Generalidades

Objetivo:

El objetivo de la auditoría es determinar si la Gobernanza de Ciberseguridad del país bajo la rectoría del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), responde al marco normativo y prácticas aplicables, en procura del establecimiento de roles y trabajo conjunto para la adecuada gestión pública y continuidad de los servicios.

Por su parte, el objetivo del presente documento es reportar condiciones susceptibles de mejora por parte del MICITT y la Comisión Nacional de Prevención de Riesgos y Atención de Emergencias (CNE), en la atención de incidentes de ciberseguridad en el marco de la emergencia nacional establecida mediante el Decreto Ejecutivo n.° 43542-MP-MICITT.

Alcance y período:

Este reporte abarca la coordinación interinstitucional y la capacidad de detección de incidentes de ciberseguridad, en el período comprendido entre el 8 de mayo de 2022 (fecha de emisión del referido Decreto Ejecutivo) y el 31 de octubre de ese mismo año.

Este es el primer reporte de la auditoría en ejecución; como parte del proceso además se emitirá un informe final.

Marco Contextual:

De conformidad con la Ley Nacional de Emergencias y Prevención del Riesgo, n.° 8488, una emergencia declarada comprende un estado de necesidad y urgencia que obliga a tomar acciones inmediatas o de primera respuesta con el fin de salvar vidas y bienes, evitar el sufrimiento y atender las necesidades de los afectados.

Decretada la emergencia, se activa un régimen de excepción con el fin de agilizar la actividad administrativa y la disposición de fondos y bienes públicos, siempre y cuando estos sean indispensables para resolver imperiosas necesidades y se determine la existencia de un nexo de causalidad entre el suceso provocador del estado de emergencia y los daños provocados en efecto, sujeto a rendir cuentas a posteriori.

Para hacer frente a los ciberataques registrados a partir de abril de 2022, el Gobierno de la República declaró emergencia nacional, para lo cual emitió el precitado Decreto Ejecutivo n.° 43542-MP-MICTT, en el cual se otorga a la Presidencia de la República, la CNE y el MICITT la responsabilidad de planear, dirigir, controlar y coordinar los procesos necesarios para la contención y solución del ciberataque.

En este sentido, la CNE es la institución competente en materia de prevención de riesgos y preparativos para atender situaciones de emergencia, de conformidad con la Ley n.° 8488. Por su parte, el MICITT como ente rector en materia de ciberseguridad cuenta con la facultad de coordinación para prevenir y responder ante los incidentes de

seguridad cibernética e informática, a través del Centro de Respuesta de incidentes de Seguridad Informática (CSIRT-CR).

Para gestionar las acciones relacionadas con la emergencia nacional por ciberataques se emitió un Plan General de la Emergencia, el cual refiere a varias instituciones que por esa causa tuvieron afectaciones en la continuidad de los servicios públicos y la seguridad de la información. El detalle de estas instituciones se presenta en la figura siguiente.

Figura n.° 1
Instituciones públicas afectadas por los ciberataques incorporadas en el Plan General de la Emergencia

*Incorporado extemporáneamente mediante Acuerdo N° 178-10-2022, de la Sesión Ordinaria Nº 18-10-2022 de la Junta Directiva de la Comisión Nacional de Prevención de Riesgos y Atención de Emergencia del día 06 de octubre del 2022.

Fuente: Elaboración CGR, con base al Plan General de la Emergencia de Ciberataques del Decreto Ejecutivo n.°43542-MP-MICITT del 08 de mayo de 2022.

Relevancia: La gobernanza abarca la forma como surgen, operan y se dirigen las redes de coordinación entre los diferentes actores involucrados en la solución de problemas públicos; lo cual implica convocar, activar y emplear los recursos financieros, tecnológicos, humanos y organizativos requeridos para su abordaje.

En el contexto de emergencia nacional de ciberseguridad, se requiere de enfoques de gobernanza sustancialmente diferentes a los aplicables a las situaciones ordinarias, ya que predomina la necesidad de una intervención rápida y radical. Para esto, resulta relevante la consolidación de un modelo de gobernanza que permita dar respuesta a las

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

necesidades existentes durante la emergencia, así como, capitalizar el aprendizaje para realimentar la gestión con enfoque preventivo, a efecto de asegurar la continuidad del servicio público y la salvaguarda de la información.

Áreas de mejora identificadas

El Decreto Ejecutivo n.° 43542-MP-MICITT, originalmente emitido el 8 de mayo de 2022, fue reformado el 28 de julio de 2022 en los artículos 1, 3 y 5. Entre otros cambios, destaca que se migró de un marco de coordinación y mando totalmente concentrado en la Presidencia de la República, a uno que además integra a la CNE y el MICITT en la atención de la emergencia, lo cual es más congruente con lo estipulado en la Ley Nacional de Emergencias y Prevención del Riesgo, n.° 8488.

Además, en cuanto a la coordinación requerida para atender la emergencia nacional, la CNE en conjunto con MICITT recibieron reportes de daños, pérdidas y compromisos por parte de las instituciones afectadas, aprobaron el Plan General de la Emergencia y establecieron la Sala de Análisis de Situación Nacional (SASN) como el mecanismo oficial de coordinación de las operaciones de emergencia.

No obstante, es necesario informar al MICITT y la CNE sobre áreas de mejora relacionadas con el funcionamiento de la instancia de coordinación establecida para gestionar la emergencia nacional, así como las capacidades instaladas del CSIRT-CR para realizar procesos de detección de incidentes de ciberseguridad, todo lo cual se presenta seguidamente.

Oportunidad de mejora en la articulación para la gestión de incidentes de ciberseguridad en el marco de la emergencia nacional

Según se indicó líneas atrás, para la atención de la emergencia declarada mediante el Decreto Ejecutivo n.° 43542-MP-MICITT, se estableció la Sala de Análisis de Situación Nacional (SASN) como el mecanismo oficial de coordinación de las operaciones de emergencia, la cual, de conformidad con el Plan General de la Emergencia, surgió por iniciativa de la CNE y está conformada por ocho instituciones públicas[1]. El funcionamiento de la SASN es relevante, debido a que la emergencia por ciberataques se encuentra en proceso de manifestación, es decir, se mantiene la posibilidad de ocurrencia de nuevos incidentes de ciberseguridad.

Al respecto, se determinó que no se efectúa una coordinación oportuna en el seno de la SASN para responder de forma ágil en la atención de la emergencia nacional de ciberseguridad, de conformidad con los principios de estado de necesidad y urgencia, coordinación e integralidad del proceso de gestión.

En ese sentido, es preciso indicar que esta Sala se mantuvo inactiva desde el 01 de julio hasta el 31 de agosto del año en curso, y para los meses siguientes, la frecuencia en las sesiones de trabajo efectuadas han disminuido y no han presentado una periodicidad, aún cuando en ese lapso se

[1] La Sala de Análisis de Situación Nacional (SASN) se conforma por las siguientes instituciones: Caja Costarricense de Seguro Social (CCSS), Comisión Nacional de Emergencias (CNE), Dirección de Inteligencia y Seguridad Nacional (DIS), Instituto Costarricense de Electricidad (ICE), MICITT-CSIRT-CR, Organismo de investigación Judicial (OIJ), Ministerio Público y Ministerio de Hacienda.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

identificaron ataques de ciberseguridad en el Ministerio de Salud y en la Municipalidad de Belén (Ver figura n.° 2).

Figura n.° 2
Reuniones efectuadas por la Sala de Análisis y Situación Nacional y acontecimientos importantes de ciberseguridad entre mayo y octubre de 2022

Fuente: Elaboración CGR.

Adicionalmente, mediante el oficio n.° MICITT-DGD-OF-217-2022 del 19 de setiembre, la Dirección de Gobernanza del MICITT comunicó al Ministro de esa cartera su preocupación por la situación actual de ciberseguridad, así como el descontento de otras instituciones representadas en la SASN ante la ausencia de participación por parte de la CNE y la falta de claridad en los procesos para la atención de esta emergencia.

En relación con la normativa que regula las debilidades descritas anteriormente, la declaración de emergencia definida en la Ley n.° 8488, se fundamenta en un estado de necesidad y urgencia, que busca gestionar, por la vía de excepción, las acciones y la asignación de los recursos necesarios para atender la emergencia, de conformidad con el artículo 180 de la Constitución Política. En esta línea, el principio de estado de necesidad y urgencia, en conjunto con el de coordinación e integralidad del proceso de gestión, obligan a tomar acciones inmediatas con el fin de salvar bienes y atender las necesidades de los afectados, así como, confluir hacia un mismo fin las competencias diversas de diferentes actores a través de la autonomía e independencia de cada uno de ellos, pero, a la vez, direcciona en forma concertada y sistémica hacia propósitos comunes.

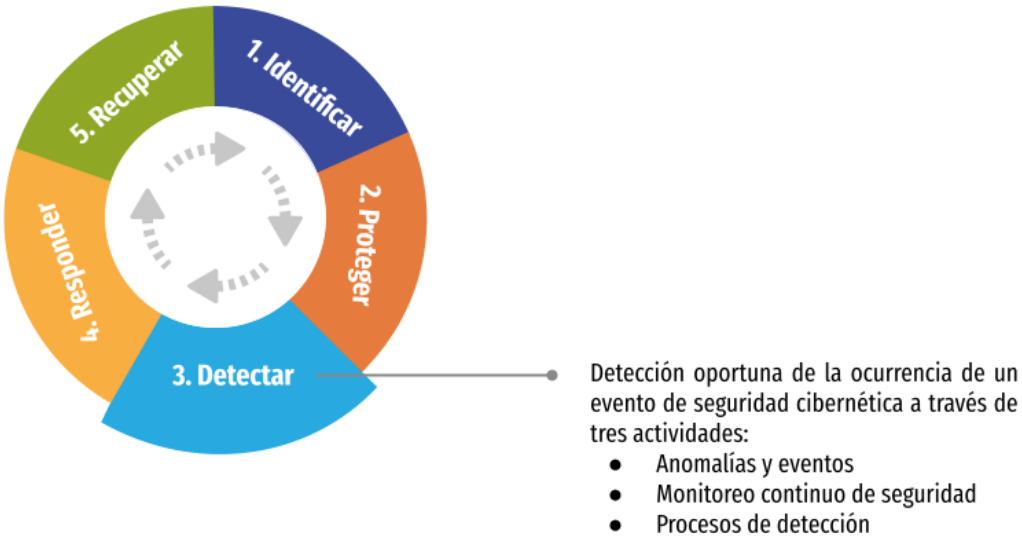
Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Específicamente, el artículo 2 del Decreto Ejecutivo n.° 43542 establece que todas las acciones, obras y servicios necesarios comprendidos en esta emergencia tienen el propósito de contener, solucionar y prevenir nuevos ataques en contra de los Sistemas de Información del Estado Costarricense. Precisamente a tal efecto, se designó a la Presidencia de la República, la CNE y el MICITT las facultades de planear, direccionar, controlar y coordinar los procesos necesarios para lograr la contención y solución del ciberataque, lo cual necesariamente debe derivar de un proceso articulado entre estas instituciones.

Necesidad de mejorar la capacidad instalada para la detección de incidentes de ciberseguridad en el sector público

El Marco para la mejora de la seguridad cibernética en infraestructuras críticas[2] del Instituto Nacional de Estándares y Tecnología, define cinco etapas que proporcionan una visión estratégica de alto nivel en el proceso de gestión de riesgos de la seguridad cibernética, los cuales son: Identificar, Proteger, Detectar, Responder y Recuperar (ver figura n.° 3). La etapa denominada "Detectar" consiste en desarrollar e implementar actividades apropiadas para el descubrimiento oportuno de eventos de seguridad cibernética que afecten la continuidad del servicio público y la salvaguarda de la información.

Figura n.° 3
Etapas del Ciclo de Ciberseguridad



Fuente: Elaboración CGR.

La etapa de detección comprende tres actividades principales: Anomalías y Eventos que consiste en la detección de eventos anómalos y el respectivo impacto que pueden llegar a tener; Monitoreo Continuo de la Seguridad en el cual se da seguimiento a los sistemas de información con el fin de identificar

[2] Instituto Nacional de Estándares y Tecnología. Marco para la mejora de la seguridad cibernética en infraestructuras críticas Versión 1.1 (2018). *Disponible en https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018es.pdf. Organización de los Estados Americanos (OEA). Ciberseguridad Marco NIST Un abordaje integral de la Ciberseguridad (2019). Disponible en: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf*

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

eventos de seguridad cibernética y verificar la eficacia de las medidas de protección; y Proceso de Detección, donde se mantienen y aprueban los procesos y procedimientos de detección para garantizar el conocimiento de los eventos anómalos.

Al respecto, se determinó que a seis meses de la declaración de la emergencia nacional y pese al rol eminentemente técnico en materia de ciberseguridad que debe asumir dentro de este marco, el CSIRT-CR a cargo del MICITT no cuenta con la suficiente capacidad instalada en términos de recursos humanos especializados y tecnológicos para la detección oportuna de incidentes de ciberseguridad.

En cuanto a los recursos humanos especializados, el Plan de Inversión del MICITT sobre la contratación de profesionales en informática para fortalecer el CSIRT-CR en la recuperación y atención de las plataformas afectadas por los ciberataques, fue aprobado mediante el acuerdo n.° 171-10-2022 de la Sesión Ordinaria de la Junta Directiva de la CNE, n.° 18-10-2022 del 06 de octubre del 2022, autorizando la contratación de ocho profesionales de informática y una persona profesional en Administración por un periodo de 12 meses; sin embargo, a la fecha el Órgano Contralor no tiene evidencia de la contratación de dicho personal.

En lo que respecta a recursos tecnológicos, el CSIRT-CR realiza un monitoreo para detectar inconvenientes con el funcionamiento de sitios web de las instituciones públicas; sin embargo, la herramienta utilizada permite esta identificación hasta el momento en que el sitio web se encuentra fuera de servicio. Este monitoreo es insuficiente para la detección oportuna de incidentes, puesto que en materia de ciberseguridad puede existir un lapso considerable entre la vulneración del sitio web y el momento en que este se reporta como fuera de servicio.

Es así como, el CSIRT-CR tiene una baja capacidad de detección de incidentes de ciberseguridad, lo cual se evidencia a través de las pruebas de vulnerabilidad de ciberseguridad efectuadas por el Órgano Contralor en septiembre de 2022, en las cuales se detectaron siete entidades públicas con incidentes materializados adicionales a las incluidas en el Plan General de la Emergencia, e incluso se identificó la firma o alias del grupo atacante, de las cuales el CSIRT-CR únicamente había detectado uno de ellos (sin que hubiese sido notificado por parte de la institución afectada), dificultando la atención oportuna y la toma de decisiones enfocada en prevenir ataques cibernéticos. Es preciso señalar que el incidente identificado persiste, pese a que fue detectado por el CSIRT-CR desde el 01 de mayo de 2022 y realizadas las gestiones a través de correos electrónicos con la institución afectada para informar las anomalías, enviar alertas y brindar apoyo.

Sobre la falta de capacidad instalada, el MICITT indicó que el CSIRT-CR opera con limitadas condiciones que no permiten desarrollar un monitoreo tan puntual y específico como los efectuados por el Órgano Contralor en las pruebas de auditoría. No obstante, las pruebas efectuadas por el Órgano Contralor comprenden la revisión de los componentes externos[3] utilizando la técnica OSINT (Open Source Intelligence) en la cual tan solo se requiere, a nivel técnico, de un navegador de internet para revisar las configuraciones al sitio web de diversas entidades públicas, que en este caso permitieron

[3] Los componentes externos abarcan las URL o dirección web pública y la dirección IP correspondiente.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

detectar sitios web comprometidos por ataque defacement[4], datos cifrados por Ransomware[5] y exfiltración de información.

En cuanto a la situación encontrada es importante recalcar que acorde con el artículo 2 del Decreto Ejecutivo n.° 43542-MP-MICITT, la declaración de emergencia nacional de ciberseguridad se establece con el propósito de realizar acciones para contener, solucionar y prevenir nuevos ataques en contra de los sistemas de información en todas las instituciones del sector público. En este sentido, la capacidad de detección de incidentes de ciberseguridad es necesaria para el cumplimiento efectivo de dicho propósito, lo cual se ve plasmado en el Plan General de la Emergencia, al incorporar como parte de la fase de reconstrucción el reforzamiento de los mecanismos de seguridad informática, mediante la adquisición de herramientas de protección, detección y alerta de virus.

Específicamente sobre el rol que ejecuta el MICITT, desde el 2012 se crea el CSIRT-CR mediante el Decreto Ejecutivo n.° 37052-MICITT, para coordinar en el sector público todo lo relacionado con la materia de seguridad informática y cibernética, así como concretar el equipo de expertos que trabajará para prevenir y responder ante los incidentes que afecten a las instituciones gubernamentales. En virtud de que las acciones para la detección de incidentes forman parte indispensable en el ciclo de la ciberseguridad, es responsabilidad del MICITT efectuar las acciones necesarias para desarrollar capacidades en la materia, a efecto de no reproducir la vulnerabilidad tanto en el contexto de la emergencia nacional como a futuro en las actividades ordinarias relacionadas con la ciberseguridad.

Firmado digitalmente por CAROLINA RETANA VALVERDE
Fecha: 2022-11-24 09:54

Licda. Carolina Retana Valverde
Gerente de Área
Área de Fiscalización para el Desarrollo Sostenible

[4] Los adversarios pueden modificar el contenido visual disponible interna o externamente a una red empresarial, afectando así la integridad del contenido original. Las razones para la desfiguración incluyen enviar mensajes, intimidar o reclamar crédito (posiblemente falso) por una intrusión. Se pueden utilizar imágenes perturbadoras u ofensivas como parte de Defacement para incomodar al usuario o para presionar el cumplimiento de los mensajes adjuntos. (mitre.org)

[5] Hacer que los datos almacenados sean inaccesibles cifrando archivos o datos en unidades locales y remotas y reteniendo el acceso a una clave de descifrado. Esto se puede hacer para obtener una compensación monetaria de una víctima a cambio del descifrado o una clave de descifrado (ransomware) o para hacer que los datos sean permanentemente inaccesibles en los casos en que la clave no se guarda o transmite.(mitre.org)

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica