em 26 jan. 2025.

6.2.2 Estudo de caso com utilização do PathoFinder Brazil®

Para fins de demonstrar a utilidade do *PathoFinder Brazil®*, efetuou-se uma busca de pesquisadores e laboratórios que possivelmente utilizam *Bacillus anthracis*, um patógeno de grandes consequências e com alto potencial de uso em bioterrorismo[125].

O resultado apresentou quatorze pesquisadores potenciais e dez locais de pesquisa, com base nas bases do programa (**Figura 39**). Reitera-se que os nomes e locais apresentam potencial de serem vinculados à manipulação e custódia, respetivamente, de antraz. Entretanto, como os resultado se baseiam na presença das palavras *Bacillus anthracis* nos títulos e/ou resumos de artigos, projetos de pesquisa ou currículos dos pesquisadores é necessária triagem posterior para a confirmação da vinculação efetiva.

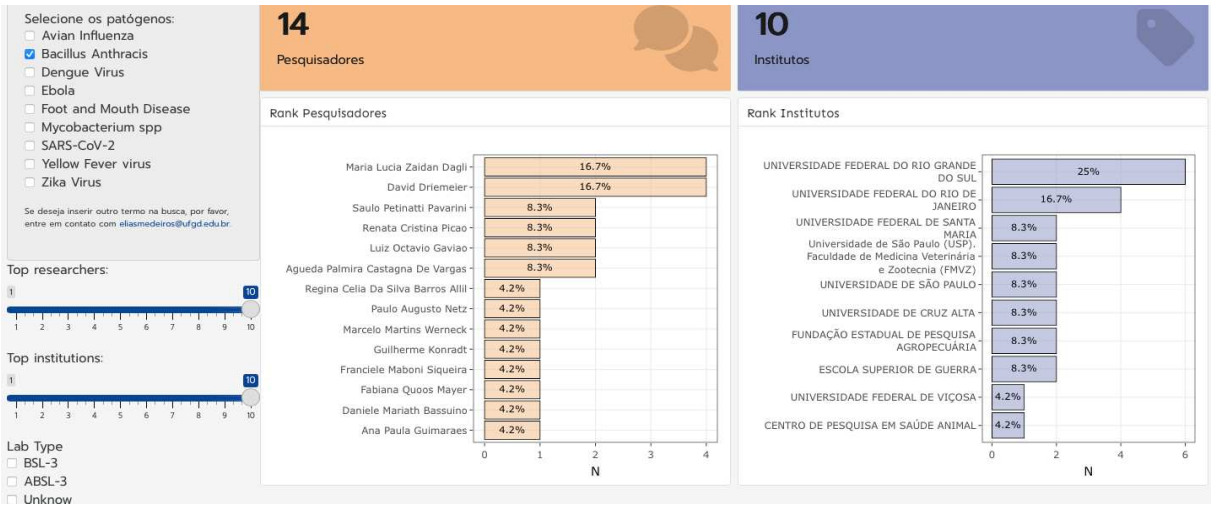


Figura 39 – Resultados gerais da busca com o agente *Bacillus anthracis* no *PathoFinder Brazil®*. Acesso em 26 jan. 2025.

Os quatorze pesquisadores encontrados estão vinculados a dez instituições: Universidade Federal do Rio Grande do Sul; Universidade de Rio de Janeiro; Universidade Federal de Santa Maria; Universidade de São Paulo (Faculdade de Medicina Veterinária); Universidade de São Paulo; Universidade de Cruz Alta/RS, Fundação Estadual de Pesquisa Agropecuária/RS, Escola Superior de Guerra, Universidade Federal de Viçosa/MG e Centro de Pesquisa em Saúde Animal/RS.

A análise da *Base de Dados - Dataset 1* - da pesquisa (**Figura 40**) permite verificar que uma mesma pesquisadora está vinculada a dois locais: USP e

FMVZ/USP, de modo que provavelmente essas duas entradas se refere ao mesmo local. Além disso, o pesquisador associado à Escola Superior de Guerra provavelmente não realiza pesquisa diretamente com o patógeno, uma vez que o local a ele associado não possui laboratório. Deste modo, restam locais de pesquisa com possíveis laboratórios que custodiam um patógeno selecionado.

	City	Institute	Researcher	Total_Termos
1	Porto Alegre	UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL	David Driemeier	2
2	Porto Alegre	UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL	Saulo Petinatti Pavarini	2
3	Rio de Janeiro	UNIVERSIDADE FEDERAL DO RIO DE JANEIRO	Renata Cristina Picao	2
4	Santa Maria	UNIVERSIDADE FEDERAL DE SANTA MARIA	Agueda Palmira Castagna De Vargas	2
5	São Paulo	UNIVERSIDADE DE SÃO PAULO	Maria Lucia Zaidan Dagli	2
6	São Paulo	Universidade de São Paulo (USP). Faculdade de Medicina Veterinária e Zootecnia (FMVZ)	Maria Lucia Zaidan Dagli	2
7		ESCOLA SUPERIOR DE GUERRA	Luiz Octavio Gaviao	2
8	Cruz Alta	UNIVERSIDADE DE CRUZ ALTA	Daniele Mariath Bassuino	1
9	Cruz Alta	UNIVERSIDADE DE CRUZ ALTA	Guilherme Konradt	1
10	Porto Alegre	UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL	Franciele Maboni Siqueira	1

Figura 40 – Resultados da análise do *Dataset 1* na busca com o agente *Bacillus anthracis* no *PathoFinder Brazil®.* Acesso em 26 jan. 2025.

A análise da *Base de Dados* - *Dataset 2* - da pesquisa (**Figuras 41 e 42**) permite refinar a busca e acessar o título das pesquisas e projetos vinculados ao antraz pelos pesquisadores encontrados e nos locais apontados pelo *PathoFinder Brazil®*,. Uma das informações obtidas é a de que o pesquisador da Escola Superior de Guerra produziu artigo sobre sítios de antraz na Antártica, de modo que nos leva à discussão sobre a possibilidade de que ele tenha utilizado sim laboratório que custodia o bacilo.

Neste caso, o seguimento da análise de inteligência laboratorial, iniciada com a busca do *PathoFinder Brazil®*,, precisaria coletar dados acessando diretamente tal pesquisa na tentativa de identificar eventual laboratório utilizado pelo pesquisador. Na hipótese de o artigo não detalhar esta informação, restaria entrevistar o pesquisador sobre seu trabalho.

Na realidade, não apenas esse pesquisador, mas todos os encontrado na busca mereceriam ação de *outreach* da fração de inteligência do órgão ou

autoridade reguladora, em razão da necessidade de confirmar o trabalho com o MBGC e averiguar a adequação de efetivo monitoramento de riscos nos laboratórios que custodiam o patógeno.

	Base	City	Institute	Researcher	Title	lat	lng
1	Fapesp	São Paulo	Universidade de São Paulo (USP). Faculdade de Medicina Veterinária e Zootecnia (FMVZ)	Maria Lucia Zaidan Dagli	Avaliação dos efeitos da toxina do Bacillus anthracis reengenheirada, ativada pela urokinase (UPA) e metaloproteinases (MMPs), para o tratamento de melanomas e de outras neoplasias de cães.	-23.569635574792	-46.73848409021802
2	Fapesp	São Paulo	Universidade de São Paulo (USP). Faculdade de Medicina Veterinária e Zootecnia (FMVZ)	Maria Lucia Zaidan Dagli	Avaliação dos efeitos da toxina do Bacillus anthracis reengenheirada, ativada pela uroquinase (uPA) e metaloproteinases (MMPs), em Hemangiossarcoma canino: estudos in vitro e in vivo	-23.569635574792	-46.73848409021802
3	Capes		CENTRO DE PESQUISA EM SAÚDE ANIMAL	David Driemeier	GENOME SEQUENCING OF TWO BACILLUS ANTHRACIS STRAINS: A VIRULENT STRAIN AND A VACCINAL STRAIN		
4	Capes		ESCOLA SUPERIOR DE GUERRA	Luiz Octavio Gaviao	PRIORITIZATION OF COLLECTION SITES FOR BACILLUS ANTHRACIS ISOLATION IN ANTARCTICA BY PROCESS OF HIERARCHICAL ANALYSIS		

Figura 41 – Resultados da análise do *Dataset 2* na busca com o agente *Bacillus anthracis* no *PathoFinder Brazil®.* Acesso em 26 jan. 2025.

5	Capes		ESCOLA SUPERIOR DE GUERRA	Luiz Octavio Gaviao	PRIORIZAÇÃO DE LOCAIS DE COLETA PARA ISOLAMENTO DE BACILLUS ANTHRACIS NA ANTÁRTICA POR PROCESSO DE ANÁLISE HIERÁRQUICA		
6	Capes		FUNDAÇÃO ESTADUAL DE PESQUISA AGROPECUÁRIA	David Driemeier	GENOME SEQUENCING OF TWO BACILLUS ANTHRACIS STRAINS: A VIRULENT STRAIN AND A VACCINAL STRAIN		
7	Capes		FUNDAÇÃO	Fabiana	GENOME		

	Base	City	Institute	Researcher	Title	lat	lng
			ESTADUAL DE PESQUISA AGROPECUÁRIA	Quoos Mayer	SEQUENCING OF TWO BACILLUS ANTHRACIS STRAINS: A VIRULENT STRAIN AND A VACCINAL		
8	Capes	Cruz Alta	UNIVERSIDADE DE CRUZ ALTA	Daniele Mariath Bassuino	BOVINE ABORTION BY A VACCINE STRAIN OF BACILLUS ANTHRACIS	-28.64427434250638	-53.60868647152397
9	Capes	Cruz Alta	UNIVERSIDADE DE CRUZ ALTA	Guilherme Konradt	BOVINE ABORTION BY A VACCINE STRAIN OF BACILLUS ANTHRACIS	-28.64427434250638	-53.60868647152397
10	Capes	São Paulo	UNIVERSIDADE DE SÃO PAULO	Maria Lucia Zaidan Dagli	EFFECTS OF ENGINEERED BACILLUS ANTHRACIS TOXIN ON CANINE OSTEOSARCOMA: IN VITRO STUDIES.	-23.56122480965239	-46.73075203007822

Figura 42 – Resultados da análise do *Dataset 2* na busca com o agente *Bacillus anthracis* no *PathoFinder Brazil®* (continuação). Acesso em 26 jan. 2025.

Verifica-se que o programa permite uma priorização do trabalho de *outreach* e fiscalização/auditoria em instalações laboratoriais biomédicas. Entre centenas de laboratórios universitários, por exemplo, o programa nos deu nove

deles que precisam prioritariamente de visita de inteligência laboratorial para coleta de informações sobre a eventual custódia de ABTS/MBGC.

Desta forma, o *PathoFinder Brazil®* aumenta a eficiência do trabalho estatal e gera economia de tempo e recursos. Ao prover oportunidade, o programa se torna relevante e estratégico para as capacidades laboratoriais nacionais, uma vez que antecipar e prevenir biorriscos laboratoriais são ações que devem ser oportunas.

Ações de *outreach* são sugeridas, a partir desses resultados com entrevistas de pesquisadores para a coleta de informações sobre eventuais laboratórios que custodiam MBGC, porque não existe, no Brasil, autoridade de gestão de biorriscos com poder de auditoria e fiscalização.

Na eventualidade do estabelecimento de tais instâncias, a ferramenta de inteligência laboratorial *PathoFinder Brazil®* também servirá para a realização de supervisões de atendimento de requisits regulatórios sobre a gestão de B2L no país.

6.2.3 Utilidade do *PathoFinder* como ferramenta de inteligência laboratorial

O programa de computador PathoFinder Brazil® serve como uma ferramenta de inteligência em saúde, mais especificamente de inteligência laborartorial, na medida em que permite a identificação de laboratórios, ocultos ou não, com possibilidade de manipular ABTS ou agentes e toxinas de interesse para a monitorização no Brasil.

Ele pode ser descrito como um programa de inteligência operacional e tática que serve grandemente para identificar pesquisadores e laboratórios passíveis de serem objeto de ações, no mínimo, de *outreach* sobre arcabouço regulatório e gestão de B2L no Brasil.

Por isso, a ferramenta apresenta potencial significativo de auxiliar na implementação do PANGEIA/ABIN ou de ações e programas governamentais similares, de inteligência em saúde e laboratorial. Seu uso permite o mapeamento de instalações que custodiam MBGC e/ou que pesquisam PAI/PGC.

A inexistência de um sistema de notificação compulsória da custódia de patógenos selecionados torna ainda mais relevante o uso de ferramentas como o

PathoFinder Brazil® como ponto de partida para uma ação fiscalizadora preventiva de ILS.

O programa permite a antecipação de risco ao fornecer uma visão abrangente do panorama acadêmico, destacando a distribuição de projetos, pesquisadores e instituições nas plataformas CNPq, FAPESP e CAPES, com a possibilidade de filtrar instituições, pesquisas e pesquisadores com potencial de manipulação de agentes biológicos selecionados.

O *dataset* final e o aplicativo *Shiny* desenvolvido oferecem uma ferramenta valiosa para explorar e visualizar esses dados de maneira interativa. Além disso, a integração bem-sucedida com o *PubMed* amplia a utilidade da busca, permitindo a análise de artigos publicados pelos pesquisadores identificados.

O processo de registro da ferramenta (aplicativo *Shiny*) junto ao Núcleo de Inovação Tecnológica da UFV demonstra o comprometimento com a inovação e a proteção intelectual associada a essa pesquisa. Assim, os resultados obtidos no âmbito da presente tese proporcionam uma ferramenta que contribui com a gestão efetiva de riscos biológicos, enfocando especialmente o monitoramento automatizado.

Há possibilidade de a ferramenta servir para a constituição de um observatório de risco biológico, na forma de um projeto de pesquisa ou de extensão universitário, ou de ser utilizada por órgãos do Sistema Brasileiro de Inteligência (SISBIN), para fins de auxílio nas atividades de inteligência de Estado do PANGEIA/ABIN ou de ações e medidas similares.

Em que pese as duas opções de uso serem razoáveis, poder-se-ia ganhar efetividade se a ferramenta pudesse ser implementada em fração de inteligência laboratorial em órgão competente para operacionalizar medidas de bioproteção laboratorial, bem como antecipar eventos de bioproteção em laboratórios no Brasil.

Mesmo que o Brasil venha a implementar, como julgado imprescindível, um sistema de notificação compulsória de ABTS, ferramentas como a PathoFinder Brazil® permitirão manter uma fiscalização preventiva, isto é, antecipatória, do sistema de notificação, além de nortear ações de formação de rede de contatos e *outreach*

Ferramentas de detecção precoce de risco e de direcionamento de recursos de inteligência laboratorial como a PathoFinder Brazil® se coadunam com o

disposto, por um lado, na PNI e na ENINT do SISBIN; e, por outro lado, na Estratégia de Inteligência Epidemiológica da OPAS/OMS.

Ademais, contribuem com o *compliance* a normas multilaterais vinculantes, como a RSI, CPAB e Resolução 1540. Desta forma, seu uso e aprimoramento devem ser incentivados por áreas de inteligência de Estado tanto quanto por órgãos de ciência e tecnologia, por meio de parcerias estratégicas.

Existe enorme potencial de aprimoramento da ferramenta *PathoFinder Brazil®* com tecnologias de aprimoramento e outras vinculadas à inteligência artificial.

A automação das análises de risco a partir dos *datasets* do PathoFinder Brazil® é promissora, no sentido de ganho de produtividade e de efetividade das buscas de instalações laboratoriais ocultas e de pesquisadores de interesse para o Estado, por exemplo.

Não se pode ignorar ainda a possibilidade de ampliação do uso do *PathoFinder Brazil®* para a busca de dados sobre produtos e tecnologias de uso dual, assim como de pesquisadores que utilizam ou trabalham com eles.

Desta forma, podemos ressaltar ao menos três aplicações e aprimoramentos potenciais da ferramenta para uso em segurança em saúde e biodefesa:

1. Aprendizado de Máquina (*Machine Learning*): o *PathoFinder Brazil®* pode identificar padrões em publicações acadêmicas e bancos de dados, antecipando tendências em pesquisas de alto risco;
2. Análise Preditiva: com base em dados históricos, o sistema pode prever áreas de risco emergentes, facilitando o direcionamento de esforços de fiscalização e biossegurança; e
3. Automação da Inteligência Laboratorial: redução da carga manual na análise de grandes volumes de dados, tornando a segurança em saúde e biodefesa mais eficientes e efetivas.

O *PathoFinder Brazil®* também pode ser relacionado com estratégias nacionais e internacionais de biodefesa. Neste sentido, a ferramenta poderia ser enquadrada dentro de um arcabouço estratégico, com possíveis conexões com diferentes atores da área.

Destacando-se ao menos três das conexões estratégicas possíveis:

1. Sistemas de Inteligência Nacional (SISBIN, ABIN, MS, MAPA, ANVISA) - O *PathoFinder Brazil®* pode ser integrado a estratégias de inteligência laboratorial, conforme supracitado;
2. Regulações Internacionais (RSI-OMS, BWC, *Global Health Security Agenda* - GHSA) - O sistema pode fornecer dados relevantes para atender exigências de monitoramento de ameaças biológicas; e
3. Forças de Segurança (Polícia Federal, Forças Armadas, INTERPOL, EUROPOL) - Auxílio em ações de contraterrorismo biológico e prevenção ao bioterrorismo.

Mais estudos voltados para outros temas de inteligência em saúde merecem ser realizados, no sentido de compreender outras aplicações da ferramenta para interesses os mais diversos. Ferramentas como o *PathoFinder Brazil®* têm potencial significativo para fortalecer a governança de gestão de biorriscos, sendo um diferencial na detecção precoce de riscos e permitindo análises mais refinadas e preditivas.

6.3 Aprimoramento e adaptação de modelo de avaliação de sistemas de controles de riscos de bioproteção laboratorial (*Checklist RAMPA* - CIR)

O Checklist RAMPA (CIR) foi estruturado para avaliar riscos em bioproteção laboratorial, biodefesa e ciberbioproteção, reconhecendo a interseção entre ameaças biológicas e vulnerabilidades digitais, que podem comprometer a segurança de instalações e dos agentes biológicos.

A OMS reconhece, conforme supracitado, que a implementação de normas e supervisão (*oversight*) de bioproteção laboratorial (BPL) está globalmente muito aquém daquelas voltadas para a biossegurança laboratorial[22, p. 45].

Ferramentas que contribuam para o planejamento e implementação de controle de riscos de bioproteção são importantes para a busca da compensação desta insuficiência normativa da BPL. No Brasil, especificamente, carecem análises sobre esta discrepância, e o foco tem sido a criação de capacidade de biossegurança[3], como ocorre há décadas na maioria dos países[22].

A mais abrangente estudo sobre os laboratórios brasileiros de alta contenção foi empreendido por MENDONÇA (2024)[3, p.251]. Percebe-se, por exemplo, na análise pelo autor da implementação brasileira dos sete passos da OMS, a ausência de menções a aspectos voltados para as ações e competências exclusivas do setor segurança-inteligência.

Não há menção às atividades do PANGEIA/ABIN na análise das competências de instituições nacionais (Passo 3). Nem as deficiências do arcabouço normativo, apontadas com muita propriedade pelo autor, refletem especificamente a dificuldade do estabelecimento de canais para a troca de informações entre setores de segurança-inteligência com os órgãos gestores laboratoriais, entre outras ausências relevantes para a análise das capacidades de gestão em B2L brasileiras.

Reconheça-se, entretanto, a menção adequada, supracitada, no passo 6 (*Estabelecimento de Redes de Integração e Parceiras Internacionais*) de que "representantes de agências de segurança[vv], como a ABIN, deveriam ser incluídos [*nas comissões nacionais de diferentes ministérios*] para promover intergração

[vv] O autor cita a ABIN como órgão de segurança, mas a presente tese prefere considerar como uma categoria à parte, isto é, inteligência, conforme explicitado na Introdução da pesquisa.

intersetorial para a prevenção e resposta a eventos biológicos [tradução e grifo nossos]"[1, 3].

Ressalte-se que as menções à importância da inclusão da inteligência, no processo de gestão de B2L, analisado por MENDONÇA (2024), são resultado da citação de dois pesquisadores Oficiais de Inteligência da ABIN, de modo que se destaca a importância de o tema da integração saúde-segurança-inteligência vir à tona com a participação transdisciplinar de especialistas e pesquisadores das três áreas.

De fato, as lacunas encontradas em documentos multilaterais, como o LBM4 e o GBP2 da OMS, e nacionais, como a NBR, devem refletir tão somente a ausência de transdisciplinaridade adequada na autoria e revisão destes documentos. Por isso, é importante que o Brasil, com a expertise de bioproteção e experiência prática da atuação da AI em integência laboratorial possa, por meios oficiais (com órgãos governamentais intermediadores) ou não oficiais (com instituições de caráter privado, como a SB3), participar da concertação global sobre requisitos e diretrizes de implementação de um arcabouço de gerenciamento de biorriscos laboratoriais.

Aém disso, a expertise adquirida pela ABIN na participação em ações de inteligência laboratorial devem ser multiplicadas, formando mais e mais especialistas neste tema tão relevante para a gestão abrangente de B2L, que não ignore aspectos essenciais de bioproteção laboratorial.

Vale enfatizar que os conceitos nas diferentes abordagens e modelos de gerenciamento de biorrisco variam segundo os autores, conforme revisto no Modelo AME e na abordagem ABRE. Apesar das discrepâncias, que podem parecer maiores pelas dificuldades de tradução à língua portuguesa de diversos termos em inglês, as ideias trazidas como passos para um adequado *risk assessment* são basicamente as mesmas e, independente do método utilizado, tende a dar resultados semelhantes, se realizadas de maneira efetiva, seja na forma do modelo supracitado, seja na forma da abordagem mencionada.

Destaca-se que a escolha da abordagem de passos ou elementos de determinada abordagem de gestão, monitoramento ou avaliação de risco não é limitante para a governança efetiva de riscos de bioproteção laboratorial.

Dito isto, fatores limitantes nos enfoques dos principais documentos recomendatórios, na pespectiva da bioproteção laboratorial, existem e merecem ser evidenciados e discutidos.

A análise da bibliografia revisada sobre o ciclo de monitoramento de risco (*risk assessment*) permite perceber o quanto os documentos recomendatórios são focados principalmente na perspectiva da biossegurança laboratorial, deixando lacunas importantes se analisados na perspectiva da bioproteção laboratorial.

O LBM4, por exemplo, quando delatalha as considerações-chave (*key considerations*) de cada passo do *framework* de monitoramento de risco (*risk assessment*) não menciona aspectos específicos de bioproteção[16, pp. 7-8].

No primeiro passo ("coletar informações"), não há menção à colea de informações sobre indivíduos ou grupos com interesse em realizar uso criminoso de MBGC/PGC. Ora, estes dados são fundamentais para a caracterização dos riscos no passo 2 ("medir os riscos")[16, p.7].

Seria de se esperar que esta lacuna fosse suplantada no documento de apoio específico sobre o monitoramento de risco da OMS, publicado no mesmo ano do LBM4, entretanto as lacunas persistem.

A maior parte da monografia específica consiste em mostrar exemplos de monitoramento de riscos sistematizados por meio de modelos (*templates*) sugeridos. No anexo 5, há um modelo longo preenchido com um exemplo de pesquisa de influenza[63, p.71].

O laboratório hipotético citado manipula vírus selvagem de *influenza* aviária tipo A, que pode infectar humanos, segundo o próprio documento da OMS, por via respiratória. No passo 2, o modelo solicita que sejam descritas "como a exposição e/ou disseminação pode ocorrer" [63, p.71].

Ora, apesar de o documento não mencionar no seu exemplo, pode-se vislumbrar que uma forma de disseminação é a intencional (indivíduos que desejem afetar uma produção aviária, por exemplo, disseminando vírus de influenza em uma granja para condumo interno ou empresa exportadora de aves de corte).

O foco do exemplo, entretanto, é voltado para a identificação de possibilidades de exposição por mal uso de EPI e realização de procedimentos laboratoriais de maneira incorreta, isto é, voltado para a identificação de cenários de riscos de biossegurança. A bioproteção continua relegada a segundo plano ou simplesmente esquecida.

A análise sobre a chance de exposição é focada na titulação de vírus ou tamanho do volume manipulado, quando da obtenção dos estoques virais, enquanto cenários de acesso indevido não são mencionados.

A lacuna é apenas vagamente resolvida quatro anos depois desta publicação, em 2024, quando o GBL2 é publicado com recomendações específicas e mais detalhadas sobre bioproteção laboratorial[22].

Porém, as recomendações práticas de como efetuar o monitoramento de riscos de bioproteção (*biosecurity risk assessment*) ou exemplos de preenchimento dos modelos de monitoramento de risco com ameaças ou riscos de bioproteção não existem, apesar do reconhecimento de que o "os riscos de biossegurança e bioproteção devem ser sempre considerados em conjunto",

> *"Entretanto, é importante definir e estabelecer um processo de monitoramento de risco sistemático e específico para a localidade dentro de uma instituição, especialmente para o trabalho com material de grande impacto. Além disso, a bioproteção laboratorial visa a lidar com riscos e ameaças laboratoriais distintas de exposição ou disseminação acidentais."*[22, p.19]

A partir do reconhecimento desta lacuna, buscou-se focar num dos aspectos do ciclo de monitoramento de risco de biossegurança e bioproteção laboratoriais para contribuir para complementá-la.

A ideia do CIR é partir da análise dos componentes de um sistema de medidas de controle de riscos de bioproteção laboratorial para se chegar a uma boa avaliação do sistema, que pode ser chamado didática e mais resumidamente como sistema de bioproteção laboratorial.

Conforme revisado, a implementação de medidas de controle de riscos efetivas pressupõe uma perspectiva cíclica do PCFA em todas as fases do monitoramento de risco, inclusive a coleta adequada de riscos[13, p.40; 22].

Deste modo, entende-se que é importante verificar se há coleta adequada de informações para avaliar se a implementação das medidas de controle é baseada em evidências continuamente coletadas e atualizadas.

Uma primeira versão do CIR consolidado está no Apêndice B (retirado da versãopublicada da tese por razões de sigilo, mas que será aprimorado para posterior publicação em periódico). Ele possui uma seção importante que busca avaliar o processo de monitoramento de risco (*risk assessment*) em si e serve de estrutura para a implementação das medidas de controles avaliadas pelo *checklist*.

6.3.1 Novos componentes de controle de riscos de bioproteção laboratorial ou sistema ampliado de controle de riscos de BPL

Os cinco componentes clássicos da bioproteção laboratorial[2], conforme revisados no item 2.2.1.3 acima, mostram-se insuficientes para a implementação adequada de um sistema efetivo de bioproteção laboratorial no contexto das ameaças e das especificadades culturais e institucionais encontradas no Brasil.

Tal insuficiência deriva grandemente da falta de integração adequada entre a área laboratorial (e de saúde) com a área de segurança-inteligência. Neste contexto, há necessidade de incluir expressamente e enfatizar medidas de integração como parte de um componente específico de bioproteção laboratorial.

Além disso, os modelos da década de 2010 ainda não trazem o elemento da informatização dos processos laboratoriais e outros avanços cibernéticos que podem caracterizar bio-ameaças (*biothreats*) contemporâneas.

Deve ser enfatizado que os riscos laboratoriais na atualidade, portanto, não são apenas físicos e biológicos, mas também digitais, necessitando integração com ciberbioproteção para a garantia de uma proteção e segurança abrangentes.

Deste modo, verfica-se importante lacuna quanto às recomendações de medidas de ciberbioproteção (*cyberbiosecurity*), de modo que este elemento precisa ser enfatizado em novos modelos transdisciplinares de gestão de biorrisco laboratorial.

Enfatiza-se ainda que a análise do LBM4 e outras normativas, mesmo que específicas para a bioproteção laboratorial, como o GBL2, embora recentes (2020 e 2024, respectivamente) não trazem considerações sobre requisitos essenciais (*core requirements*) de bioproteção laboratorial[16, 22].

Tanto as MCE quanto MCR e MCM, exemplificadas pelas últimas diretrizes/manuais da OMS, são voltadas para a redução de riscos de biossegurança laboratorial, omitindo conceitos que poderiam ser extremamente relevantes para a implementação de medidas de controle de riscos de bioproteção laboratorial.

Ora, dadas as ameaças presentes em cada localidade, a serem identificadas e medidas conforme supracitado, com intercâmbio informacional intersetorial com os órgãos de frações de segurança-inteligência, há que se falar em medidas de bioproteção essenciais.

Neste sentido, propõe-se o esquema abaixo (**Figura 43**) com medidas necessárias de controle do risco de bioproteção laboratorial basdo na chance e impacto de eventos de biorrisco.

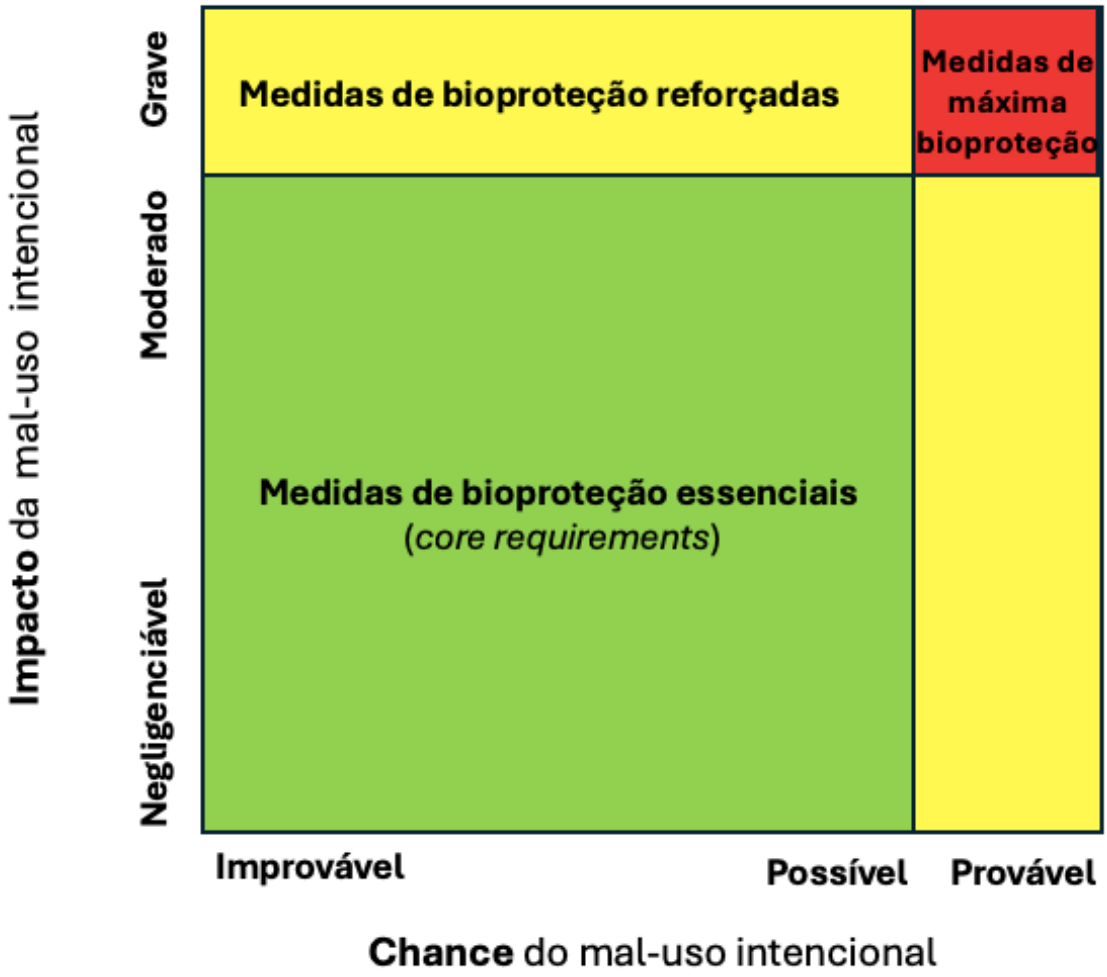


Figura 43 – *Medidas necessárias de controle do risco de bioproteção laboratoriais baseadas na chance e impacto de eventos de biorrisco (*elaborado pelo autor).

Não apenas os conceitos de MCE, MCR e MCM estão limitados para a aplicação no gerenciamento de bioproteção laboratorial. Há ausências significativas na abordagem para bioproteção quanto às estratégias de redução de risco da OMS.

A descrição das estratégias pelo LBM4, por exemplo, de eliminação e isolamento fala em “eliminar o perigo” e “isolar o perigo”, omitindo ações para eliminar e isolar “ameaças”[16, p.18].

Sabe-se que o conceito de perigo está mais intimamente ligado a biossegurança, enquanto o conceito de ameaça está mais próximo da ideia de bioproteção. Assim, ao não refletir sobre as estratégias de redução de riscos voltadas para ameaças (e não apenas para os perigos), omite-se a exemplificação necessária para facilitar a implementação de medidas voltadas para a redução de risco de bioproteção.

Assim, a estratégia de “proteção” para redução de risco tem como ações exemplificadas “usar EPI” e “vacinação de pessoal”, mas nenhuma ação para mitigar riscos de bioproteção[16, p.18]. E estas ausências não são superadas no GBL2, infelizmente.

Resulta desta análise de lacunas em diretrizes e recomendações internacionais a proposição original de um sistema de medidas de controle de risco de bioproteção laboratorial em que haja um sexto componente específico para tratar de aspectos de interseccionalidade na prevenção e na resposta a um evento de mal-uso intencional de MBGC e PAI, além da incorporação da ciberbioproteção como outro elemento central no modelo.

Reitera-se que, desde o LBM3, quando a OMS primeiramente detalhou a necessidade de um programa específico de bioproteção das instalações laboratoriais, afirma-se a importância de considerar neste programa a participação de órgãos de segurança (*law enforcement agencies*).[35, pp.47-48]

Propõe-se, portanto, para o planejamento e implementação de programas de gestão de biossegurança e bioproteção laboratoriais no Brasil (e em países com maiores desafios de integração saúde-segurança), a utilização de um sistema de medidas de controle de riscos bioproteção laboratorial ampliado, com os seguintes elementos-chave (ou componentes centrais):

1. Bioproteção das instalações;
2. Bioproteção de pessoal;
3. Bioproteção de materiais;
4. Bioproteção do transporte;
5. Bioproteção de dados e ciberbioproteção; e
6. Bioproteção intersetorial.

O conjunto destes seis componentes, que interagem entre si e se complementam, passariam a formar um modelo transdisciplinar de “sistema de medidas de controle de risco de bioproteção ampliado” ou, mais resumidamente, “sistema de bioproteção laboratorial ampliado”.

As medidas executadas em cada componente, isoladamente, em tese, configuram as partes do sistema de medidas de controle de risco de bioproteção (**Figura 44**).

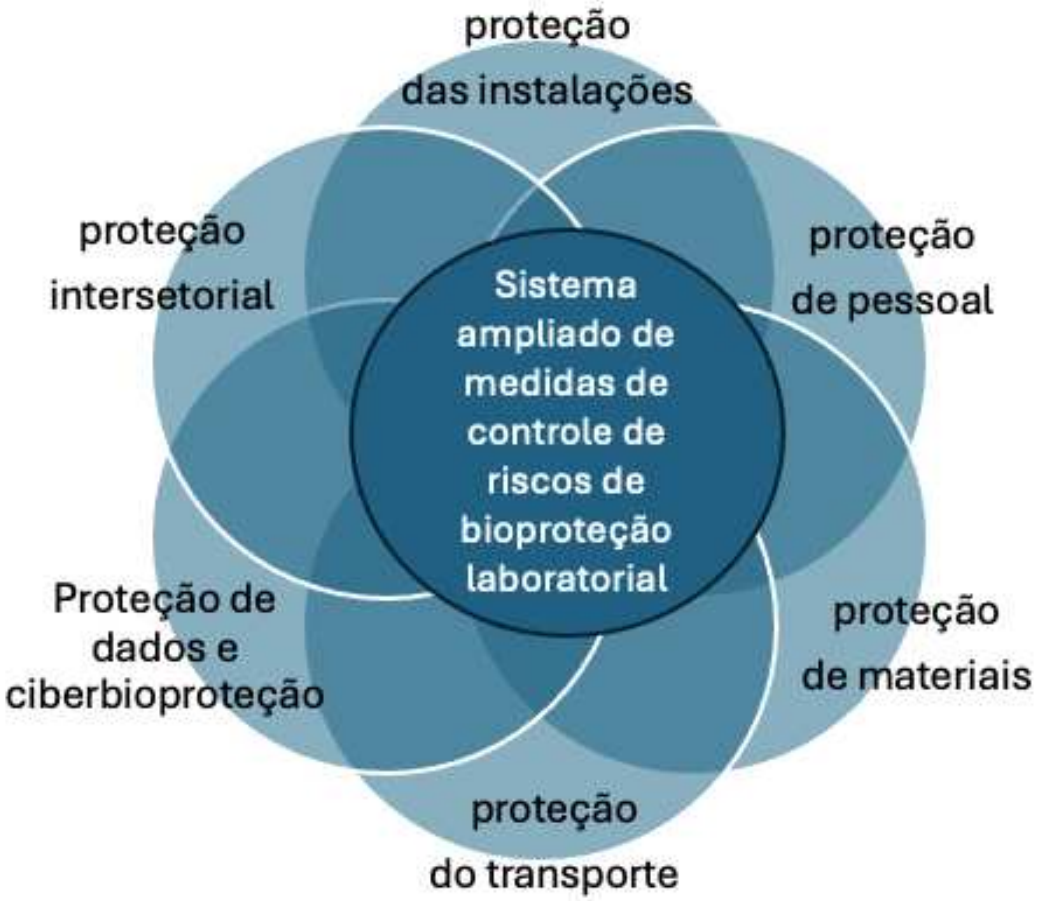


Figura 44 – Rosa *ampliada de medidas de controles de risco de bioproteção laboratorial, com os componentes de ciberbioproteção e de proteção intersetorial* (elaborado pelo autor).

Na prática, entretanto, continua a haver dificuldade na separação entre as medidas tomadas por cada um dos componentes, pois podem ser medidas de intesecção, isto é, comuns a dois ou mais componentes.

Este sistema de medidas de controle de risco de bioproteção deve ser objeto de avaliação e aprimoramento contínuos por parte do responsável pela biossegurança e bioproteção laboratoriais. A integração com as medidas de biossegurança deve ser, sempre que possível e no que couber, levada em consideração.

As medidas de bioproteção serão tanto mais robustas quanto maior os cenários de risco associados a uma estrutura laboratorial. Agentes biológicos de mairo risco, a exemplo dos agentes selecionados, requerem mais proteção do que agentes de menor risco. Deste modo, as medidas requerem implementação escalonada de acordo com o nível de risco[2]

Um sistema de bioproteção escalonado deve ser implementado na forma de camadas concêntricas de proteção em torno do agente biológico, com base no resultado da avaliação de risco. Quanto mais próxima do agente, tanto mais medidas de proteção física, proteção de pessoal e proteção de materais devem ser implementadas[2].

Proteção de dados, proteção de transportes e proteção intersetorial também variam de acordo com a avaliação pregressa de risco, mas resultam em medidas que não são necessariamente específicas para áreas internas de uma estrutura laboratorial[2].

Este tópico descreverá cada um dos seis componentes críticos de um sistema de bioproteção laboratorial.

6.3.1.1 Bioproteção das Instalações

A bioproteção das instalações é tradução adaptada do que muitos autores anglófonos chamam *physical security*. Aumentar as medidas de proteção física das instalações é geralmente a maneira mais evidente de reduzir o risco de invasores acessarem o MBGC a ser protegido pela estrutura laboratorial[2].

O objetivo da bioproteção das instalações é reduzir o risco de acesso não autorizado a áreas e objetos específicos. Isso envolve a implementação de medidas em alguns elementos fundamentais de segurança física:

1. Barreiras;
2. Controles de acesso;
3. Detecção de intrusão; e
4. Avaliação de alarmes[2].

6.3.1.1.1 Barreiras

Barreiras devem ser estabelecidas para demarcar as áreas sob algum grau de limitação de acesso. Pode haver mais de um grau de limitaração de acesso, isto é, grau de restrição. Normalmente, quanto mais próximo da área com o MBGC, maior o grau de restrição de acesso[2].

Nas instalações que custodiam agentes de risco baixo ou moderado, a sinalização pode ser suficiente para a demarcação das áreas restritas. Neste caso, podem-se dividir as áreas em dois graus de limitação de acesso apenas[2].

Nas instalações com risco maior, barreiras podem ser muros, janelas, portas, boxes de passagem (*pass-through boxes*), autoclaves (*pass-through autoclaves*), entre outros, com os perímetros podem ser preferencialmente divididos em três graus de restrições de acesso (verde, amarelo e vermelho)[2].

Portas de emergência devem ser instaladas, quando necessário, com a abertura unicamente autorizada da área restrita para a não restrita, assim como qualquer dispositivo que permita a abertura de portas e janelas, como maçanetas e fechaduras[2].

Escadas exteriores, se houver, devem ter proteção contra o acesso não autorizado ao teto ou às áreas internas[2].

A planta da instalação e a disposição de corredores e vias internas de acesso, associadas aos mecanismos de controle de acesso, devem garantir que os fluxos de pessoas, sejam habituais ou emergenciais, de empregados e de visitantes, náo tenham falhas de barreiras. Deste modo, não devem permitir rotas alternativas e não seguras para a área restrita[2].

A efetividade de força de proteção de uma área restrita resulta no tempo que um agente indevido levaria para acessar tal área. Quanto mais robusta é a barreira, mais tempo é o intervalo entre a intrusão inicial e o tempo para o adversário acessar o MBGC. Quanto maior o intervalo, maior a janela de oportunidade para a força de resposta agir para neutralizar o adversário, o que não implica necessariamente em matá-lo, após soar o alarme de detecção[2].

6.3.1.1.1 Controles de acesso

Controles de acesso objetivam garantir que apenas pessoas previamente autorizadas tenham acesso a uma área restrita. O tipo de controle de acesso escolhido depende do nível de garantia requerido para que apenas pessoas autorizadas acessem determinadas áreas.

O acesso pode ser controlado por meio de um único item, como uma chave física ou eletrônica (ex. crachá microchipado); ou por meio de informação única (*unique knowledge*), como o uso de uma senha pessoal (seja para um guarda

em ponto estratégico, seja numa fechadura eletrônica) ou o uso de uma identificação biométrica (ex. impressão digital, impressão palmar, íris etc.).

O uso de identificadores biométricos individuais é considerado mais seguro do que senhas ou do que chaves físicas/eletrônicas. Os dados biométricos poderiam só com maior dificuldade, *a priori*, ser obtidos por terceiros (ex. criminoso faz o pessoal autorizado como refém para garantir o acesso por dados biométricos).

A impressão digital pode ser substituída por próteses com a gravação das mesas, de modo que, entre os dados biométricos, é a forma menos segura.

A escolha dos controles de acesso deve levar em consideração o risco associado ao patógeno ou tecnologia de interesse, isto é, as ameaças identificadas contra o MBGC e o impacto potencial de sua disseminação intencional.

Havendo alto risco, é mister o uso de controles biométricos, preferencialmente não digitálicos. Assim, a situação de intrusão com reféns pode ser prevenida com a associação de leitura palmar ou de íris, por exemplo, e de uma senha posterior. A senha permite a criação de códigos de emergência que, se digitados num controle de acesso, acionam o alarme de intrusão, após um período pré-estabelecido.

6.3.1.1.3 Detecção de intrusões

A detecção de intrusões tem o fito de informar à equipe de segurança da instalação selecionada que indivíduos não autorizados tentaram acessar ou conseguiram acessar uma área restrita. Na sua forma mais simples, a detecção de intrusão é um alerta para a área adequada de que algo fugiu do padrão (ex. uma janela quebrada ou uma porta foi aberta).

Instalações de baixo risco podem lançar mão de pessoal treinado para fazer este alerta de situações anormais. Entretanto, instalações de alto risco podem escolher entre patrulhas de seguranças treinados para monitorar especificamente o status de segurança de áreas restritas, com foco em pontos de acesso, ou podem escolher utilizar sistemas eletrônicos de detecção.

Os sistemas eletrônicos de detecção possuem duas vantagens importantes: i. não podem ser rendidos; e ii. trabalham de maneira contínua. Normalmente, estes sistemas estão associados a controles de acesso igualmente eletrônicos.

A rede eletrônica pode ser configurada de modo que se uma linha de comunicação for interrompida (ex. alguma fiação é cortada), um alarme pode ser ativado. Sensores em vidros, de modo análogo, podem ser instalados para, caso uma janela ou equipamento seja quebrado, outro alarme soe.

Outros tipos de sensores, como os detectores de movimento, podem ser instalados, preferencialmente em áreas internas, considerando que, em ambientes externos, a movimentação de objetos (ex. folhas) e animais podem falsamente ativar os alarmes ou exigir que haja diminuição disfuncional da sensibilidade dos sensores. Na área interna, os sensores podem ser desligados quando houver fluxo de pessoal em horários de trabalho, se o objetivo for o monitoramento noturno.

Instrumentos de detecção de intrusões enviam sinais de alarme para uma central de monitoramento onde o pessoal de segurança pode monitorar o sistema completo de bioproteção e disparar comandos para as equipes de reposta. A área em que a central de monitoramento deve se localizar deve ser uma área restrita, e o pessoal de monitoramento na central deve estar sujeito a medidas adequadas de segurança de pessoal.

6.3.1.1.4 Avaliação de Alarmes

A avaliação de alarmes deve considerar, inicialmente se se trata de um alarme falso ou verdadeiro/válido. Malfuncionamento de equipamentos, acidentes e até animais não humanos podem ser a fonte de um falso alarme.

Um registro de todos os alarmes, falsos e válidos, deve ser feito contendo, no mínimo, as seguintes informações: i. data e hora do alarme; ii. causa definitiva, ou causa provável, do alarme; iii. identidade de quem recebeu o alarme; e iv. medida tomada após avaliado o alarme. A análise destes registros é fundamental para o planejamento de medidas corretivas para diminuir a taxa de alarmes-falsos.

Alarmes, quando eletrônicos, podem ser avaliados pessoalmente ou por meio de circuitos fechados de televisão (CFTV). Quando um alarme soa, o local e tipo do alarme devem ser mostrados na central de monitoramento.

A integração do circuito de câmeras com os alarmes deve ser configurada para gravar e armazenar as imagens relacionadas ao evento, antes, durante e após o alarme. E esta configuração é mais efetiva do que um sistema de monitoramento

de vídeo em que operadores humanos são os responsáveis por detectar incidentes de segurança.

Se um alarme é avaliado como verdadeiro, alguém treinado e equipado para neutralizar um intruso deve responder ao aviso e se tornar a força de resposta. Se necessário, deve ser acionada também a força de segurança policial da localidade, devidamente integrada à resposta do laboratório.

6.3.1.1.5 Integração da bioproteção das instalações com a biossegurança laboratorial

A bioproteção das instalações de um laboratório selecionado tende a contribuir com a biossegurança ao restringir o acesso de pessoas que podem ser expostas a incidentes. Neste sentido, apenas pessoas capacitadas, e eventualmente com imunização adequada, terão permissão de acesso.

Entretanto, pode haver conflito de objetivos entre as medidas de proteção e de biossegurança implementadas, se alguns cuidados não forem observados. Os controles de acesso, por exemplo, devem ser instalados respeitando as práticas de biossegurança. Leitores biométricos, por exemplo, podem ser problemáticos sob o ponto de vista da biossegurança: abertura de freezers e outros equipamentos com a impressão digital pode exigir a retirada de luvas em local de uso obrigatório.

Assim, a exigência de retirada de equipamentos de proteção individual (EPI) para acessar materiais ou áreas restritas pode resultar em falhas de biossegurança irrazoáveis. Nestes casos, alternativas de controle de acesso com chaves, crachás/cartões de acesso ou senhas podem também ser consideradas.

Os controles de acesso também devem ser instalados, de modo que não dificultem a resposta a uma emergência. Membros do laboratório devem conseguir sair durante uma emergência. Entretanto, as medidas de segurança de vida não deveriam permitir que pessoas sem autorização acessem áreas ou equipamentos restritos.

Em áreas restritas de laboratórios de risco moderado ou alto, vidros e janelas que podem ser quebrados em situações de emergência precisam de monitoramento eletrônico e/ou sistema de sensor com alarme integrado. Porém, preferencialmente, sempre que possível, serem substituídos por outras medidas de biossegurança que não afetem a bioproteção. A ativação de alarme também deve

ocorrer caso alguém acione algua trava ou martelo para quebra ou soltura de vidros/janelas em caso de emergência.

O plano de segurança precisa documentar exatamente como o sistema está ajustado para atender aos objetivos tanto de bioproteção quanto de biossegurança, no caso de uma emergência.

É importante avaliar todos os usos emergenciais possíveis dos recursos de segurança disponíveis, bem como analisar o impacto do uso nas medidas de bioproteção e biossegurança.

No âmbito do preparo, o teste ou simulação de cenários de emergência para avaliar a efetividade das medidas em situação próxima do real é recomendável, regularmente após mudanças do sistema e/ou do pessoal de segurança. Inclusive com eventual participação de bombeiros e polícias, com a finalidade igualmente importante de treino integrador.

6.3.1.2 Bioproteção de pessoal

A bioproteção de pessoal se constitui em um conjunto de medidas de bioproteção laboratorial com a finalidade de garantir que somente pessoas adequadas recebam acesso a áreas laboratoriais com algum grau de restrição.

Trata-se do principal componente para fazer frente à ameaça interna, entendida como a presença de membro interno (pessoal interno) - servidor ou prestador de serviço do laboratório - com intenção de obter MBGC ou conhecimento estratégico para fins criminosos (ex. sabotagem, bioterrorismo etc.).

A prevenção, detecção, obstrução e neutralização tanto desta ameaça interna, quanto de ameaças provenientes de público externo - visitantes - por meio da proteção de pessoal, envolve a implementação de medidas que podem ser divididas em três elementos fundamentais:

1. Identificação de pessoal;
2. Pessoal interno; e
3. Pessoal externo.

Sistemas de identificação de pessoal, por exemplo com crachás, podem utilizados na prática para identificar e dar acesso àqueles indivíduos autorizados a acessar MBGC.

Algum nível de confiança institucional deve ser obtido antes de permitir a alguém acessar materiais ou conhecimentos biológicos selecionados. Esta confiança pode ser obtida por meio de análise de antecedentes pessoais cujo aprofundamento deve variar de acordo com o nível de acesso do indivíduo ao agente biológico ou conhecimento selecionados.

Idealmente, os protocolos e diligências para fins de análise de antecedentes deveriam ser realizados por pessoas especializadas nesta tarefa, a exemplo de pessoas/frações de inteligência que detêm acesso e habilidade para uso de bancos de dados e para eventual acionamento de elementos operacionais.

Quando não é possível obter o nível desejado de confiança em uma pessoa específica, por alguma falha no processo de avaliação de antecedentes, por exemplo, inclusive falta de tempo para análise, recomenda-se o acompanhamento (escolta) do visitante durante sua permanência nas instalações. O acompanhamento pode ser físico, que tem maior poder dissuasório, ou eletrônico.

6.3.1.2.1 Identificação de pessoal

Os laboratórios precisam de alguma forma de mecanismo de identificação de quais pessoas possuem acesso a quais áreas. O uso de um crachá, ou equivalente, para este controle é item essencial para a bioproteção de pessoal.

São informações mínimas necessárias, e que precisam estar visíveis, uma foto (para pessoal interno e externo que permanecerá por maiores períodos trabalhando no laboratório), cor ou outra marcação com o indicativo da área de acesso e a validade do crachá[2].

O material do crachá não deve facilitar a falsificação e ele deve preferencialmente poder ser utilizado como chave de acesso, quando for o caso, conforme supracitado.

Seu uso deve ser visível na parte superior do tórax e a instituição deve estimular o seu pessoal interno e de segurança a questionar a locomoção interna de qualquer pessoa não identificada com crachá de modo que seja facilmente visível as informações mínimas dele.

6.3.1.2.2 Pessoal interno

O pessoal interno do laboratório são todas as pessoas empregadas, servidoras ou que prestam serviços com permanência e regularidade nas suas instalações. Neste sentido, um trabalhador temporário poderia ser classificado como pessoal interno, em razão de seu vínculo trabalhista com o laboratório.

A análise de antecedentes (*background investigation*) é apenas uma parte do processo para uma instituição determinar quem deve receber acesso a áreas restritas ou a materiais biológicos e a conhecimentos selecionados. Mas esta análise não é exaustiva; nunca será perfeitamente efetiva, por limitações as mais diversas.

Outro elemento da análise de pessoal (*pesonnel screening*), igualmente importante, é a análise de intenções presente. Ao contrário da análise de antecedentes, a análise de intenções se debruça grandemente sobre o presente, mas também o passado mais próximo, para buscar traços da personalidade e da relação interpessoal e nível de satisfação do trabalhador, a fim de buscar indícios de intenção de causar dano ou potencial aumentado para ser recrutado.

Mesmo os órgãos de segurança-inteligência mais bem equipados, não conseguem obter todo o conhecimento possível sobre antecedentes e intenções presentes de um indivíduo. Apesar disso, é necessário que, tanto maior a avaliação de risco relacionada com o laboratório e seus MBGC, mais profunda e detalhada seja a análise de antecedentes.

Ao garantir que o pessoal interno de um laboratório seja adequado para os cargos que ocupam, a instituição consegue mitigar o risco tanto de atos acidentais quanto intencionais.

Níveis baixo, moderado e alto podem ser designações associadas também a cada posição de trabalho, baseadas na responsabilidade sobre outros indivíduos que atuam no laboratório e no acesso a patógenos e conhecimentos selecionados.

Os níveis de trabalho configurariam três espécies de níveis de risco invertido, porque não tem a ver com aquilo que o trabalho gera de risco sobre o trabalhar, mas com o que o trabalhador oferece de risco ao laboratório e à sociedade.

Por exemplo, um posto de trabalho de nível de responsabilidade/acesso baixo, estaria associado a baixo risco de o seu detentor provocar um mal com o MBGC custodiado no laboratório. Em contrapartida, um posto de trabalho de nível

alto, permite ao indivíduo maior facilidade para obtenção de um MBGC com potencial de uso criminoso.

Uma lista padrão de requisitos deveria ser desenvolvida segundo os grupos de risco, considerando diferentes tipos de análise de antecedentes, de acompanhamento profissional, de dinâmicas de grupo e testes de personalidade, por exemplo.

Os requisitos de *screening* aumentariam em rigor e intensidade à medida em que o risco (invertido) do trabalho crescesse de baixo para moderado e de moderado para alto.

Pessoas em postos de baixo risco normalmente não têm contato com patógenos e toxinas selecionadas ou não possuem acesso a áreas restritas. Pessoas em postos de risco moderado, entretanto, são aquelas que executam tarefas significativamente importantes para a instituição, incluindo cientistas e técnicos laboratoriais com acesso direto a patógenos RMUC, em diferentes tarefas como transporte de material biológico, recebimento de material biológico, limpeza de áreas resritas etc.

Pessoal de tecnologia da informação sem acesso a todas as pastas do laboratório, mas a algumas pastas estratégicas (ex. fichas de pessoa, entre outras) e pessoal da segurança sem acesso a armas também podem ser considerados como pessoas em postos de nível moderado.

Pessoas em postos de alto risco, por último, são aquelas com competências de maior escopo e maior responsabilidade e autoridade no laboratório, incluindo, de maneira geral, os pontos focais e chefias de biossegurança e bioproteção e de segurança.

Trata-se de competências que são críticas para a instituição, na medida em que estão associadas a alto risco (probabilidade e impacto) de contribuir para evento selecionado se a função do posto for exercida contrariamente aos interesses da instituição.

São exemplos de postos de alto risco: i. superiores hierárquicos daqueles com posição de trabalho de risco moderado ou alto; ii. técnicos de informática com acesso completo de dados; iii. pessoal com acesso ao sistema de controle de segurança (ex. central de monitoramento, controle de alarmes, etc); iv. seguranças armados; e v. pessoas com acesso a patógenos e toxinas de RAUC e REUC.

Sob o ponto de vista da bioproteção, é preferível que a ILS prequalifique o pessoal interno que podem aceder a postos de trabalho de maior risco. Neste

sentido, antes de ser conferido maior acesso a áreas e a MBS, o funcionário já terá sido submetido a medidas de checagem de pessoal.

Em instituições que custodiam MBS, devem fazer parte da checagem de pessoal (*screening*) análises periódicas de:

1. Qualificação;
2. Pessoas de referência (pessoal e profissional);
3. Antecedentes profissionais (contato com empregadores prévios);
4. Antecedentes criminais;
5. Antecedentes financeiros; e
6. Dependência química e outras (ex. dependência de jogos de azar).

Em casos de risco extremo, deve-se avaliar a viabilidade de realizar acompanhamento psicológico regular, avaliações de personalidade e testes toxicológicos.

São informações de pessoal que podem interferir na concessão de posto de risco elevado, entre outras:

1. Associação com organizações criminosas;
2. Padrões inadequados de comportamento (abuso de substâncias, violências diversas, agressividade extrema, psicopatia, outras condutas criminosas);
3. Uso ilegal de armas;
4. Conduta inadequada em trabaho prévio (insubordinação, ansenteísmo, violação de regras); e
5. Radicalismo religioso-ideológico.

É importante que haja um protocolo bem estabelecido para a análise de pessoal, considerando um passo-a-passo e incluindo os bancos de dados a serem acessados e as informações que devem ser obtidas, assim como devem ser analisadas, de acordo com cada nível de acesso.

Mesmo que análise seja realizada por órgão de segurança-inteligência parceiro, é importante estabelecer requisitos gerais e transparentes para divulgação prévia aos postulantes dos acessos, a fim de que não haja esforço desnecessário, caso o postulante não deseje ser submetido à análise e prefira desistir do cargo/função.

Sob o ponto de vista da integração intersetorial, é importante que o(s) órgão(s) de contrainteligência do Estado custodiante do MBCG e do PAI/PGC obrigatoriamente analise a concessão de um aval de segurança (*security clearance*). Desta forma, será possível garantir que o pessoal com acesso de alto risco seja registrado e cotejado com eventuais bancos de informações sobre vínculos com Estados estrangeiros e seus serviços de inteligência.

São informações de inteligência que podem interferir na concessão de aval de segurança, entre outras:

1. Vínculos com diplomatas/oficiais de inteligência estrangeiros;
2. Viagens frequentes e inexplicadas ao exterior;
3. Residência prévia suspeita em país estrangeiro; e
4. Enriquecimento suspeito.

A presença de alguma informação desabonadora isolada e não grave pode não resultar na reprovação do candidato ao acesso postulado e, a depender do caso, pode ser esclarecida em uma entrevista individual.

As medidas de proteção de pessoal interno não devem se esgotar com a contratação ou concessão de acesso ao postulante, mas devem ser continuadas e realizadas regularmente. Toda informação obtida pela ILS durante a avaliação de pessoal deve ser tratada como classificada.

Segundo o Serviço Secreto dos EUA, em estudo sobre sabotagem de infraestruturas críticas por pessoal interno, a causa mais comum de ação interna criminosa é um evento de trabalho negativo que gerou mágoa e sentimento de vingança[44].

Neste sentido, consideram-se medidas preventivas de bioproteção de pessoal a proatividade da ILS em criar um ambiente de trabalho saudável e que minimize a transformação de problemas interpessoais em incidente de segurança. Tais condições precisam ser observadas por gerentes e pelo pessoal próximo aos envolvidos, que devem notificar à gerência.

Um programa voltado para o bem-estar do trabalhador pode buscar a solucionar estas questões. Para ser efetivo, é necessário que ele seja acessível aos trabalhadores que estejam insatisfeitos e queiram questionar a instituição sem represálias ou que tenham problemas financeiros e relacionados com saúde mental ou abuso de substâncias. Desta forma, programas de assistência se tornam uma ferramenta de biossegurança e bioproteção.

O monitoramento continuado e proativo do bem-estar mental e físico do pessoal tende a reduzir o número de eventos de falhas de proteção e segurança num laboratório.

Quanto à questão salarial, é importante que o empregador, seja estatal ou privado, reconheça que, quanto maior o risco de acesso a MBGC, maior a responsabilidade e, portanto, maior a remuneração devida. Rendimentos justos são requisito importante na gestão de biossegurança e bioproteção laboratoriais.

6.3.1.2.3 Pessoal externo

O pessoal (ou público) externo ao laboratório são todas as pessoas que visitam ou passam pelas instalações do laboratório em caráter temporário, isto é, que não enseje vínculo de permanência. Neste sentido, os estudantes estrangeiros que passam meses ou anos em um laboratório também seriam considerados público externo, em razão da natureza temporária de seu vínculo[2].

O pessoal externo pode incluir também indivíduos de organizações externas ao laboratório que possuem algum trabalho vinculado ao laboratório, por exemplo com prestação de algum serviço. Neste caso, podem ser visitantes de curto-prazo (ou visitantes casuais) ou de longo-prazo[2].

Visitantes casuais podem ser também visitantes pessoais, incluindo amigos e parentes, cujo acesso deve ser apenas às áreas não restritas e sob escolta de seus anfitriãos. Na verdade, todos os visitantes casuais devem estar vinculados a uma pessoa interna do laboratório, que se responsabilize pelo cumprimento de regras, inclusive de B2L.

Considerando as novas tecnologias de detecção facial, em laboratórios com MBGC e/u PAI/PGC com grande circulação de pessoas, pode haver a instalação de câmeras com reconhecimento facial em locais restritos e de ampla circulação, a fim de detectar aqueles que não tiveram o acesso autorizado de entrada (seja restrito ou não). Neste caso, a coleta de biometria facial seria feita com todo pessoal externo e interno, na ocasião do cadastramento.

Ressalte-se ainda que tecnologias de reconhecimento facial permitem a troca de informações com a inteligência laboratorial, seja da própria instituição ou de outros órgãos, no sentido de detectar possíveis suspeitos de intrusões pregressas ou de ameaças suspeitas que podem tentar acessar ILS ou LAC.

É importante que os registros de acesso de visitantes, seja na entrada principal seja nos controles de acesso, sejam guardados por um a cinco anos, a fim de permitir investigações futuras de segurança-inteligência, se necessário. Os dados dos visitantes também devem acompanhar os registros de acesso.

6.3.1.2.4 Integração da bioproteção de pessoal com a biossegurança laboratorial

As recomendações essenciais da proteção de pessoal trazem benefícios básicos à biossegurança laboratorial, e normalmente estão implementadas em LAC ou outros com programas efetivos e robustos de biossegurança. Conhecer os antecedentes de alguma pessoa, inclusive de treinamentos, é um ato de garantia se biossegurança também[2].

Caso o uso do crachá implique em risco indesejado de contaminação em LAC, é indicada a instalação de armários ou semelhantes em antessalas para a guarda deles e de outros itens de acessórios pessoais. Em áreas restritas, sem o acesso com crachá, é recomendável o controle por mecanismos de biometria, conforme discutido no tópico 6.3.1.1.1. (Controle de acesso).

6.3.1.3 Bioproteção de materiais

O objetivo da bioproteção de materiais (componente da bioproteção também conhecido como *materiais, controle e responsabilização* – MC&A, na sigla em inglês)[2, p.48] é criar um ambiente que afaste infiltrados de furtar e usar criminosamente os agentes biológicos. Além disso, o controle de materiais efetivo dificulta que invasores identifiquem as amostras biológicas que desejam obter.

As medidas de bioproteção de materiais contribuem para definir exatamente que materiais biológicos estão presentes na instalação, como e onde são estocados e manuseados e quem é responsável por eles[2].

Este componente envolve a implementação de medidas que podem ser divididas em três elementos fundamentais:

1. Materais;
2. Controle de materiais; e

3. Responsabilidade e auditabilidade (*accountability*)[2].

6.3.1.2.3.1 Materiais

O primeiro aspecto na bioproteção de materais é a definição de que materiais estarão sujeitos a medidas de controle; e de responsabilização e auditabilidade (*accountability*). O material biológico e as informações de pesquisa sujeitas a medidas de mitigação de risco devem ser identificadas com base em uma rigorosa avaliação de risco (*risk assessment*)[2].

A avaliação de risco, seja baseada no modelo AMP ou na abordagem ABRE, deve identificar e categorizar os materiais biológicos entre cinco níveis de risco de risco de uso criminoso: risco baixo, moderado, alto e extremo de uso criminoso (LAUC, RMUC, RAUC e REUC, respectivamente, nas siglas em português – e LMUR, MMUR, HMUR e EMUR, respectivamente, nas siglas em inglês)[ww].

Tal classificação foi proposta pelo priemiro manual específico de bioproteção laboratorial, dos SANDIA NATIONAL LABORATORIES (2007)[2, p.49], mas podem ser usadas outras escalas quantitativas ou qualitativas de risco. Recomenda-se que, a partir de risco moderado, haja medidas de controle de materais.

São estes materiais biológicos que, em função do risco atribuído pelos gestores de B2L e autoridades de segurança-inteligência necessitam de medidas mais robustas de controle, são chamados de MBGC, segundo nomenclatura da OMS[16, 22]. Outros autores preferem chamá-los de agentes biológicos perigosos (*dangerous biological agents*)[2] ou, am alguns casos, agentes biológicos selecionados[1].

As medidas não se aplicam a equipamentos, instrumentos, vestimentas e objetos laboratoriais similares que podem ser contaminados na prática laboratorial. Esses itens devem ser descontaminados e, se necessário, descartados seguindo procedimentos específicos e coloados em áreas adequadas[2].

[ww] Conforme argumentado nesta pesquisa, a atribuição de risco a materiais biológicos deve seguir padrões ou diretrizes de autoridades reguladoras e estar baseada em troca de informações de inteligência e segurança sobre ameaças de BPL, deste modo não devendo ser realizada unicamente por gestores laboratoriais. Um modelo tridimensional de governança de B2L, conforme discutido no tópico 6.1.1.4, é o ideal para garantir a qualidade de uma avaliação/monitoramento de risco efetiva(o).

6.3.1.3.2 Controle de materiais

O controle de materiais consiste na implementação de uma cadeia de custódia[xx] e outras medidas para garantir que o uso dos MBGC seja rastreável; que eles permeneçam onde previsto; que sejam utilizados para razões estabelecidas; e que sejam exclusivamente manipulados por pessoas previamente designadas e autorizadas.

Deve englobar todas as atividades que envolvem o material, como a estocagem/guarda, o uso, o transporte, o descarte. E as medidas devem ser efetivas tanto e, condições normais quanto em condições anormais, como acidentes, quedas de energia e emergências[2].

Os controles podem ser implementados de duas formas:

1. Controle físico – meio de prevenir acesso indevido (ex. abertura de *freezers* mediante senha); e
2. Controles procedimentais – são exemplos a etiquetagem de tubos de ensaio; realização de auditorias de materiais; procedimentos operacionais padrão para trabalho com MBGC, para inativação, para descarte, para retirada de MBGC do estoque e para recolocação no estoque etc.

Normalmente os controles físicos e os procedimentais estão balanceados. E se deve definir, no plano de bioproteção e em procedimentos-padrão, quais as ações previstas quando uma amostra de MBGC é percebida como faltante.

6.3.1.3.3 Responsabilidade e auditabilidade (*accountability*)

A atribuição de responsabilidade (*accountability*) é o meio de garantir que alguém seja responsável pelo MBGC guardado e/ou utilizado em uma determinada área. São aspectos da atribuição de responsabilidade e da auditabilidade: designação de pessoal qualificado para supervisionar o controle de MBGC; manter

[xx] Cadeia de custódia consiste no processo empregado para registrar quem está sob controle de uma amostra e quando. O processo da cadeia de custódia garante que o material sempre esteja sob responsabilidade de alguém, que se trona o responsável pela sua integridade.

registros oportunos e acurados; notificação de falhas; e auditorias de estoques de MBGC[2].

Cada agente biológico e toxina deve ter uma pessoa responsável pela guarda e uso (*accountable individual*). Ela será responsável por fornecer informações sobre quanto, como, quando, onde e por que "seu" patógeno foi usado, transportado, guardado ou destruído, além de manter os registros de inventário[2].

Para conferir maior proteção, o ideal é que o responsável não seja o mesmo que faz o uso em pesquisa desse MBGC. Neste sentido, haverá, no mínimo, duas pessoas que lidam com o patógeno, o que permite controle mútuo sobre sua custódia.

6.3.1.3.4 Integração da bioproteção dos materiais com a biossegurança laboratorial

O LBM4 recomenda o uso do símbolo de perigo biológico (*biohazard sign*) para laboratórios NB-2 ou maior[16]. Normalmente, a sinalização de bioperigo inclui o nome do agente, perigos específicos, e informações de contato. A identificação desses três itens pode significar vulnerabilidade de bioproteção[2].

Deve-se considerar a localização de um MBGC em um laboratório ou *freezer* como uma informação classificada e que deve ser administrativamente manejada como tal, inclusive mediante assinatura de termos de sigilo por todos que saibam esta informação.

Dependendo do local da sinalização de bioperigo, ele pode identificar onde está um MBGC àqueles que não têm legítima necessidade de conhecer essa informação. Por isso, a colocação dessa sinalização deve ser cuidadosamente planejada para evitar comprometer a proteção, enquanto mantém nível adequado de segurança.

6.3.1.4 Bioproteção do transporte

A proteção do transporte é um mecanismo de implementação de proteção de materiais (MC&A, na sigla em inglês) para reduzir os riscos de um intruso ou

outsider furtar/roubar um MBGC enquanto o material é transportado entre áreas de acesso restrito[2].

Este componente envolve a implementação de medidas que podem ser divididas em três elementos fundamentais:

1. Transporte interno; e
2. Transporte externo[2].

6.3.1.4.1 Transporte interno

O transporte interno, no contexto da bioproteção laboratorial, consiste na movimentação de MBGC entre áreas restritas de uma instalação. Tipicamente, uma pessoa originalmente de um laboratório retira uma amostra do estoque ou local de guarda, anda por áreas não restritas de uma instalação, e entrega a amostra para outra pessoa no local de recebimento.[2]

O transporte interno também pode incluir o acréscimo de MBGC de um inventário ou remoção do mesmo, como resultado de um processo de envio ou recebimento local, nacional ou internacionalmente; ou o envio de materiais para áreas de descarte, como uma autoclave ou sala com incinerador[2].

Considerando que MBGC podem ser vulneráveis ao furto/roubo enquanto estiverem fora de áreas restritas, é necessário ter cuidado na custódia de tais materiais durante o transporte. Sob o ponto de vista da bioproteção, é importante pensar o MBGC sendo transportado como se as instalações laboratoriais com todo o conjunto de medidas de bioproteção estivessem igualmente sendo transportadas. Um MBGC em trânsito é como se houvesse um laboratório de alta contenção em trânsito, guardadas as devidas proporções.

Todos os que possuírem acesso físico ao MBGC transportado devem estar sujeitos aos mesmos requisitos de proteção como os exigidos para o pessoal com acesso ao material restrito no laboratório.

Análise dos processos de transporte interno devem buscar áreas eventualmente usadas para guarda temporária, como sala de recebimento de mercadorias, entre outras. Controles de acesso e de material devem ser implementados nesses locais[2].

A documentação de cadeia de custódia deve acompanhar o material sendo transportado. E assinatura de todo pessoal de transporte que tiver contato

com o MBGC deve ser registrado, inclusive quem é o responsável por determinado trecho do transporte e para quem ele vai entregar o materal e a responsabilidade sobre o material[2].

A cadeia de custódia pode ser garantida por diversos mecanismos, como documentos em papel, mas também sistemas eletrônicos com códigos de barra ou outras ferramentas.

6.3.1.4.2 Transporte Externo

O processo do transporte externo inclui um trecho interno anterior, além da entrega para um transportador privado ou público. Pode-se falar em três fases do transporte: o pré-envio, a fase da rota em si (*en route*) e a entrega[2].

Recomenda-se, sob o ponto de vista da BPL, que haja autorização prévia de envio. A autoridade que dará a autorização prévia dependerá da do risco do transporte. Em caso de MBGC deve-se buscar uma autorização de transporte externo junto à maior autoridade regulatória, com notificação prévia extendida às frações de inteligência ou órgãos de inteligência da governança tripartite ou tridimensional.

No caso de transporte de MBGC, é importante que a estrutura de inteligência laboratorial realize uma análise de risco do transporte e participe do planejamento e implementação do deslocamento do material, avaliando a adequação de ele ser realizado por órgãos estatais (ex. Forças Armadas), no lugar de algum transportador privado.

Todo transporte de MBGC deve ter um plano de transporte realizado pelas instalações laboratoriais com participação de assessoramento de inteligência laboratorial, inclusive prevendo as medidas a serem tomadas em caso de extravio. Para tanto, é mister que se faça a notificação prévia do transporte para os órgãos de inteligência laboratorial e de segurança envolvidos.

O empacotamento deve ser realizado de maneira discreta para não chamar atenção demasiada, contendo o mínimo de informações necessárias na área externa[2].

O conteúdo deve ser preferencialmente ser vinculado a um rastreador que permita a uma (ou mais) pessoa(s) designada(s) pelos laboratórios para

acompanharem o transporte externo, à distância ou presencialmente, conseguir identificar a localização do MBGC em tempo real.

6.3.1.4.3 Integração da bioproteção do transporte com a biossegurança laboratorial

A limitação do acesso a MBGC durante o transporte é complementar às medidas de biossegurança do transporte. No caso de regras que impõem limitação de quantidade transportada (ex. 50ml para líquidos/50mg para sólidos em aviões comerciais; e 4l para líquidos e 4kg para sólidos em aviões de carga), por exemplo, elas conferem benefícios de bioproteção. Deste modo, a depender da avaliação de risco associado ao transporte, o total transportado pode ser fracionado emvários transportes, para conferir maior biossegurança e bioproteção[2].

6.3.1.5 Bioproteção de dados e ciberbioproteção

A proteção de dados é um conjunto de ferramentas e práticas usadas para proteger informações sigilosas[2]. Com a digitalização das informações, o componente bioproteção de dados cada vez mais se transforma em ciberbioproteção.

A ciberbioproteção de dados, por sua vez, deve ser compreendida como um componente essencial da bioproteção laboratorial, sendo essencial para evitar vazamentos de informações sensíveis sobre patógenos e laboratórios estratégicos.

O avanço da ciberbioproteção deve ser visto como parte essencial da bioproteção laboratorial, protegendo não apenas as infraestruturas físicas, mas também os dados críticos que podem ser alvos de ataques digitais.

Tal avanço possibilita a criação de barreiras digitais robustas contra-ataques cibernéticos que possam comprometer pesquisas estratégicas ou permitir acessos indevidos a infraestruturas laboratoriais. A implementação de tecnologias como IA e aprendizado de máquina no *PathoFinder Brazil*® podem contribuir para a detecção de vulnerabilidades e antecipação de riscos cibernéticos relacionados à bioproteção.

6.3.1.5.1 Informações sigilosas (*sensistive information*)

O primeiro passo em proteger as informações é por meio da identificação daquilo que é sigiloso e merece ser protegido[2]. Mais uma vez, o princípio de categorização do nível de sigilo pode ser utilizado, a partir de avaliações de risco, para nortear a implementação de diferentes medidas de proteção de dados, de acordo com o grau de sigilo de cada informação.

Além das pesquisas de uso dual (PUD), que precisam ser identificadas segundo os protocolos da OMS supracitados, Informações que merecem proteção e, portanto, são sigilosas (ou sensíveis) incluem as relacionadas com qualquer elemento da bioproteção laboratorial, a exemplo de:

1. Planos de B2L ou informações conexas;
2. Nível de acesso de pessoal;
3. Mapas das instalações;
4. Fotografias, impressões digitais ou biometrias diversas de pessoal;
5. Manuais de sistemas de segurança física;
6. Senhas;
7. Inventário e dados de estoque de MBGC;
8. Planos de transporte interno e externo;
9. Computadores ou *notebooks* com informações de MC&A ou outros registros de proteção[2].

Informações de pessoal precisam ser consideradas sensíveis, porque o acesso a elas por indivíduos malintencionados pode levar a abordagens direcionadas para recrutamento, entrevistas ou extorsão e outros crimes com objetivo de obter informações sigilosas laboratoriais.

O princípio de MC&A de limitação de acesso apenas a pessoas autorizadas e com necessidade de conhecer deve ser respeitado quanto ao acesso a informações físicas ou digitais.

Além disso, as informações físicas ou mídias digitais precisam estar etiquetadas como itens classificados e guardados em locais de acesso restrito. E protocolos devem considerar a transmissão e compartilhamento de informações sensíveis[2].

A destruição de informação sigilosa precisa ser garantida, de modo abrangente e definitivo, inclusive com adequado registro da destruição. Para papéis e semelhantes, isso inclui incineração ou trituração ou ambos, no caso de informações de maior nível de classificação ou envolvendo MBGC e PGC.

6.3.1.5.2 Dados eletrônicos e ciberbioproteção

Informações críticas ou sigilosas devem ser gravadas e executadas em computadores desconectados de qualquer rede interna[yy] ou externa, com ênfase para a desconexão da rede mundial de computadores, mas com garantia de *back-up* das informações em local isolado e seguro.

Todos os elementos de redes (roteadores, servidores, aplicativos, domínios, firewalls, Wi-Fi e acessos remotos, entre outros) devem ser monitorados continuamente sob a perspectiva de ciberbioproteção – impedir o acesso não autorizado.

Pessoas com acesso a todas as pastas de computadores com informações sigilosas devem ser checados com o maior nível de rigor. E todos os acessos, visualizações e impressões de informações sigilosas devem ser auditáveis.

Programas que executem o apagamento de dados digitais com segurança devem ser usados para descartar dados digitais sigilosos. Dispositivos eletrônicos contendo dados sigilosos, caso não sejam mais úteis, devem ser destruídos fisicamente (ex. *pendrive* e HD externo) ao ponto de se tornarem inoperáveis[2]. A última medida se aplica também a quaisquer mídias que porventura tenham contido informações sigilosas que não foram apagadas em caráter definitivo.

Além da identificação de laboratórios e pesquisadores envolvidos com patógenos selecionados, o *PathoFinder Brazil*® pode ser expandido para atuar na ciberbioproteção, identificando ameaças digitais que possam comprometer informações estratégicas sobre segurança em saúde e biodefesa. Ao integrar técnicas de inteligência artificial, a ferramenta pode mapear atividades suspeitas em redes acadêmicas e científicas, identificando tentativas de acesso indevido a informações laboratoriais sensíveis.

[yy] Ou na menor (e menos exposta) rede interna.

6.3.1.6 Bioproteção intersetorial

O sexto e último componente de um sistema de bioproteção, tão importante quanto os demais – e com eles interconectado -, é a bioproteção intersetorial. Trata-se de um aspecto abordado de maneira praticamente secundária na literatura revisada[2,13,15,16,17].

Apesar disso, o ciclo de um evento de furto ou roubo de MBGC, desde a sua prevenção até a eventual resposta posterior a um evento, exige intensa participação de órgãos de segurança-inteligência, isto é, atores externos ao laboratório. Desta forma, a bioproteção intersetorial é o único componente que depende precipuamente de relações externas ao laboratório e que, por isso, garante a efetividade longitudinal da gestão de B2L.

Não há planejamento adequado de bioproteção sem análise de risco, conforme supracitado. E não há análise de risco sem análise de ameaças à bioproteção. As análises de ameaça, mesmo que realizadas por frações de inteligência laboratorial vinculada ao laboratório em si ou órgãos supervisores dos laboratórios, não podem prescindir de conhecimentos de inteligência policial ou militar. As análises, portanto, não podem prescindir da integração da inteligência laboratorial com a inteligência de segurança pública.

Na atuação de resposta após um evento de falha de bioproteção, por exemplo um roubo bem-sucedido de MBI/ABTS, o trabalho é precipuamente realizado fora do LAC/ILS, como a perseguição policial; a busca de esconderijos criminosos; a obstrução e neutralização da ação disseminadora do agente biológico etc. São ações dependentes da atuação das forças de segurança estatais, que precisam entender a gravidade da situação e atuar de maneira integrada com a resposta laboratorial, inclusive para a escolha adequada de Equipamentos de Proteção Individual (EPI).

Conclui-se, portanto, que esta integração laboratório-órgãos de segurança merece ser considerado um elemento do sistema de bioproteção tão importante quanto os demais. É pouco efetivo que uma ILS, por exemplo, possua um excelente sistema de proteção de instalações, mas, no momento de um ataque, não consiga acionar a polícia, por falta de protocolo de comunicação intersetorial.

A bioproteção intersetorial deve considerar:

1. Planos de contingência para emergências por agentes biológicos, tanto específicos de órgãos (ex. Ministério da Saúde, Forças Armadas etc.) quanto planos intersetoriais municipais, estaduais e nacionais;
2. Troca de informações inicial sobre as análises de ameaças, na qual se deve basear o planejamento do projeto do sistema de bioproteção;
3. Protocolo de comunicação na vigência de ataques ou ameaças de ataques;
4. Protocolo de resposta de forças de segurança externas ao laboratório durante evento com MBI/ABTS, em cenários internos ou externos ao laboratório;
5. Capacitação e simulações (preparo) de respostas integradas a diversos cenários de eventos decorrentes de falhas de bioproteção laboratorial;
6. Avaliação permanente dos sistemas de bioproteção laboratorial; e
7. Educação continuada de bioproteção laboratorial em programas intersetoriais de *outreach*.

A consideração destes itens é fundamental para avaliar as competências dos atores internos e externos ao laboratório e seu órgão gestor sobre cada uma destas tarefas.

Propõe-se que a integração deve ocorrer vertical e horizontalmente entre os atores que participam do processo de prevenção, preparo, resposta e reconstrução (P2R2). Idealmente, estes atores deveriam constar de um plano intersetorial de contingência para emergência por agentes biológicos (ou, mais amplo, para agentes QBRN) do município ou do estado.

A integração intersetorial seria considerada vertical quando a gestão de bioproteção laboratório se comunica com instâncias inferiores ou superiores à sua: por exemplo, na interação com os gestores do laboratório ou do órgão a que o laboratório está subordinado, isto é, com atores internos.

A integração intersetorial seria horizontal quando a gestão de bioproteção do laboratório, direta ou indiretamente, interage com atores externos, cuja atuação é fundamental para a efetividade do sistema de bioproteção vigente.

Idealmente, um bom sistema de bioproteção laboratorial, em seu componente de proteção intersetorial, precisa estar alicerçado em planos de contingência verticais e horizontais.

Pode-se falar na existência de planos de contingência verticais, de um mesmo órgão (exemplo: o MS elabora um plano de P2R2 para emergências de bioproteção laboratorial com instruções a todos os laboratórios sob sua governança); e planos de contingência verticais, envolvendo o acionamento de vários órgãos, no caso de uma emergência que exija resposta multissetorial. Normalmente, os planos horizontais exigem elaboração conjunta por diversos órgãos sob coordenação supraministerial (quando no nível federal) ou suprasecretarial (quando estadual ou municipal).

Por sua vez, os planos de contingência verticais e horizontais podem ser elaborados em diversos níveis:

1. Nível 1 - nível institucional (laboratorial) - o próprio laboratório planeja a integração intersetorial vertical, em conjunto com seu órgão-gestor; e a integração intersetorial horizontal, em conjunto com as primeiras forças e parcerias externas de atuação imediata;
2. Nível 2 – nível municipal/estadual – os gestores municipais/estaduais planejam a integração intersetorial vertical, em conjunto com os gestores estaduais/federais em divisão de competências bipartite ou tripartite; e a integração intersetorial horizontal, em conjunto com os órgãos municipais/estaduais que atuarão em eventos de bioproteção laboratorial;
3. Nível 3 – nível federal - os gestores federais planejam a integração intersetorial vertical, prevendo a atuação de suas secretarias, diretorias e demais frações; e a integração intersetorial horizontal, em conjunto com os outros órgãos federais que atuarão em eventos de bioproteção laboratorial; e
4. Nível 4 – nível internacional – os gestores de órgãos multilaterais planejam a atuação vertical destes órgãos e suas estruturas vinculadas (ex. OMS com a OPAS) e com os demais atores envolvidos em nível nacional, estadual e municipal; e a integração internacional horizontal se faz com a articulação transversal de políticas, planos e diretrizes de órgãos multilaterais entre si (ex. OMS com INTERPOL).

Os gestores federais responsáveis por planos de nível 3 verticais são os órgãos federais com atuação prevista nos eventos e seus focos serão direcionar as frações dos seus próprios órgãos para as ações de P2R2.

Por outro lado, os gestores federais competentes para planejar planos de nível 3 horizontais seriam idealmente os de órgãos supraministeriais, a exemplo da Casa Civil da Presidência da República ou ainda a autoridade nacional responsável pela resposta interministerial integrada a eventos biológicos desta natureza (ex. nos EUA, seria o Departamento de Segurança Interna).

Idealmente, todos os órgãos envolvidos, nos quatro níveis, deveriam ter seus planos verticiais. E os laboratórios e atores integradores, possuir seus planos horizontais. Os planos horizontais e verticais precisam estar conectados, formando uma matriz de integração intersetorial.

6.3.2 Lacunas nas diretrizes de implementação de medidas de redução de risco

Apesar dos avanços dos documentos internacionais e multilaterais sobre monitoramento de biorrisco (*biorisk assessment*), ainda há diversas lacunas para auxiliar na implementação de medidas de controle de risco efetivas de bioproteção laboratorial.

Cabem aprimoramentos no BMBL3, LBM4, GBL2 e outros documentos relacionados, a fim de consolidar a aplicabilidade efetiva de medidas de bioproteção laboratorial.

Uma das principais causas para essas lacunas em tais documentos é a dificuldade de se tratar da integração laboratório-órgãos de segurança ou, mais amplamente, saúde-segurança-inteligência, tanto em nível nacional quanto internacional. A falta de uma visão transdisciplinar na área de biossegurança e bioproteção laboratorial deve contribuir para estas dificuldades.

Um modelo de avaliação de sistemas de medidias de controles de risco de bioproteção laboratorial adaptado para a realidade brasileira, tal como o CIR, busca suprimir lacuna teórico-prática, servindo como uma importante ferramenta de inteligência em saúde, mais especificamente de inteligência laboratorial em nível preponderantemente operacional e tático.

É grandemente útil para consolidar capacidades-chave de gestão em bioproteção, na medida em que se configura ferramenta para monitoramento de riscos de bioproteção.

Entretanto, o CIR não se restringe à avaliação das medidas de controle de risco em si, mas se preocupa em entender o processo de planejamento destas

medidas, quando da sua preocupação de coletar informações sobre o processo de monitoramento de risco (*risk assessment*)[13, 16, 22].

Conforme se verifica no Apêndice A[zz], as seções 3a (Avaliação de Perigos e Ameaças e Medição de Riscos) e 4e (Proteção Interpessoal) do ClR possuem quesitos voltados para a compreensão da qualidade dos dados obtidos e na forma de processamento desses dados durante o processo inicial de avaliação/monitoramento de risco, da qual a própria implementação das medidas de proteção é parte.

Se a biossegurança parte da análise fundamental do risco associado às características do agente biológico, a bioproteção vincula esta análise a uma avaliação sobre ameaças com potencial de disseminação intencional destes agentes, com a finalidade de definir o risco abrangente e norteador das ações de bioproteção a serem implementadas.

O conhecimento de características patogênicas, como as formas de transmissão de doenças (por gotículas ou secreções corporais, por exemplo) são requisitos para a definição de medidas efetivas de biossegurança. De maneira análoga, o conhecimento sobre pessoas e grupos que possam buscar o acesso indevido a agentes selecionados é requisito para a definição de medidas adequadas de bioproteção.

Enquanto a biossegurança laboratorial pode, portanto, *a priori*, esgotar o planejamento de ações e medidas, com um olhar "interno" para os patógenos e as estruturas do laboratório, a bioproteção laboratorial não pode prescindir do diálogo com o conhecimento externo ao laboratório sobre aspectos muitas vezes somente conhecidos por instituições de segurança-inteligência.

Conforme analisado, o primeiro passo do ciclo para monitoramento de riscos ("coletar informações") do LBM4 busca identificar os perigos (*hazards*)[16, p.7]. De maneira análoga, SALERNO & GAUDIOSO (2020) incluem na primeira etapa do monitoramento de riscos ("definir a situação") a resposta à questão "quem?", no sentido de definir as ameaças (threats)/adversários[13, p.54].

Ainda conforme supracitado, o segundo passo do ciclo para monitoramento de riscos ("medir os riscos") do LBM4 e do GBL2 consiste em medir os riscos associados aos perigos[22, p. 23]. De maneira análoga, SALERNO &

[zz] Os Apêndices A e B foram retirados da versão publicada da tese, por questões de sigilo. O ClC será posteriormente publicado em periódico.

GAUDIOSO (2020), incluem na segunda etapa do monitoramento de riscos (“definir os riscos”) a construção de cenários de risco, baseados em “como?” e “por quê?” os adversários tentariam obter criminosasmente um MBGC ou PGC.

É mister entender, portanto, que tais passos ou etapas de diferentes abordagens de monitoramento de riscos de bioproteção laboratorial exigem a troca de informações entre o laboratório e órgãos de segurança-inteligência. Como definir perigos/ameaças/adversários e suas motivações e *modus operandi* prescindindo desta troca?

O ponto de partida (monitoramento de risco) de uma gestão de biorrisco pode prescindir de troca de informações intersetoriais no tocante à biossegurança isoladamente, mas nunca no caso da bioproteção laboratorial.

Conclui-se que a biossegurança é de vocação centrípeta por sua natureza e requer um olhar institucional e preponderantemente para dentro. A bioproteção, por outro lado, é de natureza centrífuga por sua natureza e requer um olhar institucional e precipuamente para fora.

A bioproteção laboratorial requer olhar em sentido externo tanto horizontal quanto vertical. Horizontalmente, na perspectiva de compreender as ameaças que buscam acessar intencionalmente o MBGC ou PGC para a disseminação criminosa. Verticalmente, na perspectiva de que há codependência de ação: os órgãos de segurança-inteligência precisam do laboratório para prevenir ações indevidas efetivamente, assim como o laboratório precisa dos órgãos de segurança-inteligência para responder a ações indevidas efetivamente.

Conclui-se ainda que a vocação da biossegurança, além de centrípeta, é precipuamente solitária, sob o ponto de vista de planejamento e implementação, porque suas ações e medidas grandemente independem da ação de órgãos externos ao do laboratório, quando consideramos a fase de monitoramento de riscos (*risk assessment*). Todavia, a vocação da bioproteção é centrífuga e majoritariamente solidária, sob o ponto de vista de planejamento e implementação, porque suas ações e medidas grandemente dependem da ação intersetorial tanto no ponto de partida, quanto no ponto de chegada.

No ponto de partida, a ação intersetorial é tão somente responsável para a avaliação de risco com base em ameaças. No ponto de chegada, a resposta a um evento requer a articulação da força de resposta (segurança interna) ao laboratório com a força de resposta externa ao laboratório para a implementação eventual de medidas consequentes à realização de um suposto crime.

Deste modo, ao passo em que a bioproteção laboratorial é tavez a dimensão de maior fragilidade na gestão de biossegurança e bioproteção, a necessidade de seu planejamento e implementação oferece oportunidade de estreitamento de vínculos entre o setor laboratorial e o setor de segurança-inteligência.

A segurança da saúde, por conseguinte, pode ser consolidada, enquanto área de atuação do Estado, a partir da bioproteção e inteligência laboratoriais efetivas. Preferencialmente, como uma área transversal, cuja coordenação é desempenhada por frações competentes do MS, porém integrada a um subsistema de inteligência sob supervisão do próprio MS; subsistema por sua vez vinculado ao SISBIN, cujo órgão central pode ser a ABIN.

A incorporação da segurança da saúde de maneira efetiva a um sistema de inteligência amplo e moderno depende do aprofundamento da transecuritização e da transmilitarização da inteligência de Estado no Brasil, incluindo da própria ABIN[97].

Tal integração de órgãos e subsistemas, sob o arcobouço do SISBIN, poderia ser vantajoso para a sociedade, na medida em que fortalece a ação estatal para fins de proteção da sociedade.

Por outro lado, eventual inércia do SIBIN e da ABIN em planejar e implementar esta integração, conforme supracitado, não pode significar a inexistência de uma estrutura de inteligência em saúde e de inteligência laboratorial adequadamente efetivas.

Esta atuação pode lançar mão da aplicação de *checklists*, a exemplo do *Checklist RAMPA* (ClR), para a avaliação efetiva dos sistemas de bioproteção laboratoriais em LAC e ILS.

A elaboração da lista de requisitos de *screening* de segurança crescentes (incluindo os requisitos para aval de segurança ou *security clearance*) de acordo com os riscos crescentes de furto e roubo em posições de trabalho é uma das ações prioritárias no desenvolvimento de sistemas de bioproteção.

Neste sentido, a elaboração eventual de acordos de cooperação técnica ou documentos similares com órgãos de segurança-inteligência podem ser imprescindíveis, caso a fração de inteligência laboratorial não consiga sozinha acesso a bases de dados que permitam obter informações necessárias para a análise de segurança e de ameaças.

A implementação de planos de bioproteção não podem prescindir, conforme discutido, de conhecimentos de inteligência sobre ameaças à custódia de

ABTS em ILS. Por isso, estruturas de inteligência precisam incentivar a integração eventual sistema de gerenciamento de riscos biológicos brasileiro com as frações de gestão de biossegurança e bioproteção destes laboratórios.

Um dos cenários futuros possíveis de vislumbrar, dianta da falta de arcabouço normativo que garanta sistemas efetivos de bioproteção laboratorial no Brasil, é que a ausência de integração adequada, por inércia de órgãos e sistemas de inteligência preexistentes, como a ABIN e o SISBIN, respectivamente, obrigarão aos gestores de biorriscos a pressionar pela implementação de um sistema de inteligência laboratorial (ou de inteligência em saúde) desvinculado do SISBIN e da ABIN.

Não necessariamente este sistema autônomo significaria o enfraquecimento da ABIN e do SISBIN, caso estes atores não percebam como de sua competência atuar efetivamente para consolidar a troca de informações e a realização de ações e serviços concatenados com a bioproteção laboratorial.

Assim como a OMS e a OPAS criaram estratégias de inteligência epidemiológica próprias, independente da parceria com órgãos de inteligência multilaterais, a inteligência em saúde, inclusive a laboratorial, no Brasil pode seguir caminhos paralelos de atuação efetiva, com autonomia adequada e busca de cooperação com órgãos de segurança e defesa independentemente do acionamento de canais do SISBIN ou dependência de outros órgãos de inteligência nacionais para planejar e implementar sua atuação (ou ampliação, no caso a Rede CIEVS, que já funciona como estrutura de inteligência epidemiológia e, portanto, de inteligência em saúde).

Entretanto, é importante que a OMS reconheça a necessidade de valorizar, no que tange à bioproteção, os aspectos de integração entre o setor saúde e o setor de segurança-inteligência, em todos os níveis, de local a nacional.

O seu *Guia para a implementação de requisitos regulatórios de biossegurança e bioproteção em laboratórios biomédicos* [tradução nossa][123] necessita de retificação para considerar aspectos importantes de BPL que foram ignorados nos setes passos de implementação de um NBBF efetivo.

Quando, no quarto passo (*Fortalecer o conhecimento regulatório*), o Guia propõe a criação de um comitê de assessoramento científico independente - e/ou desenvolva competências de assessoramento internamente em órgãos ou agências governamentais -, não há preocupação expressa em que haja assessoramento de

segurança-inteligência no arcabouço regulatório, com a ênfase que se dá em outros assessoramentos igualmente importantes[123, p.52].

Quanto ao passo cinco (*Implementar e reforçar regulamentações*), a OMS cita diversos desafios potenciais, mas quase todos focados na implementação de aspectos de biossegurança laboratorial, conforme supracitado. A dificuldade de integração com órgãos de segurança-intelgência não é mencionada, assim como não são citados como desafios erros quanto à avaliação de ameaças e de riscos de BPL[123, pp.43-50].

Quanto ao passo seis (*Estabelecer redes de troca de informação nacionais e parcerias internacionais*), são especificadas possíveis canais interinstitucionais para troca de informações em nível nacional, mas nenhum deles emnciona a interação do setor saúde com segurança-inteligência[123, p.51].

Depreende-se dessas análises quea implementação de um modelo baseado no Guia da OMS, assim como no seu GBL2, tende a ser pouco integrado intersetorialmente e de baixa efetividade para um efetivo monitoramento de risco (*risk assessment*), que não pode prescindir do binômio segurança-inteligência.

Ferramentas como o *PathoFinder Brazil*® e o CIR têm potencial significativo para fortalecer a governança dos riscos biológicos, nesta perspectiva de atuação estruturada de uma inteligência laboratorial integrada a esta governança.

Por fim, ressalte-se que a integração de ciberbioproteção com bioproteção laboratorial e com a biodefesa é essencial para a segurança de dados e de infraestruturas críticas laboratoriais.

Em suma, os cinco principais problemas – ou lacunas normativas - apontados na discussão da pesquisa são a:

1. Ausência de MCE, MCR e MCM para controle dos riscos de bioproteção laboratorial, nos moldes do existente para riscos de biossegurança no LBM4;
2. Falta da ênfase necessária aos componentes de intersetorialidade e de ciberbioproteção nas diretrizes sobre medidas controle de risco de bioproteção laboratorial;
3. Ausência de arrolamento de ações redução de riscos de bioproteção laboratorial, com base nas estratégias de redução de risco;
4. Indisponibilidade de exemplos de análises de risco baseadas em ameaças de bioproteção laboratorial; e

5. Carência de indicações da necessidade de intergração do setor saúde com o setor segurança-inteligência na construção do NBBF segundo a OMS.

Coube ao presente estudo, no que tange a essas lacunas, servir de um ponto de partida para a necessária discussão dessas melhorias. Entende-se que os necessários aprimoramento, no campo da bioproteção laboratorial, somente serão viabilizados mediante uma maior transdisciplinaridade no debate teórico-acadêmico sobre gestão de biossegurança e bioproteção laboratoriais; e por meio de uma maior aproximação dos órgãos e frações de saúde-segurança-inteligência-defesa nos corpos editores e revisores das diretrizes nacionais e internacionais sobre tema.

6.4 Limitações do presente estudo

6.4.1 *PathoFinder Brazil®*

A ferramenta de avaliação de risco *PathoFinder Brazil®* depende da disponibilização de bases de dados sobre pesquisas e pesquisadores em fontes abertas. Ela será tanto mais efetiva, quanto mais completas as bases disponibilizadas, que comporão os *datasets* da ferramenta.

Neste sentido, o bom funcionamento da ferramenta é dependente das bases disponibilizadas por plataformas de currículos e de financiamento de pesquisas.

A versão do programa apresentada é a inicial (experimental), portanto passível de melhorias e atualizações, por isso é limitado o número de patógenos pré-selecionados para as buscas.

Há previsão de que futuras versões incluam a digitação de qualquer palavra de busca, permitindo a procura por qualquer agente biológico e toxina de interesse e até termos relacionados a PGC/PUD.

Além disso, é possível que a utilização da ferramenta por órgãos governamentais possam ampliar o acesso a bases que não estejam abertas na rede mundial, mas restritas a certos órgãos. Deste modo, a qualidade e quantidade dos resultados do *PathoFinder Brazil®* cresceria.

Ressalte-se que, por ser uma ferramenta vinculada a bases de dados de artigos científicos, pesquisas e pesquisadores, seus resultados são concentrados em locais de pesquisa em universidades ou centros de pesquisa. Essa limitação, entretanto, é de certa fora interessante, sob o ponto de vista da inteligência laboratorial, porque permite conhecer laboratórios que, no Brasil, tendem a ser mais ocultos do que os laboratórios com algum vínculo com o MAPA ou o MS.

6.4.2 *Checklist* RAMPA *(CIR)*

A apresentação de um *checklist* original de avaliação de sistemas de bioproteção como o CIR intenciona servir como um ponto de partida prático para que os laboratórios brasileiros e seus gestores possam utilizar e avaliar eventuais vulnerabilidades nos sistemas de bioproteção laboratorial.

O CIR é fruto de um trabalho teórico original, baseado na literatura especializada mais recente sobre o assunto, assim como em normas internacionais de bioproteção laboratorial.

Partiu-se do conceito igualmente original de sistema de controle ampliado de riscos de bioproteção para se chegar a dezenas de quesitos que, ao serem espondidos e detalhadas no questionário, permitem ao avaliador do sistema traçar um diagnóstico quanto às vulnerabilidades da ILS.

Estas respostas precisam ser analisadas à luz do conhecimento sobre ameaças, de modo que o questionário sozinho, *per si*, é limitado para apontas falhas de bioproteção laboratorial. Somente ao ser cotejado com as ameaças potenciais, pode-se apontar as falhas do sistema.

Por isso, e vale ressaltar, o CIR precisa ser idealmente aplicado por uma pessoa que conheça os riscos biológicos associados ao laboratório sob avaliação. Além disso, há recomendação expressa da OMS para que as pessoas envolvidas diretamente com as PGC/PAI e o trabalho laboratorial com MBGC/ABTS não sejam as responsáveis pela execução do monitoramento de risco (*risk assessment*)[22, p.22], consequentemente nem pela aplicação do CIR – que é parte do processo de monitoramento de risco.

Neste sentido, o CIR é uma ferramenta pensada não como passível de amplo uso por quaisquer especialistas em biossegurança e em bioproteção, mas de uso restrito a analistas de inteligência laboratorial, que dominem tanto os conhecimentos de ameaças àquele laboratório quanto às consequências potenciais de eventos de mal-uso dos agentes ali custodiados.

Ressalte-se ainda que o CIR precisa ser adequadamente validado mediante aplicações em LAC e ILS e posterior análise minuciosa de resultados. Encoraja-se, portanto, que ele seja aplicado por especialistas em biossegurança e bioproteção laboratoriais, a fim de seja revisado por pares quanto à sua utilização na prática.

Há margem, portanto, para mais pesquisa e consequente aprimoramento do CIR. Como toda avaliação de sistemas de proteção, na forma de questionário, ele precisa de constante atualização e adaptação ao eventual surgimento de novas tecnologias de segurança e de novas ameaças, tanto na forma de MBGC quanto na forma de PGC.

Ressalte-se que o CIR não substitui um processo completo de monitoramento de risco, tal como exemplificado e analisado nos capítulos 2 e 6. Mas

ele auxilia na obtenção de dados (passo 1); na medição de riscos (passo 2); no desenvolvimento de uma estratégia de controle de riscos (passo 3); no planejamento de medidas de controle de risco (passo 4).

Se aplicada após a implementação de medidas de controle de risco (passo 4), o CIR pode servir como auxiliar para a revisão de riscos e suas medidas de controle (passo 5).

Considerando se tratar da primeira versão do *checklist*, enfatiza-se que inicialmente voltado para a bioproteção laboratorial, ele pode ser aprimorado com a incorporação de novos e mais detalhados elementos de ciberbioproteção como: a segurança dos sistemas de tecnologias da informação laboratorial; protocolos de proteção contra ataques cibernéticos; e mecanismos de criptografia para informações sensíveis, entre outras questões especializadas e que são parte essencial da moderna proteção laboratorial.

Por fim, cabe ressaltar que o reconhecimento e análise de lacunas nas diretrizes de biossegurança e bioproteção laboratoriais não buscam resolver estas lacunas em definitivo, mas abrem espaço teórico-acadêmico para novas pesquisas sobre o tema, além de estimular pesquisadores a contribuírem diretamente com as organizações multilaterais no sentido de revisarem os documentos e buscarem preencher as lacunas existentes.

7. CONCLUSÕES

A presente tese buscou abordar de forma abrangente os desafios e as oportunidades para a gestão de biossegurança e bioproteção laboratorial no Brasil, com enfoque especial no desenvolvimento de ferramentas práticas e conceituais para fortalecer as capacidades nacionais em consonância com padrões internacionais.

A análise e discussão empreendidas se deram sob a perspectiva da inteligência de Estado, permitindo uma leitura transdisciplinar de documentos-chave de B2L. Os principais achados podem ser sintetizados e divididos em cinco tópicos principais.

7.1 Avanços conceituais em bioproteção e biodefesa laboratoriais

Foi proposta uma abordagem transdisciplinar que integra bioproteção laboratorial, biodefesa e inteligência, com destaque para a relevância da inteligência laboratorial como elo entre sistemas de biossegurança e bioproteção e os sistemas nacionais de inteligência. Essa integração permite não apenas antecipar riscos, mas também alinhar esforços intersetoriais para prevenir e mitigar eventos biológicos, intencionais ou acidentais, com impacto potencial na saúde pública.

O desenvolvimento do *PathoFinder Brazil*® demonstrou sua aplicabilidade na identificação e monitoramento de riscos biológicos, reforçando a importância da inteligência laboratorial na gestão de biossegurança e biodefesa. Além disso, a proposta do *Checklist* RAMPA (CIR) permitiu um avanço significativo na avaliação de bioproteção laboratorial, sugerindo um modelo adaptável à realidade brasileira. No entanto, os desafios persistem, especialmente na integração entre inteligência laboratorial e segurança da saúde. Recomenda-se, para pesquisas futuras, a implementação de sistemas mais avançados de IA para aprimoramento da análise preditiva e a criação de normativas específicas para a ciberbioproteção de laboratórios sensíveis.

7.2 **Desenvolvimento de ferramentas inovadoras**

Conclui-se que a ferramenta *PathoFinder Brazil*® se mostrou promissora como um recurso estratégico para identificação de laboratórios e pesquisadores com potencial de manipulação de agentes biológicos selecionados. O sistema destaca-se pela sua capacidade de mapeamento interativo e análise de risco, constituindo-se como um importante aliado na implementação de programas de monitoramento, como o PANGEIA/ABIN, e na estruturação de subsistemas de inteligência laboratorial.

O *PathoFinder Brazil*® é um programa inovador para uso em inteligência laboratorial e que atua na interseção entre biossegurança, bioproteção e biodefesa. Ao fornecer um mapeamento detalhado de laboratórios e pesquisas que lidam com agentes biológicos de interesse, permite antecipar ameaças potenciais, facilitando ações preventivas em segurança da saúde e biodefesa.

A integração de técnicas de inteligência artificial com o *PathoFinder Brazil*® permitiria uma análise mais eficiente de grandes volumes de dados sobre laboratórios, sobre pesquisadores e sobre pesquisas relacionadas a agentes biológicos de alto risco.

A aplicação de aprendizado de máquina (*Machine Learning***)** pode ampliar a capacidade preditiva do programa, tornando-o uma ferramenta essencial para antecipação e mitigação de ameaças biológicas no contexto da segurança da saúde e da biodefesa.

Paralelamente, o *Checklist RAMPA (ClR)* foi desenvolvido como um modelo prático e adaptável para avaliação de sistemas de bioproteção laboratorial. Esse instrumento fornece diretrizes operacionais para a identificação de vulnerabilidades e implementação de medidas escalonadas de proteção, alinhadas às necessidades específicas dos laboratórios de alta contenção no Brasil.

A inclusão de novos critérios de segurança, alinhados às melhores práticas internacionais, permite sua utilização em diferentes cenários laboratoriais, ampliando sua aplicabilidade prática. Além disso, a proposta de incorporação da ciberbioproteção e da intersetorialidade ao ***checklist*** representa um avanço significativo na proteção de informações estratégicas e infraestrutura laboratorial, garantindo uma abordagem mais robusta e integrada.

7.3 Fortalecimento da governança intersetorial em biossegurança e bioproteção

A tese identificou lacunas significativas na estrutura regulatória brasileira e propôs ações concretas para superá-las. Entre elas, destaca-se a necessidade de criação de um sistema nacional de monitoramento e notificação compulsória de agentes biológicos selecionados, que dialogue com padrões internacionais, como o Regulamento Sanitário Internacional (RSI) da OMS.

A aplicabilidade da plataforma *PathoFinder Brazil*® extrapola a inteligência laboratorial, podendo ser utilizada como uma ferramenta estratégica de para ações integradas de órgãos e frações de inteligência, forças de segurança e autoridades em saúde regionais e global na identificação de riscos e no fortalecimento das estratégias de biodefesa e resposta a ameaças biológicas**.**

7.4 Incorporação da ciberbioproteção ao paradigma de segurança laboratorial

Embora ainda emergente, a ciberbioproteção foi identificada como um dos elementos centrais na gestão de riscos laboratoriais, especialmente diante do aumento das ameaças digitais e do uso crescente de tecnologias conectadas. A tese sugere a adoção de medidas integradas de segurança cibernética e física para garantir a proteção de dados estratégicos, alinhando-se às melhores práticas globais.

A bioproteção e a biodefesa laboratoriais evoluem diante de novas ameaças, exigindo a integração com estratégias de ciberbioproteção. A digitalização de sistemas laboratoriais, bancos de dados e redes de compartilhamento de informações torna essencial o desenvolvimento de metodologias que contemplem não apenas a proteção física e operacional, mas também os desafios da segurança cibernética em ambientes laboratoriais. O Checklist RAMPA (CIR) se propõe a preencher essa lacuna, oferecendo uma ferramenta estruturada para avaliar e mitigar riscos de forma integrada.

Dada a crescente interdependência entre segurança digital e biológica, a ciberbioproteção deve ser considerada uma prioridade dentro das estratégias de B2L, segurança da saúde e biodefesa. A presente tese demonstrou que ferramentas como o *PathoFinder Brazil*® e o *Checklist* RAMPA (CIR) podem ser utilizadas para

integrar inteligência laboratorial, bioproteção e cibersegurança, garantindo que os laboratórios selecionados estejam protegidos não apenas contra ameaças físicas, mas também contra ataques digitais que possam comprometer a segurança humana.

7.5 Contribuição para políticas públicas e capacitação técnica

A pesquisa oferece subsídios para a formulação de políticas públicas voltadas ao fortalecimento da biossegurança e bioproteção laboratorial, além de contribuir para a capacitação de profissionais da área. As ferramentas e modelos propostos podem ser aplicados em programas de treinamento e avaliação, promovendo uma cultura de segurança e proteção alinhada às demandas do contexto brasileiro e internacional.

Em suma, a tese propõe um avanço significativo na compreensão e na prática da gestão de riscos laboratoriais no Brasil, contribuindo tanto para a segurança da saúde pública quanto para o fortalecimento da posição do país no cenário internacional. Os resultados aqui apresentados não apenas respondem às lacunas existentes, mas também abrem caminhos para futuras pesquisas e implementações, especialmente nas áreas de inteligência laboratorial, ciberbioproteção e biodefesa.

A necessidade de políticas públicas que consolidem a notificação compulsória de agentes biológicos selecionados, o fortalecimento da inteligência laboratorial e a incorporação da ciberbioproteção aos protocolos de segurança deve ser considerada prioridade para o Estado.

8. CONSIDERAÇÕES FINAIS

A presente tese propôs um modelo integrado para a gestão de B2L, na perspectiva da segurança da saúde e biodefesa, com ênfase na inteligência laboratorial, na intersetorialidade e na ciberbioproteção como elementos essenciais. A pesquisa demonstrou a necessidade de consolidar um arcabouço que contemple desde a proteção física de laboratórios até a mitigação de riscos digitais, destacando a importância de estratégias preditivas e de monitoramento contínuo para evitar eventos de bioproteção (relacionados a ameaças intencionais) em laboratórios nacionais.

Apesar do reconhecimento de que a gestão de biorriscos laboratoriais deve dar igual ênfase à biossegurança e à bioproteção[22], as lacunas supracitadas nas normas e recomendações teóricas e práticas de bioproteção laboratorial apontariam para uma maior dificuldade de planejar e implementar medidas na áera de BPL, em comparação com a área de biossegurança laboratorial, mais tradicionalmente estudada e praticada.

Na prática, tais ausências nas normas, recomendações e boas práticas de bioproteção laboratorial, ao relegar a bioproteção a um segundo plano normativo-institucional, dificultam a implementação de programas de bioproteção.

Esta realidade é ainda mais consolidada pelo fato de que um sistema de bioproteção ampliado e efetivo depende de uma adequada integração entre gestores de saúde e laboratórios com gestores de segurança e inteligência.

Caberia até questionar a classificação básica de níveis de biossegurança laboratorial (NB) para caracterizar os laboratórios. Se as medidas de biossegurança dependem de medidas de controle de riscos de bioproteção, não há que se falar em NB-1/NB-2/NB-3/NB-4, mas em Nível de Biossegurança e Bioproteção (NBB)-1/NBB-2/NBB-3/NBB-4.

É necessário mudar a cultura, ainda muito prevalente, apesar de avanços recentes descritos, da falta de integração entre biossegurança e bioproteção laboratoriais, que reflete a falta de integração entre os setores de saúde e segurança-inteligência nas estruturas do Estado.

Por isso, buscou-se demonstrar que a criação de estruturas transdisciplinares de inteligência laboratorial e/ou a participação de profissionais de segurança-inteligência no gerenciamento de biorriscos laboratoriais são necessárias

para a aproximação do setor de saúde (e laboratorial) com o setor de segurança-inteligência.

A gestão de bioproteção laboratorial é a área vinculada à inteligência laboratorial que mais se beneficiaria da integração saúde-segurança-inteligência, na medida em que depende de conhecimentos produzidos pelas polícias e por sistemas (ou subsistemas) de inteligência para caracterizar as ameaças biológicas; para identificar e medir os riscos associados a estas ameaças; e para adequar e avaliar dos sistemas de controle de tais riscos.

Considerando que a gestão efetiva de B2L se constitui capacidade-chave dos Estados perante as obrigações do RSI, a estratégia de fortalecimento da inteligência epidemiológica, no âmbito da OPAS e OMS, deveria incluir a inteligência laboratorial em toda a sua abrangência e não apenas focar no alerta precoce (*early warning*).

Caberia à OPAS e à OMS expandir a estratégia com vistas à criação de capacidade de gestão efetiva de biossegurança e bioproteção, incluindo as análises de ameaças com base nas quais devem ser planejados e implementados sistemas de bioproteção ampliados em laboratórios com os biorriscos mais relevantes.

Destarte, é possível migrar de um paradigma de resposta rápida (*rapid response*) para um outro paradigma: o de antecipação, prevenção e preparo (ou *predict, prevent, prepare* – P3)[124].

Essa ideia altera o clássico P2R2, que coloca a resposta e a reconstrução (R2) em um mesmo patamar da prevenção e do preparo (P2). Com o “novo” P3, ratifica-se a prioridade de antecipar, prevenir e se preparar contra eventos biológicos.

A ideia do P3 está vinculada ao fortalecimento da inteligência em saúde, proque a antecipação é objetivo finalístico da AI. Mas também está vinculada à ciência, porque são os conhecimentos científicos que conferem ferramentas que são muitas vezes – se não todas – requisitos para a antecipação e prevenção adequadas.

Desta forma, as ciências biomédicas e a inteligência em saúde se complementam nessa abordagem moderna e modernizante da atividade de inteligência de Estado.

Na falta de iniciativa da ABIN ou dos demais órgãos do SISBIN para ampliar os temas priorizados na atividade de inteligência brasileira incluindo aqueles de interesse da biossegurança e da bioproteção laboratoriais, o MS e a ANVISA

teriam legitimidade para planejar e implementar sistema de inteligência em saúde, incluindo a inteligência laboratorial entre os seus elementos centrais de produção e troca de informações.

Na implementação de sistemas de bioproteção laboratorial, o elemento da bioproteção intersetorial é o que impõe os maiores desafios. Não se deve prescindir do aprimoramento de integração saúde-segurança-defesa, em três níveis:

1. Local - entre os laboratórios com as forças de segurança locais, com vistas a uma resposta efetiva em caso de ameaças;
2. Estadual-Nacional - entre secretarias estaduais e polícias com os laboratórios e órgãos que administram os laboratórios; entre ministérios e órgãos federais com os laboratórios e seus órgãos; e entre os gestores estaduais e federais para a aprovação de verbas e leis que possibilitem a implementação de medidas de bioprteção efetivas;
3. Internacional – entre os laboratórios e órgãos multilaterais como a OPAS, a OMS e a INTERPOL, sem excluir o Comitê da Resolução 1540, a ISU da BWC e o RSI.

Em todos esses níveis, deve-se estabelecer troca de informações e fluxos de processos adequado. Para tanto, frações de inteligência laboratorial poderiam assumir o papel de ponto focal destas conexões.

Não há necessidade destas frações explicitarem o termo “inteligência” na sua nomenclatura. A principal rede de inteligência epidemiológica humana no Brasil se chama Rede CIEVS, por exemplo, e não dexa de ser uma estrutura de inteligência em saúde.

Sob o ponto de vista das políticas públicas, é necessário o desenvolvimento de um marco normativo que considere especificamente os aspectos próprios da bioproteção laboratorial, inclusive o componente da bioproteção intersetorial e as competências integradas, quando houve cabimento, de órgãos de segurança, inteligência e defesa.

Ressalte-se que o ponto de partida de um marco nacional de bioproteção laboratorial deveria ser a notificação compulsória da custódia de ABTS, a fim de que o Estado tenha ciência de onde estão os principais riscos biológicos laboratoratoriais em seu território, a partir da qual serão operacionalizadas medidas de garantia de sistemas efetivos de biossegurança e bioproteção laboratoriais.

Independente de um marco normativo amplo, como uma política, pode haver o estabelecimento de marcos normativos menores – no sentido de menos estratégicos -, em nível ministerial ou até infra-ministerial, por exemplo, com o fito de compor medidas necessárias para robustecer a governança de bioproteção laboratorial.

A necessidade de uma política nacional que claramente facilitaria a implementação de uma cultura e de uma governança nacional mais robusta de biossegurança e bioproteção laboratoriais não pode ser condição necessária para o planejamento de medidas “infra-estratégicas”, isto é, de medidas promulgadas como portarias ou normas ministeriais, ou até interministeriais, mas não vinculadas a políticas e estratégias nacionais subordinadoras.

A notificação compulsória de ABTS/MBGC, por exemplo, entende-se que já poderia ser implementada por meio da complementação da Lista Nacional de Notificação Compulsória de Doenças, Agravos e Eventos de Saúde Pública.

Em muitos países, a avaliação de riscos laboratoriais é uma obrigação legal[13, p.34]. No Brasil, mesmo que não seja, em nível nacional, objeto de lei ou política específicas, é também uma obrigação legal, na medida em que estamos obrigados legalmente (via ratificação do RSI) a mantermos operações laboratoriais seguras (*safe*) e protegidas (*secure*).

Como não é possível haver operação laboratorial segura e protegida sem monitoramento/avaliação de riscos, entende-se que o processo de *risk assessment* é legalmente obrigatório no Brasil, conforme padrões internacionais e esta obrigação deveria ser regulamentada por normas legais (ou infralegais na ausência destas).

Na ausência de normas regulamentadoras, não pode a gestão laboratorial se esquivar da obrigação legal. Neste sentido, a gestão laboratorial deve buscar ferramentas para cumprir a obrigação internacional, como a adequada aplicação do *Checklist RAMPA*, além de pressionar por regulamentações adequadas.

Quanto ao uso do CIR, restou claro que a interpretação de suas respostas é o que caracterizará uma avaliação adequada dos sistemas de medidas de controle de risco. Deste modo, a mera aplicação do questionário, seo devido cotejamento da identificação e medição de riscos com as medidas implementadas, não é suficiente para um efetivo monitoramento de risco. Tão importante quanto a qualificação do aplicador do questionário, é a qualificação do avaliador do CIR, que podem ser a mesma pessoa.

Ressalte-se, todavia, que o CIR não resolverá o problema da necessária integração multissetorial, que não pode prescindir de governança nomativa robusta, porque, muitas vezes, é a norma que garante o diálogo interinstitucional, sobretudo de áreas tão historicamente dissociadas quanto a saúde-segurança.

A possibilidade de colaboração com instituições multilaterais, como a OPAS, OMS, INTERPOL, Comitê da Resolução 1540 e ISU da CPABpermitiria ampliar a busca de parcerias para a construção da bioproteção laboratorial efetiva no Brasil. E esta cooperação também não pode prescindir de instrumentos normativos e programas de cooperação integrantes de uma governança robusta na área de biossegurança e bioproteção laboratoriais.

O estabelecimento de programas de preparo e treinamento em inteligência laboratorial e ciberbioproteção são fundamentais neste processo de planejamento e consolidação de estruturas da gestão de biossegurança e bioproteção laboratoriais. Afinal, o ciclo P2R2 necessita de medidas de aperfeiçoamento em cada elemento seu, e o preparo (*preparedeness*) é condição necessária para a resposta efetiva.

É mister reconhecer que o avanço no debate acadêmico e institucional brasileiro sobre gestão de biossegurança e bioproteção, materializado entre outros fatores, pela agregação multidisciplinar de especialistas sob a égide da Sociedade Brasileira de Biossegurança e Bioproteção (SB3), alça o país à condição de participante significativo dos fóruns e publicações multilaterais sobre o assunto.

A SB3 e os especialistas brasileiros, independentemente das dificuldades de implementação de medidas ideais de controle de riscos em instituições nacionais, deveriam participar das revisões de documentos-chave multilaterais sobre B2L, a exemplo do LBM e do GBL.

Cabe finalizar defendendo o incentivo, inclusive por programas estatais, para participação de especialistas brasieiros em comissões, grupos técnicos e trabalhos - até dos mais altos níveis consultivos ou decisórios - em âmbito da OPAS e OMS, entre outras organizações multilaterais que lidem indireta ou diretamente com gestão da biossegurança e da bioproteção laboratoriais.

Por fim, esta tese reafirma que a ***bioproteção laboratorial, a segurança da saúde e a biodefesa*** *devem ser entendidas como elementos fundamentais da segurança humana, exigindo um planejamento estratégico que integre* ***inteligência, tecnologia e governança****. O aprofundamento da transecuritização da inteligência brasileira e a formalização de (sub)sistemas específicos de inteligência laboratorial*

são caminhos para garantir maior efetividade na antecipação de ameaças e no fortalecimento das capacidades de resposta a riscos biológicos, muitas das quais em atendimento a obrigações internacionais.

As contribuições deste trabalho poderão servir de base para futuras pesquisas e para o aprimoramento de estratégias nacionais e internacionais de proteção contra ameaças biológicas, consolidando um novo paradigma para a segurança da saúde no século XXI.

9. REFERÊNCIAS

1. COELHO, D. **Emergências em Saúde Pública por Eventos Químicos, Biológicos, Radiológicos e Nucleares (QBRN) na Perspectiva da Inteligência Estratégica**: Recomendações em Prol da Intersetorialidade na Segurança da Saúde e na Biodefesa. Orientador: José Francisco Nogueira Paranaguá de Santana. 2017. 294 f. Dissertação (Mestrado em Políticas Públicas em Saúde) - Fundação Oswaldo Cruz, Brasília, 2017.

2. SALERNO, R.M; GAUDIOSO, J. **Laboratory Biosecurity Handbook**. Boca Raton: CRC Press, 2007.

3. MENDONÇA, A.O. **Enhancing Biosafety Management and Governance: A Comprehensive Assessment of High-Containment Biological Laboratories in Brazil**. Orientador: Cláudio Lísias Mafra de Siqueira. 2024. 398 f. Tese (Doutorado em Bioquímica Aplicada) - Universidade Federal de Viçosa, Viçosa, 2024.

4. MAFRA, C. **Pensando uma infraestrutura estratégica nacional**: o laboratório NB-4 brasileiro. 1. ed. Visconde do Rio Branco: Suprem Gráfica, 2020.

5. WORLD ECONOMIC FORUM. **The Global Risks Report 2024**. 19. ed. 124p. ISBN: 978-2-940631-09-4. Disponível em: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf. Acesso em: 02 jan. 2024.

6. DATANNI, S. **What were the death tolls from Pandemics in history? Our** World in Data, 07 dez. 2023. Disponível em: https://ourworldindata.org/historical-pandemics. Acesso em 05 jul. 2024.

7. LENTZOS, F (org.). **Biological Threats in the 21st Century**. London: Imperial College Press, 2016.

8. AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. **Doutrina da Atividade de Inteligência**. Brasília: ABIN, 2023.

9. ANDREW, C.; ALDRIGHT R. J.; WARK, W. K (org.). **Secret Intelligence – a Reader**. 2. ed. New York: Routledge, 2019.

10. PAN-AMERICAN HEALTH ORGANIZATION. **Epidemic Intelligence.** Disponível em: https://www.paho.org/en/topics/epidemic-intelligence. Acesso em 19 nov. 2024.

11. KOBLENTZ G.; LENTZOS F. **Risks, Trade-Offs & Responsible Science**. Oslo: International Law and Policy Institute; BWC Review Conference Series. 2016; 3.

12. DAVISON N. **The Role of Scientific Discovery in the Establishment of the First Biological Weapons Programmes**. Bradford Project on Strengthening the Biological and Toxin Weapons Convention (BTWC) 2005.

13. SALERNO, R.M; GAUDIOSO, J. (Editors). **Laboratory Biorisk Management:** Biosafety and Biosecurity. Boca Raton: CRC Press, 2020.

14. GLOBAL CHALLENGES FOUNDATION. **12 Risks that threaten human civilisation**. Stockholm: Global Challenges Foundation; 2015.

15. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 35001:2019. Gestión del riesgo biológico en laboratorios y otras organizaciones relacionadas**. Geneva: ISO, 2019.

16. WORLD HEALTH ORGANIZATION. **Laboratory Biosafety Manual.** 4. ed. Geneva: World Health Organization, 2020. 124p. ISBN: 978-92-9-49001131-1. Disponível em: https://www.who.int/publications/i/item/9789240011311. Acesso em: 02 de fevereiro de 2024.

17. CENTERS FOR DISEASE CONTROL AND PREVENTION. **Biosafety in Microbiological and Biomedical Laboratories**. 6. ed. Atlanta: CDC, 2020.

18. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 17069-1. Biossegurança e bioproteção – infraestrutura laboratorial. Parte 1: **Requisitos específicos para o nível de biossegurança 1 (NB-1**). Rio de Janeiro: ABNT, 2023.

19. CENTERS FOR DISEASE CONTROLE AND PREVENTION. **Biosafety in Microbiological and Biomedical Laboratories**. 5. ed. Atlanta: CDC, 2009.

20. BURNETTE, R. N (Editor). **Applied Biosecurity**: Global Health, Biodefense and Developing Technologies. Washington D.C.: Springer; 2021.

21. CHAMOVICH, H. **Biosseguridade**. Estudos Avançados 2005; 19(55): 261-269.

22. WORLD HEALTH ORGANIZATION. **Laboratory Biosecurity Guidance**. Geneva: WHO; 2024.

23. WORLD HEALTH ORGANIZATION. **Biorisk management - Laboratory biosecurity guidance** (WHO/CDS/EPR/2006.6). Geneva: WHO; 2006.

24. BRASIL. **Constituição Federal de 1988**.

25. CALDAS, M.M.; PERZ, S. **Agro-terrorism? The causes and consequences of the appearance of witch's broom disease in cocoa plantations of southern Bahia, Brazil**. Geoforum 2013; (47); 147-157.

26. ZANATTA M. Governo brasileiro se arma contra o "agroterrorismo". **Valor Econômico.** 18 out 2005. Disponível em: http://

www.defesanet.com.br/dqbrn/noticia/20722/Governo-brasileiro-se-arma-contra-o--agroterrorismo-/. Acesso em 10 out. 2023.

27. DONDOSSOLA, E. Câmeras flagram roubo ao laboratório da UFRJ, na Ilha do Fundão. **G1**. 30 jul. 2019. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/30/cameras-flagram-o-roubo-que-causou-prejuizo-incalculavel-a-laboratorio-da-ufrj-na-ilha-do-fundao.ghtml. Acesso em: 14 fev. 2024.

28. CONFEDERAÇÃO NACIONAL DA AGRICULTURA. **Panorama do Agro**. 2024. Disponível em: https://www.cnabrasil.org.br/cna/panorama-do-agro#:~:text=Atualmente%2C%20o%20Brasil%20é%20o,TradeMap%2C%20ITC%2C%202023). Acesso em: 12 out. 2024.

29. CENTRAL INTELLIGENCE AGENCY. The World Factbook – Brazil. 16 jan. 2025. Disponível em: https://www.cia.gov/the-world-factbook/countries/brazil/. Acesso em: 16 jan. 2025.

30. INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL. **PathoFinder Brazil: Localizando Patógenos Selecionados no Brasil**. 19 mar. 2024. Processo nº BR512024000746-6.

31. GEORGE MASON UNIVERSITY. **Institute for Biohealth Innovation**. Disponível em: https://ibi.gmu.edu/faculty-directory/gregory-koblentz/. Acesso em: 05 de junho de 2024.

32. KOBLENTZ, G.D. **Biosecurity Reconsidered**: Calibrating Biological Threats and Responses. International Security 2010; 34(4):96-132.

33. FOOD AND AGRICULTURE OGANIZATION OF THE UNITED NATIONS. **Biosecurity in Food and Agriculture**. Rome: Food and Agriculture Organization Committee on Agriculture; 2003.

34. FOOD AND AGRICULTURE OGANIZATION OF THE UNITED NATIONS. **Strengthening biosecurity for pest disease management**. Disponível em: https://www.fao.org/one-health/areas-of-work/biosecurity/en. Acesso em: 05 de junho de 2024**.**

35. WORLD HEALTH ORGANIZATION. **Laboratory Biosafety Manual**. 3. ed. Genebra: WHO; 2004.

36. CONVENTION ON THE PROHIBITION OF THE DEVELOPMENT, PRODUCTION AND STOCKPILING OF BACTERIOLOGICAL (BIOLOGICAL) AND TOXIN WEAPONS AND ON THEIR DESTRUCTION. **Report Of The Meeting Of State Parties**. Geneva: Meeting Of The State Parties to the BWC; 2008.

37. NATIONAL SCIENCE ADVISORY BOARD FOR BIOSECURITY. **About**. Disponível em: https://osp.od.nih.gov/policies/national-science-advisory-board-for-biosecurity-nsabb/. Acesso em: 06 de junho de 2024.

38. NATIONAL SCIENCE ADVISORY BOARD FOR BIOSECURITY. **Guidance for Enhancing Personnel Reliability and Strengthening the Culture of Responsibility.** Report of the NSABB; 2011.

39. NATIONAL SCIENCE ADVISORY BOARD FOR BIOSECURITY. **Enhancing Personnel Reliability among Individuals with Access to Select Agents.** Report of the NSABB; 2009. Disponível em: https://osp.od.nih.gov/wp-content/uploads/NSABB_Final_Report_-on_-PR-5-29-09.pdf. Acesso em: 24 jul. 2024.

40. WUNDER, R. **O Problema Político da Biodefesa no Brasil** [dissertação]. Niterói: Universidade Federal Fluminense; 2013.

41. CARDOSO T.A.O. **Análise da Construção da Competência do Brasil em Direção ao Laboratório de Contenção Máxima**: realidades e perspectivas [tese]. Rio de Janeiro: Escola Nacional de Saúde Pública Sergio Arouca; Fundação Oswaldo Cruz; 2008.

42. RAMBAUSKE D.; CARDOSO, T. A. O.; NAVARRO M. **Bioterrorismo, riscos biológicos e as medidas de biossegurança aplicáveis ao Brasil**. Revista de Saúde Coletiva 2014; 24(4): 1181-1205.

43. MINISTÉRIO DA SAÚDE. **Centro de Informações Estratégicas em Vigilância em Saúde**. Disponível em: https://www.gov.br/saude/pt-br/composicao/svsa/cievs. Acesso em: 03 set. 2024, às 16h43.

44. KEENEY J. D.; KOWALSKI, E. **Insider Threat Study**: System Sabotage in Critical Infrastructure Sectors. Washington: US Secret Service; CERT Coordination Center, 2005. p.22.

45. KAPLAN, S.; GARRICK, B.J. **On the Quantitative Definition of Risk**. Risk Analysis 1981; 1(1): 11-27.

46. ZHEN, L. **Chinese criminal gangs spreading African swine fever to force farmers to sell pigs cheaply so they can profit.** South China Morning Post, 14 dez. 2019; Olson, Kyle B., “Aum Shinrikyo: Once and Future Threat”, Emerging Infectious Diseases, Julho-Agosto 1999. Disponível em: https://www.ojp.gov/ncjrs/virtual-library/abstracts/aum-shinrikyo-once-and-future-threat#:~:text=The%20document%20questions%20whether%20the,time%2C%20seven%20people%20were%20dead. Acesso em: 19 fev. 2024.

47. ISLA, N. **Biological Weapons as a Public Health Issue**. In: Maclaughlin K, Nixdorff K. (Ed.). BWPP Biological Weapons Reader. Geneva: Bioweapons Prevention Project; 2009: p. 53-58.

48. **CONVENTION ON THE PROHIBITION OF THE DEVELOPMENT, PRODUCTION AND STOCKPILING OF BACTERIOLOGICAL (BIOLOGICAL) AND TOXIN WEAPONS AND THEIR DESTRUCTION**. 1972. Disponível em: https://front.un-arm.org/wp-content/uploads/2020/12/BWC-text-English-1.pdf. Acesso em 13 jun. 2024.

49. BOWICK, G. C.; BARRETT, A. D. T. **Comparative Pathogenesis and Systems Biology for Biodefense Virus Vaccine Development**. Journal of Biomedicine and Technology 2010; p. 1-11.

50. BALAKRISHNAN, V. S. **WHO-Germany collaboration for pandemic intelligence research**. The Lancet Microbe 2021; 2 (Julho): e290.

51. PAN-AMERICAN HEALTH ORGANIZATION. **Strategy on Epidemic Intelligence for Strengthning Early Warning of Health Emergencies 2024-2029** (CD61/12, Rev.1). 61st Directing Council. 76th Session of the Regional Committee of WHO for the Americas. Washington D.C.: 30 set. – 04 out. 2024. 14p.

52. WORLD HEALTH ORGANIZATION. **International Health Regulations**. 3.ed. 2005. Disponível em: https://iris.who.int/bitstream/handle/10665/246107/9789241580496-eng.pdf?sequence=1. Acesso em: 06 jan. 2023.

53. AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA. **Regulamento Sanitário Internacional** - RSI 2005. Brasília: ANVISA; 2009.

54. WORLD HEALTH ORGANIZATION. **Laboratory Biorisk Management Strategic Framework for Action 2012-2016**. Genebra: WHO; 2012.

55. PAN-AMERICAN HEALTH ORGANIZATION. **COVID-19 Pandemic in the Region of the Americas** (CD58.R9). 58th Directing Council. 72th Session of the Regional Committee of WHO for the Americas. Virtual Session: 28-29 set. 2024. 4p. Disponível em: https://iris.paho.org/bitstream/handle/10665.2/58229/CD58-R9-resolution_eng.pdf?sequence=1&isAllowed=y. Acesso em 30 mar. 2024.

56. ESTADOS UNIDOS DA AMÉRICA. ***Homeland Security Presidential Directive*** - 10, de 28 de abril de 2004. Biodefense for the 21st Century.

57. MINISTÉRIO DA DEFESA (BRASIL). **Portaria Normativa nº 585**, de 07 de março de 2013. Aprova as Diretrizes de Biossegurança, Bioproteção e Defesa Biológica do Ministério da Defesa. Diário Oficial da União 11 mar 2013; Seção 1.

58. BRASIL. **Decreto nº 8.905**, de 17 de novembro de 2016. Aprova a Estrutura Regimental da ABIN. Diário Oficial da União 18 nov 2016.

59. CONSELHO DE SEGURANÇA DA ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Resolução 1540**. Index: S/RES/1540. 18 abr. 2004. Disponível em: https://documents.un.org/doc/undoc/gen/n04/328/43/pdf/n0432843.pdf. Acesso em 14 jun. 2024.

60. Brasil. **Decreto nº 7.722**, de 20 de abril de 2012. Dispõe sobre a execução no Território Nacional das Resoluções no 1540 (2004), e no 1977 (2011), adotadas pelo Conselho de Segurança das Nações Unidas em 28 de abril de 2004 e em 20 de abril de 2011, as quais dispõem sobre o combate à proliferação de armas de destruição em massa e sobre a vigência do Comitê 1540.

61. CONSELHO DE SEGURANÇA DA ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Resolução 2663**. Index: S/RES/2663. 30 nov. 2022. Disponível em: https://documents.un.org/doc/undoc/gen/n22/716/75/pdf/n2271675.pdf. Acesso em 14 jun. 2024.

62. GARRAFA, V. **Da bioética de princípios a uma bioética interventiva.** Revista Bioética, 2009;13(1). Disponível em: https://revistabioetica.cfm.org.br/revista_bioetica/article/view/97. Acesso em 10 fev. 2023.

63. WORLD HEALTH ORGANIZATION. **Risk Assessment** - Laboratory Biosafety Manual Fourth Edition and Associated Monographs**.** Geneva: World Health Organization, 2020. 132p. Disponível em: https://iris.who.int/bitstream/handle/10665/337966/9789240011458-eng.pdf?sequence=1&isAllowed=y. Acesso em: 16 out. 2022.

64. WORLD HEALTH ORGANIZATION. **Strengthening WHO preparedness for and response to health emergencies** [Resolution WHA74.7]. Seventy-fourth World Health Assembly; 24 Maio–1 Junho 2021; Geneva. Geneva: WHO; 2021. Disponível em: https://apps.who.int/gb/ebwha/pdf_files/WHA74-REC1/A74_REC1-en.pdf. Acesso em: 20 out. 2023.

65. COMITE EUROPEEN DE NORMALISATION. CWA 15793:2011. **Laboratory biorisk management.** Bruxelas: CEN, 2011. Disponível em: https://internationalbiosafety.org/wp-content/uploads/2019/08/CWA-15793-English.pdf. Acesso em 27 ago. 2024.

66. ENVIRONMENTAL PROTECTION AGENCY. **An Examination of EPA Risk Assessment Principles and Practices**. 2004. Disponível em:

https://nepis.epa.gov/Exe/ZyNET.exe/100048RM.TXT?ZyActionD=ZyDocument&Client=EPA&Index=2000+Thru+2005&Docs=&Query=&Time=&EndTime=&SearchMethod=1&TocRestrict=n&Toc=&TocEntry=&QField=&QFieldYear=&QFieldMonth=&QFieldDay=&IntQFieldOp=0&ExtQFieldOp=0&XmlQuery=&File=D%3A%5Czyfiles%5CIndex%20Data%5C00thru05%5CTxt%5C00000008%5C100048RM.txt&User=ANONYMOUS&Password=anonymous&SortMethod=h%7C-&MaximumDocuments=1&FuzzyDegree=0&ImageQuality=r75g8/r75g8/x150y150g16/i425&Display=hpfr&DefSeekPage=x&SearchBack=ZyActionL&Back=ZyActionS&BackDesc=Results%20page&MaximumPages=1&ZyEntry=1&SeekPage=x&ZyPURL. Acesso em: 24 jul. 2024.

67. INTERNATIONAL CIVIL AVIATION ORGANIZATION. **SAFETY REPORT. 2023**. Disponível em: https://www.icao.int/safety/Documents/ICAO_SR_2023_20230823.pdf. Acesso em: 24 jul. 2024.

68. WORLD HEALTH ORGANIZATION. **Biorisk management advanced trainer programme**. 2014. Disponível em: https://www.emro.who.int/laboratories/lab-events/advanced-biorisk-management-training.html. Acesso em 24 jul. 2024.

69. CENTERS FOR DISEASE CONTROL. **About Tularemia**. Disponível em: https://www.cdc.gov/tularemia/about/index.html. Acesso em: 24 jul. 2024.

70. CENTERS FOR DISEASE CONTROL. **About Q Fever**. Disponível em: https://www.cdc.gov/q-fever/about/index.html. Acesso em: 24 jul. 2024.

71. MUELLER, S. **Facing the 2020 pandemic**: What does cyberbiosecurity want us to know to safeguard the future? Biosafety and Health 2021; 3:11-21.

72. PECCOUD, J.; GALLEGOS, J.E.; MURCH, R.; BUCHHOLZ, W.G.; RAMAN, S. **Cyberbiosecurity: from naive trust to risk awareness**, Trends Biotechnol. 2018; 36 (1), pp. 4–7. Disponível em: https://doi.org/10.1016/j.tibtech.2017.10.012. Acesso em 12 nov. 2024.

73. REED, J.C.; DUNAWAY, N. **Cyberbiosecurity implications for the laboratory of the future**. Front. Bioeng. Biotechnol. 7, 2019 (182). Disponíel em: https://doi.org/10.3389/fbioe. 2019.00182. Acesso em 14 nov. 2024.

74. BRASIL. **Lei nº 9.883**, de 7 de dezembro de 1999, institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, dá outras providências.

75. AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. **Missão, Visão e Valores.** Disponível em https://www.gov.br/abin/pt-br/institucional/missao-visao-e-valores-1. Acessado em em 30 nov. 2023.

76. BRASIL. **Resolução CREDEN nº 02/2009**, de 04 dez. 2009.

77. BRASIL. **Decreto nº 8.793**, de 29 jun. 2016. Fixa a Política Nacional de Inteligência. Diário Oficial da União, 30 jun. 2016.

78. BRASIL. **Decreto**, de 15 dez. 2017. Aprova a Estratégia Nacional de Inteligência. Diário Oficial da União, 18 dez. 2017, p.36.

79. GABINETE DE SEGURANÇA INSTITUCIONAL (PRESIDÊNCIA DA REPÚBLICA DO BRASIL). **Portaria nº 40**, de 03 maio 2018. Aprova o Plano Nacional de Inteligência (PLANINT).

80. GABINETE DE SEGURANÇA INSTITUCIONAL (PRESIDÊNCIA DA REPÚBLICA DO BRASIL). **Portaria nº 373**, de 03 out 2018. Aprova o Plano de Inteligência da ABIN.

81. BRASIL. **Decreto nº 11.816**, de 06 dez. 2023. Aprova a Estrutura Regimental e o Quardro Demonstrativo dos Cargos em Comissão, das Funções de Confiança e das Gratificações da Agência Brasileira de Inteligência, e remaneja e transforma cargos em comissão, funções de confiança e gratificações. Diário Oficial da União, 07 dez. 2023, 232(1): p.5.

82. AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. **Estrutura**. Atualizado em 22/05/2024. Disponível em: https://www.gov.br/abin/pt-br/institucional/estrutura. Acesso em: 25 jun. 2024.

83. AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. **Pangeia**. Atualizado em 30/11/2023. Disponível em: https://www.gov.br/abin/pt-br/institucional/acoes-e-programas/pangeia-1. Acesso em 30 jun. 2024.

84. GABINETE DE SEGURANÇA INSTITUCIONAL (BRASIL). **Portaria GSI/PR nº 112**, de 17 dez. 2018. Institui, no âmbito da Agência Brasileira de Inteligência (ABIN), o Programa Nacional de Articulação entre Empresas, Governo e Instituições Acadêmicas para a Prevenção e a Mitigação do Risco de Eventos Químicos, Biológicos, Radiológicos e Nucleares Selecionados (PANGEIA).

85. BRASIL. **Decreto nº 8.905**, de 17 nov. 2016. Aprova a Estrutura Regimental da ABIN. Diário Oficial da União, 18 nov. 2016. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8905.htm. Acesso em: 24 jul. 2024.

86. MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO. **PRONABENS**. Atualizado em 18 nov. 2022. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/cgbs/paginas/pronabens. Acesso em 15 jul. 2024.

87. SECRETARIA DE VIGILÂNCIA EM SAÚDE (MINISTÉRIO DA SAÚDE). **Portaria SVS/MS nº 30**, de 07 jul. 2005. Institui o Centro de Informações Estratégicas em Vigilância em Saúde, define suas atribuições, composição e coordenação. Disponível em: http://portalsinan.saude.gov.br/images/documentos/Legislacoes/Portaria_30_7_JULHO_2005.pdf. Acesso em: 24 jul. 2024.

88. MINISTÉRIO DA SAÚDE. **Centro de Informações Estratégicas em Vigilância em Saúde**. Disponível em: https://www.gov.br/saude/pt-br/composicao/svsa/cievs#:~:text=A%20Rede%20CIEVS%20desempenha%20um,a%20eventos%20de%20saúde%20pública. Acesso em 24 jul. 2024.

89. AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. **7 Ações**. 2019. [slide]. Apresentado em: 2ª Conferência Brasil Sul da Indústria e Produção de Ovos (Conbrasul), Gramado, 21 ago. 2019.

90. AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. **Tranversalidade Departamental**. 2019. [slide]. Apresentado em: 2ª Conferência Brasil Sul da Indústria e Produção de Ovos (Conbrasul), Gramado, 21 ago. 2019.

91. AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. **Compartimentação Temática**. 2019. [slide]. Apresentado em: 2ª Conferência Brasil Sul da Indústria e Produção de Ovos (Conbrasul), Gramado, 21 ago. 2019.

92. AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. **Integração Temática**. 2019. [slide]. Apresentado em: 2ª Conferência Brasil Sul da Indústria e Produção de Ovos (Conbrasul), Gramado, 21 ago. 2019.

93. **CARTAGENA PROTOCOL ON BIOSAFETY TO THE CONVENTION ON BIOLOGICAL DIVERSITY**. Montreal: Secretariat of the Convention on Biological Diversity; 2021. Disponível em https://www.cbd.int/doc/legal/cartagena-protocol-en.pdf. Acesso em: 12 nov. 2024.

94. CENTRAL INTELLIGENCE AGENCY. **About CIA – Mission and Vision**. Disponível em: https://www.cia.gov/about/mission-vision/. Acesso em: 24 set. 2024.

95. SECRET INTELLIGENCE SERVICE MI6. **HOME**. Disponível em: https://www.sis.gov.uk/index.html. Acesso em: 24 set. 2024.

96. SECURITY SERVICE MI5. **About Us**. Disponível em: https://www.mi5.gov.uk/about-us. Acesso em: 24 set. 2024.

97. COELHO, D. **A Modernização da Inteligência Estratégica nas Perspectiva da Segurança Humana**. Revista Brasileira de Inteligência, Brasília, Brasil, n. 12, p. 77–90, 2017. DOI: 10.58960/rbi.2017.12.143. Disponível em: https://rbi.abin.gov.br/RBI/article/view/143. Acesso em: 7 jan. 2025.

98. PERON, I. Preso pela PF, Marcelo Bormevet comandou Centro de Inteligência Nacional da Abin. **Valor Econômico**, 11 jul. 2024. Disponível em: https://valor.globo.com/politica/noticia/2024/07/11/preso-pela-pf-marcelo-bormevet-comandou-centro-de-inteligncia-nacional-da-abin.ghtml . Acesso em 25 dez. 2024.

99. SUDRÉ, L. Policial Federal de Juiz de Fora é um dos 37 indiciados em inquérito sobre tentativa de golpe. **G1**, 22 nov. 2024. Disponível em: https://g1.globo.com/mg/zona-da-mata/noticia/2024/11/22/policial-federal-de-juiz-de-fora-e-um-dos-37-indiciados-em-inquerito-sobre-tentativa-de-golpe.ghtml. Acesso em 25 dez. 2024.

100. AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. **Caderno de Realizações 2023**. Brasília: ABIN; 2023. 40p.

101. AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. **Relatório Anual 2024**. Brasília: ABIN; 2024.

102. LOPES, A.; COELHO, D.; FERREIRA, I.E.L.; LEITE, R. **Vigilância em Saúde.** Recife: EMR, 2023. 37p.

103. SIMAS, F. Orçamento de 2025 – veja os ministérios do governo Lula com as maiores e menores verbas. **TERRA**, 31 ago. 2024. Disponível em: https://www.terra.com.br/economia/orcamento-de-2025-veja-os-ministerios-do-governo-lula-com-as-maiores-e-menores-verbas,7184025868f3baef392a09d87de32ad7jx4dbb0v.html. Acesso em 24 jul. 2024.

104. OLIVEIRA, T; VARGAS, M. Abin fecha portaria de sede e reduz internet de celulares para cortasr gastos. **Folha de São Paulo**, 03 out. 2024. Disponível em: https://www1.folha.uol.com.br/poder/2024/10/abin-fecha-portaria-de-sede-e-reduz-internet-de-celulares-para-cortar-gastos.shtml. Acesso em 24 jul. 2024.

105. INTERNATIONAL STANDARDIZATION ORGANIZATION. **About ISO**. Disponível em: https://www.iso.org/what-we-do.html. Acesso em: 24 out. 2024.

106. AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. **Diretrizes ESINT 2024**. Brasília: ABIN, 2024.

107. BOBO, B. **COVID-19 and health care cybersecurity**: how to protect practices and patient data. Med Econ; 2020. Disponível em: https://www.medicaleconomics.com/view/covid-19-and-cybersecurity-protect-practices-and-patient-data. Acesso em: 12 nov. 2024.

108. MORGAN S. **Cybercrime to cost the world $10.5 Trillion annually by 2025**. Cybercrime Mag; 2020. Disponível em: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/. Acesso em: 12 nov. 2024.

109. ROBERTSON, J.; RILEY, M. **Mysterious 08 turkey pipeline blast opened new cyberwar era**. Disponível em: https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipe-line-blast-opened-new-cyberwar. Acesso em: 12 dez. 2024.

110. GEORGE MASON UNIVERSITY. **The Institute for Biohealth Innovation**. Disponível em: https://ibi.gmu.edu/faculty-directory/gregory-koblentz/. Acesso em: 24 dez. 2024.

111. TIDY, J. **Police launch homicide inquiry after German hospital hack**. BBC; 18 set. 2020. Disponível em: https://www.bbc.com/news/technology-54204356#. Acesso em: 24 dez. 2024.

112. CEPI. **Biosecurity Strategy – September 2024**. Disponível em: https://static.cepi.net/downloads/2024-09/CEPI%20Biosecurity%20Strategy_Sep%202024_Online%20Version.pdf. Acesso em: 26 dez. 2024.

113. Global Health Security Index. **Global Health Security Index**. Disponível em: https://ghsindex.org. Acesso em: 10 jan. 2025.

114. BRONZATTO, T.; BORGES, L. **Líder de grupo terrorista revela plano para matar Bolsonaro**. Revista Veja, 19 jul. 2019. Disponível em: https://veja.abril.com.br/brasil/bolsonaro-terror-capa-veja. Acesso em: 12 nov. 2024.

115. CARVALHO, J.; CAMPOREZ, P. **Presos 3 suspeitos de divulgarem ameaças contra Bolsonaro e colocarem bomba perto de igreja no DF**. O Gobo, 03 jan. 2019. Disponível em: https://oglobo.globo.com/politica/presos-3-suspeitos-de-divulgarem-ameacas-contra-bolsonaro-colocarem-bomba-perto-de-igreja-no-df-23342880. Acesso em: 12 nov. 2024.

116. Tribunal Regional Federal da 4ª Região. **Denúncia do MPF. Operação Hashtag**. 16 set. 2016.

117. POMPEU, E.L.T. **Normativas internacionais de proteção contra bioterrorismo e biocrimes: lacunas e vulnerabilidades no Brasil**. [dissertação]. Brasília: Programa de Pós Graduação em Saúde Pública e Diplomacia da Saúde, Fundação Oswaldo Cruz; 2014.

118. MEETING OF THE STATES PARTIES TO THE BWC. **Biosafety and Biosecurity**. Index: BWC/MSP/2008/MX/INF.1 Geneva: Implementation Support Unit; 24 jun. 2008. Disponível em: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://digitallibrary.un.org/record/636795/files/BWC_MSP_2008_MX_INF.1-EN.pdf&ved=2ahUKEwju_5rR8YmLAxUgppUCHUOsOecQFnoECCQQAQ&usg=AOvVaw2MlJAmJckWtmphAHH5sIGn. Acesso em 22 nov 2024.

119. INTERNATIONAL CRIMINAL POLICE ORGANIZATION. **Bioterorism**. Disponível em: https://www.interpol.int/Crimes/Terrorism/Bioterrorism. Acesso em: 08 nov. 2024.

120. UNITED NATIONS. **Biological Weapons**. Disponível em: https://disarmament.unoda.org/biological-weapons. Acesso em: 22 out. 2024.

121. AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. **Operação Hashtag**. 2019. [slide]. Apresentado em: 2ª Conferência Brasil Sul da Indústria e Produção de Ovos (Conbrasul), Gramado, 21 ago. 2019.

122. MENDONÇA, A. O.; MAFRA, C. **Política e requisitos regulatórios para biossegurança e bioproteção laboratorial no Brasil**. Revista Brasileira de Inteligência 2023; 18:13-31.

123. WORLD HEALTH ORGANIZATION. **Guidance on implementing regulatory requirements for biosafety and biosecurity in biomedical laboratories – a stepwise approach**. Geneva: WHO, 2020. Disponível em: https://www.who.int/publications/i/item/9789241516266. Acesso em 23 nov. 2024.

124. LONDON SCHOOL OF HYGIENE & TROPICAL MEDICINE. **From rapid response to 'predict, prevent, prepare'.** Disponível em: https://www.lshtm.ac.uk/research/centres/centre-climate-change-and-planetary-health/rapid-response-predict-prevent-prepare. Acesso em 02 jan. 2025.

125. FEDERAL SELECT AGENTE PROGRAM (CDC; USDA). **HHS and USDA Select Agents and Toxins**. Disponível em: https://www.selectagents.gov/sat/list.htm. Acesso em: 12 jan. 2025.

126. SIEGMAN, E. **How to prevent AI-enabled bioterrorism**. The Nuclear Threat Initiative (NTI). 19 dez. 2024. Disponível em: https://www.nti.org/risky-business/how-to-prevent-ai-enabled-bioterrorism/. Acesso em: 30 dez. 204.

127. WALSH, P.F. **Managing Emerging Health Security Threats Since 9/11**: The Role of Intelligence. International Journal of Intelligence and CounterIntelligence 2016; 29:341-367. Disponível em: https://www.tandfonline.com/doi/full/10.1080/08850607.2016.1121048. Acesso em 23 mar. 2023.

128. **INSIDE PORTON DOWN**: Britain's Secret Weapons Research Facility. Direção: Tim Usborne. Londres: BBC, 2016. Filme.

129. DELAMASTER, P. L.; STREET, E. J.; LESLIE, T. F.; YANG, Y.; JACOBSEN, K. H. **Complexity of the Basic Reproduction Number (R0)**. *Emerging Infectious Diseases*, 2019:*25*(1), 1-4. Disponível em: https://doi.org/10.3201/eid2501.171901. Acesso em: 21 nov. 2024.

ANEXO A – Resolução CREDEN nº 02/2009, de 4 de dezembro de 2009.

RESERVADO

RESOLUÇÃO CREDEN nº 02/2009, de 4 de dezembro de 2009.

A CÂMARA DE RELAÇÕES EXTERIORES E DEFESA NACIONAL, DO CONSELHO DE GOVERNO, no uso das atribuições previstas nas Leis nº 10.683, de 28 de maio de 2003, e nº 9.883, de 7 de dezembro de 1999, e no Decreto nº 4.801, de 6 de agosto de 2003, e

Considerando que compete à CREDEN formular diretrizes relacionadas à Atividade de Inteligência – RESOLVE:

Art. 1º Estabelecer as seguintes prioridades para os órgãos e entidades integrantes do Sistema Brasileiro de Inteligência, que direcionará os seus esforços, nas esferas nacional e internacional, para as áreas a seguir relacionadas, todas consideradas de igual relevância:

a) segurança pública, com vista à repressão ao crime organizado e aos ilícitos transnacionais;

b) prevenção ao terrorismo e seu financiamento, com atenção especial aos eventos esportivos e políticos, de abrangência internacional, programados para os próximos anos no Brasil;

c) segurança do patrimônio nacional com ênfase no acesso, na exploração e na evasão ilegal de recursos naturais renováveis e não-renováveis e para a proteção dos conhecimentos tradicionais indígenas e de outras populações;

d) biodefesa da população e dos recursos naturais e agropecuários;

e) origem, formação e ações de grupos que possam comprometer o estado democrático de direito;

f) oportunidades e ameaças aos interesses do País no mundo;

g) acompanhamento de assuntos internacionais de interesse estratégico para o Brasil, com ênfase na América do Sul;

h) acompanhamento da conjuntura dos países da América do Sul, visando evitar ou neutralizar sentimentos anti-Brasil nesses países;

i) conhecimento na área de Segurança das Infraestruturas Críticas do País, com prioridade para as ameaças aos setores de energia, comunicações, transportes, água e finanças;

j) segurança da informação e das comunicações e segurança cibernética, com prioridade para as ameaças às redes governamentais e à proteção do conhecimento sensível;

k) transferência de tecnologia e de conhecimentos, cujo acesso por outros países represente ameaça à segurança institucional;

l) conhecimento sobre ações e organizações ligadas ao terrorismo internacional, com ênfase nos reflexos para o Brasil e a América do Sul;

RESERVADO

RESERVADO

m) atividades de serviços de inteligência estrangeiros, com especial atenção à espionagem industrial, científica e tecnológica;

n) ocorrências de atos de pirataria no exterior e suas conseqüências para o Brasil;

o) atuação de Forças Armadas na América do Sul e no Atlântico Sul, com especial atenção a operações militares, acordos, modernização e transferência de meios militares;

p) acompanhamento de conflitos internacionais com potenciais reflexos na América do Sul e no Brasil;

q) existência, acesso, posse e uso de armas de destruição em massa e seus sistemas vetores que possam ocasionar reflexos para o Brasil;

r) tráfico de armas, munições, explosivos, materiais radioativos, tecnologias sensíveis e bens de uso dual;

s) desastres naturais e de origem humana;

t) ameaças e agressões ao meio ambiente;

u) tráfico de órgãos e seres humanos;

v) brasileiros em situação de risco no exterior;

w) produção e comércio ilícitos de substâncias psicotrópicas;

x) cultivo, processamento e tráfico de drogas ilícitas;

y) aquisição de terras por estrangeiros e atuação de ONG, empresas e órgãos de origem externa na Amazônia e em outras áreas sensíveis que possam acarretar prejuízos aos interesses do País;

z) prevenção à "lavagem" e ocultação de bens, direitos e valores; e

aa) ações contrárias à exploração soberana do pré-sal.

Art. 2º Esta Resolução entra em vigor na data de sua publicação e revoga a Resolução da CREDEN nº 01, de 24 de outubro de 2007.

JORGE ARMANDO FELIX
Ministro de Estado Chefe do Gabinete de
Segurança Institucional da Presidência da República
Presidente da Câmara de Relações Exteriores e de
Defesa Nacional do Conselho de Governo

RESERVADO

ANEXO B – Questionário Básico de Biossegurança e Bioproteção[aaa].

a. Nome da instituição (ex. Fiocruz/DF)

b. Nome do(s) laboratório(s) (ex. Laboratório de Virologia Animal I e II)

c. Endereço da Instituição e do(s) laboratório(s)

d. Qual o nível de biossegurança do(s) laboratório(s)

e. O nível de biossegurança informado foi certificado por alguma instituição externa? Caso afirmativo, qual?

f. Há agentes biológicos classificados como de Nível de Biossegurança 3 e 4 custodiados nos laboratórios? Quais? Em quais laboratório(s)? (ex. Sim, vírus da Febre Aftosa – NB3 -, no Laboratório de Virologia Animal II)

g. Há agentes biológicos e toxinas listadas no FSAP? Quais? Em quais laboratórios? (Sim, vírus da doença de Newcastle, no Laboratório de Microbiologia III)

h. O(s) laboratório(s) que custodia(m) agentes biológicos e toxinas selecionados possui(em) normas de biossegurança específicas para o laboratório? Caso afirmativo, favor anexar a este questionário.

i. O(s) laboratório(s) que custodia(m) agentes biológicos e toxinas selecionados possui(em) plano de bioproteção específicas para o laboratório? Caso afirmativo, favor anexar a este questionário.

j. O(s) laboratório(s) que custodia(m) agentes biológicos e toxinas selecionados possui(em) plano de bioproteção específicas para o laboratório? Caso afirmativo, favor anexar a este questionário.

k. O(s) laboratório(s) que custodia(m) agentes biológicos e toxinas selecionados possui(em) plano de prevenção e investigação de acidentes laboratoriais? Caso afirmativo, favor anexar a este questionário.

l. O(s) laboratório(s) que custodia(m) agentes biológicos e toxinas selecionados realizam alguma pesquisa ou produzem algo que exige sigilo?

m. Há pesquisadores ou estudantes estrangeiros com acesso aos agentes biológicos e toxinas selecionados? De que países?

n. Há visitas de comitivas estrangeiras ou inspeções nos laboratórios que custodiam agentes biológicos selecionados? Com que frenquência média anual?

o. Entre as ameaças abaixo, de acordo com a sua percepção de risco, quais as três principais no(s) laboratório(s) que custodia(m) agentes biológicos e toxinas selecionados, em ordem decrescente de risco: i. crime comum e organizado; ii. terrorismo; iii. furto e roubo de material biológico; iv. acidente laboratorial não intencional; v. espionagem; vi. falta de equipamentos adequados.

* * *

[aaa] Aplicado pelo PANGEIA/ABIN em laboratórios públicos vinculados ao Ministério da Saúde e ao então Ministério de Agricultura, Pecuária e Abastecimento (MAPA) para mapeamento de risco biológico nacional em 06 fev. 2018.