Nº 45061 -MICITT

EL PRESIDENTE DE LA REPÚBLICA

Y LA MINISTRA DE CIENCIA, INNOVACIÓN,

TECNOLOGÍA Y TELECOMUNICACIONES

Con fundamento en las atribuciones y facultades conferidas en los artículos 11, 24 párrafo segundo, 50 párrafo primero, 140 incisos 8), 18); y 146 de la "*Constitución Política de la República de Costa Rica*" del 7 de noviembre de 1949, publicada en la Colección de Leyes y Decretos del Año: 1949, Semestre; 2, Tomo: 2, Página 724. En el artículo 16 de la Ley N.° 5525 *"Ley de Planificación Nacional"* del 2 de mayo de 1974, publicada en la Colección de Leyes y Decretos Año: 1974, Semestre: 1, Tomo: 2; página 875. En los artículos 4, 11, 25 inciso 1), 27 inciso 1), 28 inciso 2 subincisos b) y j) de la Ley N.° 6227 *"Ley General de la Administración Pública"* del 2 de mayo de 1978, publicada en el Alcance N.° 90 al Diario Oficial La Gaceta N.° 102 del 30 de mayo de 1978. En los artículos 4, 5, 20 inciso e), y 21 de la Ley N.° 7169 *"Promoción Desarrollo Científico y Tecnológico y Creación del MICYT (Ministerio de Ciencia y Tecnología)"*, también denominada *''Ley de Promoción del Desarrollo Científico y Tecnológico"* del 26 de junio de 1990, publicada en el Alcance N.° 23 al Diario Oficial La Gaceta N.° 144 del 1 de agosto de 1990. En el artículo 3 de la Ley N.° 7668 *"Marco Transformación Institucional y Reforma Sociedades Laborales SAL"* del 9 de abril de 1997, publicada en el Diario Oficial La Gaceta N.° 84 del 5 de mayo de 1997. En el artículo 2 del Decreto Ejecutivo N.º 26893-MTSS-PLAN *"Reglamento a la Ley Marco de Transformación Institucional y Reformas a la Ley de Sociedades Anónimas Laborales"* del 6 de enero de 1998, publicado en el Diario Oficial La Gaceta N.° 88 del 8 de mayo de 1998. En el artículo 12 penúltimo párrafo del Decreto Ejecutivo N.° 37045-MP-MEIC *''Reglamento a la Ley de protección al Ciudadano del Exceso de Requisitos, y Trámites Administrativos''* del 22 de febrero de 2012, publicado en el Alcance N.° 36 al Diario Oficial La Gaceta N. º 60 del 23 de marzo de 2012. En los artículos 1, 2 inciso a), c), d) y e), 3, 7 inciso c) del Decreto Ejecutivo N.° 43580-MPPLAN *''Reglamento orgánico del Poder Ejecutivo"* del 1 de junio de 2022, publicado en el Alcance N.º 117 al Diario Oficial La Gaceta N.° 108 del 10 de junio de 2022; y los artículos 1 y 3 del Decreto Ejecutivo N.° 43864-PLAN *"Reglamento para el trámite y resolución de reorganización administrativa"* del 12 de enero de 2023, publicado en el Diario Oficial La Gaceta N.° 21 del 6 de febrero de 2023.

CONSIDERANDO:

I. Que el ordinal 24 párrafo segundo de la Constitución Política de la República de Costa Rica dispone; *"(.) Toda persona tiene el*

derecho fundamental al acceso a las telecomunicaciones, y tecnologías de la información y comunicaciones en todo el territorio nacional. El Estado garantizará, protegerá y preservará este derecho (...)".

II. Que el artículo 50 de la Constitución Política de la República de Costa Rica establece el deber del Estado de procurar el mayor bienestar a todos los habitantes del país.

III. Que la Ley n.° 6227 *"Ley General de la Administración Pública*" en su artículo 4°, señala: *"La actividad de los entes públicos deberá estar sujeta en su conjunto a los principios fundamentales del servicio público, para asegurar su continuidad, su eficiencia, su adaptación a todo cambio en el régimen legal o en la necesidad social que satisfacen y la igualdad en el trato de los destinatarios, usuarios o beneficiarios*."

IV. Que el artículo 4 de la Ley n.° 7169 "Ley de Promoción del Desarrollo Científico y Tecnológico" dispone el deber del Estado Costarricense de: *"(...) a) Velar por que la ciencia, la tecnología y la innovación estén al servicio de los costarricenses, les provea bienestar y les permita aumentar el conocimiento de sí mismos, de la naturaleza y de la sociedad (.) c) Proporcionar los instrumentos específicos para incentivar y estimular (...) la tecnología (...) como condiciones fundamentales del desarrollo económico, social y productivo y como elementos de la cultura universal. d) (...) orientar sobre la ejecución y el seguimiento de las políticas sobre (.) tecnología (...) i) Impulsar la incorporación selectiva de la tecnología moderna en la Administración Pública, a fin de agilizar y actualizar, permanentemente, los servicios públicos, en el marco de una reforma administrativa, para lograr la modernización del aparato estatal costarricense, en procura de mejores niveles de eficiencia (...)".*

V. Que de conformidad con lo dispuesto en el artículo 20 inciso e) de la Ley n.° 7169, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones es el órgano rector en materia de ciencia, innovación, tecnología y telecomunicaciones; y como tal, entre otras atribuciones le corresponde *"(.) e) Promover la creación y el mejoramiento de los instrumentos jurídicos y administrativos necesarios para el desarrollo científico, tecnológico y de la innovación del país (...)".*

VI. Que el artículo 21 de la Ley n.° 7169 *"Ley de Promoción del Desarrollo Científico y Tecnológico"* dispone que: *"Las competencias del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Micitt) serán ejercidas por su ministro, salvo que sean delegadas por él mismo o por disposición del reglamento, siempre que no sean las reservadas al Poder Ejecutivo, según la Constitución Política y los artículos 27 y 28 de la Ley 6227, Ley General de la Administración Pública, de 2 de mayo de 1978".*

VII. Que según lo establecido por el artículo 16 de la Ley n.° 5525 *"Ley de Planificación Nacional",* el Micitt al igual que otras instituciones deberá llevar a cabo una labor de mejora continua y sistemática, para modernizar su organización, procesos y procedimientos, con el fin de aumentar la eficiencia, eficacia, pertinencia, calidad, sostenibilidad y productividad de sus actividades y con el propósito de lograr el mejor cumplimiento de los objetivos que persigue el Sistema Nacional de Planificación.

VIII. Que de conformidad con el artículo 2 del Decreto Ejecutivo N.° 26893-MTSSPLAN *"Reglamento a la Ley Marco de Transformación Institucional y Reformas a la Ley de Sociedades Anónimas Laborales", " (.) La aprobación de la organización administrativa de órganos, entes y empresas públicas será competencia de Ministerio de Planificación Nacional y Política Económica (MIDEPLAN) (.) De previo a la aprobación por parte de MIDEPLAN y como requisito de validez, toda propuesta de reorganización de órganos, entes y empresas públicas deberá contar con la autorización del respectivo Ministro Rector del Sector al que pertenezca el órgano, ente o empresa (.)".*

IX. Que el *"Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR)"* fue creado mediante el Decreto Ejecutivo N.° 37052-MICIT del 9 de marzo del 2012, *"(...) con sede en las instalaciones del Ministerio de Ciencia y Tecnología, con facultades suficientes para coordinar con los poderes del Estado, instituciones autónomas, empresas y bancos del Estado todo lo relacionado con la materia de seguridad informática y cibernética y concretar el equipo de expertos en seguridad de las Tecnologías de la Información que trabajará para prevenir y responder ante los incidentes de seguridad cibernética e informática que afecten a las instituciones gubernamentales (...)".*

X. Que, en octubre del año 2020, las Unidades de Informática y de Análisis Prospectivo y Política Pública del Ministerio de Planificación Nacional y Política Económica (Mideplan), emitieron el documento denominado *"Ciberseguridad en el Sistema de Planificación Nacional", con el fin de "(...) plasmar la importancia que tiene la seguridad tecnológica en el Sistema Nacional de Planificación y, a su vez, ser una guía para entender el contexto al que nos enfrentamos y mostrar la hoja de ruta planteada por los entes gubernamentales rectores en materia de ciberseguridad para hacer frente a los retos tecnológicos del futuro mediante inversión y política pública".*

XI. Que en fecha 21 de abril de 2022, el Poder Ejecutivo emitió la Directriz N.° 133-MPMICITT "*Dirigida a la administración pública central y descentralizada sobre las mejoras en materia de ciberseguridad para el sector público del estado".*

XII. Que, el Micitt en el año 2022 emitió la *"Estrategia Nacional de Ciberseguridad de Costa Rica 2023-2027*", siendo su misión *"Establecer un marco de acción integral que permita prevenir y mitigar los riesgos y amenazas en el entorno digital, fomentar la innovación y el desarrollo de soluciones en ciberseguridad, fortalecer la capacidad de respuesta ante incidentes de ciberseguridad, promover una cultura de seguridad sólida, con el fin de ayudar a garantizar la estabilidad del país y su economía, proteger la información personal y crítica del Estado y de la ciudadanía, y mantener la confianza en el uso de los sistemas digitales (...)".*

XIII. Que la *"Estrategia de Transformación Digital 2023 - 2027"* emitida en el año 2022 por el Micitt, procura *"(.) que la transformación digital se asiente en una Gobernanza y Gobierno digital consolidados desde una gestión pública eficiente, que promueva una cultura basada en información segura, contribuyendo con la productividad, la competitividad y el desarrollo socioeconómico con sostenibilidad ambiental; apertura y participación ciudadana, promoviendo una digitalización inclusiva, solidaria, que involucra promoción y acceso universal a las telecomunicaciones, la habilitación del espectro radioeléctrico, la sostenibilidad de las ciudades y comunidades con calidad en los servicios, el desarrollo y uso significativo de tecnologías digitales y servicios emergentes en todos los sectores".*

XIV. Que mediante el oficio N.° MIDEPLAN-AME-URI-IT-0008-2024 del 16 de abril de 2024, emitido por la Unidad de Reforma Institucional del Área de Modernización del Estado del Ministerio de Planificación Nacional y Política Económica, fue recomendado: *". a) Aprobar la propuesta de reorganización administrativa parcial planteada por el MICITT, con excepción de la nomenclatura propuesta para la Dirección Nacional de Ciberseguridad, la cual se cambia por Dirección de Ciberseguridad".*

XV. Que según consta en el oficio MIDEPLAN-DVM-OF-0017-2024 del 17 de abril de 2024, emitido por el Sr. Marlon Navarro Álvarez, en su condición de viceministro del Ministerio de Planificación Nacional y Política Económica: *"(...) se aprueban las modificaciones planteadas por la institución (...); por lo tanto, la estructura organizacional del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones queda conformada de la siguiente manera: (...) Dirección de Ciberseguridad. Departamento Centro de Respuesta a Incidentes de Ciberseguridad. . Departamento Centro de Operaciones de Ciberseguridad (.)".*

XVI. Que mediante el informe técnico n.° MICITT-DC-INF-034-2025 del 24 de marzo de 2025, el señor Gezer Ramiro Molina Colomer, director de Ciberseguridad del Micitt - entre otras cosas - señaló: *". El presente informe tiene como finalidad justificar técnica y*

estratégicamente la necesidad de reformar, formalizar e implementar el marco normativo del CSIRT-CR, con base en los hallazgos de la auditoría, las mejores prácticas internacionales en ciberseguridad y las necesidades del ecosistema digital costarricense. A través de este análisis, se detallan las limitaciones actuales, el avance importante que ha realizado MICITT hoy en día, cumpliendo de forma operativa las etapas del ciclo de la ciberseguridad, se proponen soluciones concretas y se presentan las acciones necesarias para fortalecer la capacidad operativa y normativa del CSIRT-CR, garantizando su alineación con los estándares internacionales y con los objetivos estratégicos del país en materia de ciberseguridad (...)

Por otro lado, la reorganización del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), incluyendo la creación de la Dirección de Ciberseguridad, representa un avance sustancial en la postura de seguridad del país. Esta reestructuración permitió pasar de una respuesta limitada y reactiva hacia un enfoque integral, estratégico y proactivo, destacando la creación del SOC-CR para monitoreo constante y el reforzamiento del CSIRT-CR para una gestión eficaz de incidentes. Este cambio estratégico, sumado a la implementación de soluciones tecnológicas avanzadas como MDR y Protección DNS, ha fortalecido significativamente la resiliencia cibernética del Estado y la capacidad nacional para hacer frente a las amenazas actuales y futuras.

Finalmente, la adopción del marco NIST CSF 2.0 por parte del MICITT representa un alineamiento exitoso con estándares internacionales de ciberseguridad, lo que ha permitido avances importantes en los índices globales de seguridad digital. Es importante indicar que al día de hoy la Dirección de Ciberseguridad está de forma operativa junto con sus dos departamentos CSIRT-CR y SOC-CR gracias a la reorganización del MICITT, cumpliendo con las etapas del ciclo de la ciberseguridad propuesto por la Contraloría General de la República en su informe N° DFOESOSIF- 00014-2022, no obstante, se requiere reformar el marco normativo del CSIRT-CR establecido bajo el decreto Nº [Sic] 37052-MICIT permitirá fortalecer significativamente la gestión integral de la ciberseguridad nacional mediante la adopción del marco actualizado, incrementando la capacidad operativa . mejorando la coordinación interinstitucional y asegurando una respuesta más rápida y efectiva frente a incidentes cibernéticos, lo cual contribuirá directamente a la protección de infraestructuras críticas, reducción de riesgos y mejora en la resiliencia digital del país. La cooperación internacional (.) ha resultado fundamental para fortalecer las infraestructuras críticas del país. Las medidas de sensibilización y capacitación implementadas reflejan un compromiso con la creación de una cultura robusta de ciberseguridad en la sociedad, necesaria para mantener la resiliencia y sostenibilidad del ecosistema digital nacional ante futuros desafíos (...)".

XVII. Que, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, sometió la propuesta de "Reglamento para la Gobernanza en Ciberseguridad y la Resiliencia Cibernética de las

Instituciones Gubernamentales" a consulta pública no vinculante, el día 6 de mayo de 2025, mediante publicación en el sitio web institucional, apartado "Consultas Públicas", confiriendo un plazo de 10 días para la formulación de observaciones, iniciando el 2 de mayo de 2025, y finalizando el 15 de mayo de 2025.

XVIII. Que, de conformidad con los artículos 12 y 12 Bis del Decreto Ejecutivo n.° 37045- MP-MEIC *"Reglamento a la Ley de Protección al Ciudadano del Exceso de Requisitos y Trámites Administrativos",* y sus reformas, el Micitt procedió a llenar el Formulario de Evaluación Costo-Beneficio en la Sección I denominada Control Previo de Mejora Regulatoria, siendo que el mismo dio resultado negativo, y se determinó que esta regulación no contiene, no establece ni modifica trámites, requisitos, o procedimientos que el administrado deba cumplir ante la Administración Central, razón por la cual no se procede con el trámite de control previo.

POR TANTO:

DECRETAN:

Reglamento para la Gobernanza en Ciberseguridad y la Resiliencia Cibernética

de las Instituciones Gubernamentales y derogatoria del Decreto Ejecutivo N.°

37052-MICIT del 9 de marzo del 2012

Artículo 1º-. Objeto. El presente reglamento tiene por objeto establecer el marco de gobernanza en materia de ciberseguridad y definir las condiciones en las cuales debe gestionarse la resiliencia cibernética de la Administración Central, y colaborar con los demás Poderes del Estado y la Administración Descentralizada, con el fin de fortalecer integralmente la ciberseguridad nacional.

Ficha articulo

Artículo 2º-. Definiciones. Para efectos de aplicación de este reglamento se establecen las siguientes definiciones:

a) Resiliencia cibernética: es la capacidad de una organización para anticiparse, resistir, responder y recuperarse eficazmente de incidentes cibernéticos, asegurando la continuidad operativa y minimizando el impacto negativo sobre sus activos digitales y procesos críticos.

b) Gobernanza de ciberseguridad: es el conjunto de procesos, políticas, estructuras organizativas y mecanismos establecidos para dirigir, controlar y evaluar la gestión de la ciberseguridad dentro de una organización, con el propósito de proteger sus activos digitales, gestionar los riesgos cibernéticos, asegurar el cumplimiento normativo y apoyar los objetivos estratégicos institucionales.

c) Incidente de ciberseguridad: Cualquier suceso que afecte o tenga un impacto negativo o comprometa la confidencialidad, integridad y disponibilidad de los activos de información de las organizaciones. Ejemplos: ataques cibernéticos.

d) Vulnerabilidad de seguridad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos.

e) Evento de seguridad: Cualquier suceso u ocurrencia observable en un sistema, red o activo o dispositivo tecnológico.

Ficha articulo

Artículo 3º-. Atribuciones del rector en materia de ciberseguridad. De conformidad con lo dispuesto en el artículo 20 párrafo primero e incisos a) y e) de la Ley N.° 7169, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Micitt) es el órgano rector en materia de ciencia, innovación, tecnología y telecomunicaciones, y tiene la atribución de elaborar la política pública en materia de ciencia, tecnología e innovación, asegurar el debido cumplimiento y dar seguimiento a su ejecución, en el marco de coordinación del Sistema Nacional de Ciencia, Tecnología e Innovación; y promover la creación y el mejoramiento de los instrumentos jurídicos y administrativos necesarios para el desarrollo científico, tecnológico y de la innovación del país.

El Micitt en su condición de órgano rector y en observancia a las limitaciones que impone el ordenamiento jurídico, podrá coordinar con los Poderes del Estado, y la Administración Descentralizada, que gestionan sistemas de información o servicios tecnológicos esenciales, en temas de desarrollo e implementación de políticas públicas, marcos normativos, estándares técnicos y procedimientos de seguridad cibernética, conforme con los principios de gobernanza, responsabilidad compartida y mejora continua.

Ficha articulo

Artículo 4º-. Objetivo de la Dirección de Ciberseguridad del Micitt (DC). La DC tiene por objetivo fortalecer la resiliencia y seguridad de la infraestructura digital del país. Por tanto, es la dependencia designada por el Micitt para liderar y coordinar a nivel nacional, con los poderes del Estado, instituciones autónomas, empresas y bancos estatales, todo lo relacionado con la seguridad informática y cibernética.

En este contexto, es responsable de identificar, definir y establecer cuáles son las infraestructuras críticas de información del Estado, considerando su relevancia estratégica y la necesidad de asegurar la continuidad operativa ante posibles incidentes de ciberseguridad.

Ficha articulo

Artículo 5°-. Funciones de la Dirección de Ciberseguridad. Son funciones de la DC las siguientes:

1. Promover políticas y estrategias nacionales de ciberseguridad, estableciendo estándares y buenas prácticas para proteger la infraestructura digital del país.

2. Fungir como el punto central de coordinación en la respuesta a incidentes de ciberseguridad a nivel nacional, asegurando una respuesta rápida y efectiva a las amenazas.

3. Liderar iniciativas de capacitación y formación al público, empresas e instituciones gubernamentales sobre los riesgos de ciberseguridad y cómo mitigarlos.

4. Proporcionar asesoramiento y consultoría a otras organizaciones gubernamentales y otros sectores sobre cómo mejorar su postura de ciberseguridad.

5. Coordinar la evaluación de riesgos de ciberseguridad a nivel nacional y proponer medidas para mitigarlos.

6. Dirigir las acciones para el desarrollo de investigaciones sobre las amenazas cibernéticas actuales y emergentes.

7. Emitir criterio técnico y orientación basados en la evidencia sobre las amenazas cibernéticas.

8. Colaborar con agencias de ciberseguridad de otros países y organizaciones internacionales para compartir información sobre amenazas y mejores prácticas.

9. Realizar alianzas estratégicas para el fortalecimiento del ecosistema de seguridad cibernética.

10. Coordinar con el Comité Interamericano contra el terrorismo (CICTE), y otras entidades nacionales e internacionales sobre el diseño y aplicación de políticas, estrategias y lineamientos en la adquisición de bienes y servicios en materia de la seguridad de las tecnologías de la información y la comunicación, con los estándares que observen las normativas vigentes internacionales para la implementación y/o aplicación en el sector público.

11. Cualquier otra función que se le designe según el marco normativo de su competencia.

Ficha articulo

Artículo 6°-. Modelo de gestión aplicable en la DC en materia de ciberseguridad. El modelo de gestión de la DC en materia de ciberseguridad se fundamenta en estándares internacionales reconocidos, la gestión de riesgos y otras directrices adoptadas por organismos multilaterales en ciber resiliencia gubernamental. Dicho modelo incorpora, de manera integral y sistémica, las siguientes funciones esenciales del ciclo de ciberseguridad:

1. Gobernanza: establecimiento de políticas, roles, responsabilidades y mecanismos de supervisión.

2. Identificación: evaluación de activos críticos, amenazas, vulnerabilidades y riesgos.

3. Protección: implementación de controles, capacidades de defensa y cultura de seguridad.

4. Detección: monitoreo continuo y análisis proactivo de eventos de seguridad.

5. Respuesta: coordinación ágil ante incidentes para minimizar su impacto.

6. Recuperación: restablecimiento de funciones críticas, aprendizaje y mejora continua.

La DC deberá identificar, administrar y mitigar los riesgos asociados a sus funciones estratégicas y operativas, mediante planes de gestión de riesgos, continuidad operativa y controles compensatorios, dentro del ámbito de su competencia.

Asimismo, el Micitt promoverá que todas las instituciones que conforman la Administración Pública, y con las que mantenga relaciones de coordinación, adopten e implementen sus propios planes institucionales de gestión de riesgos cibernéticos y continuidad del servicio, siguiendo metodologías armonizadas, controles mínimos esenciales,

y herramientas homologadas. Estas acciones deberán estar alineadas con el marco rector establecido por el Micitt, mediante la DC; y estarán sujetas a auditoría técnica periódica.

Ficha articulo

Artículo 7°-. Estructura organizativa de la DC. Para el cumplimiento de sus fines, estratégicos, operativos y técnicos, la Dirección de Ciberseguridad del Micitt tendrá bajo su dependencia el Departamento Centro de Respuesta a Incidentes de Ciberseguridad (CSIRT-CR), y el Departamento Centro de Operaciones de Ciberseguridad (SOC-CR), cuyos objetivos y fines se detallarán.

El proceso de gestión administrativa y técnica del CSIRT-CR y del SOC-CR estará a cargo de la Dirección de Ciberseguridad del Micitt.

El funcionamiento, objetivos específicos, atribuciones internas y procedimientos de coordinación del CSIRT-CR y del SOC-CR serán definidos por la DC, y aprobados por la persona jerarca Institucional, en concordancia con los estándares internacionales vigentes.

Ficha articulo

Artículo 8°-. Objetivo y Funciones del Departamento Centro de Respuesta a Incidentes de Ciberseguridad. El CSIRT-CR tiene como objetivo responder a incidentes de seguridad cibernética que afecten a las instituciones de gobierno y operadores de infraestructura crítica; y sus funciones son las siguientes:

1. Ejecutar las acciones de respuesta ante incidentes cibernéticos que se presenten en las plataformas tecnológicas de las instituciones públicas.

2. Coordinar las acciones interinstitucionales e internacionales necesarias para la atención de incidentes y el fortalecimiento del ecosistema de seguridad digital del país.

3. Proporcionar orientación técnica al órgano correspondiente en el diseño de políticas, estrategias y acciones en materia de seguridad cibernética e informática, así como elaborar programas nacionales en materia de seguridad de tecnologías de la información y la comunicación.

4. Promover la implementación de políticas, planes, estrategias e iniciativas públicas y privadas en materia de ciberseguridad, así como lineamientos de seguridad cibernética orientados a lograr una mayor protección a las infraestructuras tecnológicas y la ciberseguridad de la persona ciudadana.

5. Proponer los lineamientos para la construcción de planes de contingencia, recuperación ante desastres y continuidad de negocio para las instituciones públicas.

6. Elaborar informes de incidentes para las diferentes instituciones gubernamentales cuando se requiera.

7. Realizar análisis de ciberinteligencia enfocados en la seguridad contra amenazas cibernéticas.

8. Realizar análisis forense post incidente para la identificación de la causa raíz del incidente y su remediación, así como brindar apoyo a las autoridades judiciales si es requerido.

9. Elaborar la normativa en materia de seguridad de las tecnologías de la información y la comunicación, que se requiera para el cumplimiento de las políticas públicas en la materia.

10. Asesorar, apoyar y coordinar a las múltiples partes interesadas para la adecuada gestión de los riesgos cibernéticos e incidentes digitales.

11. Asesorar y apoyar en la respuesta a incidentes de seguridad, lo que incluye la contención y erradicación de la amenaza, así como el acompañamiento en la recuperación de los sistemas afectados.

12. Generar notificaciones de alertas tempranas y emitir recomendaciones para la prevención de amenazas cibernéticas.

13. Cualquier otra función que se le designe según el marco normativo de su competencia.

Ficha articulo

Artículo 9°-. Objetivo y Funciones del Departamento Centro de Operaciones de Ciberseguridad. El SOC-CR tiene como objetivo, proteger y monitorear las infraestructuras críticas de las instituciones públicas definidas por Micitt; y sus funciones son las siguientes:

1. Realizar el monitoreo 24/7 de las redes y los sistemas de las instituciones incluidas en el SOC-CR con el objetivo de identificar y detectar amenazas y actividades sospechosas.

2. Proteger en tiempo real las plataformas tecnológicas de las instituciones públicas incluidas en el SOC-CR mediante las herramientas y soluciones de seguridad implementadas.

3. Elaborar informes periódicos de monitoreo y detección de amenazas.

4. Analizar los eventos de ciberseguridad para determinar su origen, impacto y la forma en que se está propagando.

5. Apoyar al CSIRT-CR proporcionando información detallada sobre amenazas detectadas e información relevante para la gestión de incidentes, además de aplicar medidas de seguridad para mitigar las amenazas cibernéticas.

6. Realizar análisis de vulnerabilidades en los sistemas de las instituciones públicas.

7. Velar porque las instituciones cumplan con los estándares y regulaciones de seguridad de la información relevantes propuestos por el Micitt.

8. Apoyar en la prevención, identificación, detección y análisis de posibles incidentes cibernéticos para apoyar en la respuesta a un incidente de ciberseguridad al CSIRTCR.

9. Asesorar en la aplicación de políticas de seguridad y mejores prácticas en las infraestructuras tecnológicas.

10. Definir, implementar y gestionar las soluciones de seguridad avanzada necesarias para el monitoreo, detección, respuesta y mitigación de ciberataques que afecten a las instituciones públicas y operadores de servicios esenciales del Estado.

11. Cualquier otra función que se le designe según el marco normativo de su competencia.

Ficha articulo

Artículo 10°-. De los recursos asignados a la DC. El Micitt, en la medida de sus posibilidades y en apego al ordenamiento jurídico, aportará los recursos humanos y financieros básicos para el funcionamiento de la Dirección de Ciberseguridad y sus departamentos CSIRT-CR y SOC-CR; para tal fin además podrá contar con el apoyo de cualquier otra institución; así como con recursos provenientes de la cooperación nacional e internacional.

Ficha articulo

Artículo 11°-. De las disposiciones técnicas, administrativas y jurídicas emitidas por el Micitt en materia de Ciberseguridad. Todos los lineamientos técnicos, protocolos, estándares, directrices, procedimientos operativos, manuales e instrumentos jurídicos y administrativos emitidos por el Micitt en materia de ciberseguridad, deberán estar disponibles, actualizados, completos y accesibles en el sitio web oficial del ministerio en la sección de Ciberseguridad.

Cada vez que se apruebe, modifique, sustituya o derogue alguno de estos instrumentos, el Micitt deberá emitir un comunicado dirigido al Sector Público, a través de los

canales oficiales de comunicación disponibles en la institución, informando lo correspondiente.

Ficha articulo

Artículo 12°-. De la obligatoriedad del marco del fortalecimiento de la resiliencia cibernética del Estado Costarricense. Se instruye a las personas jerarcas de la Administración Central cumplir con las siguientes obligaciones, en el marco del fortalecimiento de la resiliencia cibernética del Estado costarricense:

1. Adoptar e implementar medidas de gobernanza en ciberseguridad, que al menos considere la designación de responsables institucionales, la elaboración de políticas internas, planes de gestión de riesgos cibernéticos, continuidad operativa y recuperación ante incidentes, conforme a las directrices técnicas emitidas por el Micitt, a través de la Dirección de Ciberseguridad.

2. Aplicar los lineamientos técnicos, protocolos, estándares, procedimientos, instrumentos normativos y buenas prácticas que emita el Micitt en materia de ciberseguridad, asegurando su incorporación en los procesos institucionales de planificación, adquisiciones tecnológicas, desarrollo de sistemas, prestación de servicios digitales y gestión de datos.

3. Cumplir con las medidas técnicas emitidas por la Dirección de Ciberseguridad del MICITT, orientadas a mejorar las capacidades de prevención, detección, respuesta y recuperación ante ciberamenazas, así como los niveles de madurez en seguridad de la información.

4. Brindar de manera oportuna y veraz la información requerida por la Dirección de Ciberseguridad, cuando esté relacionada con la evaluación de riesgos, incidentes, capacidades tecnológicas, cumplimiento normativo u otros asuntos de interés público y estratégico en el ámbito de su competencia.

5. Reportar de forma obligatoria, dentro de un plazo máximo de veinticuatro (24) horas, cualquier incidente de ciberseguridad que comprometa, o pueda comprometer, la disponibilidad, integridad, confidencialidad o autenticidad de los sistemas tecnológicos, redes, plataformas digitales, servicios institucionales o datos bajo su custodia. Este reporte deberá realizarse ante el Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT-CR), conforme a los protocolos, formatos y canales establecidos por la DC.

6. Colaborar activamente con los procesos de respuesta y mitigación de incidentes, incluyendo la conformación de equipos técnicos institucionales o sectoriales especializados, según lo requiera la DC para la atención coordinada de eventos críticos que afecten la infraestructura pública digital.

7. Facilitar el acceso a personal técnico autorizado, a los entornos tecnológicos pertinentes, cuando así se requiera para la ejecución de medidas urgentes de contención o análisis técnico forense, siempre respetando el marco legal vigente en materia de protección de datos, derechos fundamentales y debida diligencia.

El cumplimiento de estas obligaciones permitirá fortalecer la capacidad nacional de prevención y respuesta ante incidentes cibernéticos, asegurar la protección de servicios públicos esenciales y mantener una postura de ciberseguridad moderna, interoperable y alineada con las mejores prácticas internacionales ante un entorno de amenazas dinámico y complejo.

Además, se insta a la Administración Descentralizada y demás Poderes del Estado, a implementar las disposiciones contenidas en este artículo.

Ficha articulo

Artículo 13°-. Declaratoria de interés público. Se declaran de interés público todas las acciones, proyectos institucionales orientados al fortalecimiento de la ciberseguridad, la resiliencia cibernética y la protección de la infraestructura digital del país, tanto en el ámbito público como privado.

En virtud de dicha declaratoria, las entidades públicas y privadas quedan autorizadas, para que, dentro de su disponibilidad presupuestaria y en observancia al marco legal respectivo, apoyen las labores que realice el Micitt en materia de ciberseguridad, a través de:

1. La participación en mesas técnicas, redes sectoriales, grupos de trabajo, ejercicios de simulación y espacios de coordinación operativa liderados por la Dirección de Ciberseguridad (DC).

2. El intercambio responsable de información técnica, gestión proactiva de amenazas, buenas prácticas y experiencias que fortalezcan el ecosistema nacional de ciberseguridad.

3. El desarrollo conjunto de investigaciones, tecnologías, mecanismos de detección temprana o herramientas de gestión de incidentes.

4. El apoyo logístico, técnico o financiero a programas de capacitación, campañas de concientización, fortalecimiento institucional o adquisición de infraestructura crítica, cuando ello sea posible conforme al marco jurídico aplicable.

5. Y todas las acciones de fortalecimiento de la ciberseguridad que el marco normativo permita.

Toda colaboración deberá garantizar el respeto a la soberanía nacional, la protección de datos personales, los derechos fundamentales, y los principios de legalidad, transparencia, proporcionalidad y responsabilidad institucional.

Ficha articulo

Artículo 14°-. De la comunicación de incidentes de ciberseguridad. Se instruye a las personas jerarcas de la Administración Central, a cumplir con las siguientes obligaciones:

1. Reportar de forma obligatoria al CSIRT-CR cualquier incidente de ciberseguridad que afecte o pueda afectar:

- La continuidad de los servicios institucionales.

- La disponibilidad, integridad o confidencialidad de los sistemas o datos.

- La seguridad de infraestructuras críticas o de servicios esenciales.

2. El reporte deberá realizarse:

- En un plazo no mayor a 24 horas desde la detección del incidente.

- A través del instrumento oficial que el CSIRT-CR habilite para este fin.

- Incluyendo al menos una descripción preliminar del evento, sistemas afectados, medidas adoptadas y datos de contacto técnico.

3. La DC podrá establecer niveles de criticidad y priorización para incidentes reportados, conforme a una clasificación estandarizada (crítico, alto, medio, bajo), mismas que se desarrollarán en los lineamientos técnicos).

4. Las instituciones deberán colaborar activamente en la investigación, contención y mitigación de los incidentes, siguiendo las instrucciones técnicas del CSIRT-CR.

Además, se insta a la Administración Descentralizada y demás Poderes del Estado, a implementar las disposiciones contenidas en este artículo.

Ficha articulo

Artículo 15°-. Evaluaciones de madurez y mejora continua: La Dirección de Ciberseguridad implementará un modelo de evaluación de madurez cibernética.

1. Esta evaluación incluirá al menos:

- Nivel de adopción de políticas y controles de ciberseguridad.

- Capacidades técnicas y humanas instaladas.

- Existencia de planes de continuidad, respuesta a incidentes y resiliencia operativa.

2. Los resultados permitirán clasificar a las instituciones en niveles de madurez (básico, intermedio, avanzado), y establecer prioridades de inversión, capacitación y asistencia técnica.

3. La participación y respuesta en el modelo nacional de madurez cibernética es de acatamiento obligatorio para la Administración Pública Central y de sus órganos con desconcentración mínima o máxima, y se recomienda a los entes de la Administración Pública Descentralizada, incluidas las empresas públicas del Estado su participación en la misma.

Ficha articulo

Artículo 16°-. Derogatorias. Se deroga el Decreto Ejecutivo N.° 37052-MICIT *"Crea Centro de Respuesta de Incidentes de Seguridad Informática CSIRT-CR"* del 9 de marzo de 2012, publicado en el Diario Oficial La Gaceta N.° 72 del 13 de abril de 2012".

Ficha articulo

Artículo 17°-. Rige a partir de la fecha de su publicación en el Diario Oficial *La Gaceta*.

Dado en la Presidencia de la República. -San José, a los 16 días del mes de junio del año dos mil veinticinco.

Ficha articulo

Ir al principio del documento