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

Durante el mes de marzo de 2023, como parte de las soluciones para mitigar los ciberataques sufridos en Costa Rica durante el 2022, el Gobierno de los Estados Unidos de América, ofreció la donación al Gobierno de Costa Rica 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..."* 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 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".

En atención a la ejecución del Proyecto de referencia se emiten los siguientes lineamientos 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 (CSIRT-CR), para efectos de implementación del proyecto denominado ***"Fortalecimiento de las capacidades en Ciberseguridad del país"*** en el contexto del apoyo financiero y técnico brindado a la República de Costa Rica por parte del Gobierno de los Estados Unidos de América.

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

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

2. **Definiciones operativas y acrónimos.** Se utilizan las definiciones operativas que se indican en este Lineamiento para la ejecución del Proyecto de fortalecimiento de las 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 no autorizado gana 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 una variedad de técnicas, incluyendo el uso de inteligencia artificial y aprendizaje automático.

d. **CSIRT:** Centro de Respuesta de incidentes de Seguridad Informática CSIRT-CR creado mediante el decreto ejecutivo n.° 37052-MICITT del 9/3/2012.

e. **DDoS: (Ataque de Denegación de Servicio Distribuido):** Este tipo de ataque sobrecarga un servidor o una red con tráfico de Internet, lo que hace que el sistema sea inaccesible para los 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 la 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 seguridad de los puntos finales y permite respuestas rápidas para mitigarlas.

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

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

j. **Firewall (Cortafuegos):** 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 externas. Funciona mediante el bloqueo o la limitación de ciertos tipos de tráfico de red.

k. **IDS (Sistema de 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 Detection and Response):** Es un método para detectar y prevenir amenazas a la ciberseguridad a nivel de red. NDR utiliza análisis de comportamiento 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 entidad legítima.

r. **Ransomware:** Es un tipo de 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 la 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 es donde se recopilan, se analizan y se responden las alertas de seguridad.

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

v. **EE. UU / USA/ US:** United States of America / Estados Unidos de América.

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

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

y. **WAF** (Web Application Firewall): Es un tipo específico de cortafuegos que se centra en proteger las 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. El objetivo es proporcionar una visión más completa y una respuesta más efectiva a las amenazas de seguridad.

3. Financiamiento del proyecto: El proyecto *"Fortalecimiento de las Capacidades en Ciberseguridad del País"* se realizará por medio de la donación del Gobierno de los Estados Unidos de América a favor del Gobierno de la 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 dólares ($ 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 un equipo de personas especializadas para monitorear, detectar, prevenir eventos de ciberseguridad en las redes informáticas, así como atender incidentes de ciberseguridad que se puedan presentar en las instituciones públicas, así como para mantener una posición proactiva en el fortalecimiento de la ciberseguridad en el sector público como una política integral.

4. Competencia de la gestión administrativa y técnica del CSIRT-CR. Con fundamento en lo dispuesto en el artículo 4° del Decreto Ejecutivo N.° 37052-MICITT, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones tendrá la competencia para aprobar las donaciones de los bienes informáticos a favor de las instituciones públicas seleccionadas para la ejecución 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 utilizados en la prevención y lucha contra la ciberdelincuencia el Ministerio

de Ciencia, Innovación, Tecnología y Telecomunicaciones a través del CSIRT, será responsable de:

a. Definir las instituciones que serán beneficiadas. Tendrán prioridad aquellas instituciones que sean consideradas de infraestructura crítica o de actividades sensibles para la población, iniciando con los 18 ministerios pertenecientes al Poder Ejecutivo.
b. Organizar un equipo de trabajo temporal con el objetivo de diagnosticar el nivel de ciberseguridad de las instituciones públicas y recomendar la donación de determinadas licencias de programas especializados en ciberseguridad, capacitaciones a beneficiarios, equipos de cómputo, equipos periféricos y de telecomunicaciones.

Vincular a las instituciones beneficiarias 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 incidentes de ciberseguridad que se puedan presentar en las instituciones públicas, así como para mantener una posición proactiva en el fortalecimiento de la ciberseguridad en la institucionalidad costarricense.

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

a. Infraestructura Crítica o servicio esencial: Organizaciones que operan infraestructuras críticas. Esto incluye sectores como energía, financiera, salud, transporte, servicios públicos y comunicaciones. Una vulneración en estos sistemas podría tener consecuencias graves 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 recursos insuficientes para la gestión de riesgos cibernéticos deben ser priorizadas para fortalecer su postura de seguridad. Cuentan con SOC y soluciones de seguridad.
c. Historial de Amenazas y Ataques: Historial de ciberataques y amenazas de las organizaciones. Aquellas que 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 instituciones públicas que hayan sido previamente seleccionadas como beneficiarias por el CSIRT-CR del MICITT, deberán conformar un grupo institucional profesional especializado interno que atienda la

temática de ciberseguridad quienes coordinarán 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 le 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 Micitt mediante el CSIRT será la entidad encargada de coordinar con el equipo de trabajo interno de cada institución y el punto de contacto para efectos de instalación de los equipos y programas de cómputo especializado en ciberseguridad, así como la capacitación en cuanto a su uso, instalación y mantenimiento, incluyendo la entrega de manuales técnicos y de usuario.

9. Deberes del 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 instituciones en el que se incluya:

a. Inventario de los equipos donados, donde se indicará con claridad la cantidad de equipos, que se han entregado, incluyendo;
   - **i.** Cantidad de Programas de cómputo o "software"
   - **ii.** Tipo de programa, marca comercial.
   - **iii.** Período de la licencia de uso, fecha de instalación 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 la correcta identificación de los bienes objeto de la donación, incluyendo también manuales técnicos y de usuario, así como las garantías del fabricante.

b. Coordinar lo pertinente para garantizar que se cumplen con los principios básicos de seguridad física y lógica en cuanto a accesos, niveles de confianza, 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 los servicios 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 los servicios brindados**. El Micitt mediante el CSIRT deberá elaborar y distribuir entre las instituciones beneficiarias las recomendaciones de mantenimiento preventivo de los equipos y los servicios brindados, prohibiciones de uso, limitaciones de las licencias de software, registros de los equipos o programas, cuando ello sea de carácter obligatorio, por recomendación del 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 con las garantías ofrecidas por el fabricante o el prestador de servicio, si aún estuviese en ese período de protección o ejecución.

Además, el Micitt a través del CSIRT, tendrá la competencia para dar seguimiento a los procesos, implementación 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 y protección de los equipos donados**. Corresponderá a cada institución pública beneficiaria de este proyecto, desde la persona enlace y el equipo conformado para este 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, incluyendo el firmware de los equipos.

Será responsabilidad de cada uno de los entes públicos beneficiarios, la adquisición y mantenimiento de los servicios de protección avanzada en ciberseguridad posterior al vencimiento de los equipos donados o trasladados, de manera que se garantice que los 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 garantizar la integridad, disponibilidad y confidencialidad de la información y servicios tecnológicos.

Para estos efectos, las instituciones beneficiarias deberán prever en sus respectivos presupuestos a partir del 2025 para ser ejecutado a partir del año 2026, y posteriores, los fondos necesarios para cubrir los rubros indicados. Con el fin de que las 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 a 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 Gobierno de los Estados Unidos de América, no habrá adquisición monetaria ni concurso de bienes y servicios por parte del Gobierno de Costa Rica o de sus instituciones para la adquisición de los productos informáticos 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 respectiva institución beneficiada.

El fin de dichos convenios será la transferencia mediante donación de equipos, programas de cómputo, periféricos, manuales técnicos y de usuarios, que deberán incluir una descripción detallada de los beneficios que recibirá la institución, incluyendo cualquier detalle importante de identificación a criterio del CSIRT del Micitt.

Los convenios de cooperación interinstitucional deberán ser firmados por las personas jerarcas de las instituciones 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:

Gezer Molina Colomer
Director de Ciberseguridad, CSIRT
MICITT