

MEMORANDO DE ENTENDIMENTO
SOBRE
COOPERAÇÃO NA ÁREA DE SEGURANÇA CIBERNÉTICA
ENTRE
O GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA
DA REPÚBLICA FEDERATIVA DO BRASIL
E
O CENTRO CRIPTOLÓGICO NACIONAL DO CENTRO NACIONAL DE
INTELIGÊNCIA DO REINO DA ESPANHA

O Gabinete de Segurança Institucional da Presidência da República Federativa do Brasil e o Centro Criptológico Nacional do Centro Nacional de Inteligência do Reino da Espanha são referidos a seguir individualmente como "Partícipe" e conjuntamente como "Partícipes";

Considerando que governos, empresas e cidadãos estão cada vez mais sujeitos a uma variedade de ameaças cibernéticas e que é necessário melhorar continuamente a prontidão para a segurança dos computadores e aumentar a conscientização sobre a importância de manter os sistemas seguros e promover práticas e procedimentos de segurança;

Reconhecendo que o ritmo de desenvolvimento de novas tecnologias e aplicativos, em conjunto com o maior número de acessos, oferece oportunidades significativas para o desenvolvimento econômico e social;

Tendo em conta que a dependência de redes cada vez mais interconectadas também expõe os Estados a novos riscos cibernéticos, os quais podem causar impacto no bem-estar da sociedade;

Reafirmando nosso compromisso de promover um ambiente cibernético aberto, seguro, estável, acessível e pacífico, baseado no respeito aos direitos humanos e às liberdades fundamentais, conducentes ao desenvolvimento social e econômico;

Reconhecendo a necessidade de maior cooperação entre todas as partes interessadas, dentro e fora das fronteiras nacionais, nas ações contra o uso malicioso do espaço cibernético;

Desejando desenvolver a cooperação entre os Partícipes na área de segurança cibernética, em consonância com as suas respectivas leis, regras e regulamentos nacionais; com as suas obrigações internacionais; e com base nos princípios de reciprocidade e benefício mútuo;

Reconhecendo a importância de expandir a cooperação bilateral no campo da segurança cibernética como contribuição de relevo para a manutenção da segurança internacional e nacional, com o objetivo de impedir atividades que danifiquem intencionalmente e substancialmente a disponibilidade ou a integridade geral da Internet;

Os Partícipes concordaram com o seguinte entendimento:

ARTIGO 1

Princípios Básicos

Os Partícipes confirmam sua intenção, de acordo com este Memorando de Entendimento (MoU), de promover cooperação mais estreita e intercâmbio de informações referentes à segurança cibernética, criando parceria que reflita os valores compartilhados, as tradições democráticas, os direitos humanos, o estado de direito, a segurança nacional e o desenvolvimento econômico dos Partícipes.

Este Memorando de Entendimento não se destina a criar, manter ou impor quaisquer obrigações, direitos ou benefícios juridicamente vinculantes entre os Partícipes ou entre os Partícipes e terceiros.

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

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

As Partes 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 espaço cibernético ocorre dentro das empresas privadas e que as múltiplas dimensões da segurança cibernética exigem cooperação entre governos e seus respectivos setores privados.

ARTIGO 2

Escopo da Cooperação

O escopo da cooperação entre os Partícipes pode incluir áreas relacionadas à segurança cibernética com as quais os Partícipes possam concordar mutuamente, como as seguintes:

- a. Compartilhamento de experiências sobre legislação, regulamentação, estratégias, políticas e melhores práticas nacionais;
- b. Promoção de medidas de cooperação entre os Partícipes para facilitar, de acordo com as respectivas legislações nacionais, o intercâmbio de informações sobre ameaças cibernéticas e vulnerabilidades e de capacidades, inclusive por meio de treinamento, aprimoramento de processos, diálogo e consultas, conforme necessário;
- c. Promoção da cooperação e da troca de informações entre os CERTs ou CSIRTs nacionais designados, com definição do Ponto de Contato (PoC) por quem as notificações serão adequadamente tratadas e priorizadas;
- d. Compartilhamento das melhores práticas de avaliação, de desenvolvimento e de implementação de padrões para a segurança cibernética e para mecanismos de certificação, bem como fortalecimento da segurança de processos, de produtos e de serviços digitais, durante todo o seu ciclo de vida e a sua cadeia de suporte;
- e. Promoção da cooperação nas áreas de pesquisa e desenvolvimento relacionados à segurança cibernética, padrões de segurança cibernética e testes de segurança, incluindo processos de credenciamento e de desenvolvimento de soluções de segurança cibernética, considerando novas consultas sobre tais questões;
- f. Promoção da cooperação nas áreas de educação, conscientização, sensibilização, treinamento, capacitação e intercâmbio de conhecimento entre especialistas;
- g. Estabelecimento de mecanismos institucionais para troca periódica de pontos de vista sobre novos desafios relacionados aos incidentes cibernéticos e às ameaças atuais;
- h. Estudo da possibilidade de realizar exercícios de segurança cibernética conjuntos;
- i. Intercâmbio de experiências em estratégias de promoção da integridade da cadeia de suprimento, a fim de aumentar a confiança dos usuários na segurança dos produtos e dos serviços de tecnologias da informação e comunicação; e
- j. Favorecimento de atividades para desenvolver melhores práticas avançadas de segurança cibernética para todos os atores do ciberespaço.

ARTIGO 3

Implementação

A fim de implementar o escopo de cooperação identificado no Artigo 2, os Partícipes comprometem-se a viabilizar as seguintes ações, quando aplicáveis:

- a. Avisar sobre possíveis incidentes de segurança cibernética de que venha a ter conhecimento e que possam estar comprometendo ativos de informação do outro Partícipe;
- b. Apoiar-se mutuamente na tomada de medidas combinadas, a fim de evitar a recorrência de incidentes de segurança cibernética e aprimorar seus esforços para aumentar o compartilhamento de informações sobre ameaças;
- c. Compartilhar avaliações das tendências prevalentes de segurança cibernética, conforme observado por cada país;
- d. Organizar visitas ou encontros virtuais de representantes de ambos os Partícipes regularmente para discutir questões atuais sobre segurança cibernética;
- 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 segurança cibernética;
- f. Compartilhar experiências sobre métodos de tratamento de incidentes por meio de padrões reconhecidos;
- g. Compartilhar dados de inteligência de ameaças por meio de canais de comunicação previamente estabelecidos;
- h. Compartilhar informações sobre pontos de contato, ameaças cibernéticas e vulnerabilidades em segurança cibernética; e
- i. Quaisquer outras ações de cooperação relacionadas à segurança cibernética mutuamente acordadas.

ARTIGO 4

Ponto de Contato

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 (PoC) designados serão responsáveis por obter a aprovação necessária para a realização de atividades cooperativas específicas de seus respectivos governos.

Os representantes dos Partícipes responsáveis pela implementação do escopo de cooperação, conforme estabelecido no Artigo 2, poderão realizar tratativas para identificar e definir atividades futuras previstas ou relacionadas no Artigo 3 e revisar atividades em andamento ou discutir assuntos relacionados a essas atividades.

Quando necessário, e de acordo mútuo, os Partícipes poderão realizar reuniões de trabalho alternadamente em cada país, em datas mutuamente acordadas. Os principais resultados esperados para cada encontro serão sugeridos pelos Partícipes antes de cada reunião.

ARTIGO 5

Formas de Cooperação

Todas as atividades de cooperação nos termos dos Artigos 2, 3 e 4 deste Memorando de Entendimento serão conduzidas de acordo com as leis, regras e regulamentos aplicáveis de cada país.

Todas as atividades de cooperação previstas nos Artigos 2, 3 e 4 deste Memorando de Entendimento estarão sujeitas à disponibilidade de fundos e outros recursos dos Partícipes.

Para executar as atividades de cooperação estabelecidas neste Memorando de Entendimento, convidados do setor privado, equipes de tratamento e resposta a incidentes cibernéticos, sociedade civil e academia poderão ser autorizados a participar, se acordado mutuamente pelos Partícipes.

ARTIGO 6

Direito de Propriedade Intelectual

Cada Partícipe garantirá a proteção adequada dos Direitos de Propriedade Intelectual (DPI) gerados a partir da cooperação nos termos deste Memorando, de acordo com suas respectivas leis, regulamentos e acordos internacionais.

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

Divulgação da Informação

Nenhum dos Partícipes divulgará nem distribuirá a terceiros quaisquer informações transmitidas pela outra Parte no processo de atividades cooperativas sob este Memorando de Entendimento, exceto com o consentimento prévio por escrito do outro Partícipe.

ARTIGO 8

Resolução de Litígios

Toda e qualquer 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

Emendas

Este Memorando de Entendimento pode ser alterado por consentimento mútuo por escrito dos Partícipes, que será formalizado por meio de canais diplomáticos. A entrada em vigor das emendas ao presente Memorando de Entendimento estará sujeita ao mesmo procedimento utilizado para a entrada em vigor do Memorando de Entendimento.

ARTIGO 10

Confidencialidade

Sem prejuízo das obrigações internacionais derivadas do Acordo relativo à troca e proteção mútua de informações classificadas assinado entre Espanha e Brasil em 15 de abril de 2015, os Titulares de Unidades concordam que toda colaboração e troca de informações realizadas no âmbito deste memorando de entendimento será tratado de forma sigilosa, evitando-se sua divulgação e transmissão a terceiros.

ARTIGO 11

Entrada em Vigor, Duração, Rescisão

Este Memorando de Entendimento entra em vigor imediatamente após a assinatura de ambos os Partícipes.

O presente Memorando de Entendimento permanecerá em vigor pelos próximos cinco anos. Se não houver manifestação dos Partícipes em rescindir o Memorando de Entendimento, o prazo de vigência será prorrogado por períodos sucessivos de mesma duração.

A eventual rescisão deste Memorando de Entendimento não afetará as atividades de cooperação nos termos dos Artigos 2 e 3 que já estiverem em andamento até sua conclusão, a menos que os Partícipes determinem, por escrito, o contrário.

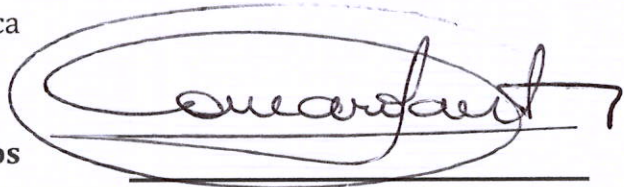
O acima exposto representa os entendimentos alcançados entre os Partícipes sobre as matérias referidas neste Memorando de Entendimento.

Assinado em dois exemplares originais, nos idiomas Português e Espanhol, ambos igualmente autênticos, na cidade de Brasília, Distrito Federal, em 3 de fevereiro de 2025.

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

**Marcos Antonio Amaro Dos
Santos**

Ministro de Estado Chefe do
Gabinete de Segurança
Institucional da Presidência da
República

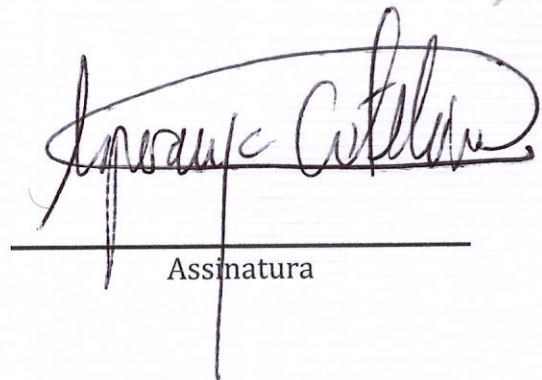
A handwritten signature in dark ink, appearing to read 'marcos', is written over a horizontal line. The signature is enclosed within a large, loopy oval shape.

Assinatura

Assinado em nome do Centro
Criptológico Nacional do
Centro Nacional de Inteligência
do Reino da Espanha

**Esperanza Casteleiro
Llamazares**

Secretária de Estado Diretora
do Centro Criptológico
Nacional do Centro Nacional de
Inteligência do Reino da
Espanha

A handwritten signature in dark ink, appearing to read 'Esperanza Casteleiro', is written over a horizontal line. The signature is enclosed within a large, loopy oval shape.

Assinatura