MEMORANDO DE ENTENDIMIENTO
SOBRE
COOPERACIÓN EN MATERIA DE CIBERSEGURIDAD
ENTRE
EL GABINETE DE SEGURIDAD INSTITUCIONAL DE LA PRESIDENCIA DE LA REPÚBLICA FEDERATIVA DEL BRASIL
Y
EL CENTRO CRIPTOLÓGICO NACIONAL DEL CENTRO NACIONAL DE INTELIGENCIA DEL REINO DE ESPAÑA

El Gabinete de Seguridad Institucional de la Presidencia de la República Federativa del Brasil y el Centro Criptológico Nacional del Centro Nacional de Inteligencia del Reino de España son referidos a seguir individualmente como "Partícipe" y conjuntamente como "Partícipes";

Considerando que los gobiernos, empresas, y los ciudadanos están cada vez más sujetos a una variedad de amenazas cibernéticas y que existe la necesidad de mejorar continuamente la preparación para la seguridad de los computadores y crear conciencia sobre la importancia de mantener los sistemas seguros y promover prácticas y procedimientos de seguridad.;

Reconociendo que el ritmo del desarrollo de nuevas tecnologías y aplicaciones, junto con el mayor número de acceso, ofrece importantes oportunidades para el desarrollo económico y social;

Teniendo en cuenta que la dependencia de las redes cada vez más interconectados también expone a los Estados a nuevos riesgos cibernéticos, que pueden impactar en el bienestar de la sociedad;

Reafirmando nuestro compromiso de promover un entorno cibernético abierto, seguro, estable, accesible, pacífico y interoperable, basado en el respeto de los derechos humanos y las libertades fundamentales, propicio para el desarrollo social y económico;

Reconociendo la necesidad de mayor cooperación entre todas las partes interesadas, dentro y fuera de las fronteras nacionales, en acciones contra el uso malicioso del espacio cibernético;

Deseando desarrollar la cooperación entre los Partícipes en la área de ciberseguridad, en consonancia con sus respectivas leyes, reglas e reglamentos nacionales, con sus obligaciones internacionales, e con base en los principios de reciprocidad y beneficio mutuo;

Reconociendo la importancia de ampliar la cooperación bilateral en el campo de la seguridad cibernética como una contribución importante al mantenimiento de la seguridad internacional y nacional, con el fin de prevenir actividades que intencional y sustancialmente dañen la disponibilidad o la integridad general de Internet;

Los Partícipes se ponen de acuerdo con el siguiente entendimiento:

ARTÍCULO 1
Principios Básicos

Los Partícipes confirman su intención, de conformidad con este Memorando de Entendimiento (MoU), de promover una cooperación más estrecha y el intercambio de informaciones en materia de seguridad cibernética, creando una asociación que refleje valores compartidos, tradiciones democráticas, derechos humanos, estado de derecho, seguridad nacional y desarrollo económico de los Partícipes.

Este Memorando de Entendimiento no crea, mantiene ni impone obligaciones, derechos o beneficios legalmente vinculantes entre los Partícipes o entre los Partícipes y terceros.

Este Memorando de Entendimiento se implementará de conformidad con las leyes, reglamentos, políticas y obligaciones internacionales de los Partícipes.

Los Partícipes se comprometen a promover la seguridad y la estabilidad en el ciberespacio, reconociendo la aplicabilidad del derecho internacional, en particular la Carta de las Naciones Unidas, a la conducta de los Estados en el ciberespacio y las normas voluntarias de comportamiento responsable de los Estados en el ciberespacio.

Las Partes entienden la necesidad de trabajar en estrecha colaboración con el sector privado, en particular con las entidades consideradas parte de la infraestructura crítica,

reconociendo que gran parte de la innovación y la inversión que da forma al ciberespacio tiene lugar dentro de las empresas privadas y que las múltiples dimensiones de la seguridad cibernética requieren la cooperación entre gobiernos y sus respectivos sectores privados.

ARTÍCULO 2
Alcance de la Cooperación

El alcance de la cooperación entre los Participantes incluirá áreas relacionadas con la ciberseguridad, para que los Participantes puedan acordar mutuamente, tales como las siguientes:

a. Intercambiar experiencias sobre legislación, regulación, estrategias, políticas y mejores prácticas;
b. Promover medidas de cooperación entre los Partícipes para facilitar, de conformidad con sus respectivas legislaciones nacionales, el intercambio de información sobre amenazas cibernéticas y vulnerabilidades y capacidades, incluso a través de capacitación, mejora de procesos, diálogo y consultas, según sea necesario;
c. Promover la cooperación y el intercambio de información entre los CERTs o CSIRTs nacionales designados, definiendo el Punto de Contacto (PoC) mediante el cual se manejan y priorizan adecuadamente las notificaciones;
d. Compartir mejores prácticas para evaluar, desarrollar e implementar estándares de ciberseguridad y para mecanismos de certificación, así como fortalecer la seguridad de los procesos, productos y servicios digitales, a lo largo de su ciclo de vida y cadena de soporte;
e. Promover la cooperación en las áreas de investigación y desarrollo relacionadas con la ciberseguridad, los estándares de ciberseguridad y las pruebas de seguridad, incluidos los procesos de acreditación y el desarrollo de soluciones de seguridad cibernética, considerando consultas adicionales sobre dichos temas;
f. Promover la cooperación en las áreas de educación, concientización, sensibilización, capacitación, desarrollo de capacidades e intercambio de conocimientos entre especialistas;

g. Establecer mecanismos institucionales para el intercambio periódico de punto de vista sobre nuevos desafíos relacionados con incidentes cibernéticos y amenazas actuales;
h. Estudiar la posibilidad de realizar ejercicios conjuntos de ciberseguridad;
i. Intercambiar experiencias en estrategias para promover la integridad de la cadena de suministro, con el fin de aumentar la confianza de los usuarios en la ciberseguridad de los productos y servicios de la tecnología de la información y las comunicaciones; y
j. Favorecer actividades para desarrollar mejores prácticas de ciberseguridad avanzada para todos los actores en el ciberespacio.

ARTÍCULO 3
Implementación

A fin de implementar el alcance de la cooperación identificado en el Artículo 2, los Partícipes se comprometen a habilitar las siguientes acciones, cuando corresponda:

a. Advertir sobre posibles incidentes de ciberseguridad de los que tenga conocimiento y que puedan estar comprometiendo los activos de información del otro Partícipe;
b. Apoyarse mutuamente para tomar medidas concertadas para evitar la recurrencia de incidentes de ciberseguridad y mejorar sus esfuerzos para aumentar el intercambio de información sobre amenazas;
c. Compartir evaluaciones de las tendencias de seguridad cibernética predominantes observadas por cada país;
d. Organizar visitas o reuniones virtuales de representantes de ambos Partícipes de manera regular para discutir temas de ciberseguridad actuales;
e. Invitar a representantes gubernamentales, así como del sector privado, la academia y la sociedad, a seminarios y conferencias que se celebren en los respectivos países para discutir temas de ciberseguridad;
f. Compartir experiencias sobre métodos de manejo de incidentes a través de estándares reconocidos;
g. Compartir datos de inteligencia de amenazas a través de canales de comunicación preestablecidos;

h. Comparta información sobre puntos de contacto, amenazas cibernéticas y vulnerabilidades de seguridad cibernética; y
i. Cualquier otra acción de cooperación relacionada con la ciberseguridad mutuamente acordada.

ARTÍCULO 4
Punto de Contacto

Con el objetivo de identificar y facilitar las acciones previstas en el Artículo 3, los Partícipes designarán representantes para mantener contacto entre sí. Los puntos de contacto designados (PoC) serán responsables de obtener la aprobación necesaria para llevar a cabo actividades de cooperación específicas de sus respectivos gobiernos.

Los representantes de los Partícipes responsables de implementar el alcance de la cooperación, tal como se establece en el Artículo 2, pueden realizar negociaciones para identificar y definir las actividades futuras previstas o enumeradas en el Artículo 3 y revisar las actividades en curso o discutir asuntos relacionados con estas actividades.

Cuando sea necesario, y de mutuo acuerdo, los Partícipes podrán celebrar reuniones de trabajo en forma alterna en cada país, en fechas mutuamente acordadas. Los principales resultados esperados para cada reunión serán sugeridos por los Partícipes antes de cada reunión.

ARTÍCULO 5
Formas de Cooperación

Todas las actividades de cooperación de conformidad con los Artículos 2, 3 y 4 de este Memorando de Entendimiento se llevarán a cabo de conformidad con las leyes, normas y reglamentos aplicables de cada país.

Todas las actividades de cooperación previstas en los Artículos 2, 3 y 4 de este Memorando de Entendimiento estarán sujetas a la disponibilidad de fondos y otros recursos de los Partícipes.

Para ejecutar las actividades de cooperación establecidas en este Memorando de Entendimiento, se permitirá la participación de invitados del sector privado, equipos de respuesta y manejo de incidentes cibernéticos, la sociedad civil y la academia, si así lo acuerdan los Partícipes.

ARTÍCULO 6
Derechos de Propiedad Intelectual

Cada Partícipe garantizará la protección adecuada de los Derechos de Propiedad Intelectual (en lo sucesivo, DPI) generados a partir de la cooperación de conformidad con este Memorando de conformidad con sus respectivas leyes, normas, reglamentos y acuerdos internacionales.

Los Partícipes no asignan ningún derecho ni obligación que surja de los DPI generados por las invenciones o actividades realizadas en virtud de este instrumento a ningún tercero sin el consentimiento del otro Partícipe.

ARTÍCULO 7
Liberación de Información

Ninguno de los Partícipes distribuirá a ningún tercero la información transmitida por la otra Parte en el proceso de actividades de cooperación en virtud del presente instrumento, excepto con el consentimiento previo por escrito del otro Partícipe.

ARTÍCULO 8
Solución de Conflictos

Todas y cualquier una de las disputas entre los Partícipes relacionadas con la interpretación o implementación de este instrumento se resolverán de manera amistosa mediante consultas o negociaciones entre los Partícipes.

ARTÍCULO 9
Enmiendas

Este Memorando de Entendimiento puede ser enmendado por consentimiento mutuo por escrito entre los Partícipes, el cual se formalizará mediante los canales diplomáticos. La entrada en vigor de las enmiendas a este Memorando de Entendimiento estará sujeta al mismo procedimiento utilizado para la entrada en vigor del Memorando de Entendimiento.

ARTÍCULO 10
Confidencialidad

Sin perjuicio de las obligaciones internacionales derivadas del Acuerdo relativo al intercambio y la protección mutua de la información clasificada suscrito entre España y Brasil el 15 de abril de 2015, los Partícipes acuerdan que toda la colaboración e intercambio de información realizada dentro del ámbito de este memorando de entendimiento se tratará de manera confidencial, evitando su difusión y transmisión a terceros.

ARTÍCULO 11
Entrada en Vigor, Duración y Terminación

El presente Memorando de Entendimiento entrará en vigor en la fecha de su firma por ambos Partícipes.

El presente Memorando permanecerá en vigor durante los próximos cinco años. Si ninguna de los Partícipes expresa interés en dar por terminado, el plazo de vigencia será extendido por periodos sucesivos de igual tiempo.

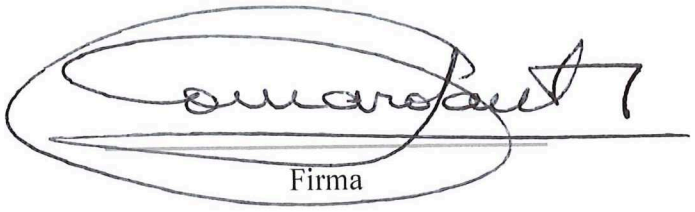
La terminación de este instrumento no afectará las actividades de cooperación conducidas bajo los Artículos 2 y 3 que ya estén en curso y hasta su finalización, a menos que las Partes determinen lo contrario por escrito.

Lo anterior representa los entendimientos alcanzados entre los Partícipes sobre las materias a que se refiere el presente Memorando de Entendimiento.

Firmado en dos originales cada uno en portugués y en español, siendo ambas versiones igualmente auténticas, en la ciudad de Brasilia, Distrito Federal, Brasil, el 3 de febrero de 2025.

Firmado por y en nombre del Gabinete de Seguridad Institucional de la Presidencia de la República de Brasil.

Marcos Antonio Amaro Dos Santos
Ministro de Estado Jefe del Gabinete de Seguridad Institucional de la Presidencia da la República Federativa de Brasil



Firma

Firmado por y en nombre del Centro Criptológico Nacional del Centro Nacional de Inteligencia del Reino de España

Esperanza Casteleiro Llamazares
Secretaria de Estado Directora del Centro Criptológico Nacional del Centro Nacional de Inteligencia del Reino de España

Firma