MEMORANDO DE ENTENDIMENTO

ENTRE

O GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA
DA REPÚBLICA FEDERATIVA DO BRASIL

E

A AUTORIDADE NACIONAL DE SEGURANÇA
DA REPÚBLICA ESLOVACA

SOBRE COOPERAÇÃO
NA ÁREA DE SEGURANÇA CIBERNÉTICA

MEMORANDO DE ENTENDIMENTO

ENTRE

O GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA FEDERATIVA DO BRASIL

E

A AUTORIDADE NACIONAL DE SEGURANÇA DA REPÚBLICA ESLOVACA

SOBRE COOPERAÇÃO NA ÁREA DE SEGURANÇA CIBERNÉTICA

O Gabinete de Segurança Institucional da Presidência da República Federativa do Brasil e a Autoridade Nacional de Segurança da República Eslovaca, a seguir designados coletivamente por "Partícipes" e individualmente por "Partícipe":

Reconhecendo as relações amigáveis existentes entre a Presidência da República Federativa do Brasil e a República Eslovaca, bem como os progressos consideráveis no desenvolvimento das tecnologias da informação e da comunicação;

Reconhecendo ainda que a segurança das redes e dos sistemas de informação e serviços se tornou primordial, uma vez que os incidentes de segurança e os ciberataques têm o potencial cada vez maior de impor graves desafios às infraestruturas de informação que apoiam os serviços essenciais à sociedade;

Notando o interesse comum em fortalecer a cooperação em matéria de cibersegurança entre os Partícipes, com base nos princípios da igualdade e da reciprocidade, contribuindo assim para o benefício mútuo e para as relações de amizade entre os dois países;

Reafirmando o nosso empenho em promover um ambiente de ciberespaço aberto, seguro, estável, acessível, pacífico e interoperável, assente no respeito dos direitos humanos e das liberdades fundamentais, em que o desenvolvimento social e econômico possa prosperar;

Desejando continuar a desenvolver a cooperação entre a Presidência da República Federativa do Brasil e a República Eslovaca no domínio da cibersegurança através do fortalecimento do intercâmbio de informações, do compartilhamento de tecnologias e do desenvolvimento de capacidades;

Acreditando que essa cooperação servirá aos interesses comuns e contribuirá para o desenvolvimento da cibersegurança entre os Partícipes;

Respeitando os princípios da soberania, da integridade territorial, do respeito mútuo e da não interferência nos assuntos internos de cada Partícipe; e

Em conformidade com as disposições e regulamentações legais, bem como com os compromissos internacionais dos Partícipes;

Os Partícipes concordaram com o seguinte entendimento:

ARTIGO 1
Objetivo

O objetivo deste Memorando de Entendimento (doravante denominado "Memorando") é promover parcerias e fornecer uma estrutura para aprimorar a cooperação no campo da cibersegurança entre os Partícipes.

ARTIGO 2
Princípios Básicos

1. Os Partícipes confirmam a sua intenção, no âmbito do presente Memorando de Entendimento, de promover uma cooperação mais estreita e privilegiada e o intercâmbio de informações relativas à cibersegurança, criando parceria que reflita os valores comuns, as tradições democráticas, os direitos humanos, o estado de direito, a segurança nacional e o desenvolvimento econômico dos Partícipes.

2. Este Memorando de Entendimento não cria, mantém ou impõe quaisquer obrigações, direitos ou benefícios juridicamente vinculantes entre os Partícipes ou entre os Partícipes e terceiros.

3. Este Memorando de Entendimento deve ser implementado de acordo com as leis, os regulamentos, as políticas e as obrigações internacionais dos Partícipes.

4. Os Partícipes estão comprometidos a promover a segurança e a estabilidade no ciberespaço, reconhecendo a aplicabilidade do direito internacional, em particular a Carta das Nações Unidas, à conduta dos Estados no ciberespaço e as normas voluntárias de comportamento responsável do Estado no ciberespaço.

5. Os Partícipes entendem a necessidade de trabalhar em estreita colaboração com o setor privado, principalmente com entidades consideradas como parte das infraestruturas críticas, reconhecendo que grande parte da inovação e do investimento que molda o ciberespaço ocorre dentro das empresas privadas e que as múltiplas dimensões da cibersegurança exigem cooperação entre governos e seus respectivos setores privados.

ARTIGO 3
Escopo da Cooperação

O escopo da cooperação entre os Partícipes pode incluir áreas relacionadas à cibersegurança com as quais serão capazes de concordar mutuamente, como as seguintes:

1. Fortalecer a resposta a incidentes:

a. reforçar as capacidades de resposta a ameaças e ataques no domínio da cibersegurança;
b. alertar o outro Partícipe, caso seja detectada atividade maliciosa que afete sistema de informação da rede do outro Partícipe;
c. prestar assistência ao outro Partícipe na investigação de incidentes e na atenuação do seu impacto, se solicitado;
d. nos casos de incidentes considerados de alta prioridade por ambos os Partícipes, poderão ser realizadas consultas mútuas sobre as medidas a serem tomadas nas respostas a emergências e sobre planos de ação específicos.

2. Cooperação bilateral em matéria de investigação conjunta, incluindo:

a. desenvolvimento de atividades operacionais e metodologias no domínio da cibersegurança;
b. melhores práticas baseadas em casos reais, para criar um ambiente de rede seguro.

3. Construção de capacidades:

a. apoiar a construção de capacidades e oferecer treinamentos, se for o caso;
b. intercâmbio mútuo e apoio ao desenvolvimento de exercícios conjuntos de cibersegurança;
c. concessão de bolsas de estudo;
d. sensibilização e aumento do nível habilidades digitais no domínio da cibersegurança e da segurança da informação;
e. visitas; e
f. outras formas de cooperação na área.

4. Compartilhamento de informações

Ambos os Partícipes compartilharão informações sobre estratégia, regulação, políticas, melhores práticas e implementações nas áreas de:

a. cibersegurança;
b. criptografia;
c. proteção das infraestruturas nacionais críticas;
d. proteção dos direitos humanos e da liberdade no ciberespaço;
e. conscientização e competência em matéria de segurança da informação; e
f. melhoria da eficácia da gestão da segurança da informação.

ARTIGO 4
Implementação

A fim de implementar o escopo de cooperação definido no artigo 3, os Partícipes buscarão desenvolver o seguinte programa:

a. Identificar oportunidades para discutir incidentes de cibersegurança de interesse mútuo (por exemplo: atividades relacionadas a ameaças persistentes avançadas - APT, ransonware, ataques de negação de serviço, phishing, ataques de varredura, falsificação de sites do governo e outras formas de incidentes cibernéticos);
b. Apoiar-se mutuamente na tomada de medidas combinadas, a fim de evitar a recorrência de incidentes de cibersegurança e aprimorar seus esforços para aumentar o compartilhamento de informações sobre ameaças (por exemplo: troca de indicadores de comprometimento – IoC´s e de técnicas, táticas e procedimentos – TTP´s);
c. Compartilhar avaliações das tendências prevalecentes de segurança das TIC, conforme observado por cada país, periódicamente;
d. Organizar visitas ou encontros virtuais de representantes de ambos os Partícipes regularmente para discutir questões atuais sobre cibersegurança;
e. Convidar representantes de governo, bem como representantes do setor privado, da academia e da sociedade, para seminários e conferências realizados nos respectivos países para discutir questões de cibersegurança; e
f. Quaisquer outras ações de cooperação relacionadas à cibersegurança mutuamente acordadas.

ARTIGO 5
Ponto de Contato

1. Com o objetivo de identificar e facilitar as ações previstas no Artigo 3, os Partícipes designarão representantes para manter contato entre si. Os pontos de contato designados serão responsáveis por obter a aprovação necessária para a realização de atividades cooperativas específicas de seus respectivos governos.

2. Os representantes dos Partícipes responsáveis pela implementação do escopo de cooperação, conforme estabelecido no Artigo 3, poderão realizar consultas para identificar e definir atividades futuras previstas ou relacionadas no Artigo 4, assim como revisar atividades em andamento ou discutir assuntos relacionados a essas atividades. Quando necessário, e mediante acordo mútuo, os Partícipes poderão realizar reuniões de trabalho alternadamente na República Federativa do Brasil e na República Eslovaca em uma data mutuamente acordada.

3. Ambos os Partícipes nomeiam, respetivamente, pontos de contato específicos responsáveis pelo contato e pela coordenação entre si. Detalhes sobre os pontos de contato (PoC) constam do Anexo do presente Memorando de Entendimento.

4. Uma notificação formal ao outro Partícipe no Memorando é suficiente para alterar o PoC. Essa informação entrará em vigor a partir do momento de sua comunicação por escrito à outra parte. A alteração do Anexo ao Memorando não afeta a alteração do próprio Memorando.

ARTIGO 6
Direito de Propriedade Intelectual

1. Cada Partícipe garantirá a proteção adequada dos Direitos de Propriedade Intelectual (DPI) que possam ser gerados a partir da cooperação nos termos deste Memorando, de acordo com suas respectivas leis, regulamentos e acordos internacionais a que ambos os Partícipes estão comprometidos.

2. Os Partícipes não cederão nenhum direito e obrigação decorrente do DPI gerado a invenções ou atividades realizadas sob este Memorando a terceiros sem o consentimento do outro Partícipe.

ARTIGO 7
Disposições financeiras

1. Cada Partícipe arcará com seus próprios custos associados às atividades e à participação no presente Memorando de Entendimento.

2. Não há qualquer obrigação de pagamento ao outro Partícipe no que diz respeito à cooperação prevista no presente Memorando.

3. Os Partícipes podem adotar mutuamente outras disposições financeiras, que serão confirmadas por acordo escrito.

ARTIGO 8
Resolução de litígios

Toda disputa entre os Partícipes relativa à interpretação ou implementação deste Memorando de Entendimento deve ser resolvida amigavelmente por meio de consultas ou negociações entre os Partícipes.

ARTIGO 9
Confidencialidade e Divulgação da Informação

1. Ambos os Partícipes utilizarão as informações e os conhecimentos obtidos no curso das atividades contempladas neste Memorando de Entendimento exclusivamente para fins de sua implementação. Nenhum dos Partícipes divulgará ou distribuirá a terceiros quaisquer informações transmitidas pela outra parte no processo de atividades de cooperação previstas neste Memorando de Entendimento, exceto com o consentimento prévio por escrito do outro Partícipe.

2. Os Partícipes tomarão todas as medidas adequadas para proteger a confidencialidade das informações, documentos, tecnologias e/ou dados trocados e/ou gerados entre os Partícipes no âmbito do presente Memorando contra qualquer divulgação não autorizada, em conformidade com a legislação, regulamentação, políticas e diretivas nacionais dos Partícipes.

3. Em conformidade com a legislação nacional e com a legislação dos Partícipes em matéria de proteção de informações classificadas, acordos de não divulgação e acordos informais de não divulgação, incluindo, mas não exclusivamente, o Protocolo de Sinalização por Cores (*Traffic Light Protocol* - TLP), as informações trocadas de acordo com o presente Memorando de Entendimento devem limitar-se à utilização interna por ambos os Partícipes e não devem ser divulgadas a terceiros, exceto com a autorização escrita do Partícipe que as fornece.

4. Quaisquer informações trocadas no âmbito do presente Memorando de Entendimento não serão consideradas confidenciais nas seguintes condições:

a. forem já do conhecimento do Partícipe que as recebe no momento do compartilhamento;
b. forem, ou se tornarem, do conhecimento público sem qualquer relação com o Partícipe receptor;
c. Forem transmitidas ao Partícipe receptor por uma terceira parte em um canal sem restrições; ou
d. For claramente assinalada como divulgação autorizada pelo Partícipe de origem.

ARTIGO 10
Alteração

Os Partícipes podem revisar ou alterar o presente Memorando de Entendimento em qualquer tempo, mediante consentimento mútuo por escrito. Essas revisões ou alterações entrarão em vigor em data a ser determinada pelos Partícipes e farão parte do presente Memorando de Entendimento.

ARTIGO 11
Entrada em Vigor, Duração e Rescisão

1. O presente Memorando de Entendimento entrará em vigor na data da sua assinatura por ambos os Partícipes por um período de 5 (cinco) anos, sendo automaticamente prorrogado por períodos adicionais de 5 (cinco) anos.

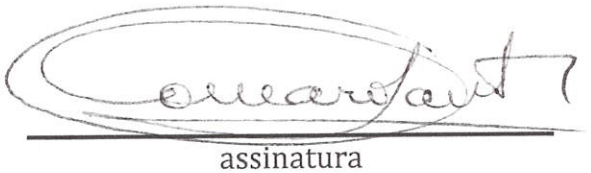
2. Qualquer um dos Partícipes poderá pôr fim a este Memorando de Entendimento a qualquer momento, mediante notificação ao outro Partícipe com 3 (três) meses antes da data prevista para o término. O Memorando de Entendimento será terminado na data prevista para o seu termo quando o outro Partícipe confirmar a recepção da notificação acima referida.

3. Qualquer intenção de finalizar ou prorrogar o presente Memorando de Entendimento será comunicada não somente por meio dos canais diplomáticos.

Os abaixo assinados, devidamente autorizados para o efeito pelos respectivos Governos, assinaram o presente Memorando de Entendimento.

Assinado em Bratislava, aos 29 dias do ano de 2025, em três originais nas línguas portuguesa, eslovaca e inglesa, sendo todos os textos igualmente válidos. Em caso de divergência de interpretação, prevalecerá o texto em inglês.

Assinado por e em nome do
Gabinete de Segurança
Institucional da Presidência da
República Federativa do Brasil



assinatura

Marcos Antonio Amaro dos Santos
Ministro de Estado Chefe do
Gabinete de Segurança
Institucional da Presidência da
República

29/5/25

data

Assinado por e em nome do Chefe
da Autoridade Nacional de
Segurança da República Eslovaca

assinatura

Roman Konečný
Diretor
de Autoridade de Segurança
Nacional

29/5/25

data

ANEXO

Ao Memorando de Entendimento entre o Gabinete de Segurança Institucional da Presidência da República Federativa do Brasil e a Autoridade Nacional de Segurança da República Eslovaca

Pontos de contato designados para a partilha de informações no âmbito do Memorando de Entendimento:

O Gabinete de Segurança Institucional da Presidência da República Federativa do Brasil:

- **Serviço de assistência:** ctir@ctir.gov.br (Tel) +55 613411-3477, INOC-DBA BR: 266031*800, Cel: +55 61999957859
- **PoCs:**

Tópico	PoC	E-mail	Tel. fixo	Tel. celular
Tratamento de incidentes	Adão dos Santos	adao.santos@presidencia.gov.br	+5561992203732	+55613411-3978
Cooperação e Informação	Cesar Montenegro Justo	cesar.montenegro@presidencia.gov.br	+5561983423915	+55613411-3195
Gestão da Informação	Daniel Maier de Carvalho	daniel.maier@presidencia.gov.br	+5561999957859	+55613411-1554

Horário de funcionamento: Segunda-feira a sexta-feira 9:00 - 18:00 (GMT -3)
Serviço de plantão: para parceiros (MoU) 24/7

Autoridade Nacional de Segurança da República Eslovaca:

- **Serviço de assistência:** sk-cert@nbu.gov.sk (Tel) +421 2 6869 2915, (Fax) +421 2 6869 1700, GSM: +421 903 993 706
- **PoCs:**

Tópico	PoC	E-mail	Tel. fixo	Tel. celular
Tratamento de incidentes	Ján Doboš	incident@nbu.gov.sk	+421 2 6869 2997	+421 903 993 706
Cooperação e Informação	René Baran	rene.baran@nbu.gov.sk	+421 2 6869 2350	+421 903 993 163
Credenciamento e Certificação	Matej Šalmík	matej.salmik@nbu.gov.sk	+421 2 6869 2858	+421 903 993 723
Estudos de Segurança e Estratégia Nacional	Jaroslav Krcheň	jaroslav.krchen@nbu.gov.sk	+421 2 6869 2262	+421 903 993 151
Gerente de Ligações Internacionais	Jaroslav Ďurovka	jaroslav.durovka@nbu.gov.sk	+421 2 6869 2150	+421 905 011 225

Horário de funcionamento: segunda-feira - sexta-feira 7:30 - 15:30 (GMT+1 / GMT+2 com DST que começa no último domingo de março e termina no último domingo de outubro)
Serviço de plantão: para parceiros (MoU) 24/7