RESOLUCIÓN 01-2024

Que crea y conforma el Comité de Ciberseguridad de la Dirección General de Información y Defensa de los Afiliados a la Seguridad Social (DIDA)

La **DIRECCION GENERAL DE INFORMACION Y DEFENSA DE LOS AFILIADOS A LA SEGURIDAD SOCIAL (DIDA),** entidad pública autónoma y descentralizada, dotada de personalidad jurídica, a cargo de la provisión de información y gestión de reclamos y quejas de los afiliados a la seguridad social, mediante el artículo 5 de la Ley No. 13-20, de fecha 7 de febrero del 2020, que modifica el artículo 29 de la Ley No.87-01, del 9 de mayo de 2001, que crea el Sistema Dominicano de Seguridad Social; provisto(a) del Registro Nacional de Contribuyentes (RNC) **401515881**, con su domicilio social en Av. Tiradentes No. 33, Torre de la Seguridad Social, Ensanche Naco, Santo Domingo de Guzmán, Distrito Nacional, República Dominicana; debidamente representada de conformidad con el Decreto No. 477-20, de fecha 18 de septiembre del año 2020, por la Licenciada **CAROLINA SERRATA MENDEZ**, de nacionalidad dominicana, Licenciada en Derecho, mayor de edad, portadora de la cédula de identidad y electoral No. 001-1793256-6, domiciliada y residente en esta ciudad de Santo Domingo, Distrito Nacional, quien actúa en calidad de Directora General, de igual domicilio que la entidad, emite la siguiente resolución:

CONSIDERANDO: Que en los últimos treinta años, las tecnologías de la información y las comunicaciones (TIC) han estado en constante evolución y han revolucionado desde la forma en que trabajamos hasta la forma como nos relacionamos, y que de la misma manera en que el uso de las TIC se amplia cotidianamente de manera significativa, así también se multiplican los riesgos y peligros asociados a su uso, a medida que aparecen nuevos servicios basados en las TIC.

CONSIDERANDO: Que en el artículo 16 de la Ley núm. 1-12, que establece la Estrategia Nacional de Desarrollo 2030, del 25 de enero de 2012, relativo al uso de las tecnologías de la información y la comunicación (TIC), se establece que en el diseño y ejecución de los programas, proyectos y actividades en que se concretan las políticas públicas, se deberá promover el uso de las tecnologías de la información y comunicación como instrumento para mejorar la gestión pública y fomentar una cultura de transparencia y acceso a la información, mediante la eficientización de los procesos de provisión de servicios públicos y la facilitación del acceso a los mismos.

Av. Tiradentes no. 33, Torre de la Seguridad Social, Presidente Antonio Guzman Fernandez, Ensanche Naco, Santo Domingo, República Dominicana
(809) 472-7800 asistencia@dida.gob.do www.dida.gob.do

CONSIDERANDO: Que la Ciberseguridad constituye la garantía para que los Estados salvaguarden sus infraestructuras críticas y el derecho de sus habitantes de utilizar las tecnologías de la información y la comunicación (TIC) de manera segura y confiable, basándose en la colección de herramientas, dispositivos, normativas, regulaciones y mejores prácticas para proteger el ciberespacio, y los activos de los usuarios y organizaciones.

CONSIDERANDO: Que, en el marco de los actuales esfuerzos de modernización del Estado, y tomando en cuenta el período de vigencia de la actual Estrategia Nacional de Ciberseguridad, es oportuno actualizar esta, en consonancia con la tendencia internacional, para fortalecer las directrices y políticas públicas orientadas a detectar, mitigar y gestionar incidentes generados en los sistemas de información del Estado y en todas las infraestructuras críticas nacionales establece las líneas de acción a ser implementadas para mitigar el riesgo, minimizar el impacto de las amenazas cibernéticas en los sistemas de información y proteger las infraestructuras críticas para que la población utilice de manera confiada los servicios que se ofrecen a través de las tecnologías de la información y la comunicación (TIC).

CONSIDERANDO: Que el Estado dominicano necesita fortalecer la Ciberseguridad del sector público para robustecer los sistemas de información y para asegurar la confianza de la población en estos sistemas como una opción viable para el desarrollo económico, social y la seguridad nacional.

CONSIDERANDO: Que el Estado dominicano debe hacer frente a las amenazas cibernéticas fomentando el trabajo en conjunto y creando un ambiente de colaboración e intercambio de mejores prácticas de gestión y gobernanza en la Ciberseguridad.

CONSIDERANDO: Que el Centro Nacional de Ciberseguridad (CNCS), como dependencia del Ministerio de la Presidencia, es el encargado de velar por la seguridad cibernética de las infraestructuras de tecnologías de la información y comunicación de la Administración pública y de las infraestructuras críticas de la Republica Dominicana.

CONSIDERANDO: Que la alta incidencias de las telecomunicaciones y las tecnologías de la información y comunicación (TIC) en el desarrollo de las actividades económica, sociales y gubernamentales, hace imprescindible la adaptación de medidas que garanticen la protección de los activos críticos de información del Estado y la seguridad de la información por parte de las instituciones públicas.

Av. Tiradentes no. 33, Torre de la Seguridad Social. Presidente Antonio Guzman Fernández, Ensanche Naco, Santo Domingo, República Dominicana.
(809) 472 1900 info@dida.gov.do www.dida.gob.do

CONSIDERANDO: Que la Republica Dominicana cuenta con el Equipo Nacional de Respuesta a Incidentes Cibernéticos (CSIRT-RD), adscrito al Centro Nacional de Ciberseguridad (CNCS), que funge como el punto de contacto, a nivel nacional, para la prevención, detección y gestión de incidentes generados en los sistemas de información del Gobierno y en las infraestructuras criticas nacionales.

CONSIDERANDO: Que mediante el Decreto núm. 313-22, de fecha 14 de junio del año 2022, quedó establecido la Estrategia Nacional de Ciberseguridad 2030, con el objeto de fortalecer el marco nacional de Ciberseguridad, formando la concientización y creación de entornos digitales seguros, confiables y resilientes, que promuevan una sociedad digital dentro de un esquema de inclusión y respeto a los derechos fundamentales.

CONSIDERANDO: Que en fecha 09 de diciembre del año 2022, se firmó el Acuerdo de Cooperación Interinstitucional entre el Centro Nacional de Ciberseguridad (CNCS) y la Dirección General de Información y Defensa de la Seguridad Social (DIDA), con el objetivo de establecer un marco general de cooperación y colaboración interinstitucional e 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.

CONSIDERANDO: Que mediante Decreto 685-2022, de fecha 18 de noviembre de 2022, se establecieron los principios y lineamientos generales que servirían de base a los entes y órganos de la Administración pública para la adopción de controles, políticas y estándares para incrementar los niveles de madurez cibernética en el sector público, la notificación obligatoria de eventos e incidentes de Ciberseguridad, así como el intercambio de información sobre amenazas cibernéticas, conforme lo dispuesto en el Decreto núm. 313-22, del 14 de junio de 2022, que establece la Estrategia Nacional de Ciberseguridad 2030.

VISTA: La Constitución de la Republica Dominicana, proclamada el 13 de junio de 2015

VISTO: El Convenio sobre la Cibercriminalidad, suscrito en Budapest, en fecha 23 de noviembre de 2001, ratificado por el Congreso Nacional, mediante Resolución núm. 158-12, del 11 de junio de 2012.

VISTA: La Ley núm. 53-07, del 23 de abril de 2007, sobre Crímenes y Delitos de Alta Tecnología.

VISTA: La Ley núm. 1-12, del 25 de enero de 2012, que establece la Estrategia Nacional de Desarrollo 2030.

Av. Tiradentes no. 33, Torre de la Seguridad Social. Presidente Antonio Guzman Hernández. Ensanche Naco, Santo Domingo, República Dominicana.
(809) 472 1900 info@dida.gov.do www.dida.gob.do

VISTA: La Ley núm. 87-01, que rige el Sistema Dominicano de Seguridad Social (SDSS), promulgada en fecha 09 de mayo de 2001 y publicada en la Gaceta Oficial núm. 10086, de fecha 01 de agosto de 2001, que creó la Dirección de Información y Defensa de los Afiliados a la Seguridad Social (DIDA), modificada por la Ley núm. 13-20, que fortalece la Tesorería de la Seguridad Social (TSS) y la Dirección General de Información y Defensa del Afiliado (DIDA), promulgada en fecha 07 de febrero de 2020 y publicada en la Gaceta Oficial núm.10970.

VISTO: El Decreto núm. 189-07, del 3 de abril de 2007, sobre Directiva de Seguridad y Defensa Nacional.

VISTO: El Decreto núm. 230-18, del 19 de junio de 2018, que establece y regula la Estrategia Nacional de Ciberseguridad 2018-2021.

VISTA: El Decreto núm. 71-21, del 8 de febrero de 2021, que establece el Gabinete de Transformación Digital.

VISTO: El Decreto núm. 527-21, del 26 de agosto de 2021, que adopta la Agenda Digital 2030 de la Republica Dominicana.

VISTO: El Decreto núm. 313-22, del 14 de junio de 2022, que establece la Estrategias Nacional de Ciberseguridad 2030.

VISTO: El Decreto núm. 685-22, del 18 de noviembre de 2022, que establece los principios y lineamientos generales que servirán de base a los entes y órganos de la Administración Pública para la adopción de controles, políticas y estándares para incrementar los niveles de madurez cibernética en el sector público, la notificación obligatoria de eventos e incidentes de Ciberseguridad, así como el intercambio de información sobre amenaza cibernéticas, servicios, sistema de información e infraestructura tecnológicas para el funcionamiento de la Administración Pública.

POR TALES MOTIVOS, en uso de las atribuciones que le confiere la ley, dicta lo siguiente:

RESUELVE

ARTÍCULO PRIMERO: Se crea el Comité de Ciberseguridad de la Dirección General De Información y Defensa de los Afiliados a la Seguridad Social (DIDA), que tendrá como función principal, diseñar y ejecutar las políticas institucionales para orientar, detectar, mitigar y gestionar incidentes generados en los sistemas de información de la institución, y establecer las líneas de acción a ser implementadas para mitigar el riesgo, minimizar el impacto de las amenazas

Av. Tiradentes no. 33, Torre de la Seguridad Social. Presidente Antonio Guzman Fernandez, Ensanche Naco, Santo Domingo, República Dominicana.
(809) 472 1900 info@dida.gov.do www.dida.gob.do

cibernéticas en los sistemas de información y proteger las infraestructuras críticas, para que la población utilice de manera confiada los servicios que se ofrecen a través de las Tecnologías de la Información y la Comunicación (TIC).

ARTICULO SEGUNDO: Designa al equipo de servidores público la DIDA que conformará dicho comité, a saber:

- **Richard Arias**, Encargado de la Dirección de Tecnología de la Información y Comunicación, quien fungirá como coordinador o quien ocupe el cargo;
- **Violeta Matos Peñaló**, Encargada de la División de Operaciones de TIC, en calidad de miembro suplente del coordinador o quien ocupe el cargo;
- **Miledy Jardines**, Encargada de la Dirección de Financiera, en calidad de miembro o quien ocupe el cargo;
- **Marlen Berroa Martich**, Encargada de la Dirección Jurídica, en calidad de miembro o quien ocupe el cargo;
- **Xiomara De Coo**, Encargada de la Direccion de Planificación y Desarrollo, en calidad de miembro o quien ocupe este cargo.
- **Juan Beriguete**, Responsable de Acceso a la Información, en calidad de miembro o quien ocupe el cargo;
- **Daridys Muñoz**, Encargada de la Dirección de Recursos Humanos, en calidad de miembro o quien ocupe el cargo;

ARTÍCULO TERCERO: El Comité de Ciberseguridad de la Direccion General De Información y Defensa de los Afiliados a la Seguridad Social (DIDA), se encargará de lo siguiente:

a) **Adopción de normas, políticas y procedimientos.** Adoptar e implementar normas, políticas y procedimientos en materia de Ciberseguridad, alineados a las directivas, estándares y legislación sectorial, así como a la Norma General de Seguridad de la Información vigente y su normativa complementaria emitidas por la Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC), en los casos que aplique, conforme a su tamaño, naturaleza, complejidad, perfil de riesgo e importancia sistémica.

a) **Gestión de riesgos cibernéticos.** Tratar adecuadamente los riesgos cibernéticos en sus servicios, aplicaciones, sistemas de información e infraestructura tecnológica conforme las normas, estándares y políticas vigentes en la institución y en la Administración pública.

b) **Evaluación de riesgos.** Realizar anualmente una evaluación de riesgo de Ciberseguridad de su infraestructura tecnológica.

Av. Tiradentes no. 33, Torre de la Seguridad Social, Presidente Antonio Guzmán Fernández, Ensanche Naco, Santo Domingo, República Dominicana.
(809) 472 1900 info@dida.gov.do www.dida.gob.do

c) **Clasificación de los Incidentes de Ciberseguridad.** Agrupar los incidentes de seguridad cibemetica y de la infamación, conforme al nivel de criticidad e impacto.

d) **Gestión de incidentes.** Establecer un proceso de gestión de los incidentes de Ciberseguridad, con el fin de prevenir, identificar, responder, remediar, documentar y notificar de manera efectiva los eventos o cadena de eventos que vulneren dicha seguridad, procurando recuperarse del o los incidentes y minimizar su impacto en el menor plazo posible, contemplando el diseño de medidas contra ataques e incidentes cibernéticos, la aplicaci6n de correctivos de emergencia y la aplicación de protocolos e investigaciones forenses.

e) **Reporte obligatorio de incidentes.** Reportar los incidentes de Ciberseguridad que les afecten, siguiendo las políticas y procedimientos de gestión de incidentes de su institución al Centro Nacional de Ciberseguridad (CNCS), al ente u órgano regulador sectorial competente o al CSIRT sectorial correspondiente. Estos comunicaran el incidente dentro de las primeras 24 horas de haber sido detectado, acompañando toda la información necesaria para valorar su impacto, a fin de que se articulen desde el Equipo Nacional de Respuesta a Incidentes Cibernéticos (CSIRT-RD) o del CSIRT sectorial, según corresponda, todas las gestiones adecuadas y necesarias tendientes a lograr la solución del incidente declarado. Independientemente a que el evento haya sido subsanado o mitigado en la brevedad, este debe ser comunicado, con fines de alerta temprana a terceros o acciones de coordinación adicionales.

a) **Gestión de vulnerabilidades y amenazas cibernéticas.** Establecer un proceso de análisis, monitoreo y evaluación integral de las vulnerabilidades y amenazas tecnológicas a sus sistemas, infraestructuras y proceso tecnológicos para minimizar la materializaci6n de incidentes y eventos relacionados a la Ciberseguridad, contemplando aspectos para la actualizaciones de seguridad, la protección contra el *software* malicioso, el registro de eventos, el monitoreo continuo de los sistemas de información y la prevención y detección de intrusos.

b) **Notificación de violaciones a la seguridad de los datos.** En caso de existir datos que se encuentren comprometidos ante un incidente detectado, reportar este incidente al CSIRT-RD, así como también notificar esta situación a los individuos afectados, comunicando los hechos confirmados y las acciones tomadas o a tomar para su investigación o mitigación.

Av. Tiradentes no. 33, Torre de la Seguridad Social. Presidente Antonio Guzmán Fernández. Ensanche Naco, Santo Domingo, República Dominicana.
(809) 472 1900 info@dida.gov.do www.dida.gob.do

Sin embargo, mientras exista una investigación en curso, este comité no podrá publicar información sobre dicho incidente, salvo aquello coordinado con el Ministerio Publico, conforme a las guías y lineamientos que este establezca para informar de manera clara y certera, sin comprometer la investigación.

a) **Acción penal pública.** Poner en conocimiento inmediato del Ministerio Publico, aquellos incidentes de Ciberseguridad que pudieran constituir un hecho de relevancia penal pública conforme lo estipulado en la legislación de ciberdelito vigente.

ARTÍCULO CUARTO: Ordena la notificación de la presente resolución a servidores que fueron designados para conformar el Comité de Ciberseguridad de la Direccion General De Información y Defensa de los Afiliados a la Seguridad Social (DIDA), así como su publicidad en el portal institucional.

Dada y firmada en la ciudad de Santo Domingo, Distrito Nacional, Capital de la República Dominicana, a los veintiséis (26) días del mes de febrero del año dos mil veinticuatro (2024).

Aprobada por:

CAROLINA SERRATA MENDEZ
Directora General
Máxima Autoridad Ejecutiva (MAE)
Dirección General de Información y Defensa de los Afiliados a la Seguridad Social (DIDA)

Av. Tiradentes no. 33, Torre de la Seguridad Social, Presidente Antonio Guzmán Fernández, Ensanche Naco, Santo Domingo, República Dominicana.
(809) 472 1900 info@dida.gov.do www.dida.gob.do