ACUERDO DE COOPERACIÓN INTERINSTITUCIONAL ENTRE EL CENTRO NACIONAL DE CIBERSEGURIDAD Y LA OFICINA NACIONAL DE DERECHO DE AUTOR (ONDA).

ENTRE: De una parte, el **CENTRO NACIONAL DE CIBERSEGURIDAD (CNCS),** dependencia del Ministerio de la Presidencia, creado por mandato del artículo 10 del Decreto No. 230-18, de fecha 19 de junio del año 2018, que establece y regula la Estrategia Nacional de Ciberseguridad, con su domicilio ubicado en la Ave. México esq. Calle Dr. Delgado, sector Gazcue, Palacio Nacional, de esta ciudad de Santo Domingo de Guzmán, Distrito Nacional, República Dominicana; debidamente representada de conformidad con el artículo 15, literal c), del Decreto No. 230-18, de fecha 19 de junio del año 2018, por el Director Ejecutivo, Coronel **JUAN GABRIEL GAUTREAUX MARTÍNEZ,** P.N., dominicano, mayor de edad, provisto de la Cédula de Identidad No. 001-0061362-9, de igual domicilio que la entidad, que en lo que sigue del presente Acuerdo de Cooperación Interinstitucional se denominará por su propio nombre o como **"CNCS";** y,

De la otra parte, la **OFICINA NACIONAL DE DERECHO DE AUTOR (ONDA),** institución gubernamental creada de acuerdo por la Ley núm. 65-00, de fecha 21 de agosto del 2000 y su reglamento núm. 362, del 14 de marzo del 2001, con su domicilio y oficinas en la calle Paseo de Los Locutores, núm. 28, del Ensanche Piantini, Distrito Nacional, capital de la República Dominicana, con Registro Nacional de Contribuyente (RNC) núm. 4-01-50879-6, debidamente representada por el Licdo. **JOSÉ RUBÉN GONELL COSME**, dominicano, mayor de edad, portador de la cédula de identidad y electoral núm. 047-0108208-5, designado en virtud del Decreto núm. 329-20, de fecha 16 de agosto del 2020, facultado por su cargo para representarle, que en lo que sigue del presente Acuerdo de Cooperación Interinstitucional, se denominará por su propio nombre o como **ONDA".**

El **CNCS** y la **ONDA**, en lo que sigue de este Acuerdo de Cooperación Interinstitucional, serán identificados individualmente por sus respectivos nombres o como **"PARTE"** y cuando sean designadas de manera conjunta, se denominarán **"LAS PARTES"**.

PREÁMBULO:

POR CUANTO (1) : De conformidad con lo establecido en los artículos 10 y 11 del Decreto No. 230-18, de fecha 19 de junio de 2018, el **CNCS** es una dependencia del Ministerio de la Presidencia, que tiene por objeto: (i) la elaboración, desarrollo, actualización y evaluación de la Estrategia Nacional de Ciberseguridad; (ii) la formulación de políticas derivadas de la Estrategia y la definición de las iniciativas, programas y proyectos que lleven a la realización exitosa de la Estrategia; y (iii)

la prevención, detección y gestión de incidentes generados en los sistemas de información relevantes del Estado dominicano e infraestructuras críticas nacionales.

POR CUANTO (2): Que mediante el Decreto núm. 313-22, de fecha 14 de junio del año 2022, Se aprueba la Estrategia Nacional de Ciberseguridad 2030, con vigencia hasta el 31 de diciembre de 2030, con el objeto de fortalecer el marco nacional de ciberseguridad, fomentando la concientización y creación de entornos digitales seguros, confiables y resilientes, que promuevan una sociedad digital dentro de un esquema de inclusión y de respeto a los derechos fundamentales.

POR CUANTO (3): De conformidad con el artículo 5 del referido Decreto, la Estrategia Nacional de Ciberseguridad 2030, se encuentra conformada por objetivos estratégicos, objetivos específicos y líneas de acción.

POR CUANTO (4): Que el OBJETIVO ESTRATÉGICO 1, establece: Fortalecimiento de la capacidad institucional. Fortalecer las capacidades de las entidades y organismos especializados de apoyo, para mejorar la prevención, detección, respuesta y recuperación en materia de ciberseguridad. Asimismo, contribuir al fortalecimiento de las instituciones del Estado, en todo el contexto de la ciberseguridad.

Objetivo específico 1.1: Fortalecimiento integral de las entidades y organismos especializados de apoyo en el ámbito de la gestión y seguimiento de ciberseguridad.

Línea de acción 1.1.1: Fortalecer las entidades y organismos especializados de apoyo en la gestión, seguimiento, monitoreo y evaluación de ciberseguridad, a nivel de recursos tecnológicos, financieros, humanos, entre otros.

Línea de acción 1.1.2: Fortalecer la gobernanza de las entidades y organismos especializados de apoyo y de las instituciones de investigación y persecución del ciberdelito.

Línea de acción 1.1.3: Desarrollar planes de formación, capacitación y sensibilización para funcionarios y servidores en materia de ciberseguridad.

Línea de acción 1.1.4: Crear mecanismos seguros y ágiles para reportes y denuncias de forma presencial y digital, así como también simplificar dichos trámites.

Objetivo específico 1.2: Fortalecimiento de las instituciones del Estado en materia de ciberseguridad a nivel de estructuras, formación, estándares y lineamientos para el fortalecimiento de la seguridad de la información.

PRESIDENCIA DE LA REPÚBLICA DOMINICANA
MINISTERIO DE LA PRESIDENCIA
Dirección Ejecutiva, Centro Nacional de Ciberseguridad

DR. OSCAR MOQUETE CUEVAS
ABOGADO NOTARIO PÚBLICO
STO. DGO. DISTRITO NACIONAL
MAT.: 3900

ONDA

Línea de acción 1.2.1: Articular la revisión de las estructuras actuales de tecnologías de la información (TI) de las instituciones del Estado para establecer una estructura independiente, enfocada en la ciberseguridad, conforme a las buenas prácticas internacionales, con fines de priorizar los pilares fundamentales de la seguridad de la información en las instituciones del Estado.

Línea de acción 1.2.2: Diseñar un plan de formación, capacitación y sensibilización en ciberseguridad para personal responsable de la seguridad de la información en las instituciones del Estado.

Línea de acción 1.2.3: Elaborar, definir y garantizar cumplimiento de los estándares para la seguridad de las Tecnologías de la Información y Comunicación (TIC) en el Estado.

POR CUANTO (5): Que el OBJETIVO ESTRATÉGICO 2, establece: Protección y resiliencia de infraestructuras. Asegurar el continuo funcionamiento de las infraestructuras críticas nacionales y las infraestructuras de tecnologías de la información (TI) del Estado.

Objetivo específico 2.1: Fortalecer la protección de las infraestructuras críticas nacionales y las de tecnologías de la información (TI) del Estado.

Línea de acción 2.1.1: Elaborar y establecer un plan nacional de respuesta a incidentes de ciberseguridad, y contingencias a riesgos, que procure la adecuada actuación en la gestión de incidentes cibernéticos, riesgos de emergencia y crisis nacional.

Línea de acción 2.1.2: Identificar y apoyar los organismos principales en el área de respuesta a incidentes que puedan proporcionar soporte a las infraestructuras críticas nacionales y a las infraestructuras tecnologías de la información (TI) del Estado y del sector privado en función al Plan Nacional de Respuesta a Incidentes de Ciberseguridad.

Línea de acción 2.1.3: Desarrollar y establecer los protocolos de activación y acción para los organismos de respuesta, y todo el ciclo de gestión de los incidentes.

Línea de acción 2.1.4: Elaborar y establecer un plan nacional de comunicación e intercambio de información ante crisis de incidentes de seguridad cibernética.

Línea de acción 2.1.5: Fortalecer los Equipos Sectoriales de Respuestas a Incidentes Cibernéticos (CSIRT) y promover el establecimiento de los mismos en los sectores críticos nacionales.

Línea de acción 2.1.6: Diseñar, establecer y poner en marcha un plan de ejercicios de simulación de incidentes cibernéticos para las infraestructuras críticas nacionales y las instituciones del Estado.

PRESIDENCIA DE LA REPÚBLICA DOMINICANA
MINISTERIO DE LA PRESIDENCIA
Dirección Ejecutiva, Centro Nacional de Ciberseguridad

DR. OSCAR MOQUETE CEBALLOS
ABOGADO NOTARIO PÚBLICO
MAT. 3000
STO. DGO. DISTRITO NACIONAL

ONDA

Objetivo específico 2.2: Fortalecer la gestión de riesgos, identificar las infraestructuras críticas nacionales y las infraestructuras de tecnologías de la información (TI) relevantes del Estado y efectuar un análisis de riesgo.

Línea de acción 2.2.1: Establecer una metodología común para la gestión de los riesgos cibernéticos, y sus lineamientos, así como los mecanismos de gobernabilidad, para la supervisión, evaluación y medición periódica de implementación y cumplimiento de las políticas de tecnologías de información, los planes de riesgos y de continuidad operativa, en conformidad con las mejores prácticas, y alineada a los estándares y metodologías internacionales para las infraestructuras criticas nacionales y de las instituciones del Estado, y promover su adopción en el sector privado.

Línea de acción 2.2.2: Establecer los criterios que determinan el grado de criticidad de una infraestructura, basado en los estándares internacionales en la materia.

Línea de acción 2.2.3: Catalogar las infraestructuras críticas nacionales e infraestructuras tecnologías de la información (TI) relevantes del Estado de acuerdo con los criterios que determinan su grado de criticidad, incluyendo los servicios colaterales que las soportan.

Línea de acción 2.2.4: Efectuar análisis de riesgo sobre las infraestructuras críticas nacionales e infraestructuras tecnologías de la información (TI) relevantes del Estado y determinar su nivel de vulnerabilidad, contemplando la inclusión de los perfiles de riesgos sectoriales más críticos para la sociedad y la economía nacional.

Objetivo específico 2.3 Elaborar los reglamentos, normas, estándares y lineamientos para el fortalecimiento de la coordinación y respuesta a incidentes de ciberseguridad en las infraestructuras críticas nacionales y de tecnologías de la información (TI) del Estado.

Línea de acción 2.3.1: Evaluar las normas y reglamentaciones emitidas por reguladores sectoriales para someter propuestas de actualizaciones a estos órganos, atendiendo a estándares internacionales.

Línea de acción 2.3.2: Apoyar la elaboración y el establecimiento de reglamentos sectoriales y en el diseño del modelo de gobernanza del sector.

Línea de acción 2.3.3: Elaborar y establecer los protocolos de intercambio de información entre los Equipos Sectoriales de Respuestas a Incidentes Cibernéticos (CSIRT), las instituciones del Estado, las infraestructuras críticas y el Equipo Nacional de Respuesta a Incidentes Cibernéticos (CSIRT-RD), para la gestión de los incidentes de ciberseguridad.

POR CUANTO (6): Que el OBJETIVO ESTRATÉGICO 3, establece: Educación y cultura. Promover y fortalecer la educación, sensibilización y cultura nacional de ciberseguridad.

Objetivo específico 3.1: Fomentar la inclusión de la formación y sensibilización en ciberseguridad en todos los niveles del sistema educativo.

Línea de acción 3.1.1: Establecer una política de desarrollo de competencias digitales en la población con énfasis en la ciberseguridad, contemplando programas de educación, formación técnica, sensibilización y concientización para lograr un ciberespacio más seguro.

Línea de acción 3.1.2: Fortalecer los programas de educación en ciberseguridad de las instituciones de educación superior y técnicos, en los diferentes niveles de grado, técnico, licenciatura, maestrías y doctorado, para aumentar la disponibilidad y calidad de las ofertas académicas y profesionales especializados.

Línea de acción 3.1.3: Incorporar contenidos básicos de ciberseguridad, en las asignaturas de tecnología de información de los programas de formación de las diferentes carreras, en las instituciones de educación superior y técnicos superior para fortalecer la concienciación y cultura de la ciberseguridad a nivel profesional.

Línea de acción 3.1.4: Incorporar en el programa de educación básica e intermedia, contenidos de ciberseguridad para fortalecer la sensibilización, concienciación y cultura de la ciberseguridad en los estudiantes y profesores de esos niveles.

Línea de acción 3.1.5: Diseñar un programa de cooperación para la implementación de formaciones especializadas en coordinación con las instituciones académicas.

Línea de acción 3.1.6: Implementar sistema de certificación emitida por institución acreditada para formación especializada en ciberseguridad.

Línea de acción 3.1.7: Diseñar e implementar programas de pasantías para fomentar nuevos talentos en materia de ciberseguridad con el apoyo y cooperación de las instituciones de educación intermedia, superior y técnicos profesional.

Línea de acción 3.1.8: Diseñar un programa de desarrollo de cibertalentos para apoyar la demanda de recursos especializados en el sector de la seguridad de la información.

Objetivo específico 3.2: Impulsar una cultura nacional de ciberseguridad en todo el país enfocada a las diferentes poblaciones vulnerables.

Línea de acción 3.2.1: Desarrollar un programa general de concientización para sensibilizar y fortalecer el entendimiento de ciberseguridad, conocer los riesgos, amenazas y forma de abordar los estos temas, para niños, adolescentes, adultos mayores, mipymes, el sector público y privado, entre otros.

Línea de acción 3.2.2: Desarrollar campañas de sensibilización, en medios tradicionales y digitales, con el apoyo del sector público, privado, la academia, organizaciones de medios y las organizaciones de la sociedad civil para fortalecer la cultura de ciberseguridad, promover la protección en línea de la información personal, y buenas prácticas en el uso de plataformas en línea y redes sociales.

Línea de acción 3.2.3: Implementar programas de reconocimiento para diversos sectores en apoyo a la cooperación en los esfuerzos de concientización y cultura de ciberseguridad a la población.

POR CUANTO (7): Que el OBJETIVO ESTRATÉGICO 4, establece: Alianzas públicas y privadas, nacionales e internacionales. Establecer alianzas nacionales e internacionales entre los sectores público y privado, sociedad civil y organismos e instituciones internacionales, para facilitar la cooperación técnica, operativa y de capacitación, así como generar los mecanismos que permitan una mejor articulación de las políticas exteriores relacionadas con la ciberseguridad.

Objetivo específico 4.1: Realizar alianzas nacionales e internacionales para fortalecer la cooperación.

Línea de acción 4.1.1: Establecer acuerdos marcos de cooperación técnica, operativa y de capacitación para el fortalecimiento de la ciberseguridad

Línea de acción 4.1.2: Fortalecer las alianzas con el sector privado, organizaciones de la sociedad civil y la academia para reafirmar la confianza ciudadana en la seguridad cibernética.

Línea de acción 4.1.3: Fomentar la relación con organismos e instituciones internacionales para facilitar la cooperación transfronteriza.

Línea de acción 4.1.4: Asegurar la participación de la República Dominicana en los foros internacionales.

Línea de acción 4.1.5: Monitorear y evaluar el nivel de cumplimiento país con los acuerdos y gobernanza del ciberespacio a nivel internacional.

POR CUANTO (8): Que el OBJETIVO ESTRATÉGICO 5, establece: Investigación y desarrollo. de la ciberseguridad y su entorno. Promover el análisis, la investigación y el desarrollo de la ciberseguridad y su entorno a nivel nacional e internacional.

Objetivo específico 5.1 Fomentar la investigación, el desarrollo y la innovación de la ciberseguridad y su entorno.

Línea de acción 5.1.1: Promover programas de emprendimientos e innovaciones en la industria de ciberseguridad.

Línea de acción 5.1.2: Incentivar el análisis y las investigaciones para el fortalecimiento y desarrollo de capacidades a nivel país.

Línea de acción 5.1.3: Desarrollar estudios, y promover la generación de estadísticas y creación de indicadores para apoyar en el desarrollo de políticas públicas, basadas en evidencias, vinculado al ecosistema de ciberseguridad.

Línea de acción 5.1.4: Realizar encuestas regionales o nacionales, análisis de datos, y evaluaciones para medir el impacto de la Estrategia Nacional de Ciberseguridad 2030 en diferentes sectores.

Línea de acción 5.1.5: Promover estudios de investigación en el desarrollo y adopción de nuevas tecnologías disruptivas y su impacto en la ciberseguridad.

POR CUANTO (9): Que la **ONDA** es la autoridad nacional competente responsable de cautelar y proteger administrativamente el derecho de autor y los derechos afines.

POR CUANTO (10): Que la base legal de la **ONDA** está contenida en las disposiciones establecidas en la ley 65-00, promulgada el 21 de agosto del año 2000 (G.O. Núm.10056, del 24 de agosto del 2000 y su reglamento de aplicación núm. 362-01, 14 de marzo del 2001 sobre Derecho de Autor (G.O. Núm.10076 del 14 de marzo del 2001).

POR CUANTO (11): Que en el artículo 21 de la Ley No. 1-12 de la Estrategia Nacional de Desarrollo 2030, del 25 de enero del año 2012, establece que se procura lograr el Objetivo General 1.1 "Administración Pública eficiente, transparente y orientada a resultados" y el Objetivo Específico de "Estructurar una administración pública eficiente que actúe con honestidad, transparencia y rendición de cuentas y se oriente a la obtención de resultados en beneficio de la sociedad y el desarrollo nacional y local".

POR CUANTO (12): Que la profesionalización de los recursos humanos de la Administración Pública, mediante el desarrollo de sus conocimientos y competencias, constituye la base para lograr mayores niveles de eficiencia y transparencia en el servicio público.

POR CUANTO (13): Que es interés del Estado Dominicano alcanzar la profesionalización y desarrollo de capacidades en todos los servidores públicos.

POR CUANTO (14): Que la Ley núm. 65-00, sobre Derecho de Autor, establece que la Oficina Nacional de Derecho de Autor es la autoridad nacional competente responsable de cautelar y proteger administrativamente el derecho de autor y los derechos afines, y posee autonomía técnica, funcional y administrativa para el ejercicio de las funciones asignadas a su cargo.

OSCAR MOQUETE CUEV ABOGADO NOTARIO PUBLICO MAT.: 3900

POR CUANTO (15): Tanto el **CENTRO NACIONAL DE CIBERSEGURIDAD (CNCS)** como la **OFICINA NACIONAL DE DERECHO DE AUTOR (ONDA)**, entienden que la cooperación técnica entre ambas instituciones constituye un elemento fundamental para promover la efectiva aplicación de sus respectivas legislaciones y normativas relacionadas.

POR CUANTO (16): En el marco de lo antes expuesto y teniendo como objetivo esencial la implementación de los objetivos estratégicos 2, 3, 4 y 5 de la Estrategia Nacional de Ciberseguridad, **LAS PARTES** han considerado oportuno proceder a la discusión, elaboración y suscripción del presente Acuerdo Interinstitucional, a los fines de establecer mecanismos permanentes de cooperación y colaboración interinstitucional, para impulsar y promover una cultura nacional de ciberseguridad que se fundamente en la protección efectiva del Estado dominicano, sus habitantes y en general, del desarrollo y la seguridad nacional y que derive en un ciberespacio más seguro, en el que puedan desarrollarse de manera confiable y permanente las actividades productivas y lúdicas de toda la población, acorde con la Misión y Visión de la Estrategia Nacional de Ciberseguridad.

POR TANTO, y en el entendido de que el preámbulo anterior forma parte integral del presente Acuerdo de Cooperación Interinstitucional, **LAS PARTES**, libre y voluntariamente,

HAN CONVENIDO Y PACTADO LO SIGUIENTE:

ARTÍCULO 1. OBJETO.

1.1 El presente Acuerdo tiene por objeto establecer un marco general de cooperación y colaboración interinstitucional entre **LAS PARTES,** con el objetivo de impulsar y promover desde sus respectivos ámbitos de competencia institucional, una cultura nacional de ciberseguridad que se fundamente en la protección efectiva del Estado dominicano, sus habitantes y en general, del desarrollo y la seguridad nacional y que derive en un ciberespacio más seguro, en el que puedan desarrollarse de manera confiable y permanente las actividades productivas y lúdicas de toda la población, acorde con la Misión y Visión de la Estrategia Nacional de Ciberseguridad y en particular, sus Objetivos Estratégicos 2, 3, 4 y 5.

ARTÍCULO 2. ALCANCE.

2.1 El presente Acuerdo comprende el establecimiento de los mecanismos de coordinación, interacción, cooperación y reciprocidad que faciliten la realización de actividades de interés y beneficio mutuo, orientadas a dar cumplimiento al objeto del presente Acuerdo y en

particular, a la implementación de los Objetivos Estratégicos 2, 3, 4 y 5 de la Estrategia Nacional de Ciberseguridad.

2.2 El presente Acuerdo no crea asociación, sociedad, consorcio, conjunto económico ("joint venture") o ninguna otra figura jurídica similar entre **LAS PARTES**, por lo que cada **PARTE** es la única responsable de los actos y obligaciones derivados de sus respectivas competencias. Por lo tanto, este Acuerdo no implica calidad de ninguna de **LAS PARTES** para representar a la otra **PARTE** en ningún contexto, ni otorga el derecho a una de **LAS PARTES** a comprometer a la otra **PARTE** ni incurrir en deudas u obligaciones en nombre de la otra **PARTE,** por ningún concepto relacionado o no con la ejecución de este Acuerdo.

2.3 El presente Acuerdo no establece vínculo alguno de exclusividad entre **LAS PARTES,** por lo que éstas podrán discutir con terceros, acuerdos no vinculados con este Acuerdo.

ARTÍCULO 3. ACTIVIDADES A DESARROLLAR.

3.1 **LAS PARTES** se comprometen a promover un esquema conjunto de actividades encaminadas a:

a.- Difundir el contenido de sus respectivas leyes y normativas reglamentarias;

a. Intercambiar políticas, experiencias, conocimientos, mejores prácticas, material bibliográfico y normativo, estadísticas y cualesquiera otros materiales o *know how* que resulten de mutuo interés;

b. Diseñar y ejecutar tareas tendentes a compartir recursos humanos y tecnológicos;

c. Movilizar sus recursos humanos y tecnológicos de acuerdo a la programación establecida y las tareas a desarrollar;

d. Celebrar conferencias, seminarios, talleres, cursos, programas de formación y otros encuentros académicos, que generen espacios para la discusión y el intercambio de experiencias y para la difusión de información a los ciudadanos, en materia de ciberseguridad y de uso responsable de las tecnologías de la información;

e. Ejecutar, de forma conjunta, proyectos de cooperación de interés mutuo, contemplando una posible integración de otras entidades del sector público y privado y de la sociedad civil; así como cualesquiera otras actividades propias de las respectivas

competencias institucionales de **LAS PARTES** y que estén enmarcadas en los propósitos del presente Acuerdo;

f. Colaboración en la transferencia e intercambio de conocimiento, información y experiencias para la implementación de proyectos de ciberseguridad, tanto a nivel estratégico como a nivel operativo o técnico en el ámbito de la Ciberseguridad;

g. Colaboración en acciones coordinadas, dirigidas a la sensibilización, concienciación, capacitación y formación en ciberseguridad.

3.2 Cada una de **LAS PARTES** se compromete a reconocer a la otra **PARTE** sus contribuciones para la ejecución de las iniciativas pactadas en el presente Acuerdo, en las publicaciones, informes, material informativo, mensajes, publicidad y cualquier otro medio de difusión de estas actividades.

3.3 El personal técnico de la **ONDA,** informará de inmediato al **CNCS**, a través del Equipo Nacional de Respuesta a Incidentes Cibernéticos (CSIRT-RD), sobre cualquier incidente generado en alguno de los sistemas de información relevantes, de los que pudiere tener conocimiento en el ejercicio de sus atribuciones, a los fines de que el **CNCS** pueda aplicar oportunamente los procedimientos establecidos en las leyes aplicables.

ARTÍCULO 4. INTERCAMBIO DE INFORMACIÓN.

4.1 Siempre y cuando la naturaleza de la información lo permita, **LAS PARTES** se comprometen a intercambiar información sobre eventos de amenazas de ciberseguridad y consultas sobre aspectos administrativos y/o técnicos que puedan ser de mutuo interés para lograr sus respectivos objetivos. No obstante, lo anterior, el intercambio de información a que se comprometen **LAS PARTES** se realizará sin menoscabo del carácter confidencial que pudiesen tener las informaciones de que se trata, según disponga la normativa aplicable a cada una de **LAS PARTES**.

4.2 **LAS PARTES** convienen expresamente que mantendrán la confidencialidad de toda información recibida de la otra **PARTE** durante la vigencia del presente Acuerdo y su posterioridad. No obstante, el tratamiento a ser dispensado a dicha información deberá estar conforme a las disposiciones de la Ley General de Libre Acceso a la Información Pública (y su Reglamento de Aplicación), así como a las obligaciones de secreto, reserva y confidencialidad establecidas en los artículos 19, 20, 21 y 22 del Decreto No. 230-18, de fecha 19 de junio de 2018.

4.3 Sin perjuicio de lo pactado en la sección 4.2 precedente, las informaciones que intercambien **LAS PARTES**, salvo dispensa especial otorgada por escrito por la **PARTE** que la divulga, estarán sujetas a las siguientes normas:

a. Serán tratadas de forma confidencial por la **PARTE** receptora y sólo podrán ser usadas para los propósitos de la ejecución del presente Acuerdo;

b. No serán reproducidas total ni parcialmente, excepto cuando fuere necesario para el uso antes autorizado, y sólo se harán del conocimiento de aquellos empleados y/o funcionarios que tuvieren necesidad de estar familiarizados con dichas informaciones;

c. La documentación o los medios que las sustenten serán devueltos junto con las copias que de ellas se hubieren hecho, cuando se tornaren innecesarias, o serán destruidas en presencia de los representantes designados a estos propósitos por cada **PARTE**, cuando hayan sido grabadas en aplicaciones de "software" u otros medios de la tecnología.

4.4 **LAS PARTES** declaran "información confidencial", entre otras, a todas aquellas informaciones que califiquen como excepciones a las denominadas informaciones de carácter público, así como todos los informes, estudios, análisis, planes, programas, especificaciones, diseños y otros documentos preparados por **LAS PARTES** durante la ejecución del presente Acuerdo y, en general, las informaciones vinculadas con las operaciones de cada una de **LAS PARTES.** Sin perjuicio de lo establecido en la normativa sobre libre acceso a la información pública

4.5 **LAS PARTES** se obligan a usar la información confidencial exclusivamente para los propósitos del presente Acuerdo, sin que pueda ninguna de ellas divulgar información confidencial, salvo que cuente con el consentimiento previo, expreso y escrito de la otra **PARTE,** otorgado por la máxima autoridad de dicha **PARTE.**

4.6 La recepción de la información confidencial propiedad de cualesquiera de **LAS PARTES** no puede considerarse como una licencia, cesión, mandato o agencia, para hacer usar o enajenar de alguna manera, dicha información o los servicios generados por el desarrollo o uso de los conceptos o ideas en ellos contenidos.

4.7 Si alguna persona física o moral, pública o privada, requiere información confidencial derivada de los términos de este Acuerdo y/o de las tareas y actividades ejecutadas en

virtud del presente Acuerdo, la **PARTE** a quien se solicite la información deberá comunicarlo inmediatamente a la otra **PARTE,** previo a divulgar la información de que se trate.

4.8 La violación por cualquiera de **LAS PARTES** a lo estipulado en el presente artículo, conllevará a la terminación automática del presente Acuerdo, sin perjuicio de otra acción que las leyes dominicanas pongan a disposición de la **PARTE** afectada.

ARTÍCULO 5. NATURALEZA DEL ACUERDO.

5.1 **LAS PARTES** convienen que, tratándose de un Acuerdo de Cooperación Interinstitucional, el mismo no supone ni implica transferencia de recursos económicos ni pago de contraprestación alguna entre **LAS PARTES.** En tal sentido, cada **PARTE** deberá sufragar los costos/gastos que se originen de su participación en el presente Acuerdo y la implementación de iniciativas y actividades derivadas del mismo. No obstante, **LAS PARTES** podrán acordar inversiones conjuntas para el desarrollo de alguna actividad, acto o iniciativa derivada de la ejecución del objeto de este Acuerdo, en cuyo caso **LAS PARTES** definirán de mutuo acuerdo, los recursos humanos, tecnológicos y financieros a ser aportados/cubiertos por cada **PARTE,** de acuerdo a su disponibilidad presupuestaria.

5.2 Cada una de **LAS PARTES** será exclusivamente responsable de las obligaciones que le pudiere corresponder como el empleador respecto de sus empleados con relación de dependencia, asociados, afiliados, agentes y consultores, en la ejecución del presente Acuerdo, incluyendo leyes de trabajo, seguro social, indemnizaciones por accidentes de trabajo o de carácter civil, y cualquier otra similar; en general, frente a cualquier otra ley, decreto o resolución de esta naturaleza.

5.3 El presente Acuerdo no establece entre **LAS PARTES** una relación de tipo laboral, por lo que expresamente, **EL CNCS** y la **ONDA,** se exoneran y liberan expresa y mutuamente frente a terceros, de toda acción, reclamación o demanda que pudiere ser intentada en su contra, sin importar que se trate en materia civil, laboral, administrativa, fiscal o de cualquier naturaleza, derivada del incumplimiento y ejecución del presente Acuerdo.

ARTÍCULO 6. MESA DE TRABAJO INTERINSTITUCIONAL.

6.1 Para el logro de los objetivos del presente Acuerdo y las coordinaciones que fueran necesarias para su seguimiento, monitoreo, supervisión y evaluación, **LAS PARTES** se

comprometen a mantener una Mesa de Trabajo Interinstitucional que estará integrada por cuatro (4) miembros: dos (2) de cada una de **LAS PARTES.**

6.2 La Mesa de Trabajo Interinstitucional deberá celebrar reuniones que podrán ser convocadas por cualquiera de los miembros y conforme a las necesidades que surjan de las actividades propias de cada una de **LAS PARTES.** De manera enunciativa y no limitativa esta Mesa de Trabajo Interinstitucional tendrá a su cargo:

a. Fortalecer los lazos de cooperación y coordinación de **LAS PARTES**, para impulsar los objetivos de este Acuerdo;

b. Definir los principios y crear los mecanismos y procedimientos que permitan la implantación y ejecución efectiva de las actividades a desarrollar en virtud del presente Acuerdo.

6.3 **LAS PARTES** podrán intercambiar experiencias y prácticas del personal propio de cada una, mediante el mecanismo de asignación provisional de recursos humanos a los proyectos que vayan a ser implementados de forma conjunta; sin que esta asignación provisional implique bajo ningún concepto, criterio o circunstancia una transferencia de personal conforme las previsiones de las normativas que regulan las actuaciones de las **PARTES.** El proceso de aplicación y formalización de la asignación provisional será coordinado entre las Direcciones de Gestión Humana de **LAS PARTES.**

ARTÍCULO 7. PROCEDIMIENTO DE EJECUCIÓN.

7.1 Para la ejecución del presente Acuerdo, **LAS PARTES** se comprometen a respetar los siguientes lineamientos:

a. Las más altas autoridades de cada una de **LAS PARTES,** o quien ellas designen en su representación, mantendrán contacto de manera constante y permanente, a fines de mantener el intercambio de ideas e iniciativas tendentes al cumplimiento de los objetivos dispuestos en el presente Acuerdo.

b. Luego de que se defina el plan de desarrollo de los objetivos del presente Acuerdo y aquellos otros surgidos de la Mesa de Trabajo Interinstitucional que sean cónsonos con el presente Acuerdo, la ejecución de acciones específicas se documentará mediante comunicaciones, las cuales deberán incluir, en cada caso, los detalles y requerimientos específicos del sub-proyecto de que se trata, sus objetivos, medios de acción, formas

PRESIDENCIA DE LA REPÚBLICA DOMINICANA
MINISTERIO DE LA PRESIDENCIA
Dirección Ejecutiva, Centro Nacional de Ciberseguridad

DR. OSCAR MOQUETE CUEVAS
ABOGADO NOTARIO PÚBLICO
MAT.: 2000
D.N. DISTRITO NACIONAL

ONDA

de participación, obligaciones específicas de **LAS PARTES,** actividades solicitadas (en caso de haberlas), contribuciones técnicas, financieras, de recursos humanos o tecnológicos, apoyo institucional y demás elementos que aseguren el normal y adecuado cumplimiento de lo pactado en cada caso.

c. Para los aspectos técnicos y administrativos vinculados a este Acuerdo, regirán las normas y procedimientos contables y financieros de cada **PARTE.**

ARTÍCULO 8. ENMIENDAS Y MODIFICACIONES.

8.1 El presente Acuerdo Marco de Cooperación Interinstitucional podrá enmendarse o modificarse por escrito y por mutuo acuerdo, cuando resulte necesario para la mejor realización de su objeto, siguiendo los mismos trámites establecidos para su suscripción.

ARTÍCULO 9. VIGENCIA.

9.1 El presente Acuerdo entrará en vigor en la fecha de su suscripción y se mantendrá en vigencia por un período indefinido, hasta que cualquiera de **LAS PARTES.** notifique a la otra **PARTE** su decisión de no proceder a su renovación.

9.2 El presente Acuerdo podría ser revisado a solicitud de cualquiera de **LAS PARTES**, vencido el plazo de tres (3) años, a partir de la firma de este.

9.3 Cualquiera de **LAS PARTES** podrá notificar a la otra **PARTE** la terminación del presente Acuerdo, en cualquier momento y sin responsabilidad, mediante comunicación por escrito dirigida a la máxima autoridad de la otra **PARTE,** con al menos treinta (30) días calendario de antelación a la fecha efectiva de terminación. No obstante, **LAS PARTES** de mutuo acuerdo podrán pactar todo cuanto fuere necesario para la culminación satisfactoria de las tareas y actividades que estuvieren en curso al momento en que la **PARTE** notificare la terminación de este Acuerdo.

ARTÍCULO 10. LEY APLICABLE Y SOLUCIÓN DE CONTROVERSIAS.

10.1 Para todos los efectos legales derivados del presente Acuerdo, **LAS PARTES** se someten expresamente a las leyes de la República Dominicana.

10.2 Cualquier discrepancia, problema de interpretación y/o controversia derivada de la ejecución o aplicación del presente Acuerdo se resolverá, en principio, por las discusiones y el mutuo acuerdo de **LAS PARTES** en respeto a las reglas de la buena fe y común intención, comprometiéndose cada **PARTE** a brindar sus mejores esfuerzos para lograr una solución armoniosa cualesquiera que fueran las circunstancias, en atención al espíritu de cooperación mutua que anima a la celebración del presente Acuerdo. En caso de que no fuere posible una solución amigable, luego de transcurrir un plazo de treinta (30) días calendario desde la fecha en que surgió la disputa entre **LAS PARTES,** dicha disputa será resuelta por ante la jurisdicción ordinaria.

ARTÍCULO 11. ELECCIÓN DE DOMICILIO Y NOTIFICACIONES.

11.1 Para los fines y consecuencias legales del presente Acuerdo, **LAS PARTES** hacen elección de domicilio en las direcciones mencionadas al inicio de este Acuerdo.

11.2 Las notificaciones y otras comunicaciones que deban ser hechas por cualquiera de **LAS PARTES** bajo este Acuerdo, deberán ser enviadas a las direcciones elegidas por cada **PARTE**.

ARTICULO 12. DISPOSICIONES DIVERSAS.

12.1 El presente Acuerdo es realizado y será ejecutado de buena fe, sin perjuicio o limitación alguna a cualquier convención legalmente pactada entre **LAS PARTES.** El hecho de que una de **LAS PARTES** no realice o ejecute una acción, no significará renuncia a la misma, sin importar el plazo que haya transcurrido.

12.2 La nulidad de cualquier disposición o cláusula de este Acuerdo no afectará la validez o exigibilidad de ninguna otra disposición o cláusula acordada bajo este Acuerdo, en el entendido de que en caso de que una cualquiera de las cláusulas de este Acuerdo fuese declarada nula por la jurisdicción competente a dichos fines, **LAS PARTES** acordarán de buena fe una nueva disposición que permita cumplir con el objeto de aquella cuya nulidad se hubiese declarado.

12.3 Ninguna de las disposiciones contenidas en este Acuerdo podrán ser interpretadas como una renuncia de **LAS PARTES,** a menos que así se estipule, de manera expresa y por escrito.

12.4 El significado e interpretación de los términos y condiciones del presente Acuerdo, se hará al amparo de las leyes de la República Dominicana.

12.5 El presente Acuerdo ha sido redactado en español, que es el idioma oficial de la República Dominicana, idioma control para todos los asuntos relacionados con el significado e interpretación de los términos y condiciones de este Acuerdo.

12.6 Los títulos que siguen al número de los artículos en el presente Acuerdo, sólo tienen un propósito ilustrativo y no servirán como base para interpretar el artículo completo, alterar o modificar el significado de los mismos.

12.7 Los derechos y obligaciones establecidas en el presente Acuerdo son considerados intransferibles, por lo que ninguna de **LAS PARTES** podrá ceder o traspasar ninguno de los derechos otorgados, sin el consentimiento previo, expreso y por escrito de la otra **PARTE,** manifestado por la máxima autoridad de dicha **PARTE.**

12.8 Todos los gastos en los que incurra cada **PARTE** en relación con la preparación del presente Acuerdo y la consumación de su objeto, correrán por cuenta de la **PARTE** que haya incurrido en tales gastos.

12.9 **LAS PARTES** representan y garantizan que:

a. Tienen el poder, autoridad y derecho legal total para asumir las obligaciones, ejecutar, entregar y cumplir con los términos y disposiciones de este Acuerdo;

b. Este Acuerdo constituye obligaciones legales válidas y exigibles a **LAS PARTES,** de conformidad con sus términos;

c. Son entidades debidamente organizadas y existentes de conformidad con las leyes de la República Dominicana.

ARTICULO 13. ESTIPULACIONES.

13.1 **LAS PARTES** aceptan todas las estipulaciones contenidas en el presente Acuerdo y para las no previstas, se remiten a las disposiciones vigentes en el derecho común de la República Dominicana.

HECHO Y FIRMADO en tres (3) originales de un mismo tenor y efecto, uno para cada una de **LAS PARTES** y uno para el Notario Público actuante, en la ciudad de Santo Domingo de Guzmán,

Distrito Nacional, Capital de la República Dominicana, a los treinta y uno (31) días del mes de agosto del año dos mil veintidós (2022).

POR EL CNCS:

JUAN GABRIEL GAUTREAUX MARTÍNEZ
Director Ejecutivo

POR LA ONDA:

JOSÉ RUBÉN GONELL COSME
Director

Yo, _____, Abogado, Notario Público de los del Número del Distrito Nacional, Miembro del Colegio Dominicano de Notarios, Inc., Matrícula núm._____, **CERTIFICO Y DOY FE**: que las firmas que anteceden en este documento de los señores **JUAN GABRIEL GAUTREAUX MARTÍNEZ** y **JOSÉ RUBÉN GONELL COSME,** de generales y calidades que constan y a quienes doy fe conocer, fueron puestas libre y voluntariamente en mi presencia por dichas personas, quienes me declaran bajo la fe del juramento que son esas las firmas que acostumbran a usar en todos los actos de su vida pública y privada. En la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los 31 (31) días del mes de Agosto del año dos mil veintidós (2022).

NOTARIO PÚBLICO