Presidência da República
Casa Civil
Agência Brasileira de Inteligência

Ofício nº 845/2024/GAB/DG/ABIN/CC/PR

Brasília, na data da assinatura digital.

A Sua Excelência o Senhor
Senador RENAN CALHEIROS
Presidente da Comissão Mista de Controle das Atividades de Inteligência (CCAI)
Senado Federal, Praça dos Três Poderes, Palácio do Congresso
70.165-900 Brasília/DF

Assunto: **Ingresso das Unidades da Federação no Sistema Brasileiro de Inteligência (Sisbin).**

Referência: Processo nº 00091.008739/2024-73.

Anexos: I - Portaria GAB/DG/ABIN/CC/PR Nº 2091, publicada em 03 jun. 2024 1244807;

II - Formulário de Adesão (Órgão Federado) 1244876;

III - Cartilha para Preenchimento Formulário de Adesão (Órgão Federado) 1244880

Senhor Senador Presidente da Comissão Mista de Controle das Atividades de Inteligência (CCAI),

1. A Agência Brasileira de Inteligência recebeu o Ofício nº 01/2024-CCAI (1265813), acerca do Ofício nº 01, de 2024, que encaminha proposta de ingresso de Unidades Federadas para compor o Sistema Brasileiro de Inteligência (Sisbin). Na qualidade representante do Órgão Central do Sisbin, agradeço o interesse e as orientações apontadas no Parecer, e busco com o presente ofício oferecer esclarecimentos com as seguintes considerações e de acordo aos tópicos delineados em seu Ofício.

1. CRITÉRIOS E DIRETRIZES GERAIS ESTABELECIDOS PELA ABIN PARA QUE NOVOS MEMBROS ORIUNDOS DAS UNIDADES DA FEDERAÇÃO ADIRAM AO SISBIN;

1.1. De fato, passados quase 25 anos da instituição do Sisbin, é a primeira vez que as Unidades da Federação solicitam ingresso de seus órgãos e entes no Sistema. A iniciativa deve-se à alteração feita pelo Decreto nº 11.693, de 2023. Para que façam parte do Sisbin, as Unidades da Federação devem observar os critérios definidos neste Decreto e em demais procedimentos e padrões a serem estabelecidos em ato do Diretor-Geral da Abin.

1.2. O documento que estabelece esses procedimentos é a Portaria GAB/DG/ABIN/CC/PR Nº 2.091, publicada em 03 jun. 2024 no Diário Oficial da União e que anexamos ao presente ofício. Nela, os artigos 7º a 11º detalham o processo de entrada das Unidades da Federação e dos órgãos federados para compor o Sisbin, lastreado nos requisitos impostos pela Lei 9.883/1999 e pelo Decreto

11.693/2023.

1.3. Exatamente pelo fato de a figura dos "órgãos federados" ter sido instituído por norma infralegal, optou-se pela separação dos processos de adesão das Unidades da Federação ao Sisbin, manifestação de caráter eminentemente política, do processo de adesão de cada um dos órgãos indicados pela Unidade da Federação, de caráter eminentemente técnica, com avaliação de critérios que demonstrem "tanto o interesse quanto sua adequação aos parâmetros da comunidade de inteligência da qual farão parte."

1.4. Como a Lei 9.883/1999 estabelece que quem pode compor o Sisbin são as Unidades da Federação, busca-se antes de tudo, especificar que apenas órgãos e entidades das Unidades da Federação que manifestem interessem em compor o Sisbin possam compor o sistema.

1.5. Entende-se que esse procedimento é cauteloso a fim de evitar qualquer manifestação de disputa federativa ou de pressões setoriais de órgãos locais que queiram participar do sistema à revelia dos chefes de governo. Deu-se liberdade aos chefes de governo, contudo, para que nominassem, na sua esfera de governo, os órgãos e entidades estaduais ou municipais que eles entendem que podem compor o sistema com o status de "órgãos federados". No entanto, a entrada dos órgãos não é automática ou desprovida da necessidade de comprovação de requisitos e critérios, conforme explicaremos adiante.

1.6. Também se exigiu que, no ato de solicitação de adesão, fosse determinado um ponto focal para tramitação do ingresso da Unidade da Federação:

> "Art. 7º A proposta de ingresso de Unidade da Federação para compor o Sisbin deverá ser encaminhada ao Órgão Central e indicar:
>
> I - os órgãos ou entidades em sua esfera que integrarão o Sisbin; e
>
> II - ponto focal para comunicação e tramitação do acordo de adesão."

1.7. Após ato dos chefes das Unidades da Federação, conforme determina a Lei nº 9.883/1999, submeteu-se os pedidos para manifestações tanto do órgão de controle externo da atividade de Inteligência como dos órgãos permanentes do Sisbin, exatamente com a finalidade de colher sugestões e ressalvas como a exarada no Relatório de Vossa senhoria:

> "§ 1º Os órgãos permanentes do Sisbin serão ouvidos sobre os pedidos de ingresso previstos neste artigo e poderão se manifestar em prazo não inferior a cinco dias úteis.
>
> § 2º O órgão de controle externo da atividade de Inteligência será ouvido sobre o pedido de ingresso no Sisbin da Unidade da Federação e dos órgãos e entidades por ela indicados."

1.8. Uma vez ouvidas e endereçadas as manifestações tanto da CCAI como de órgãos permanentes do Sisbin, a adesão da Unidade da Federação poderá ser concluída por meio de **acordo de adesão**:

> "Art. 8º A Unidade da Federação passará a compor o Sisbin após celebração de acordo de adesão com o Órgão Central, em que deverá constar:
>
> I - os órgãos ou entidades em sua esfera que integrarão o Sisbin; e
>
> II - indicação de ponto focal para comunicação com a Unidade da Federação.
>
> § 1º Após a celebração do acordo de adesão, as Unidades da Federação poderão indicar outros órgãos ou entidades para integrar o Sisbin, desde que sejam ouvidos o órgão de controle externo da atividade de Inteligência e os órgãos permanentes do Sisbin.
>
> § 2º A entrada de novos órgãos ou entidades será feita por meio de aditivo ao acordo de adesão celebrado."

1.9. Com a assinatura do acordo de adesão, a Unidade da Federação passa a compor o Sisbin conforme estabelecido pela Lei nº 9.883/1999, e **abre-se a possibilidade, e tão somente a possibilidade**, de que órgãos e entidades de sua esfera possam ingressar o Sistema na categoria de "órgãos federados" preconizada no Decreto nº 11.693, de 2023

1.10. Vencida a etapa eminentemente política, os órgãos indicados pelos chefes das Unidades da Federação deverão percorrer processo criterioso para adesão, similar ao exigido para um órgão

federal, baseado nos critérios estipulados no decreto, conforme o disposto abaixo:

> "Art. 9º Após celebrado o acordo de adesão, ou aditivo, previsto no art. 8º, os órgãos e entidades nele mencionados encaminharão ao Órgão Central formulário de adesão preenchido que informará acerca dos critérios dispostos no art. 3º.
>
> Parágrafo único. Caberá ao Órgão Central fornecer formulário de adesão modelo para preenchimento dos órgãos e entidades indicados pelas Unidades da Federação para integrarem o Sisbin.
>
> Art 10. O órgão ou entidade de Unidade da Federação será enquadrado como órgão federado quando, atender aos seguintes critérios:
>
> I - em relação a suas competências, tratar de temas relacionados à Política Nacional de Inteligência;
>
> II - em relação à sensibilidade de dados, informações e conhecimentos, tratar dados, informações ou conhecimentos associados à Política Nacional de Inteligência;
>
> III - em relação ao padrão de segurança, existirem no órgão ou entidade normas e controles relativos à governança, à segurança física, à segurança de pessoas e à segurança cibernética compatíveis com a sensibilidade dos dados, informações e conhecimentos em sua custódia;
>
> IV - em relação aos recursos de pessoal, dispuser de efetivo com cursos de formação ou capacitação relacionados às áreas de Inteligência, de segurança da informação e cibernética ou áreas correlatas de ao menos vinte horas-aula nos últimos cinco anos;
>
> V - em relação aos recursos de suporte tecnológico, dispuser de recursos de suporte de tecnologia tais como inventários de ativos de **hardware** e **software** corporativos, além de procedimentos e tratamento para ativos de **software** e ativos de **hardware** não autorizados; e
>
> VI - em relação aos recursos de estrutura organizacional, dispuser de unidade como ponto de contato para assuntos relativos ao Sisbin."

1.11. O Órgão Central compartilha a ressalva exarada no Parecer do eminente senador Espiridião Amin de que alguns órgãos indicados possam, salvo melhor juízo, ter pouca relação com a atividade de inteligência. Ao mesmo tempo, também se entende que não cabe ao Poder Executivo Federal exercer juízo de valor *a priori* da manifestação de vontade de um chefe de Unidade da Federação.

1.12. Como exemplo, podem existir entidades que *a priori* não parecem ter grande relevância para a atividade de inteligência, mas que custodiam infraestruturas críticas estratégicas nas esferas subnacionais, ou que custodiam dados que podem ser integrados para análises mais profundas e oportunas de acontecimentos como ataques a escolas, crises de abastecimento ou eventos climáticos extremos, que se desenrolam na maior parte das vezes na escala local.

1.13. Este Órgão Central atuará com diligência e responsabilidade na avaliação dos critérios estipulados no Decreto, sendo dever imposto pelo Decreto nº 11.693/2023 e pela Portaria GAB/DG /ABIN/CC/PR Nº 2.091/2024, assim como o faz para a avaliação de qualquer órgão federal, e se coloca ao lado da CCAI para garantir que apenas aqueles órgãos e entidades que demonstrem sua capacidade de participar do Sistema seja integrado. Nos termos da supracitada Portaria:

> "Art. 11. O órgão federado passará a integrar o Sisbin quando:
>
> I - a Unidade da Federação compuser o Sisbin e o houver indicado em seu acordo de adesão ou por meio de aditivo;
>
> II - o Órgão Central aprovar formulário de adesão encaminhado conforme previsto no art. 10; e
>
> IV - for celebrado plano de trabalho com o Órgão Central."

1.14. Tal como previsto no Decreto nº 11.693/2023, este Órgão Central se compromete a enviar toda a documentação enviada por todos os órgãos federados (formulário de adesão, planos de trabalho) para eventuais manifestações antes de edição de nova Portaria que altere a lista de órgãos e entidades pertencentes ao Sisbin, previsão determinada também pelo supracitado Decreto.

1.15. Importante destacar que o ingresso dos órgãos federados das Unidades da Federação **não franqueia de forma automática o acesso a dados, conhecimentos e documentos de forma indiscriminada** e que o compartilhamento de dados no Sistema, mesmo entre membros do Sisbin Federal, deve respeitar a legislação em vigor e notadamente decisões judiciais sobre o assunto,

especialmente no tocante a necessidade de conhecer e nos requisitos de motivação e finalidade para acesso.

1.16. Entretanto, o ingresso desses órgãos e entidades, além de ampliar o marco legal para trocas e compartilhamento de documentos de Inteligência, franqueia que eles possam ter acesso a ferramentas de comunicação segura e acesso a futuras plataformas de intercambio, granularizado de acordo com os níveis de segurança e necessidade de conhecer equivalentes. Isso permite que as trocas dentro do Sistema se dêem de forma mais segura e confiável, aumentando também os controles relativos a autenticidade e confiabilidade dos dados tramitados.

1.17. Por fim, quanto aos mecanismos de controle externo exercidos pelas Unidades da Federação, embora seja desejável que sejam institucionalizados, não nos cabe enquanto órgão do Executivo Federal impor um rito. Não obstante, entende-se que enquanto não são criadas por assembleias estaduais ou camaras municipais comissões semelhantes à CCAI, esta Comissão, conforme disposto Resolução Nº 2, de 2013 do Congresso Nacional, possui prerrogativa para fiscalizar e exercer o controle externo de todos os órgãos e entidades componentes do Sisbin, sem distinção das categorias estabelecidas no Decreto nº 11.693/2023.

2. AS RAZÕES PELAS QUAIS CADA ÓRGÃO DEVERÁ SER MEMBRO DO SISBIN;

2.1. Como explicado no item 1.9, com a assinatura do acordo de adesão, a Unidade da Federação passa a compor o Sisbin conforme estabelecido pela Lei nº 9.883/1999, e **abre-se a possibilidade, e tão somente a possibilidade**, de que órgãos e entidades de sua esfera possam ingressar o Sistema na categoria de "órgãos federados" preconizada no Decreto nº 11.693, de 2023;

2.2. Esses órgãos deverão fornecer formulário de adesão ao órgão central (Anexo II) em que deixem de forma clara as razões pelas quais Quais as competências o órgão possui relacionadas à Política Nacional
de Inteligência (PNI).

2.3. Além disso, conforme disposto no Art. 11 da Portaria GAB/DG/ABIN/CC/PR Nº 2.091/2024, após o Órgão Central aprovar formulário de adesão encaminhado pelo órgão federado, deverá ser celebrado plano de trabalho com o Órgão Central.

2.4. Conforme o disposto no Art. 12 da Portaria GAB/DG/ABIN/CC/PR Nº 2.091/2024, especialmente nos incisos III e IV, no plano de trabalho há previsão de que os órgãos federados entrantes justifiquem de forma clara as razões pelas quais ele deve ser membro do Sisbin, assim como os objetivos gerais e específicos e resultados esperados com a adesão:

> "DOS PLANOS DE TRABALHO
> Art. 12. O planos de trabalho de Inteligência deverá conter os seguintes itens:
> I - diagnóstico, que demonstre a situação anterior que ensejou a necessidade do ajuste e os benefícios esperados com a cooperação;
> II - abrangência, compreendida pelo âmbito territorial de atuação do órgão ou entidade e sua capacidade de alcance para os resultados esperados;
> III - justificativa para ingresso ou permanência no Sisbin;
> IV - objetivos gerais e específicos estabelecidos em comum acordo e resultados esperados, que incluam, no mínimo:
> a) compartilhamento com o Órgão Central de dados, informações e conhecimentos necessários à produção de conhecimentos relacionados com ações de Inteligência previstas nos planos de trabalho, obedecida a Política Nacional de Inteligência;
> b) apoio a ações de capacitação e de formação, sob coordenação do Órgão Central, previstas no plano de trabalho; e
> c) participação, em caráter voluntário, nos centros integrados de inteligência;
> V - identificação dos pontos de contato do órgão ou entidade para assuntos relativos ao Sisbin; e
> VI - plano de ação que defina indicadores e prazos específicos, nos casos em que couber."

2.5. No entanto, como explicado anteriormente, esta etapa se dá após a entrada da Unidade da Federação *per se*, e tem efeitos apenas para o órgão específico. Como ainda estamos na fase de adesão das Unidades da Federação, esta etapa ainda não ocorreu em caso concreto.

2.6. Enquanto Órgão Central, a Abin se compromete a enviar à CCAI toda a documentação enviada pelos órgãos federados quando assinados os planos de trabalho, inclusive para que ele passe a ser objeto de controle como qualquer outro órgão do Sisbin.

3. DOCUMENTOS QUE COMPROVEM O ATENDIMENTO ÀS DISPOSIÇÕES ESTABELECIDAS PELO DIRETOR-GERAL DA ABIN E AOS DEMAIS CRITÉRIOS DISPOSTOS NO ART. 8º DO DECRETO Nº 11.693, DE 2023, QUAIS SEJAM:

A) COMPETÊNCIAS QUE O ÓRGÃO OU A ENTIDADE EXERCE E SUA CORRELAÇÃO COM TEMAS DA POLÍTICA NACIONAL DE INTELIGÊNCIA;

B) SENSIBILIDADE DOS DADOS, DAS INFORMAÇÕES E DOS CONHECIMENTOS A SEREM COMPARTILHADOS OU POTENCIALMENTE ACESSADOS PELO ÓRGÃO OU PELA ENTIDADE;

C) PADRÃO DE SEGURANÇA DO ÓRGÃO OU DA ENTIDADE; E

D) RECURSOS DISPONÍVEIS DE PESSOAL, SUPORTE TECNOLÓGICO E ESTRUTURA ORGANIZACIONAL.

3.1. Como explicado no item 1.3, optou-se pela separação dos processos de adesão das Unidades da Federação ao Sisbin, manifestação de caráter eminentemente política, do processo de adesão de cada um dos órgãos indicados pela Unidade da Federação, de caráter eminentemente técnica, com avaliação de critérios que demonstrem "tanto o interesse quanto sua adequação aos parâmetros da comunidade de inteligência da qual farão parte."

3.2. Com a assinatura do acordo de adesão, a Unidade da Federação passa a compor o Sisbin conforme estabelecido pela Lei nº 9.883/1999, e **abre-se a possibilidade, e tão somente a possibilidade**, de que órgãos e entidades de sua esfera possam ingressar o Sistema na categoria de "órgãos federados" preconizada no Decreto nº 11.693, de 2023.

3.3. Vencida a etapa eminentemente política, a Portaria GAB/DG/ABIN/CC/PR Nº 2.091/2024 definiu rito em que os órgãos indicados pelos chefes das Unidades da Federação deverão percorrer processo criterioso para adesão:

> "Art. 9º Após celebrado o acordo de adesão, ou aditivo, previsto no art. 8º, os órgãos e entidades nele mencionados encaminharão ao Órgão Central formulário de adesão preenchido que informará acerca dos critérios dispostos no art. 3º.
>
> Parágrafo único. Caberá ao Órgão Central fornecer formulário de adesão modelo para preenchimento dos órgãos e entidades indicados pelas Unidades da Federação para integrarem o Sisbin.
>
> Art 10. O órgão ou entidade de Unidade da Federação será enquadrado como órgão federado quando, atender aos seguintes critérios:
>
> I - em relação a suas competências, tratar de temas relacionados à Política Nacional de Inteligência;
>
> II - em relação à sensibilidade de dados, informações e conhecimentos, tratar dados, informações ou conhecimentos associados à Política Nacional de Inteligência;
>
> III - em relação ao padrão de segurança, existirem no órgão ou entidade normas e controles relativos à governança, à segurança física, à segurança de pessoas e à segurança cibernética compatíveis com a sensibilidade dos dados, informações e conhecimentos em sua custódia;
>
> IV - em relação aos recursos de pessoal, dispuser de efetivo com cursos de formação ou capacitação relacionados às áreas de Inteligência, de segurança da informação e cibernética ou áreas correlatas de ao menos vinte horas-aula nos últimos cinco anos;
>
> V - em relação aos recursos de suporte tecnológico, dispuser de recursos de suporte de tecnologia tais como inventários de ativos de **hardware** e **software** corporativos, além de procedimentos e tratamento para ativos de **software** e ativos de **hardware** não autorizados; e
>
> VI - em relação aos recursos de estrutura organizacional, dispuser de unidade como ponto de contato para assuntos relativos ao Sisbin."

3.4. Essas informações serão informadas por meio de formulários de adesão ao Órgão Central, que os avaliará. No entanto, como explicado anteriormente, esta etapa se dá após a entrada da Unidade da Federação *per se*, e tem efeitos apenas para o órgão específico. Como ainda estamos na fase de adesão das Unidades da Federação, esta etapa ainda não ocorreu em caso concreto.

3.5. Enquanto Órgão Central, a Abin se compromete a enviar à CCAI toda a documentação enviada pelos órgãos federados por ocasião de sua adesão, inclusive para que ele passe a ser objeto de controle como qualquer outro órgão do Sisbin.

4. OS CONVÊNIOS OU PROTOCOLOS ESTABELECIDOS ENTRE A ABIN E ESSES ENTES DAS UNIDADES DA FEDERAÇÃO, BEM COMO O TEOR DA PARTICIPAÇÃO NO SISBIN

4.1. Conforme explicações prestadas no presente ofício, toda a documentação do processo de entrada de Unidades da Federação, bem como a adesão dos órgãos indicados por estas em um segundo momento, serão encaminhadas à CCAI em seu inteiro teor, inclusive para que ele passe a ser objeto de controle como qualquer outro órgão do Sisbin.

4.2. Nesse compasso, o proximo passo é a elaboração de Acordos de Adesão com as Unidades da Federação que já demonstraram interesse em compor o Sisbin, de forma a endereçar seus pedidos de ingresso.

4.3. Em um segundo momento cada órgão indicado por cada Unidade da Federação terá de apresentar não só seus formulários de ingresso, que deverão ser aprovados pelo Órgão Central, como subscrever planos de trabalho.

5. CONSIDERAÇÕES FINAIS

2. A entrada de Unidades da Federação para compor o Sisbin é inovação que amplia o marco legal para trocas e compartilhamento de documentos de Inteligência, franqueia acesso a ferramentas de comunicação segura e acesso a futuras plataformas de intercambio. Isso permite que as trocas dentro do Sistema se dêem de forma mais segura e confiável, aumentando também os controles relativos a autenticidade e confiabilidade dos dados tramitados.

3. A participação da CCAI neste processo, mais do que simples etapa formal estipulada pelos legisladores na Lei 9.883/1999, vai de encontro aos desejos da sociedade por uma atividade de inteligência moderna, ancorada na defesa do Estado Democrático de Direito, e cujo controle anda lado a lado ao desenvolvimento das ações, motivo pelos quais a ABIN, na condição de Órgão Central, agradece mais uma vez a acolhida e as manifestações exaradas no Ofício nº 01/2024-CCAI (1265813).

4. Aproveito o ensejo para renovar os votos de elevada estima e consideração, e coloco a ABIN à disposição para eventuais esclarecimentos.

Respeitosamente,

LUIZ FERNANDO CORRÊA
Diretor-Geral

Documento assinado eletronicamente

Documento assinado eletronicamente por **LUIZ FERNANDO CORREA**, **Diretor-Geral**, em 18/12/2024, às 16:56, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.abin.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1266866** e o código CRC **9152F530**.

Boletim de Serviço Eletrônico em 04/06/2024
DOU de 04/06/2024, seção 1, página 4/5

Presidência da República
Casa Civil
Agência Brasileira de Inteligência

PORTARIA GAB/DG/ABIN/CC/PR Nº 2091, DE 03 DE JUNHO DE 2024.

Estabelece os critérios e procedimentos de ingresso de órgãos e entidades no Sistema Brasileiro de Inteligência como órgãos dedicados, associados e federados.

O DIRETOR-GERAL DA AGÊNCIA BRASILEIRA DE INTELIGÊNCIA DA CASA CIVIL DA PRESIDÊNCIA DA REPÚBLICA, tendo em vista o disposto no art. 8º do Decreto nº 11.693, de 6 de setembro de 2023,

RESOLVE:

Art. 1º Esta Portaria estabelece os critérios e procedimentos de ingresso de órgãos e entidades no Sistema Brasileiro de Inteligência – Sisbin como órgãos dedicados, associados e federados.

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 2º O Sisbin é integrado por órgãos e entidades nas seguintes categorias:

I - Órgão Central, a Agência Brasileira de Inteligência – ABIN;

II - órgãos permanentes;

III - órgãos dedicados;

IV - órgãos associados; e

V - órgãos federados.

§ 1º Os órgãos permanentes de que trata o inciso II do **caput** deste artigo são aqueles previstos no art. 7º, § 1º do Decreto nº 11.693/2023, cujas competências estão relacionadas à governabilidade, à defesa externa, à segurança interna e às relações exteriores do País.

§ 2º Os órgãos dedicados de que trata o inciso III do **caput** deste artigo são órgãos ou entidades do Poder Executivo federal com unidades dedicadas às atividades de Inteligência ou atividades similares e que atuam em assuntos

estratégicos relacionados a temas da Política Nacional de Inteligência.

§ 3º Os órgãos associados de que trata o inciso IV do **caput** deste artigo são órgãos ou entidades do Poder Executivo federal que integram o Sisbin, não enquadrados nos incisos I a III do **caput** deste artigo, que tratam de temas relacionados à Política Nacional de Inteligência.

§ 4º Os órgãos federados de que trata o inciso V do **caput** deste artigo são os órgãos e entidades das Unidades da Federação, que integram o Sisbin, ouvido o órgão de controle externo da atividade de Inteligência a que se refere o art. 6º da Lei nº 9.883, de 7 de dezembro de 1999.

Art. 3º O ingresso de novos integrantes no Sisbin será avaliado a partir dos seguintes critérios:

I - competências que o órgão ou a entidade exerce e sua correlação com temas da Política Nacional de Inteligência;

II - sensibilidade dos dados, das informações e dos conhecimentos a serem compartilhados ou potencialmente acessados pelo órgão ou pela entidade;

III - padrão de segurança do órgão ou da entidade; e

IV - recursos disponíveis de pessoal, suporte tecnológico e estrutura organizacional.

Parágrafo único. O Órgão Central poderá apoiar os órgãos e entidades solicitantes em seus pedidos de ingresso no Sisbin, fornecendo formulários, padrões e referências de boas práticas existentes para o cumprimento dos critérios estipulados no **caput** deste artigo.

CAPÍTULO II

DO INGRESSO NO SISBIN

Seção I

Dos Órgãos ou Entidades da União

Art. 4º O pedido de ingresso de órgão ou entidade do Poder Executivo federal no Sisbin será encaminhado ao Órgão Central e deverá:

I - indicar as principais áreas com potencial de cooperação na troca de dados, informações e conhecimentos atinentes à execução da Política Nacional de Inteligência;

II - informar a situação do órgão quanto aos dos critérios estipulados no art. 3º; e

III - indicar ponto focal para comunicação e tramitação do pedido de ingresso, e elaboração de plano de trabalho.

§ 1º Os órgãos permanentes do Sisbin serão ouvidos sobre os pedidos de ingresso previstos neste artigo e poderão se manifestar em prazo não inferior a cinco dias úteis.

§ 2º Caberá ao Órgão Central aprovar o ingresso de órgãos ou entidades do Poder Executivo federal no Sisbin, assim como determinar a categoria de seu enquadramento, baseando sua análise nos fatores dispostos no art 5º e art. 6º.

§ 3º A entrada do órgão ou entidade do Poder Executivo federal no Sisbin ocorrerá após celebração de plano de trabalho com o Órgão Central, observado o

disposto no art. 11º.

Órgãos Dedicados

Art. 5º O órgão ou entidade do Poder Executivo federal será enquadrado como órgão dedicado quando atender aos seguintes critérios:

I - em relação a suas competências, atuar em assuntos estratégicos relacionados a temas da Política Nacional de Inteligência;

II - em relação à sensibilidade de dados, informações e conhecimentos, tratar dados, informações ou conhecimentos associados à Política Nacional de Inteligência considerados imprescindíveis à segurança da sociedade ou do Estado, nos termos do art. 23 da Lei nº 12.527, de 18 de novembro de 2011;

III - em relação ao padrão de segurança, existirem no órgão ou entidade normas e controles relativos à governança, à segurança física, à segurança de pessoas e à segurança cibernética compatíveis com a sensibilidade dos dados, informações e conhecimentos em sua custódia;

IV - em relação aos recursos de pessoal, dispuser de efetivo com cursos de formação ou capacitação relacionados às áreas de Inteligência, de segurança da informação e cibernética ou áreas correlatas de ao menos quarenta horas-aula nos últimos cinco anos;

V - em relação aos recursos de suporte tecnológico, dispuser de recursos de suporte de tecnologia tais como inventários de ativos de **hardware** e **software** corporativos, procedimentos e tratamento para ativos de **software** e ativos de **hardware** não autorizados, além de possuir gestão automatizada de **patches** de sistemas operacionais e de aplicativos; e

VI - em relação aos recursos de estrutura organizacional, dispuser de unidade como ponto de contato para assuntos relativos ao Sisbin que seja dedicada às atividades de Inteligência ou atividades similares.

Órgãos Associados

Art. 6º O órgão ou entidade do Poder Executivo federal será enquadrado como órgão associado quando atender aos seguintes critérios:

I - em relação a suas competências, atuar em temas relacionados à Política Nacional de Inteligência;

II - em relação à sensibilidade de dados, informações e conhecimentos, tratar dados, informações ou conhecimentos associados à Política Nacional de Inteligência;

III - em relação ao padrão de segurança, existirem no órgão ou entidade normas e controles relativos à governança, à segurança física, à segurança de pessoas e à segurança cibernética compatíveis com a sensibilidade dos dados, informações e conhecimentos em sua custódia;

IV - em relação aos recursos de pessoal, dispuser de efetivo com cursos de formação ou capacitação relacionados às áreas de Inteligência, de segurança da informação e cibernética ou áreas correlatas de ao menos vinte horas-aula nos últimos cinco anos;

V - em relação aos recursos de suporte tecnológico, dispuser de recursos de suporte de tecnologia tais como inventários de ativos de **hardware** e **software** corporativos, além de procedimentos e tratamento para ativos de **software** e ativos de **hardware** não autorizados; e

VI - em relação aos recursos de estrutura organizacional, dispuser de

unidade como ponto de contato para assuntos relativos ao Sisbin.

Parágrafo único. Os órgãos associados poderão solicitar a alteração de categoria para a de órgão dedicado, observados os requisitos estabelecidos no art. 5º.

Seção II

Dos Órgãos ou Entidades dos Estados, do Distrito Federal e dos Municípios

Unidades da Federação

Art. 7º A proposta de ingresso de Unidade da Federação para compor o Sisbin deverá ser encaminhada ao Órgão Central e indicar:

I - os órgãos ou entidades em sua esfera que integrarão o Sisbin; e

II - ponto focal para comunicação e tramitação do acordo de adesão.

§ 1º Os órgãos permanentes do Sisbin serão ouvidos sobre os pedidos de ingresso previstos neste artigo e poderão se manifestar em prazo não inferior a cinco dias úteis.

§ 2º O órgão de controle externo da atividade de Inteligência será ouvido sobre o pedido de ingresso no Sisbin da Unidade da Federação e dos órgãos e entidades por ela indicados.

Art. 8º A Unidade da Federação passará a compor o Sisbin após celebração de acordo de adesão com o Órgão Central, em que deverá constar:

I - os órgãos ou entidades em sua esfera que integrarão o Sisbin; e

II - indicação de ponto focal para comunicação com a Unidade da Federação.

§ 1º Após a celebração do acordo de adesão, as Unidades da Federação poderão indicar outros órgãos ou entidades para integrar o Sisbin, desde que sejam ouvidos o órgão de controle externo da atividade de Inteligência e os órgãos permanentes do Sisbin.

§ 2º A entrada de novos órgãos ou entidades será feita por meio de aditivo ao acordo de adesão celebrado.

Órgãos Federados

Art. 9º Após celebrado o acordo de adesão, ou aditivo, previsto no art. 8º, os órgãos e entidades nele mencionados encaminharão ao Órgão Central formulário de adesão preenchido que informará acerca dos critérios dispostos no art. 3º.

Parágrafo único. Caberá ao Órgão Central fornecer formulário de adesão modelo para preenchimento dos órgãos e entidades indicados pelas Unidades da Federação para integrarem o Sisbin.

Art 10. O órgão ou entidade de Unidade da Federação será enquadrado como órgão federado quando, atender aos seguintes critérios:

I - em relação a suas competências, tratar de temas relacionados à Política Nacional de Inteligência;

II - em relação à sensibilidade de dados, informações e conhecimentos, tratar dados, informações ou conhecimentos associados à Política Nacional de Inteligência;

III - em relação ao padrão de segurança, existirem no órgão ou entidade

normas e controles relativos à governança, à segurança física, à segurança de pessoas e à segurança cibernética compatíveis com a sensibilidade dos dados, informações e conhecimentos em sua custódia;

IV - em relação aos recursos de pessoal, dispuser de efetivo com cursos de formação ou capacitação relacionados às áreas de Inteligência, de segurança da informação e cibernética ou áreas correlatas de ao menos vinte horas-aula nos últimos cinco anos;

V - em relação aos recursos de suporte tecnológico, dispuser de recursos de suporte de tecnologia tais como inventários de ativos de **hardware** e **software** corporativos, além de procedimentos e tratamento para ativos de **software** e ativos de **hardware** não autorizados; e

VI - em relação aos recursos de estrutura organizacional, dispuser de unidade como ponto de contato para assuntos relativos ao Sisbin.

Art. 11. O órgão federado passará a integrar o Sisbin quando:

I - a Unidade da Federação compuser o Sisbin e o houver indicado em seu acordo de adesão ou por meio de aditivo;

II - o Órgão Central aprovar formulário de adesão encaminhado conforme previsto no art. 10; e

IV - for celebrado plano de trabalho com o Órgão Central.

CAPÍTULO III

DOS PLANOS DE TRABALHO

Art. 12. O planos de trabalho de Inteligência deverá conter os seguintes itens:

I - diagnóstico, que demonstre a situação anterior que ensejou a necessidade do ajuste e os benefícios esperados com a cooperação;

II - abrangência, compreendida pelo âmbito territorial de atuação do órgão ou entidade e sua capacidade de alcance para os resultados esperados;

III - justificativa para ingresso ou permanência no Sisbin;

IV - objetivos gerais e específicos estabelecidos em comum acordo e resultados esperados, que incluam, no mínimo:

a) compartilhamento com o Órgão Central de dados, informações e conhecimentos necessários à produção de conhecimentos relacionados com ações de Inteligência previstas nos planos de trabalho, obedecida a Política Nacional de Inteligência;

b) apoio a ações de capacitação e de formação, sob coordenação do Órgão Central, previstas no plano de trabalho; e

c) participação, em caráter voluntário, nos centros integrados de inteligência;

V - identificação dos pontos de contato do órgão ou entidade para assuntos relativos ao Sisbin; e

VI - plano de ação que defina indicadores e prazos específicos, nos casos em que couber.

§ 1º O plano de trabalho poderá ser consensualmente atualizado.

§ 2º O Órgão Central poderá especificar no plano de trabalho proposta de aprimoramento da situação do solicitante em relação aos critérios dispostos nos incisos III e IV do **caput** do art. 3º.

§ 3º O Órgão Central e os órgãos permanentes ficam dispensados da elaboração de planos de trabalho.

§ 3º O Órgão Central poderá solicitar aos órgãos permanentes suas políticas, estratégias e planos de Inteligência, bem como dos subsistemas dos quais participem.

DISPOSIÇÕES FINAIS

Art. 13. Fica revogada a Portaria GAB/DG/ABIN/CC/PR Nº 925, de 6 de setembro de 2023.

Art. 14. Tornar sem efeito a Portaria GAB/DG/ABIN/CC/PR Nº 2039, de 15 de maio de 2024, publicada no Boletim de Serviço Eletrônico em 29 de maio de 2024.

Art. 15. Esta Portaria entra em vigor na data de sua publicação.

LUIZ FERNANDO CORRÊA

Documento assinado eletronicamente

Documento assinado eletronicamente por **LUIZ FERNANDO CORREA**, **Diretor-Geral**, em 03/06/2024, às 17:19, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.abin.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1131955** e o código CRC **04CE96E7**.

Formulário de adesão – Órgão federado

Entidade: _____

Data: _____

Formulário de adesão – Órgão federado

As perguntas abaixo buscam fornecer subsídios para a análise dos critérios de ingresso, conforme o art. 9º da Portaria GAB/DG/ABIN/CC/PR nº 2.091, de 03 de junho de 2024. *A cartilha anexa explica, detalhadamente, os critérios adotados e pode ser usada para dirimir dúvidas de preenchimento.*

1. Quais as competências o órgão possui relacionadas à Política Nacional de Inteligência (PNI)?

(Listar as competências com relação, direta ou indireta, com temas da PNI)

1.
2.
3.
4.
5.
6.

2. Com quais dados, informações ou conhecimentos associados à Política Nacional de Inteligência o órgão trabalha? Em sua avaliação, qual o grau de sensibilidade deles?

(Consultar cartilha para instruções de preenchimento)

Dados, informações ou conhecimentos	Grau de sensibilidade
1.	☐Elevado ☐Intermediário ☐Baixo
2.	☐Elevado ☐Intermediário ☐Baixo
3.	☐Elevado ☐Intermediário ☐Baixo
4.	☐Elevado ☐Intermediário ☐Baixo
5.	☐Elevado ☐Intermediário ☐Baixo
6.	☐Elevado ☐Intermediário ☐Baixo
7.	☐Elevado ☐Intermediário ☐Baixo

3. Em relação ao padrão de segurança, marque as caixas que contém dispositivos existentes em seu órgão:

GOVERNANÇA
☐Política ou normativo interno que define a arquitetura estratégica e a governança do órgão.
☐Política ou normativo interno que estabeleça princípios, finalidades e diretrizes que fundamentem o planejamento, a normatização e a execução da segurança institucional.
☐Política ou normativo interno que institua diretrizes, competências e responsabilidades relativas à segurança da informação, com a finalidade de assegurar a confidencialidade, a integridade e a disponibilidade das informações tratadas.

Formulário de adesão – Órgão federado

☐Princípio do sigilo aplicado à segurança institucional.
☐Princípio compartimentação aplicado à segurança institucional.
☐Princípio da responsabilidade ou equivalente aplicado à segurança da informação.
☐Princípio do mínimo privilégio de acesso ou equivalente aplicado à segurança da informação é fundamentada.
☐Princípio do acesso seguro ou equivalente aplicado à segurança da informação.
☐Política ou normativo interno que estabeleça diretrizes para o registro, concessão, revogação e autenticação de acesso a ativos da informação.
☐ Política ou normativo interno que estabeleça diretrizes para a identificação, classificação, mapeamento, registro e parametrização da gestão do ciclo de vida dos ativos de informação.
☐Política ou normativo interno que estabeleça diretrizes para a guarda, proteção e recuperação em caso de perda dos ativos de informação.
☐Política ou normativo interno que estabeleça regras de identificação, avaliação, documentação, gestão, comunicação e remediação de vulnerabilidades dos ativos de informação.
☐Política ou normativo interno que estabeleça regras relacionadas à coleta, armazenamento, uso e exclusão de logs de auditora para os ativos da informação.
☐ Política ou normativo interno que disponha sobre os procedimentos de segurança para tratamento de documentos sigilosos.
☐Política ou normativo interno que disponha sobre os procedimentos de segurança para admissão de pessoal.
☐ Política ou normativo interno que disponha sobre os procedimentos de segurança para afastamento, movimentação ou desligamento de pessoal.
☐Política ou normativo interno que disponha sobre o controle de acesso físico às áreas e instalações institucionais.
SEGURANÇA FÍSICA
☐Áreas e instalações institucionais situadas em região de baixo índice de criminalidade.
☐Áreas e instalações institucionais situadas em região suprida por serviços essenciais.
☐ Áreas e instalações institucionais situadas em edificação que satisfaz os requisitos técnicos normativos vigentes de desempenho estrutural, durabilidade, utilização, prevenção e combate a incêndio e acessibilidade.
☐Existência de sistema de proteção física.
☐Sistema de proteção física fundamentado no princípio da proteção em profundidade.
☐Sistema de proteção física fundamentado no princípio da proteção balanceada.
☐Sistema de proteção física apresenta mínima consequência diante de falha.
☐Sistema de proteção física com profissionais competentes, treinados, equipados e aptos para zelar pelo patrimônio, detectar, neutralizar ou obstruir acessos físicos não autorizados.
☐ Sistema de proteção física com subsistema de controle de acesso eletrônico, auditável, de múltiplos métodos de autenticação.
☐Subsistema de controle de acesso considera diferentes credenciais e perfis de usuários, baseados na necessidade de conhecer.
☐Sistema de proteção física conta com subsistema de videomonitoramento.
☐Subsistema de videomonitoramento é capaz de promover a cobertura das áreas mais sensíveis.
☐ Subsistemas de controle de acesso eletrônico e videomonitoramento estão, no mínimo, integrados.
☐Sistema de proteção física conta com centro de operações de segurança física (SOC)

Formulário de adesão – Órgão federado

☐O centro de operações de segurança física (SOC) é composto por profissionais treinados e qualificados.
☐Sistema de proteção física conta com procedimentos e dispositivos para resposta em caso de óbices ou sinistros.
SEGURANÇA DE PESSOAS
☐Existência de procedimentos de segurança na admissão de novos servidores.
☐Existência de procedimentos de segurança na admissão de colaboradores.
☐Investigação social e funcional prévias a admissão de pessoal orgânico.
☐Investigação social para contratação de prestadores de serviço.
☐Avaliação psicológica prévia à admissão de pessoal orgânico.
☐Entrevista de segurança prévia ao credenciamento de pessoal orgânico.
☐Orientação inicial para todo recém-admitido, previamente ao efetivo início das atividades, sobre as políticas, normas e procedimentos de segurança vigentes no órgão.
☐Orientação específica sobre as normas de segurança que devem ser observadas no desempenho do cargo ou função.
☐Orientação específica sobre os procedimentos a serem adotados em contato com a imprensa.
☐Orientação específica sobre os procedimentos a serem adotados em contato com estrangeiros ou representantes de instituições estrangeiras ou internacionais.
☐Orientação periódica em matéria de segurança institucional ou atualização de políticas, normas e procedimentos de segurança.
☐Concessão de credencial de acesso físico fundamentada na necessidade de conhecer do indivíduo.
☐Revogação de credencial de acesso físico fundamentada na necessidade de conhecer do indivíduo.
☐Concessão de credencial de acesso lógico a bases de dados e sistemas informacionais fundamentada na necessidade de conhecer do indivíduo.
☐Revogação de credencial de acesso lógico a bases de dados e sistemas informacionais fundamentada na necessidade de conhecer do indivíduo.
☐Entrevista de segurança no momento do desligamento do servidor.
SEGURANÇA CIBERNÉTICA
☐Inventário e controle de ativos de hardware corporativos*
☐Inventário e controle de ativos de softwares corporativos*
☐Procedimentos e tratamento para ativos de software não autorizados*
☐Procedimentos e tratamento para ativos de hardware não autorizados*
☐Proteção de dados
☐Configuração segura de ativos corporativos e software
☐Gestão de contas
☐Gestão de controle de acesso
☐Gestão contínua de vulnerabilidades
☐Gestão de registros de auditoria
☐Proteções de e-mail e navegador Web
☐Defesas contra malware
☐Recuperação de dados
☐Gestão da infraestrutura de rede
☐Monitoramento e defesa da rede
☐Conscientização sobre segurança e treinamento de competências

Formulário de adesão – Órgão federado

☐Gestão de provedor de serviços
☐Segurança de aplicações
☐Gestão de respostas a incidentes
☐Testes de invasão

*Os itens destacados em amarelo também são utilizados para avaliar o critério V do art. 9º da Portaria nº 2.091/2024 da Portaria (recursos de suporte de tecnológico). Para maiores detalhamentos, consultar a cartilha.

4. O órgão dispõe de efetivo com cursos de formação ou de capacitação relacionados às áreas de Inteligência, segurança da informação e cibernética ou áreas correlatas com, ao menos, 20 horas-aula nos últimos cinco anos? Caso responda não, é possível assumir o compromisso descrito abaixo:

(Anexar certificado ou declaração de conclusão de curso de servidor ao formulário que comprove o requisito mínimo de 20h)

☐SIM ☐NÃO

☐Assumo o compromisso, firme e irrevogável, de capacitar, ao menos, um servidor ou funcionário efetivo nas áreas de Inteligência, Segurança da Informação, cibernética ou áreas correlatas com no mínimo 20 horas-aula, nos próximos 24 meses, a partir da efetiva entrada no Sisbin.

5. Indicar a unidade que atuará como ponto de contato para assuntos relativos ao Sisbin e o contato institucional.

Unidade	E-mail	Telefone

Local/UF, XX de XXXX de 20XX

Assinatura eletrônica do Partícipe Aderente

CARTILHA PARA PREENCHIMENTO DO FORMULÁRIO DE INGRESSO

ÓRGÃO FEDERADO

Agência Brasileira de Inteligência - ABIN

ABIN

Critérios de Ingresso SISBIN

Órgão federado

Com base na Portaria 2.091, de 3 de junho de 2024

Segundo o art. 10 da Portaria 2.091, de 3 de junho de 2024, o órgão ou entidade de Unidade da Federação será enquadrado como órgão federado quando, atender aos seguintes critérios:

I - Em relação a suas **competências**, tratar de temas relacionados à Política Nacional de Inteligência;

II - Em relação à **sensibilidade de dados, informações e conhecimentos**, tratar dados, informações ou conhecimentos associados à Política Nacional de Inteligência;

III - Em relação ao **padrão de segurança**, existirem no órgão ou entidade normas e controles relativos à governança, à segurança física, à segurança de pessoas e à segurança cibernética compatíveis com a sensibilidade dos dados, informações e conhecimentos em sua custódia;

IV - Em relação aos **recursos de pessoal**, dispuser de efetivo com cursos de formação ou capacitação relacionados às áreas de Inteligência, de segurança da informação e cibernética ou áreas correlatas de ao menos vinte horas-aula nos últimos cinco anos;

V - Em relação aos **recursos de suporte tecnológico**, dispuser de recursos de suporte de tecnologia tais como inventários de ativos de hardware e software corporativos, além de procedimentos e tratamento para ativos de software e ativos de hardware não autorizados; e

VI - Em relação aos **recursos de estrutura organizacional**, dispuser de unidade como ponto de contato para assuntos relativos ao Sisbin.

COMPETÊNCIAS

As competências do órgão são tratadas na primeira questão do formulário. Deve-se inserir cada competência em uma das linhas da tabela, formando uma lista. As competências listadas devem ser dotadas de potencial para contribuir para o assessoramento ao processo decisório atrelado às ameaças elencadas na Política Nacional de Inteligência (PNI), quais sejam, Espionagem, Atividades ilegais envolvendo bens de uso dual e tecnologias sensíveis, Sabotagem, Armas de destruição em massa, Interferência Externa, Criminalidade Organizada, Ações contrárias à soberania nacional, Corrupção, Ataques cibernéticos, Ações contrárias ao Estado democrático de Direito e Terrorismo.

Exemplo de preenchimento

1. Quais as competências o órgão possui relacionadas à Política Nacional de Inteligência (PNI)?

(Listar as competências com relação, direta ou indireta, com temas da PNI)

1. Apuração das infrações penais e elaboração de inquérito policial
2. Organizar e realizar ações de Inteligência, destinadas ao exercício das funções de polícia judiciária e à apuração de infrações penais

SENSIBILIDADE

Segundo a Portaria 2091/2025, para que órgãos federados atendam ao padrão mínimo de entrada, no critério "Sensibilidade", basta que o órgão trate de dados, informações ou conhecimentos associados à Política Nacional de Inteligência (PNI).

Esse critério é avaliado por meio da pergunta 2 do formulário de ingresso (*Com quais dados, informações ou conhecimentos associados à Política Nacional de Inteligência o órgão trabalha? Em sua avaliação, qual o grau de sensibilidade deles?).*

O conceito de "tratamento" utilizado é semelhante ao da Lei Geral de Proteção de Dados Pessoais (LGPD), qual seja, "coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

Os temas da PNI (2016) em vigor são: Espionagem, Atividades ilegais envolvendo bens de uso dual e tecnologias sensíveis, Sabotagem, Armas de destruição em massa, Interferência Externa, Criminalidade Organizada, Ações contrárias à soberania nacional, Corrupção, Ataques cibernéticos, Ações contrárias ao Estado democrático de Direito e Terrorismo.

Portanto, ao tratar de dados, informações ou conhecimentos associados a um ou mais dos temas da PNI elencados acima o órgão atende, plenamente, ao critério mínimo de entrada no Sisbin.

O formulário, todavia, também solicita uma auto avaliação sobre a sensibilidade desses dados, informações ou conhecimentos. Essa segunda parte da pergunta visa a propiciar subsídios para orientar a resposta da pergunta 3 e para detectar eventuais necessidades de ações para fortalecimento da segurança do órgão. Não se trata de critério de entrada no Sisbin, no caso específico dos órgãos federados.

Sensibilidade é a propriedade de determinada matéria ou ação poder gerar tensões ou prejuízos, caso seja indevidamente revelada e explorada. O nível elevado está relacionado à incidentes de segurança de dados, informações e conhecimentos imprescindíveis a segurança da sociedade ou do Estado. O art. 23 da Lei de Acesso à Informação define informações imprescindíveis à segurança da sociedade ou do Estado e pode ser usado como referência:

Lei nº 12.527/2011, art. 23. São consideradas imprescindíveis à segurança da sociedade ou do Estado e, portanto, passíveis de classificação as informações cuja divulgação ou acesso irrestrito possam:

Pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;

Prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais;

Pôr em risco a vida, a segurança ou a saúde da população;

Oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;

Prejudicar ou causar risco a planos ou operações estratégicas das Forças Armadas;

Prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional;

Pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou

Comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações.

O órgão solicitante deve avaliar seu caso e determinar se os dados, informações ou conhecimentos tratados têm nível de sensibilidade elevado, intermediário ou baixo. Para isso, devem-se utilizar os casos elencados no art. 23 acima como parâmetro de alto nível de sensibilidade e realizar ponderação caso a caso. Se houver mais de um conjunto de dados, eles devem ser discriminados no formulário.

Exemplo de preenchimento (a parte em itálico é somente para ilustrar a racionalidade envolvida na classificação e seu teor não deve constar na resposta do formulário)

2. **Com quais dados, informações ou conhecimentos associados à Política Nacional de Inteligência o órgão trabalha? Em sua avaliação, qual o grau de sensibilidade deles?**

(Consultar cartilha para instruções de preenchimento)

Dados, informações ou conhecimentos	Grau de sensibilidade
1. Dados de cadastros da identificação civil e criminal*	☒Elevado ☐Intermediário ☐Baixo
2. Dados, informações e conhecimentos sobre multas por crimes ambientais**	☐Elevado ☒Intermediário ☐Baixo
3. Dados sobre registro de ocupação hospitalar***	☐Elevado ☐Intermediário ☒Baixo
4. Conhecimento sobre *modus operandi* de constituição de empresas de fachada****	☐Elevado ☒Intermediário ☐Baixo

** enquadra-se na hipótese VII - Comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações.*

*** não se enquadra nos casos do art. 23 da Lei de Acesso à Informação, mas, a partir de julgamento subjetivo, foi considerado intermediário por tratar de dados pessoais em setor estratégico para o País.*

**** a despeito de dado relevante para consciência situacional sobre determinado contexto sanitário, a capacidade de poder gerar tensões ou prejuízos, caso indevidamente revelada e explorada, é baixa, sendo, costumeiramente, um dado público.*

***** apesar de oferecer risco à estabilidade financeira, econômica ou monetária, não chega a apresentar elevado risco à estabilidade financeira ou monetária do País como um todo.* "

PADRÃO DE SEGURANÇA

O nível de segurança do órgão é avaliado por meio da questão 3 do formulário de ingresso. Solicita-se, ao órgão entrante, que relate as características de segurança mais relevantes e compatíveis com o nível de sensibilidade dos dados, informações e conhecimentos tratados, avaliados no quesito anterior.

Os subcritérios de padrão de segurança dialogam com preocupações quanto a criticidade dos ativos no que tange sua governança, segurança física, segurança de pessoas e segurança cibernética.

Os itens listados foram elencados a partir do levantamento de padrões de segurança presentes em decretos e portarias de políticas relacionadas, manuais de boas práticas de entidades públicas com reconhecida atuação na área de referência e mecanismos internos de supervisão e mitigação de riscos da ABIN.

Na lista dos itens da tabela, constam quatro destacados em amarelo. São itens que são usados, também, para avaliar o critério **recursos de suporte tecnológico.** A decisão de inseri-los na avaliação dos critérios de padrão de segurança deu-se porque representam, também, aspectos relevantes para a análise do subcritério de segurança cibernética. Dessa forma, optou-se por evitar redundâncias de preenchimento. O detalhamento pormenorizado desses itens específicos está descrito na seção sobre Recursos de Suporte Tecnológico abaixo.

A avaliação de adequação é feita pelo Órgão Central usando metodologia própria baseada em outras metodologias (a exemplo da usada pelo *Center for Internet Security*) e no cálculo de pontuação, ponderada segundo o nível de importância, dos recursos assinalados como existentes. Ao final, coteja-se a pontuação final com o nível de sensibilidade dos dados, informações e conhecimentos tratados pelo órgão pleiteante.

Algumas definições para auxiliar no preenchimento:

Princípio do sigilo	Necessidade de restrição de acesso a dado ou a conhecimento, em decorrência de determinação legal, inclusive no que se relaciona à segurança da sociedade e do Estado.
Princípio compartimentação	Restrição do acesso com base na necessidade de conhecer e no credenciamento de segurança.
Princípio da responsabilidade	Os agentes públicos são responsáveis pela implementação e manutenção da segurança dos ativos de informação sob sua custódia ou daqueles a que tiverem acesso, sem distinção de cargo ou função.
Princípio do mínimo privilégio de acesso	O nível de acesso a ativos de informação deve se basear em políticas adaptativas e dinâmicas fundadas no controle de autorizações e permissões que preveja acesso tão somente aos ativos necessários para o desempenho da competência regimental ou contratual do agente público interessado, relativo a situações determinadas que justifiquem o acesso.
Princípio do acesso seguro:	O acesso aos ativos de informação deve se basear na desconfiança da entidade que o busca, independentemente da origem da solicitação ou do teor do ativo.
Serviços essenciais:	Compreendem assistência à saúde, saneamento ambiental, transporte e segurança pública.
Sistema de proteção física:	Sistema composto por pessoas, equipamentos e procedimentos para a proteção de ativos contra danos, roubo, sabotagem e outros prejuízos causados por ações humanas não autorizadas, conforme gestão da segurança física e ambiental.
Proteção em profundidade:	Utilização de múltiplas camadas de proteção. Tem como premissa exigir que um ofensor transponha múltiplos layers até atingir o seu objetivo (e.g. acessar um ativo sensível). Cada

	camada deve conter dispositivos que requeiram um ato distinto e separado para que o adversário prossiga com sua intrusão.
Proteção balanceada:	Considera que, a despeito do método e percurso empregados pelo adversário para obter o acesso não autorizado, o ofensor deve se deparar com elementos distintos, mas igualmente eficazes, de proteção física.
Mínima consequência diante de falha	Diante de um eventual óbice ou ação adversa, o sistema apresenta redundância suficiente para garantir a perpetuidade de seu funcionamento em níveis de desempenho satisfatórios (e.g. garantir que acessos indevidos não ocorrerão mesmo com a falha de alguma barreira ou com a suspensão, ainda que temporária, do fornecimento de energia elétrica).
Prestadores de serviço	Indivíduos que têm vínculo empregatício com contratadas prestadoras de serviços à instituição e/ou autônomos que realizam regularmente atividades de apoio nas dependências do órgão, tais como terceirizados, estagiários, bolsistas, pesquisadores.
Entrevista de segurança	Consiste em diálogo planejado, conduzido por profissional treinado em matéria de segurança, com a finalidade de a averiguar eventuais inconsistências nos dados fornecidos pelo interessado e a presença de indicadores de comprometimento neste indivíduo (e.g. antecedentes criminais, vícios).
Credenciamento de segurança	Processo de certificação institucional de que o credenciado atende a requisitos de segurança necessários para o acesso a dados ou conhecimentos sigilosos
Necessidade de conhecer	Condição pessoal inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para acesso a dados ou conhecimentos sigilosos.

RECURSOS DE PESSOAL

O critério mínimo de atendimento ao requisito "recursos de pessoal" para órgãos federados é bastante objetivo. Basta que o órgão tenha, ao menos, um servidor com cursos de formação ou capacitação relacionados às áreas de Inteligência, de segurança da informação e cibernética ou áreas correlatas de ao menos vinte horas-aula nos últimos cinco anos.

Esse critério é avaliado pela pergunta 4 do formulário, em que o órgão entrante deve apenas marcar "sim", caso atenda ao requisito, ou "não", caso não atenda. Em caso positivo, o comprovante da formação ou capacitação deve ser anexado ao formulário.

Salienta-se que a entrada ao Sisbin na condição de órgão federado é possível mesmo que o órgão entrante não possua servidor com essa condição. Nesse caso, o órgão deve marcar a caixa seguinte, em que assume "o compromisso, firme e irrevogável, de capacitar, ao menos, um servidor ou funcionário efetivo nas áreas de Inteligência, Segurança da Informação, cibernética ou áreas correlatas com no mínimo 20 horas-aula, nos próximos 24 meses, a partir da efetiva entrada no Sisbin".

Nesse caso, a capacitação necessária poderá ser fornecida pelo Órgão Central, a partir do reconhecimento da demanda.

RECURSOS DE SUPORTE TECNOLÓGICO

Os recursos de suporte tecnológico são avaliados por meio dos itens destacados em amarelo na tabela da questão 3 do formulário, referente aos padrões de segurança, no subcritério Segurança Cibernética. Esses itens têm destaque sobre os demais pois foram considerados, pelo Órgão Central, como de maior relevância para a segurança da informação, sobretudo tendo em vista que a troca de dados, informações e conhecimento é um pilar fundamental da efetividade do Sisbin.

A Portaria 2.091/2024 traz os requisitos mínimos de entrada para os órgãos federados (Art. 10, V), quais sejam, que o órgão entrante disponha de recursos de suporte de tecnologia e de procedimentos e tratamentos para ativos de software e ativos de hardware não autorizados.

Entre os recursos de suporte de tecnologia elencados estão o inventário e controle de ativos de hardware e software corporativos. Os inventários são documentos em que constam os ativos de TI (hardware e software) que o órgão detém juntamente com informações sobre o ciclo de vida (criação, processamento, armazenamento, transmissão, exclusão e destruição) e sua documentação, a exemplo das licenças dos produtos, atualizações, números de série e datas de garantia.

Os procedimentos e tratamento para ativos não autorizados referem-se a processos de detecção, impedimento de uso e correição de ativos não autorizados, a exemplo de softwares piratas e hardwares externos à instituição.

Para maiores detalhamentos sobre os recursos de suporte tecnológico que embasaram a Portaria 2.091/2024, ver a norma **ABNT NBR ISO 27002.**

RECURSOS DE ESTRUTURA ORGANIZACIONAL

Os recursos de estrutura organizacional são avaliados por meio de uma simples pergunta no item 5 do formulário, referente à presença, no órgão pleiteante, de unidade como ponto de contato para assuntos relativos ao Sisbin.

Diferentemente do critério adotado para órgãos dedicados, em que a Portaria 2.091/2024 demanda unidade de ponto de contato para assuntos relativos ao Sisbin que seja dedicada às atividades de Inteligência ou atividades similares, para os órgãos federados, basta que a unidade ponto de contato fique responsável para lidar com assuntos relativos ao Sisbin. Portanto, a unidade não tem que, necessariamente, ser dedicada à atividade de Inteligência ou similares.