NÚMERO: 685-22

CONSIDERANDO: Que mediante el Decreto núm. 313-22, del 14 de junio del año 2022, quedó establecida la Estrategia Nacional de Ciberseguridad 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. A su vez, dejó a cargo del Centro Nacional de Ciberseguridad (CNCS), a través de su Dirección Ejecutiva, la responsabilidad de monitorear y dar seguimiento al desarrollo e implementación de la Estrategia Nacional de Ciberseguridad 2030.

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 República Dominicana.

CONSIDERANDO: Que la alta incidencia de las telecomunicaciones y de las tecnologías de la información y comunicación (TIC) en el desarrollo de las actividades económicas, sociales y gubernamentales, hace imprescindible la adopción 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 y privadas y demás sectores que han incorporado el uso de las tecnologías de la información.

CONSIDERANDO: Que el uso de las tecnologías para el desarrollo y transformación de los procesos, y la optimización y mejora de todos los servicios públicos y privados, ha cambiado todo el escenario de retos y riesgos para la ciberseguridad, y que amenazas como el *ransomware* han generado gran impacto a nivel mundial, motivando iniciativas internacionales en la que la República Dominicana se ha unido como parte del esfuerzo de cooperación.

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 la República 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 críticas nacionales.

CONSIDERANDO: Que la cooperación entre los sectores público y privado es esencial para la ciberseguridad, dado que la mayor parte de los sistemas de información son propiedad u operados por el sector privado. A tal fin, es esencial fomentar el intercambio de información entre ellas, buenas prácticas y asesoramiento sobre aspectos relacionados con la ciberseguridad de los sistemas de información.

CONSIDERANDO: Que se hace imprescindible para el país contar con un mecanismo que contribuya a determinar cuáles sistemas de información cumplen los criterios para ser considerados infraestructuras críticas sobre los cuales se prestan servicios esenciales.

CONSIDERANDO: Que el artículo 5 de la Estrategia Nacional de Ciberseguridad 2030, al referirse al objetivo estratégico 1, sobre el Fortalecimiento de la capacidad institucional, indica que se deben fortalecerse 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. En tal virtud, se ordena al 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.

CONSIDERANDO: Que, asimismo, el citado artículo 5 señala que, en cuanto al objetivo estratégico 2, sobre protección y resiliencia de infraestructuras, el Estado dominicano deberá asegurar el continuo funcionamiento de las infraestructuras críticas nacionales y las infraestructuras de tecnologías de la información (TI) del Estado, lo que incluye la gestión de riesgos, identificar las infraestructuras críticas nacionales y las infraestructuras de tecnologías de la información (TI) relevantes del Estado, así como la elaboración de 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.

CONSIDERANDO: Que debido a la gravedad y peligro que algunos incidentes y amenazas cibernéticas representan para las infraestructuras críticas y, en consecuencia, a los intereses de la República Dominicana, es obligatorio diseñar un régimen sobre los estados de emergencia cibernética que prevean las medidas que se deben tomar a nivel nacional para salvaguardar la

ciberseguridad en caso de ocurran estos eventos, de conformidad con lo dispuesto por la Ley núm. 147-02, sobre Gestión de Riesgos y su reglamento de aplicación.

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

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

VISTO: 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 República Dominicana.

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

En ejercicio de las atribuciones que me confiere el artículo 128 de la Constitución de la República, dicto el siguiente

DECRETO:

Artículo 1. Objeto. El presente decreto tiene por objeto establecer 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 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.

Artículo 2. Alcance. El alcance de este decreto comprende los lineamientos generales para la notificación de incidentes que pudieran afectar la disponibilidad, confidencialidad e integridad de la información, las aplicaciones, servicios, sistemas de la información e infraestructura tecnológica para el funcionamiento de la Administración pública.

Artículo 3. Ámbito de aplicación. Las disposiciones del presente decreto serán aplicables a todos los entes y órganos que conforman la Administración pública, bajo la dependencia del Poder Ejecutivo, incluyendo los organismos desconcentrados, autónomos y descentralizados.

Párrafo. Los demás poderes del Estado y órganos constitucionales podrán acogerse, si así lo entendieran conveniente, al presente decreto y a las disposiciones del Centro Nacional de Ciberseguridad (CNCS) y de otros entes u órganos dependientes del Poder Ejecutivo con competencias en la materia.

Artículo 4. Definiciones:

a) **Activos de información.** Recursos utilizados por un sistema de seguridad de la información para que la organización funcione y consiga sus objetivos. Los mismos incluyen, pero no se limitan a los archivos de la institución, ya sea en formato electrónico, en papel o en otros medios, los sistemas *hardware* y *software*, equipos y redes en los que se almacenan, procesan, desarrollan o transmiten la información institucional, así como también el conocimiento específico acerca de estos activos.

b) **Amenaza.** Actividad, conocida o sospechosa que, de producirse, tendría o podría tener un efecto adverso sobre la ciberseguridad de una o más infraestructuras críticas o alguno de sus componentes, incluyendo sistemas informáticos complementarios o accesorios.

c) **Confidencialidad.** Propiedad o acceso a la información por parte únicamente de quienes estén autorizados.

d) **Disponibilidad.** Acceso a la información y sus sistemas de tratamiento por parte de los usuarios autorizados cuando lo requieran.

e) **Evento.** Cualquier hecho u ocurrencia observable en un sistema, red, o activo o dispositivo tecnológico.

f) **Indicadores de compromiso.** Informaciones relevantes que describen cualquier incidente de ciberseguridad, evento, actividad o artefacto malicioso, mediante el análisis de sus patrones de comportamiento.

g) **Incidente de ciberseguridad.** Todo evento que tenga o, inminentemente pueda tener, un efecto adverso sobre la ciberseguridad de una o más infraestructuras críticas, de alguno de sus componentes, de la información procesada, almacenada o transmitida por esta, o que constituye una violación o amenaza inminente de violación de las políticas o procedimientos de ciberseguridad vigentes o de las políticas de uso aceptable.

h) **Integridad.** Mantenimiento de la exactitud y completitud de la información y sus métodos de procesamiento.

i) **Servicio esencial.** Cualquier servicio o función que resulte ser necesario para salvaguardar la seguridad nacional, defensa, relaciones exteriores, economía, salud, seguridad u orden público de República Dominicana.

j) **Violación de la seguridad de los datos personales.** Todo atentado contra la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos.

k) **Vulnerabilidad.** Cualquier debilidad en un sistema de información, sus procedimientos de seguridad, su implementación o en sus controles internos, que podrían permitir la materialización de una amenaza.

Artículo 5. Adopción de normas, políticas y procedimientos. Los entes y órganos de la Administración pública deberán 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.

Párrafo. En el caso de las empresas que sean propiedad del Estado y que no pertenezcan a la Administración pública, aplicarán los reglamentos, regulaciones y normas dictadas por el órgano regulador o supervisor del sector económico al que estas pertenezcan.

Artículo 6. Gestión de riesgos cibernéticos. Los entes y órganos de la Administración pública deberán 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.

Artículo 7. Evaluación de riesgos. Los entes y órganos de la Administración pública deberán realizar anualmente una evaluación de riesgo de ciberseguridad de su infraestructura tecnológica.

Párrafo I. Las evaluaciones de riesgos tecnológicos deben llevarse a cabo a través de una metodología que contemple, entre otros aspectos, la identificación de las amenazas y vulnerabilidades tecnológicas, la probabilidad de ocurrencia y el posible impacto previsto a las operaciones para determinar el riesgo potencial. Además, deberán incluir la divulgación no

autorizada de información, la corrupción accidental o deliberada, la manipulación a la información y la disponibilidad de los ambientes en cualquier intervalo de tiempo.

Párrafo II. Los riesgos cibernéticos deben ser tratados de acuerdo con los requerimientos del ente u órgano y los lineamientos definidos en las normativas, estándares y políticas vigentes.

Artículo 8. Clasificación de los Incidentes de Ciberseguridad. Los incidentes de seguridad cibernética y de la información deberán agruparse correspondiente a su nivel de criticidad e impacto, conforme la siguiente clasificación:

a) **Nivel bajo.** Se utilizará cuando las consecuencias de un incidente cibernético de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio mínimo, o incluso nulo, sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados. Se entenderá por perjuicio bajo cuando se cumplan las siguientes circunstancias:

    1. Que no haya reducción de la capacidad del ente u órgano para atender eficazmente con sus obligaciones corrientes, las cuales se siguen desempeñando normalmente.

    2. Que no haya daño o con daño mínimo de activos del ente u órgano, así sean financieros, de información, de imagen u otra naturaleza.

    3. Que no haya perjuicio a individuos.

b) **Nivel medio.** Se utilizará cuando las consecuencias de un incidente cibernético de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio parcial sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados. Se entenderá por perjuicio medio cuando se cumplan las siguientes circunstancias:

    1. La reducción parcial a más de un 30 % de la capacidad del ente u órgano para atender eficazmente a sus obligaciones fundamentales, aunque sigan desempeñándose.

    2. El daño parcial de los activos del ente u órgano, así sean financieros, de información, de imagen u otra naturaleza.

    3. Daño reputacional comprobable.

    4. Causar un perjuicio moderado a algún individuo.

    5. Otros de naturaleza análoga.

c) Nivel alto. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad y supongan un perjuicio grave para los objetivos del ente u órgano, sus activos críticos o los individuos afectados. Se entenderá por perjuicio alto cuando se cumplan las siguientes circunstancias:

1. La anulación en más de un 70 % de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales.

2. Interrupción de la prestación del servicio superior a una hora.

3. El daño grave de los activos de la organización, sean financieros, de información, de imagen o de otra naturaleza.

4. Daños reputacionales muy elevados y cobertura en medios de comunicaciones internacionales.

5. Causar un perjuicio grave a individuos, de difícil o imposible reparación.

6. El incumplimiento de alguna ley o regulación.

d) Nivel crítico. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad y supongan un perjuicio muy grave o total para los objetivos de la organización, sus activos críticos o los individuos afectados. Se entenderá por perjuicio crítico cuando se cumplan las siguientes circunstancias:

1. La anulación en más de un 90 % de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales.

2. Los activos, sistemas o aplicaciones afectadas son utilizadas por más de un servicio esencial o institución del Estado.

3. Interrupción de la prestación del servicio superior a ocho horas.

4. El daño muy grave e, incluso, irreparable de los activos de la organización, sean financieros, de información, de imagen o de otra naturaleza.

5. Daños reputacionales muy elevados de la imagen del país y cobertura en medios de comunicaciones internacionales.

6. Afecta la seguridad nacional y ciudadana.

7. El incumplimiento de alguna ley o regulación sobre la materia.

Párrafo. Cuando un sistema maneje diferentes informaciones o preste diferentes servicios, el nivel de criticidad en cada dimensión será el mayor de los establecidos para cada información y cada servicio.

Artículo 9. Gestión de incidentes. Los entes y órganos de la Administración pública deberán 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 aplicación de correctivos de emergencia y la aplicación de protocolos e investigaciones forenses.

Artículo 10. Gestión de vulnerabilidades y amenazas cibernéticas. Los entes y órganos de la Administración pública deben establecer un proceso de análisis, monitoreo y evaluación integral de las vulnerabilidades y amenazas tecnológicas a sus sistemas, infraestructuras y procesos tecnológicos para minimizar la materialización 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.

Artículo 11. Divulgación responsable de vulnerabilidades. No se considerará que una persona infringió disposiciones legales sobre la confidencialidad, integridad y disponibilidad de datos y sistemas de información o que incurrió en un incumplimiento de leyes, reglamentos, contratos y códigos de conducta profesionales por el hecho de comunicar, publicar o divulgar vulnerabilidades, siempre que dicha divulgación se haga conforme los lineamientos definidos por el Centro Nacional de Ciberseguridad (CNCS).

Párrafo I. Con la finalidad de asegurar la buena fe de la persona que divulgue una vulnerabilidad, se deberá tomar en cuenta que:

a) No se haya solicitado recompensa bajo coerción o amenaza de publicación de la información.

b) No se otorgue un tiempo razonable para solucionar la vulnerabilidad antes de publicarla o divulgarla.

c) La persona que divulga una vulnerabilidad debe considerar el impacto de dicha divulgación y tener un cuidado razonable para minimizar el daño que pueda causarse por tal divulgación.

Párrafo II. Del proceso de identificación de vulnerabilidades basadas en la buena fe, quedan excluidos métodos que pudieran conducir a denegación de servicio, a pruebas físicas, utilización de código malicioso, ingeniería social y alteración, eliminación, exfiltración o destrucción de data.

Artículo 12. Reporte obligatorio de incidentes. Los entes y órganos de la Administración pública, inmediatamente y sin demora, deberán 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 comunicarán 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.

Párrafo I. Los responsables de seguridad de la información de los entes y órganos de la Administración pública deberán cuidar que las medidas de mitigación o control del incidente no comprometan la evidencia o la información relevante para la investigación inmediata o a futuro de este.

Párrafo II. El CSIRT-RD desarrollará, habilitará y dará a conocer las herramientas y plataformas necesarias para facilitar a los denunciantes los procesos de notificación, comunicación e información de incidentes.

Artículo 13. Reportes complementarios. Los entes y órganos de la Administración pública deberán, inmediatamente reciban la información, efectuar los reportes adicionales o complementarios que permitan al CSIRT-RD actualizar la información sobre el incidente, en caso de que se descubriera información adicional o diferente a la declarada inicialmente.

Artículo 14. Acciones para prevenir y gestionar incidentes de ciberseguridad. Cuando el Centro Nacional de Ciberseguridad haya recibido información sobre una amenaza o incidente de ciberseguridad, deberá informar al ente u órgano regulador sectorial competente o al CSIRT sectorial correspondiente para que, ejerciendo sus facultades, realice todas las acciones que sean necesarias para prevenir y gestionar la amenaza o incidente de ciberseguridad, procurando:

1. Evaluar el impacto o el potencial impacto de la amenaza o incidente de ciberseguridad.

2. Eliminar la amenaza de ciberseguridad o prevenir cualquier daño o daño adicional derivado del incidente de ciberseguridad.

3. Prevenir que un nuevo incidente de ciberseguridad que se derive de esa amenaza o incidente de ciberseguridad en otras organizaciones y sectores.

Párrafo. Igualmente, entes y órganos de la Administración pública deberán informar, inmediatamente, como mínimo, del estado en que se encuentren las acciones que hayan sido recomendadas por el Centro Nacional de Ciberseguridad (CNSC), hasta su resolución para un cierre apropiado.

Artículo 15. Punto de contacto único. Los entes y órganos de la Administración pública notificarán al Centro Nacional de Ciberseguridad (CNSC), al ente u órgano regulador sectorial competente o, si lo hubiese, al CSIRT sectorial, la designación de su oficial de seguridad o quien haga sus funciones, que servirá como punto de contacto único entre este y el CSIRT-RD y el CSIRT sectorial, según corresponda.

Artículo 16. Intercambio de información e inteligencia de amenazas. El CSIRT-RD deberá establecer los protocolos, mecanismos, interfaces y herramientas para facilitar el intercambio de información e inteligencia de amenazas cibernéticas, así como indicadores de compromiso a los entes y órganos de la Administración pública con el propósito de fortalecer los controles internos.

Artículo 17. Notificación de violaciones a la seguridad de los datos. En caso de existir datos que se encuentren comprometidos ante un incidente detectado, es obligación de los organismos y entidades del Estado 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.

Párrafo. El CSIRT-RD deberá facilitar los formatos y los mecanismos de notificación de incidentes y deberá proveer asistencia a las instituciones que así lo requieran.

Artículo 18. Protección de Sistemas Críticos. . El Centro Nacional de Ciberseguridad (CNCS), si lo estima necesario para prevenir, detectar o contrarrestar cualquier amenaza grave e inminente a la prestación de cualquier servicio esencial en la Administración pública, puede tomar las medidas que sean necesarias para la protección de un sistema de información con el acompañamiento de la entidad afectada. De manera enunciativa y no limitativa, las medidas podrán incluir:

a) Exigir que se le proporcione cualquier información, incluyendo información en tiempo real del evento, que sea necesaria para identificar, detectar o contrarrestar cualquier amenaza de este tipo.

b) Exigir que se le proporcione información relacionada con el diseño, configuración, operación o la ciberseguridad de cualquier sistema de información.

c) Requerir que se apliquen medidas como la eliminación de *software* malicioso de un sistema de información, la instalación de actualizaciones de *software* para hacer frente a las vulnerabilidades de ciberseguridad y desconectar temporalmente los sistemas de información infectados de una red.

Párrafo. En caso de que el sistema de información se vea en peligro inminente por una amenaza o incidente de ciberseguridad que puede dañarlo o destruirlo significativamente, el Centro Nacional de Ciberseguridad puede sugerir que se suspenda la utilización de este sistema o cualquiera de sus componentes hasta que se elimine la causa que lo amenaza.

Artículo 19. Atribuciones del Centro Nacional de Ciberseguridad (CNCS). En adición a las atribuciones que le son conferidas al Centro Nacional de Ciberseguridad (CNCS) por el Decreto núm. 230-18, de fecha 19 de junio de 2018, tendrá las siguientes atribuciones:

a) Coordinar la actuación de los distintos actores que inciden en el ciclo de vida de la gestión y respuesta a incidentes de ciberseguridad que pudiera afectar a la Administración pública.

b) Elaborar y difundir los protocolos, guías y pautas para la prevención, detección, notificación, respuesta y recuperación a incidentes de ciberseguridad.

c) Proveer información oportuna para la toma de decisiones rápidas ante cualquier amenaza cibernética que pudiera afectar a una determinada institución gubernamental.

d) Establecer los protocolos de comunicación, coordinación, intercambio de información y actuación entre el Equipo Nacional de Respuesta a Incidentes Cibernéticos (CSIRT-RD) y los equipos sectoriales ante la ocurrencia de incidentes de seguridad cibernética.

e) Proponer y recomendar medidas para la corrección y prevención futura de ataques cibernéticos.

Párrafo I. Dependiendo de la naturaleza del incidente, de la solicitud o cooperación de un actor involucrado en un incidente y los procedimientos establecidos, el Centro Nacional de Ciberseguridad (CNCS) podrá colaborar en la aplicación de acciones de contención inmediata, así como también en la investigación y análisis del sistema comprometido junto a los organismos de seguridad del Estado responsables de investigar los ciberdelitos descritos en la legislación aplicable.

Párrafo II. Los entes y órganos de la Administración pública serán responsables de la aplicación de las acciones y recomendaciones que derivan de la gestión de un incidente, siendo estas una atribución del equipo de seguridad cibernética de cada entidad y sus responsables designados para administrar el recurso comprometido o afectado, conforme los lineamientos definidos por el Centro Nacional de Ciberseguridad (CNCS).

Párrafo III. El Centro Nacional de Ciberseguridad (CNCS) podrá intervenir de forma inmediata en la respuesta a incidentes cuyo impacto pudiera representar un riesgo para el funcionamiento adecuado de la Administración pública, el funcionamiento de la infraestructura crítica nacional, o el desempeño de sectores económicos estratégicos, sin menoscabo de las funciones y atribuciones de los equipos internos de las instituciones, articulando las acciones necesarias para la resolución del incidente y la aplicación de medidas de recuperación.

Párrafo IV. El Equipo Nacional de Respuesta a Incidentes Cibernéticos (CSIRT-RD) deberá apoyar a los equipos sectoriales, en la gestión de incidentes significativos que pudieran comprometer la seguridad de dos o más sectores, el funcionamiento de la Administración pública o que pudiera afectar la seguridad nacional o cualquier otra situación que trascienda su comunidad atendida.

Artículo 20. Mecanismos de reporte de incidentes e intercambio de información de amenazas cibernéticas. El Centro Nacional de Ciberseguridad (CNCS), a través del CSIRT-RD, establecerá los lineamientos generales para el reporte de incidentes e información de amenazas cibernéticas por parte de los entes y órganos de la Administración pública.

Artículo 21. Acción penal pública. Los entes y órganos de la Administración pública deberán poner en conocimiento del Ministerio Público aquellos incidentes de ciberseguridad que pudieran constituir un hecho de relevancia penal pública conforme lo estipulado en la legislación de ciberdelito vigente de manera inmediata.

Párrafo I. El Centro Nacional de Ciberseguridad (CNCS) deberá proveer el debido acompañamiento al ente u órgano afectado por el incidente en el proceso de notificación al

Ministerio Público, el cual deberá mantener informado al Centro Nacional de Ciberseguridad (CNCS) en cada una de sus fases.

Párrafo II. Durante el proceso de gestión de incidentes cibernéticos de seguridad, el Centro Nacional de Ciberseguridad (CNCS), así como los entes y órganos involucrados en el incidente notificado, seguirán los lineamientos emitidos por el Ministerio Público para la preservación de la evidencia probatoria de contenido digital.

Artículo 22. Información al público. En caso de que la información al público sea necesaria debido a los intereses y derechos comprometidos y de acuerdo a la Ley núm. 200-04, de Libre Acceso a la Información Pública, toda publicación deberá ser coordinada previamente por el Centro Nacional de Ciberseguridad (CNCS).

Párrafo. Mientras exista una investigación en curso, los entes y órganos de la Administración pública involucrados, no podrán publicar información sobre los incidentes, salvo aquella coordinada con el Ministerio Público, conforme a las guías y lineamientos que este establezca para informar de manera clara y certera, sin comprometer la investigación. Los organismos y entidades del Estado no deberán realizar comunicados sobre incidente cibernético de seguridad sin que estos hayan sido confirmados por el responsable de seguridad de la información designado del ente u órgano que ha sido atacado o afectado, y éstos hayan sido notificados al Centro Nacional de Ciberseguridad (CNCS) conforme al presente decreto.

Artículo 23. Información a titulares de derechos afectados. En caso de que el incidente hubiera afectado derechos o libertades de terceros, los organismos y entidades del Estado deberán informar obligatoriamente a los titulares afectados dicho acontecimiento según lo establezcan las leyes vigentes y tratados suscritos, sin dilatación alguna, de manera clara y precisa, debiendo incluir como mínimo:

a) La naturaleza del incidente.

b) Los datos o servicios comprometidos.

c) Las acciones correctivas realizadas de forma inmediata.

d) Las recomendaciones a los afectados sobre las medidas que estos puedan adoptar para proteger sus intereses.

Párrafo. Esta obligatoriedad no será aplicable en caso de que hubiera evidencia suficiente y que el Centro Nacional de Ciberseguridad (CNCS) u otro organismo de seguridad del Estado

compruebe que el incidente cibernético constituye un hecho de interés de seguridad nacional, mientras hubiera una investigación en curso.

Artículo 24. Política de no divulgación de información sobre incidentes. El Centro Nacional de Ciberseguridad (CNCS), definirá una política de no divulgación detallada de información sobre incidentes, salvo en aquellos casos en los que estime necesario para evitar futuros incidentes similares, tomando como base información que ya haya sido de público conocimiento o que hubiera sido autorizada explícitamente por los afectados.

Párrafo. El Centro Nacional de Ciberseguridad (CNCS) podrá publicar información estadística, así como también información anonimizada sobre incidentes concretos, únicamente con fines de concienciación y capacitación en el sector público, sin revelar datos que permitan identificar a víctimas o divulgar detalles que pongan en riesgo a actores involucrados.

Artículo 25. Remisión del presente decreto. Envíese a las instituciones correspondientes, para su conocimiento y ejecución.

DADO en la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los dieciocho (18) días del mes de noviembre del año dos mil veintidós (2022); año 179 de la Independencia y 160 de la Restauración.

LUIS ABINADER