N° 44487-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, 50, 140 inciso 8 y 146 de la ***"Constitución Política de la República de Costa Rica"*** del 7 de noviembre de 1949; en los artículos 4, 11, 25 inciso l), 27 inciso l), 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 Diario Oficial *La Gaceta* N.° 102, Alcance N.° 90 del 30 de mayo de 1978; en los artículos 3 inciso b), 4 incisos a), c), d), i), 10, y 20 incisos a), c), e), j), 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 Diario Oficial *La Gaceta* N.° 144, Alcance N.° 23 del 1 de agosto de 1990; en el artículo 8° de la **Ley N.° 8292** *"Ley General de Control Interno"* del 31 de julio de 2002, publicada en el Diario Oficial *La Gaceta* N.° 169 del 4 de setiembre de 2002. En el artículo 12 del **Decreto Ejecutivo N.° 37045-MPMEIC** del 22 de febrero de 2012, publicado en el Alcance N.° 36 a *La Gaceta* N.° 60 del 23 de marzo de 2012. En los 1 y 2 del **Decreto N.° 43542-MP-MICITT** *"Declara estado de emergencia nacional en todo el sector público del Estado costarricense, debido a los cibercrímenes que han afectado la estructura de los sistemas de información*" del 8 de mayo de 2022, publicado en el Alcance N.° 94 a *La Gaceta* N.° 86 del 11 de mayo de 2022. En los artículos 2 incisos a), c), e); 3, 7 inciso c) del **Decreto N.° 43580-MP-PLAN** *"Reglamento orgánico del Poder Ejecutivo"* del 1 de junio de 2022, publicado en el Alcance N.° 117 a *La Gaceta* N.° 108 del 10 de junio de 2022. En la **Directriz N.° 133-MP-MICITT** *"Mejoras en materia de ciberseguridad para el sector público del Estado"* del 21 de abril de 2022, publicada en el Diario Oficial *La Gaceta* N.° 78 del 29 de abril de 2022.

Considerando:

I.-Que el ordinal 24 de la Constitución Política de la República de Costa Rica dispone, que *"(.) 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 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 la Ley N.° 7169 *"Ley de Promoción del Desarrollo Científico y Tecnológico"* en su artículo 3°, inciso b), establece que uno de los objetivos específicos para el desarrollo científico y tecnológico es: *"Apoyar la actividad científica, tecnológica y de innovación que realice cualquier entidad privada o pública, nacional o extranjera, que contribuya a la productividad, al intercambio científico y tecnológico con otros países, o que esté vinculada con los objetivos del desarrollo nacional. Asimismo, generar las políticas públicas que garanticen el derecho de los habitantes a obtener servicios de telecomunicaciones, así como asegurar la aplicación de los principios de universalidad y solidaridad del servicio de telecomunicaciones y fortalecer los mecanismos de universalidad y solidaridad de las telecomunicaciones, garantizando el acceso a los habitantes que lo requieran*".

V.-Que el artículo 4 de la ley N.° 7169 *"Ley de Promoción del Desarrollo Científico y Tecnológico"* impone al Estado Costarricense el deber 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 las investigaciones, la transferencia del conocimiento, la ciencia, la tecnología e innovación, 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 ciencia, 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 (...)".*

VI.-Que el artículo 10 de la ley N.° 7169 *"Ley de Promoción del Desarrollo Científico y Tecnológico"* establece: *"Por medio del Sistema Nacional de Ciencia, Tecnología e Innovación se pretende alcanzar la*

concertación de intereses de los órganos y entidades de los sectores mencionados y su colaboración, a efectos de lograr la coordinación nacional en materia de ciencia, tecnología e innovación para el desarrollo integral del país. Con ello se establecerán las directrices y las políticas que serán vinculantes para el sector público y orientadoras para el sector productivo y el sector académico, ambos nacionales e internacionales."

VII.-Que el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de conformidad con lo dispuesto en el artículo 20 de la Ley N.° 7169, es el órgano rector en materia de ciencia, innovación, tecnología y telecomunicaciones, y dentro de sus atribuciones le corresponde: *"(...) e) Promover la creación y el mejoramiento de los instrumentos jurídicos y administrativos necesarios para el desarrollo ... tecnológico ... del país".* Así como: *". j) Promover la democratización y apropiación de la ciencia, la tecnología y la innovación, en el marco de los derechos humanos que hagan del conocimiento un instrumento para el desarrollo de las comunidades del país (...)"*.

VIII.-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"*.

IX.-Que en el año 2022 se produjeron ataques cibernéticos que afectaron la estructura de los sistemas de información costarricense, y dadas sus consecuencias, el Poder Ejecutivo emitió el Decreto N.° 43542-MP-MICITT *"Declara estado de emergencia nacional en todo el sector público del Estado costarricense, debido a los cibercrímenes que han afectado la estructura de los sistemas de información"*, y dispuso en su artículo 4 que: *". De conformidad con los artículos 46 y 47 de la Ley Nacional de Prevención de Riesgos y Atención de Emergencias, la Administración Pública Centralizada, Administración Pública Descentralizada, empresas del Estado, municipalidades, así como cualquier otro ente u órgano público están autorizados para dar aportes, donaciones, transferencias al Fondo Nacional de Emergencias, así como prestar la ayuda y colaboración necesarias a la Presidencia de la República Costarricense, para cubrir los gastos que esta Emergencia Nacional haya y pueda provocar"*.

X.-Que en fecha 21 de abril de 2022 fue emitida la Directriz N.° 133-MP-MICITT *"Mejoras en materia de ciberseguridad para el sector público del Estado"*, en el que -entre otras cosas- se instruyó a la Administración Pública Central y se instó a la Administración Pública Descentralizada *"(.) a cumplir las recomendaciones y medidas técnicas que emanen del Ministerio de Ciencia, Innovación, Tecnología y*

Telecomunicaciones, por medio de la Dirección de Gobernanza Digital y el Centro de Respuesta de Incidentes de Seguridad Informática (en adelante CSIRT-CR), como ente coordinador de la ciberseguridad nacional, referentes a ciberseguridad y seguridad de la información, con el fin de mejorar las capacidades técnicas, de atención y de gestión de la ciberseguridad y seguridad de la información en las instituciones".

XI.-Que en el mes de marzo de 2023, como parte de las soluciones para mitigar los ciberataques sufridos en la República de Costa Rica, el Gobierno de los Estados Unidos de América, ofreció la donación del equivalente a veinticinco millones de dólares ($25.000.000.00), como *". apoyo financiero y técnico para el establecimiento de un Centro de Operaciones de Seguridad (SOC), como una plataforma que permita la supervisión y administración de la seguridad del sistema de información a través de herramientas de recogida, correlación de eventos e intervención remota; con el propósito de fortalecer las capacidades de ciberseguridad en las fases de detección, protección, respuesta y recuperación en las instituciones públicas..."*

XII.-Que el proyecto denominado *"Fortalecimiento de las capacidades en Ciberseguridad del País"*, referente al aporte ofrecido por el Gobierno de los Estados Unidos de América fue aprobado por el Ministerio de Planificación Nacional y Política Económica según consta en el oficio MIDEPLAN-ACI-OF-0132-2023 del 10 de agosto de 2023, conforme al Plan Nacional de Desarrollo y de Inversión Pública 2023-2026 (PNDIP 2023-2026), correspondiente al Sector de Ciencia, Tecnología, Innovación y Telecomunicaciones, en la intervención Pública número 4 de Promoción de la cultura para la ciberseguridad".

XIII.-Que según Informe Técnico N.° MICITT-DGDCFDDRII- INF-0099-2024 versión *2 "Informe técnico: LINEAMIENTOS PARA LA IMPLEMENTACIÓN DEL PROYECTO DE FORTALECIMIENTO DE LAS CAPACIDADES EN CIBERSEGURIDAD DEL PAÍS"*, emitido por el señor Gezer Ramiro Molina Colomer, director del Centro de Respuesta ante Incidentes del MICITT, en fecha 18 de marzo de 2024, se indica que:

"(...) Es fundamental destacar la importancia del proyecto que busca robustecer las capacidades de ciberseguridad en Costa Rica, así como adoptar medidas proactivas para proteger la infraestructura tecnológica y los datos sensibles de las instituciones públicas contra amenazas cibernéticas crecientes y evolutivas. La cooperación internacional, representada por el significativo apoyo financiero y técnico del Gobierno de los Estados Unidos, facilita la implementación de soluciones avanzadas de ciberseguridad, incluyendo la creación de un Centro de Operaciones de Seguridad (SOC), herramientas de detección y respuesta gestionadas (MDR), y el fortalecimiento del NSOC del MICITT. Este proyecto se alinea con los esfuerzos nacionales e internacionales para mejorar la postura de seguridad cibernética, abordando tanto la detección y prevención de incidentes cibernéticos como la respuesta y

recuperación ante estos. La donación y el apoyo técnico ofrecido por el Gobierno de los Estados Unidos constituyen un paso fundamental hacia el fortalecimiento de la resiliencia cibernética de Costa Rica, asegurando la protección de las infraestructuras críticas y servicios esenciales para la ciudadanía. Además, el enfoque en el desarrollo de capacidades y la formación de una fuerza laboral especializada el ciberseguridad refleja una inversión a largo plazo en la sostenibilidad y autodefensa del ecosistema digital nacional (...) el proyecto no solo busca mitigar los riesgos y vulnerabilidades actuales sino también preparar al país para enfrentar desafíos futuros en el ámbito de la ciberseguridad.

La colaboración intersectorial e internacional, junto con la implementación de tecnologías avanzadas y el desarrollo de competencias, son esenciales para garantizar un entorno digital seguro y resiliente. Este esfuerzo conjunto resalta la importancia de la ciberseguridad como un componente integral del desarrollo nacional, la seguridad pública y el bienestar económico y social de Costa Rica (.)".

XIV.-Que en fecha 13 de noviembre de 2023 fue presentada por parte del Gobierno de la República la ***"Estrategia Nacional de Ciberseguridad de Costa Rica 2023 - 2027"***, cuyo objetivo principal consiste en *"(...) 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; así como la concientización de los ciudadanos con el fin ayudar a garantizar la estabilidad del país y su economía, proteger la información personal y crítica del Estado y de los ciudadanos, y mantener la confianza en el uso de los sistemas digitales*

(...)".

XV.-Que el artículo 8° de la Ley N.° 8292 *"Ley General de Control Interno"* , dispone como parte de los objetivos de un sistema de control interno en la Administración Pública, el deber de proteger y conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal.

En línea con lo expuesto y, en observancia al ordenamiento jurídico vigente, las entidades y órganos sujetos a la fiscalización de la Contraloría General de la República deben de contar con un marco normativo que regule la distribución del apoyo financiero y técnico que se reciba.

XVI.-Que, de conformidad con el Reglamento a la Ley de Protección al Ciudadano del Exceso de Requisitos y Trámites Administrativos, Decreto Ejecutivo N° 37045-MPMEIC del 22 de febrero

de 2012 y sus reformas, se determinó que ni el presente Decreto Ejecutivo ni los lineamientos que oficializa, establecen ni modifican trámites, requisitos o procedimientos que el administrado deba cumplir, razón por la cual no se procede con el trámite de control previo, ni consulta pública. **Por tanto:**

Decretan:

OFICIALIZACIÓN DE LOS LINEAMIENTOS PARA

LA IMPLEMENTACIÓN DEL PROYECTO DE

FORTALECIMIENTO DE LAS CAPACIDADES

EN CIBERSEGURIDAD DEL PAÍS

Artículo 1°-**Oficialización.** Se oficializa el documento llamado *"Lineamientos para la implementación del proyecto de fortalecimiento de las capacidades en ciberseguridad del país"*, que corresponde a las disposiciones emitidas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones para recibir, asignar y distribuir los recursos donados por el Gobierno de los Estados Unidos de América, con el propósito de fortalecer las capacidades de ciberseguridad de las instituciones públicas en las fases de detección, protección, respuesta y recuperación.

(Nota de Sinalevi: Los Lineamientos para la implementación del proyecto de fortalecimiento de las capacidades en ciberseguridad del país, se extrajeron del sitio web del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones y se transcribe a continuación:)

DE

LINEAMIENTOS PARA LA IMPLEMENTACIÓN DEL PROYECTO DE FORTALECIMIENTO DE LAS CAPACIDADES EN CIBERSEGURIDAD PAÍS

Durante el mes de marzo de 2023, como parte de las soluciones para mitigar los ciberataques sufridos en Costa Rica durante el 2022, e! Gobierno de los Estados Unidos de America, ofreció la donación al Gobierno de Costa Rica del equivalente a veinticinco "millones de dólares ($25.000.000.00), como "apoyo financier y técnico para el establecimiento de un Centro de Operaciones de Seguridad (SOC), como una plataforma que permita la supervisión y administración de la

seguridad del sistema de información a traves de herramientas de recogida, correlación de eventos de intervención remota, con el con el propósito de fortalecer las capacidades de ciberseguridad en las fases de detección, protección, respuesta y recuperación en las instituciones públicas". El proyecto referente a dicho aporte fue aprobado por el Ministerio de Planificación y Política Económica según consta en oficio MIDEPLAN-ACI-OF-0132-2023 del 10 de agosto de 2023, para el Proyecto de "Fortalecimiento de las capacidades en Ciberseguridad del País", y conforme a: Plan Nacional de Desarrollo de Inversión Pública 22232026 [PNDIP 2023-2026), correspondiente a: Sector de Ciencia, Tecnología, Innovación y Telecomunicaciones, en la intervención Pública número 4 de Promoción de la cultura para la ciberseguridad"

En atención a la ejecución del Proyecto de referencia se emiten los siguientes lineamiertos que serán utilizados por todas las instituciones bajo la cobertura del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones como órgano rector en materia de Tecnología, telecomunicaciones y gobierno digital, mediante el Centro de Respuesta de Incidentes de Seguridad Informática (CSIRTCR), para efectos de implementación del proyecto derominado "Fortalecimiento de capacidades en Ciberseguridad del país" en el contexto del apoyo financiero y técnico brindado a la República de Costa Rica por parte de: Gobierno de Estados Unidos de a

1. Objetivo del instrumento. El objetivo de estos lineamientos es administrar, direccionar, y supervisar la ejecución de la implementacion de; proyecto de Fortalecimiento de las Capacidades en Ciberseguridad del País", en el contexto del apoyo financiero y técnico brindado a la Repúbica de Costa Rica por parte del Gobierno de los Estados Unidos de América.

2. Definiciones operativas y acrónimos. Se utilizar das definiciones operativas que se indican en este Lineamiento para la ejecución del Proyecto de fortalecimiento de capacidades en ciberseguridad del país.

a. Antispam: Se refiere a cualquier software, hardware o proceso que se utiliza para detectar y bloquear el correo no deseado, también conocido como spam. El antispam a menudo utiliza filtros y otras técnicas para identificar el spam basándose en características comunes.

b. **APT (Amenaza Persistente Avanzada):** Este es un ataque en el que un intruso autorizado gane acceso a una red y permanece allí sin ser detectado durante un período prolongado de tiempo. El propósito suele ser robar datos en lugar de causar daño a la red o a la organización.

c. **ATP (Advanced Threat Protection):** Es un tipo de seguridad diseñada para defender una red o sistema contra amenazas sofisticadas y avanzadas que los métodos tradicionales de protección pueden no ser capaces de detectar o prevenir. ATP puede incluir unoa variedad de técnicas, incluyendo el uso de inteligencia artificial apredizaje automático.

d. **CSIRT:** Centro de Respuesta de incidentes de Seguridad Informática CSIR--CR creado mediante el decreto ejecutivo n. ^{0} 37052-MICTT del 9/3/2012.

e. **DDos: (Ataque de Denegación de Servicio Distribuido**): Este tipo de ataque soorecarga un servidor o una red con tráfico de Internet, lo que hace que el sistema sea inaccesible para usuarios legítimos.

f. **DNS (Domain Name System:** Es el sistema que traduce los nombres de dominio en direcciones de internet (IP)

g. **EDR (Endpoint Detection and Response):** Este es un enfoque de seguridad de información que se centra en proteger los puntos finales de la red, como computadoras y teléfonos móviles. El EDR proporciona información sobre las amenazas de seguricad de puntos finales y permite respuestas rápicas para mitigarlas.

h. **ENC:** Estrategia Nacional de Ciberseguridad.

i. **Equipo:** hernmientas de seguridad avanzada ,hardware, software)

j. **Firewat: (Cortafeegos):** Es una barrera de seguridad que se utiliza para proteger una red interna o un sistema individual de amenazas que provienen de Internet o de otras redes externa, Funciona mediante el bloqueo o la limitación de ciertos tipos de tráfico de red.

k. **IDS (Sistema ae Detección de intrusos):** este es un dispositivo o aplicación que monitorea una red o sistemas para actividad maliciosa o violaciones de políticas.

l. **IPS (Sistema de Prevención de Intrusos):** Es una mejora del IDS que, además de detectar intrusos, también tiene la capacidad de bloquear o prevenir ataques.

m. **MDR: (Manage Detection and Respond por sus siglas en inglés)**: Gestión de detección y respuestas administrado.

n. **MICITT:** Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones.

o. NDR (Network Detectiot and Response): Es método para detectar y prevenir amenazas a la ciberseguridad a nivel de red. NDR utiliza análisi de ccmportamiento y técnicas avanzadas de inteligencia artificial para identificar actividad sospechosa o maliciosa.

p. **NSOC:** Centro de Operaciones de Seguridad Nacional.

q. **Phishing:** Es un método de ataque en el que se engaña a los usuarios para que revelen información personal, como contraseñas y números de tarjetas de crédito, haciéndose pasar por una entiaad legítima.

r. **Ransomware:** Es tipo ce malware que encripta los archivos del usuario y exige un rescate para desbloquearlos.

s. **SIEM (Gestión de Eventos e Información de Seguridad):** Combina la gestión de eventos de seguridad (SEM) y gestión de información de seguridad (SIM) en un solo sistema de seguridad.

t. **SOC (Centro de Operaciones de Seguridad):** Es un centro de comando centralizado donde se maneja la seguridad informática. Aquí donde se recopilan, se analizan y se responden las alertas de seguridad.

u. **SOCaaS:** Servicio de suscripción que proporciona funciones de opernciones de seguridad gestionadas y externalizadas, como monitoreo y respuesta amenazas cibernéticas, sin requerir infraestructura interna especializada.

v. **EE. UU / OSA/ US:** United State: America / Estados Unidos de América

w. **VPN (Red Privada VirtuaZ):** Es una tecnología que permite a los usuarios crear una conexión segura a a través de una red menos segura, como internet.

x. **SOC:** Centro de Operaciones de Seguridad Virtual.

y. **WAF (Web Application Firewall):** es tipo específico de cortafuegos que se centra en proteger aplicaciones web contra ataques como inyecciones de código SQL, ataques de scripting entre sitios [XSS) y ataques de falsificación de solicitudes entre sitios (CSRF).

z. **XDR (Extended Detection and Response):** Este término se refiere a una estrategia de seguridad que unifica múltiples productos de seguridad en una sola plataforma objetivo es proporcionar una visión mas complete y una respuesta más efectiva a las amenazas de seguridad.

3. Financiamiento de proyecto: El proyecto "Fortalecimiento de las Capacidades en Ciberseguridad del País" se realizará por medio de donacion del Gobierno de los Estados Unidos de América a favor del Gobierno de República de Costa Rica; que será ejecutada por medio de la Fundación Civil de Investigación y Desarrollo de Estados Unidos; por el equivalente a veinticinco millones de cólares ($ 25.000.000.00) para la adquisición de Equipo especializado en ciberseguridad implementación del Centro de Operaciones de Ciberseguridad como servicio temporal; el cual consiste en equipo de personas especializadas para monitorear, detectar, prevenir eventos de ciberseguridad en las redes informáticas, asi como attender incidentes de ciberseguridad que se puedan presentar en las instituciones públicas, así como para mantener una posición proactiva en el fortalecimiento de ciberseguridad en el sector público como una política integral.

4.Competencia de la gestión administrativa y técnica del CSIRT-CR. Con fundamento en lo dispnesto en el Artículo 4° del Decreto Ejecutivo N°' 37052-MICTT, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones tendrá la competencia para aprobar las donaciones de los bienes infomáticos a favor de las instituciones públicas seleccionadas pare la ejecucion del proyecto denominado "Fortalecimiento de las capacidades en Ciberseguridad del país"

El Centro de Respuesta a incidentes informáticos (CSIRT) será la instancia técnica del Micitt encargada de realizar el seguimiento y supervisión de la ejecución del proyecto, así como los resultados de los procesos de donación que sean "realizados por medio de la Proveeduría Institucional, en observancia al marco jurídico vigente y aplicable.

5. Selección de las instituciones que serán beneficiadas con el proyecto. Con el fin de que los bienes donados sean utlizados en prevención y lucha contra la ciberdelincuencia del Ministerio de Cencia, Innovación, Tecnología y Telecomuricaciones a través del CSIRT, será responsable de:

a. Definir las instituciones que serán beneficiarias. Tendrán prioridad aquellas instituciones que sean consideradas de infraestructura crítica de actividades sersibles nara la población, iniciando con los 18 ministerios pertenecientes a: Poder Ejecutivo.

b. organizar un equipo de trabajo tempora; con e: objetivo de diagnosticar el nivel de ciberseguridad de las instituciones públicas y recomendar la donación determinadas licencias de programas especializaaos en ciberseguridad capacitaciones a beneficiarios, equipos de cómputo, equipos periféricos y de

Vincular a instituciones beneficiaria con el centro de Operaciones de Ciberseguridad como servicio temporal el cual consiste. en un equipo de personas especializadas para monitorear, detectar, prevenir eventos de ciberseguridad en las redes informáticas, así como atender incicentes de ciberseguridad que se puedan presentar en las instituciones públicas, así como para mantener una posición proactive en e fortalecimie,to de ciberseguridad en la institucionalidad costarricense.

6. Parámetros pata ta definición de las instituciones beneficiarias Que el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones a través del CSIRT como instancia Institucioral competente, y en complemento a los diagnósticos y evaluaciones reatizadas, con el fin de proporcionar recursos de ciberseguridad y un servicio de Detección y Respuesta Gestionadas (MDR) para proteger su infraestructura tecnológica, utilizará siguientes parámetros para la definición de las instituciones beneficiarias:

a. Infraestructura Crítica o servicio esencial: Organizaciones que operan infraestructuras críticas. Ésto incluye sectores como energía, financiera, salud, transporte, servicios públicos y comunicaciones, Una vulneración en estos sistemas podría tener corsecuencias gaves para la seguridad nacional y el bienestar público.

b. Capacidad de Respuesta interna: Capacidad actual de ciberseguridad de la organización. Las que tienen capacidades

limitadas o recurso insuficientes para la gestión de riesgos ciber néticos deben ser priorizadas para fortalecer su postura de seguridad. Cuenta con SOC soluciones de seguridad .

c. Historial de Amenazas y Ataques: Historial de ciberataques y amenazas de las organizaciones. Aquellas cue han sido previamente atacadas o que están constantemente bajo amenaza pueden necesitar recursos adicionales para mejorar su defensa contra futuros ataques.

7. Conformación del grupo profesional institucional especializado. Las públicas que hayan sido previamente seleccionadas como beneficiarias por el CSIRT-CR del MICITT, deberán conformar un grupo institucional profesional especializado que atienda la temática de ciberseguridad quienes coordinaran con el CSIRT del MICITT, para facilitar en tiempo y forma los diagnósticos, debilidades, amenazas o falencias en materia de seguridad física y lógica, y toda la información requerida que facilitará la toma de decisión sobre los bienes digitales y servicios que se te donarán.

Dentro del equipo que se designe de la institución beneficiaria se deberá destacar una persona que funja como punto de contacto y coordinación entre la institución y el CSIRT del Micitt.

8. Coordinación del equipo de trabajo institucional. El Mictt mediante el CSIRT será la entidad encargada de con el equipo de trabajo interno de cada institución y el punto de contacto para efectos de instalación de equipos y programas de cómputo especializado en ciberseguridad, así como la capacitación en cuanto a su uso, instalación y martenimiento, incluyenao la entrega de manuales técnicos y de usuario.

9. Deberes de CSIRT. El MICITT mediante el CSIRT deberá:

Llevar un registro detallado de las instituciones beneficiarias de las donaciones y se conforme el expediente administrativo correspondiente para cada una de las institucioaes en el que se incluya:

a. Inventario de equipos donados, donde se inditará con claridad la cantidad de equipos, se han entregado, incluyendo;

i.Cantidad de Programas de cómputo software"

ii. Tipo de programa, marca comercial.

iii.Período de la ljcencia de uso, fecha de instaiación y fecha de caducidad; y para los equipos o "hardware"

iv. Marca de los equipos.

v.Modelo de los equipos.

vi.Número de serie.

vii. Reseña de la ubicación física dentro de la institución pública.

viii. Cualquier otro dato o característica necesaria que ayude a correcta identificación de bienes objeto de la donación, incluyendo también manuales técnicos 'y de usuario, así como las garantías del fabricante.

b. Cooçdinar lo pertinente para garantizar que se cumplen con los principios básicos de seguricad física y lógica en cuanto a accesos, niveles de seguridad de los equipos, protección de voltajes, etc., de acuerdo con las mejores prácticas y recomendaciones generalmente reconocidas

c. Llevará registro de las personas que han recibido capacitación, incluyendo al menos fechas de capacitación, tipo de capacitación, puesto, género.

d. Registro de brindados a las instituciones beneficiarias, que incluya al menos el tipo de servicios, periodo en que se brindó, infraestructuras cubiertas.

10. Recomendaciones de mantenimiento preventivo de los equipos y servicios brindados. El Micitt mediante el CSIRT deberá elaborar y entre las instituciones beneficiarias las recomendaciones de mantenimiento preventivo de los equipos y los servicios brindados, prohibiciones de uso, limitaciones de licencias de software, registros de los equipos o programas, cuando ello sea de carácter obligatorio, recomendación de fabricante, o del proveedor del servicio, o bien por exigirse así en la respectiva licencia de uso.

De igual forma la institución beneficiaria, en caso de mal funcionamiento de los equipos o servicios recibidos, o una deficiencia en el funcionamiento de estos, deberá ponerse en contacto de inmediato

con el CSIRT del Micitt para efectos de hacer cumplir las garantías o ofrecidas por el fabricante o el prestador de servicio, si aún estuviese en ese período de proteccion o ejecución.

Además, el Micitt a traves del CSIRT, tendrá la competencia para dar seguimiento a los procesos, implementaciór y avance de los alcances de esta cooperación y la aplicación de buenas prácticas en ciberseguridad para que los equipos donados puedan garantizar el cumplimiento de sus objetivos.

11. Recomendaciones sobre actualizaciones, lineamientos, mantenimiento protección de los equipos doñados. Corresponderá a cada institucion publica beneficiaria de este proyecto, desde la persona enlace y el equipo conformado conformado para éste fin, coordinar todas las acciones necesarias para el cumplimiento de las recomendaciones del CSIRT en cuanto a las actualizaciones, lineamientos, mantenimiento y protección de los equipos donados, el firmware de los equipos.

Será responsabilidad de cada uno de los entes públicos beneficiarios, la adquisición y mantenimiento de los servicios de protecciór. avanzada en ciberseguridad posterior al vencimiento de los equipos dañados o trasladados, de manera que se garantice servicios de protección que se adquieran presenten características de protección que sean, como mínimo, equivalentes o superiores a los implementados en el marco de este proyecto, con el fin de garantiza la integridad, disponibilidad y confidencialidad de la información y servicios tecnológicos.

Para efectos, las instituciones beneficiarias deberán prever en sus respectivos presupuestos a oartir del 2225 para ser ejecutado a partir del año 2026, y posteriores, los fondos necesarios para cubrir los rubros indicados. Con el fin de que instituciones garanticen la sostenibilidad de los servicios de seguridad en sus infraestructuras de forma permanente, sostenida y sin interrupciones.

12 Destino de las donaciones. Los equipos, que sean objeto de esta donación, pasarán formar parte del patrimonio de cada institución beneficiaria, por los que corresponderá a éstas incluirlas e identificarlas debidamente dentro de su acervo institucional, en observancia a lo dispuesto en el ordenamiento jurídico vigente, en materia de donación de bienes.

13. Distribución de las donaciones. Por tratarse de una donación en especie por parte del Gooierno de los Estaaos Unidos de América, no habrá adquisición monetaria ni concurso bienes y servicios por parte del Gobierno de Costa Rica o de sus instituciones para la adquisición de los

productos y programáticos, conforme lo señalado en el apartado 3 de estos lineamientos.

14. Formalización para el otorgamiento del beneficio. Para la formalización del beneficio de las instituciones que hagan parte del proyecto se utilizará la figura de "convenio interinstitucional" entre el Ministerio de Innovación, Ciencia, Tecnología y Telecomunicaciones y la respectiza institución beneficiada.

El fin de dichos convenios la transferencia mediante donación de equipos, programas de cómputo, periféricos, manuales técnicos x, de usuarios, que deberá incluir una descripción de los beneficios que recibirá la institución, incluyendo cualquier detalle importante de identificación a criter;o del CSIRT del Micitt.

Los convenios de cooperación interinstitucional deberar. ser firmados por las personas jerercas de las instituciores parte; (Micitt e institución beneficiaria), previo cumplimiento de las disposiciones normativas que regulan los procedimientos de donación establecidos en el ordenamiento jurídico para los efectos.

Emitido por:

Director de Ciberseguridad, CSIRT MIC'TT

Ficha articulo

Artículo 2°-**Aplicación obligatoria.** Estos lineamientos son de acatamiento obligatorio para todas las instituciones que en el marco del proyecto denominado ***"Fortalecimiento de las capacidades en Ciberseguridad del país"*** sean seleccionadas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones para ser beneficiarias de los recursos donados por el Gobierno de los Estados Unidos de América.

Ficha articulo

Artículo 3°-**Actualización de los lineamientos.** Corresponde al Micitt mantener actualizados los *"Lineamientos para la implementación del proyecto de fortalecimiento de las capacidades en ciberseguridad del país*", y garantizar su acceso directo en su sitio web institucional www.micitt.go.cr de manera permanente.

Ficha articulo

Artículo 4°-**Vigencia.** Rige a partir de su publicación en el Diario Oficial *La Gaceta*, y hasta la finalización formal del proyecto *"Fortalecimiento de las Capacidades en Ciberseguridad del País*".

Dado en la Presidencia de la República, San José, a los 02 días del mes de mayo de dos mil veinticuatro.

Ficha articulo

Fecha de generación: 7/1/2026 08:56:38