INFORME N° DFOE-SOS-IF-00014-2022

INFORME DE AUDITORÍA DE CARÁCTER ESPECIAL ACERCA DE LA GOBERNANZA DE LA CIBERSEGURIDAD EN EL SECTOR PÚBLICO

2022

División de Fiscalización Operativa y Evaluativa

Área de Fiscalización para el Desarrollo Sostenible

Contraloría General de la República

CONTENIDO

Resumen Ejecutivo

¿Qué examinamos?

La auditoría tuvo como propósito determinar si la gobernanza de la ciberseguridad del país responde al marco normativo y prácticas aplicables, en procura del establecimiento de roles y trabajo conjunto para la continuidad de la gestión pública y los servicios. El periodo analizado comprendió entre el 1 de enero de 2021 al 30 de noviembre de 2022.

Debido a que a partir de mayo de 2022 el Gobierno de la República decidió gestionar los ciberataques recibidos por varias instituciones públicas, al amparo de una declaratoria de estado de emergencia, en esta auditoría se analizó la articulación entre los actores en el marco de gobernanza instaurado mediante el respectivo Decreto Ejecutivo n.° 43542-MP-MICITT. Así también, se examinaron las acciones efectuadas por el MICITT para asumir un liderazgo que contribuya a la transición en la gobernanza de la ciberseguridad una vez finalizada la emergencia, bajo la premisa de que regresar a las dinámicas de gestión previas implicaría reproducir la vulnerabilidad y la imposibilidad de capitalizar el aprendizaje para realimentar la gestión con enfoque preventivo.

¿Por qué es importante?

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 caso de la ciberseguridad la gobernanza es crítica, por cuanto la Administración Pública ha migrado hacia un entorno predominantemente digital, en el cual la prestación de servicios se apoya en herramienta tecnológicas y se generan grandes cantidades de información que en muchos casos es considerada sensible.

¿Cómo lo auditamos?

Para la ejecución de esta auditoría se aplicó un enfoque ágil a partir del cual se comunicó un reporte de auditoría en el que se detallaron dos áreas susceptibles de mejora a efecto de que el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) y la Comisión Nacional de Prevención de Riesgos y Atención de Emergencias (CNE) implementaran cambios oportunos. Al respecto, las instituciones lograron iniciar con la implementación de los planes de inversión para mejorar la capacidad instalada del Centro de Respuesta de incidentes de Seguridad Informática (CSIRT-CR) en la atención del estado de emergencia en términos de recursos humanos y tecnológicos; sin embargo, persisten debilidades que se detallan en el presente informe, en conjunto con dos hallazgos adicionales configurados con posterioridad al reporte comunicado.

¿Qué encontramos?

Las acciones efectuadas por el MICITT y la CNE para la gestión de incidentes de ciberseguridad, tanto en el marco del estado de emergencia como en las actividades ordinarias a través del CSIRT-CR, cumplen parcialmente con lo establecido en el marco jurídico y técnico aplicable.

Lo anterior, ya que no se evidencia un nivel de coordinación interinstitucional propio de un estado de necesidad y urgencia en el caso de los ciberataques. En este sentido, se creó la Sala de Análisis de Situación Nacional (SASN) para responder de forma ágil a los ataques cibernéticos en el sector público; sin embargo, la coordinación en su seno es inoportuna, pues la Sala se mantuvo inactiva entre julio y agosto, y para los meses posteriores, la participación de la CNE ha sido

intermitente, pese a estar llamado a ser líder en la emergencia, de conformidad con el Decreto Ejecutivo n.° 43542-MP-MICITT.

Además, se determinó la falta de oportunidad en la gestión de incidentes de ciberseguridad por parte del CSIRT-CR, a cargo del MICITT. Al respecto, mediante pruebas de auditoría enfocadas en vulnerabilidad, efectuadas por la Contraloría General, se encontraron siete entidades públicas en septiembre 2022 con incidentes materializados, de los cuales el CSIRT-CR únicamente había detectado uno. Asimismo, las gestiones efectuadas por ese Centro para poner a las instituciones afectadas en autos de estos nuevos incidentes, tuvieron lugar hasta 44 días naturales después de que se hicieron de su conocimiento por parte del Órgano Contralor.

Por su parte, el MICITT señala que efectúa alertas técnicas a las instituciones del sector público; no obstante, de la revisión de 197 de estas alertas, se constató que estas son de carácter general y meramente informativas, con el fin de que sus receptores tomen precauciones o acciones específicas debido a la probabilidad del impacto de un fenómeno o la existencia de una vulnerabilidad. De esta forma, se trata de alertas que distan sustancialmente de los incidentes de ciberseguridad que le reportó el Órgano Contralor, pues a diferencia, estos últimos se centran en eventos que causan, o pueden causar, una interrupción o reducción en la calidad de dicho servicio.

También, el modelo de gestión del CSIRT-CR presenta limitaciones que impiden responder a las necesidades actuales y futuras en ciberseguridad; así como, efectuar una adecuada transición del sector público para gestionar la ciberseguridad de forma ordinaria, de cara a la cesación del estado de emergencia. Estas limitaciones se evidencian al comparar las funciones del CSIRT-CR con otras entidades creadas bajo la misma figura de centros de respuestas a incidentes en la región latinoamericana, cuyas funciones les permiten tener un mayor alcance en las etapas de detección, respuesta y recuperación ante incidentes de ciberseguridad. Así también, no existe certeza sobre cómo se garantizará la continuidad en la gestión de la ciberseguridad y la adquisición de licencias informáticas para proteger al sector público en su actividad ordinaria, posterior a la cesación del estado de emergencia.

Ante las debilidades planteadas, el sector público se enfrenta ante la incertidumbre latente de no tener claridad sobre la magnitud y cantidad de incidentes que actualmente han logrado vulnerar los sistemas informáticos, con el potencial de afectar la continuidad de los servicios públicos y la salvaguarda de la información.

¿Qué sigue?

Se dispone a la CNE y MICITT para que en conjunto implementen, ya sea para la Sala de Análisis de Situación Nacional o el mecanismo de coordinación interinstitucional que en adelante se determine, los objetivos, funciones, roles, responsabilidades, periodicidad de la coordinación, la estrategia de ejecución de decisiones y su seguimiento, a fin de propiciar desde el nivel estratégico y operativo un trabajo proactivo en la atención de la emergencia. Por otra parte, se dispone al MICITT implementar procedimientos que permitan gestionar oportunamente los incidentes de ciberseguridad en el sector público; así como, reformar el marco normativo que regula el modelo de gestión del CSIRT-CR para que responda al ciclo de la ciberseguridad. También, implementar un mecanismo en el que se incorporen las acciones requeridas por parte del MICITT para efectuar una transición de cara a la cesación del estado de emergencia, declarado mediante el Decreto Ejecutivo n.° 43542, de tal forma que la gestión de incidentes de ciberseguridad pueda ser llevada a cabo como parte de las actividades ordinarias de la Administración Pública y el CSIRT-CR.

INFORME Nro. DFOE-SOS-IF-00014-2022

DIVISIÓN DE FISCALIZACIÓN OPERATIVA Y EVALUATIVA
ÁREA DE FISCALIZACIÓN PARA EL DESARROLLO SOSTENIBLE

BORRADOR DE INFORME DE AUDITORÍA DE CARÁCTER ESPECIAL ACERCA DE LA GOBERNANZA DE LA CIBERSEGURIDAD EN EL SECTOR PÚBLICO

1. Introducción

Origen de la Auditoría

1.1. La presente auditoría se realizó en cumplimiento del Plan Anual Operativo de la División de Fiscalización Operativa y Evaluativa y sus modificaciones, con fundamento en las competencias que le son conferidas a la Contraloría General de la República en los artículos 183 y 184 de la Constitución Política, y los artículos 12, 17 y 21 de su Ley Orgánica, n.° 7428.

1.2. Durante el año 2022 el sector público costarricense se vio afectado por una serie de ciberataques que vulneraron los sistemas de información, limitando la continuidad del servicio público y la salvaguarda de la información. Para hacer frente a esta situación, el Gobierno de la República de Costa Rica declaró estado de emergencia, para lo cual emitió el Decreto Ejecutivo n.° 43542-MP-MICTT, que 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.

1.3. Ante la necesidad de implementar acciones por parte de la Administración Pública bajo un estado de necesidad y urgencia, resulta relevante consolidar un modelo de gobernanza que considere las redes de coordinación entre los actores involucrados en el citado estado de emergencia y la activación y ejecución de recursos financieros, tecnológicos, humanos y organizativos requeridos para su abordaje.

1.4. De igual forma, en vista de la tendencia creciente de ciberataques a nivel mundial, se busca capitalizar los aprendizajes obtenidos durante la emergencia para adoptar una gestión pública resiliente en la que se fortalezca las medidas tanto preventivas como reactivas en materia de ciberseguridad.

Objetivos

1.5. Determinar si la gobernanza de ciberseguridad del país, 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 públicos.

Alcance

1.6. La auditoría abarcó la determinación de si la gobernanza de ciberseguridad del país responde al marco normativo, los principios de buena gobernanza y prácticas aplicables. El periodo de análisis comprendió del 1 de enero al 31 de octubre de 2022.

Criterios de Auditoría

1.7. Los criterios de auditoría fueron presentados en reunión sostenida por videoconferencia mediante la plataforma Meet de Google, el lunes 14 de noviembre de 2022, con la participación de los señores Alejandro Picado Eduarte, Presidente Ejecutivo; Sigifredo Pérez Fernández; Director Ejecutivo; Milena Mora Lammas, Unidad Asesoría Legal; Jorge Rovira Guzmán, Director de Gestión del Riesgo; Carlos Picado Rojas, Jefe Unidad de Desarrollo Estratégico; Wilgen Saborío Cordoba, Jefe Unidad de Tecnología de la Información, todos de la CNE. Además, Carlos Alvarado Briceño, Ministro; Paula Brenes Ramírez, Directora de Gobernanza Digital; Juan Ignacio Rodríguez Araya, Asesor Despacho; Olivier Gómez Salas, Dirección de Gobernanza Digital; Andrea Marcela García, Jefa Despacho Ministro, todos del MICITT. También estuvo presente la Licda. Elizabeth Castillo Cerdas y Giovanni Monge Guillen, Auditoría Interna de la CNE y Auditor Interno del MICITT.

1.8. Estos criterios también fueron comunicados por escrito mediante el oficio n.° DFOE-SOS-0513-2022 (22412) del 12 de noviembre de 2022.

Metodología aplicada

1.9. La auditoría se realizó de conformidad con las Normas Generales de Auditoría para el Sector Público, con el Manual General de Fiscalización Integral de la CGR y el Procedimiento de Auditoría vigente, establecido por la DFOE. Para el desarrollo de esta auditoría se utilizó la información suministrada por el MICITT y la CNE en respuesta a solicitudes de información efectuadas por el Órgano Contralor, asimismo, se aplicaron entrevistas a personas funcionarias de ambas instituciones, expertos en la materia y otras partes interesadas.

1.10. Como parte de los procedimientos, se aplicaron pruebas de auditoría enfocadas en vulnerabilidad, mediante las cuales se examinaron componentes externos de sitios web utilizando la técnica OSINT (Open Source Intelligence), en la cual se revisaron las configuraciones al sitio web de diversas entidades públicas para identificar posibles incidentes de ciberseguridad.

1.11. La auditoría aplicó los Lineamientos generales para la ejecución de auditorías con enfoque ágil en la DFOE, n.° R-DFOE-GE-I-01-2020 del 12 agosto de 2020. Este enfoque permite la obtención de resultados de fiscalización más oportunos, promoviendo mejoras en la gestión de las instituciones fiscalizadas a partir de la generación de valor público para las partes.

Generalidades acerca del objeto auditado

1.12. De conformidad con la Ley Nacional de Emergencias y Prevención del Riesgo, ley n.° 8488 del 11 de enero del 2006 y sus reformas, 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.

1.13. Decretado el estado de emergencia, se activa un régimen de excepción con el fin de agilizar la actividad administrativa, así como 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.

1.14. Para hacer frente a los ciberataques registrados a partir de abril de 2022, el Gobierno de la República declaró estado de emergencia, para lo cual emitió el Decreto Ejecutivo n.° 43542-MP-MICITT vigente a partir del 11 de mayo del 2022, 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.

1.15. 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 cuenta con la facultad de coordinación para prevenir y responder ante los incidentes de seguridad cibernética e informática, a través del CSIRT-CR.

1.16. Para gestionar las acciones relacionadas con el estado de emergencia por ciberataques se emitió el Plan General de la Emergencia (PGE) aprobado mediante Acuerdo N° 141-07-2022, de la Sesión Ordinaria de la Junta Directiva de la CNE Nº 13-07-2022 del 21 de julio del 2022, 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.

1.17. Por su parte, el PGE refiere a la expectativa de que para los siguientes ejercicios presupuestarios las instituciones cuenten con la planificación y los recursos necesarios para hacer frente a la

amenaza de ataques cibernéticos como parte de sus propias gestiones en su actividad ordinaria. Ante esta situación, resulta necesario efectuar una adecuada transición del sector público para gestionar la ciberseguridad de forma ordinaria, de cara a la cesación del estado de emergencia.

Comunicación preliminar de los resultados de la auditoría

1.18. En reunión efectuada el 19 de diciembre de 2022 se presentaron los resultados, conclusiones y disposiciones que se derivan de la auditoría a los siguientes funcionarios del MICITT: Carlos Enrique Alvarado Briceño,Ministro, Paula Brenes Ramírez, Directora de Gobernanza Digital, Juan Ignacio Rodríguez Araya Asesor Despacho, Dayana Mejía García, Asesora Despacho, Olivier Gómez Salas, Dirección de Gobernanza Digital. Por parte de la CNE estuvieron presentes los siguientes funcionarios: Sigifredo Pérez Fernández, Director Ejecutivo, Milena Mora Lammas, Unidad Asesoría Legal, Jorge Rovira Guzmán, Director de Gestión del Riesgo, Carlos Picado Rojas, Jefe Unidad de Desarrollo Estratégico, Wilgen Saborío Córdoba, Jefe Unidad de Tecnología de la Información, Guillermo Villegas Chaves, Fiscalizador especialista en Ciberseguridad de la Unidad de Gestión de Procesos de Reconstrucción. Además estuvo presente Elizabeth Castillo Cerdas, Auditora Interna de la CNE y Giovanni Monge Guillen, Auditor Interno del MICITT.

Siglas

1.19. A continuación, se indica el detalle de las siglas utilizadas en este informe:

SIGLA	Significado
CGR	Contraloría General de la República
DFOE	División de Fiscalización Operativa y Evaluativa de la CGR
CNE	Comisión Nacional de Prevención de Riesgos y Atención de Emergencias
CSIRT-CR	Centro de Respuesta de incidentes de Seguridad Informática
LGCI	Ley General de Control Interno
MICITT	Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones
OEA	Organización de Estados Americanos
PGE	Plan General de la Emergencia
SASN	Sala de Análisis de Situación Nacional
SOC	Centro de Operaciones de Seguridad (Security Operations Center, por sus siglas en Inglés)

2. Resultados

2.1. La coyuntura actual ha implicado que la ciberseguridad en el sector público se gestione de forma temporal a través de un estado de emergencia; sin embargo, de cara a la tendencia creciente de ciberataques a nivel nacional e internacional, surge la necesidad de ejecutar las acciones correctivas con visión estratégica y sostenible en el tiempo.

2.2. Bajo este escenario, con la presente auditoría se busca tener incidencia en áreas relevantes de la gobernanza de la ciberseguridad que presentan oportunidades de mejora (ver figura n.° 2), tanto en el contexto del estado de emergencia, como fuera de este.

Figura n.° 2
Áreas de mejora en la gobernanza de ciberseguridad

Fuente: Elaboración CGR.

Articulación para la gestión de incidentes de ciberseguridad

2.3. 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 del estado de emergencia, lo cual es más congruente con lo estipulado en la Ley Nacional de Emergencias y Prevención del Riesgo, n.° 8488.

2.4. Además, en cuanto a la coordinación requerida para atender el estado de emergencia, la CNE en conjunto con el 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, persisten áreas de mejora que limitan la articulación requerida para gestionar los incidentes de ciberseguridad, según se describe a continuación:

Falta de articulación para la atención del estado de emergencia por ciberataques

2.5. Tal como se indicó líneas atrás, para la atención del estado de emergencia declarado mediante el Decreto Ejecutivo n.° 43542-MP-MICITT, se estableció la Sala de Análisis de Situación Nacional (SASN) como el mecanismo 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 el estado de emergencia por ciberataques se encuentra en proceso de manifestación, es decir, se mantiene la posibilidad de ocurrencia de nuevos incidentes de ciberseguridad.

2.6. 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 del estado de emergencia de ciberseguridad, de conformidad con los principios de estado de necesidad y urgencia, coordinación e integralidad del proceso de gestión.

[1] La Sala de Análisis de Situación Nacional (SASN) se conforma por las siguientes instituciones: Caja Costarricense de Seguro Social (CCSS), Comisión Nacional de Prevención de Riesgos y Atención 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.

2.7. En ese sentido, es preciso indicar que esta Sala se mantuvo inactiva desde el 02 de julio hasta el 14 de agosto del año en curso y para los meses siguientes, tuvo sesiones quincenales, aún cuando en ese lapso se identificaron ataques de ciberseguridad en el Ministerio de Salud y en la Municipalidad de Belén, lo que ameritaba una mayor actividad de parte de las entidades responsables de gestionar el estado de emergencia (ver figura n.° 3). Posteriormente, a partir de noviembre, aumentó la frecuencia de reuniones en la SASN pero sin una participación activa por parte de la CNE, la cual estuvo presente sólo en dos de cuatro sesiones. Cabe destacar que la evidencia documental sobre las minutas que hacen constar las reuniones efectuadas, carece de formalidad, pues ninguna acredita la firma digital de las personas participantes.

Figura n.° 3
Reuniones efectuadas por la Sala de Análisis y Situación Nacional y acontecimientos importantes de ciberseguridad entre mayo y octubre de 2022

Fuente: Elaboración CGR.

2.8. Al respecto, mediante el oficio n.° MICITT-DGD-OF-217-2022 del 19 de setiembre de 2022, 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 del estado de emergencia.

2.9. En relación con la normativa que regula las debilidades descritas anteriormente, la declaración de estado 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 este estado de 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.

2.10. Específicamente, el artículo 2 del Decreto Ejecutivo n.° 43542 establece que todas las acciones, obras y servicios necesarios comprendidos en este estado de 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.

2.11. La situación descrita obedece a que siendo la CNE y el MICITT las entidades encargadas de coordinar el planeamiento, dirección y control de los procesos necesarios para contener y solucionar los ciberataques, el mecanismo de coordinación que se estableció para la gestión del estado de emergencia carece de una definición formal de propósito, funciones, roles, responsabilidades, periodicidad, así como de la estrategia de comunicación, ejecución y seguimiento de la toma de decisiones.

2.12. Lo anterior limita la intervención rápida y radical durante el estado de emergencia, y dificulta la coordinación de acciones entre los diferentes actores. Asimismo, se compromete la gestión con enfoque preventivo a efecto de asegurar la continuidad del servicio público y la salvaguarda de la información, que se garantiza a través de una solución efectiva de eventuales ciberataques.

Gestión de incidentes de ciberseguridad en el sector público

Debilidades en la gestión oportuna de incidentes de ciberseguridad en el sector público

2.13. Ante incidentes de ciberseguridad se debe responder rápidamente, pasando de las prioridades habituales de una organización hacia la situación de crisis, ya que en caso contrario se pierde un tiempo inicial que da ventaja a los grupos atacantes, al no asegurarse una rápida intervención.[2] Sin embargo, se determinó que las actividades ejecutadas por el CSIRT-CR para la gestión de incidentes de ciberseguridad no se realizan de forma oportuna.

2.14. Al respecto, mediante pruebas de auditoría enfocadas en vulnerabilidad, efectuadas por el Órgano Contralor en septiembre de 2022, se encontraron siete entidades públicas con incidentes materializados e incluso se identificó la firma o alias del grupo atacante. Sobre estos casos, el CSIRT-CR únicamente había detectado uno de ellos, dificultando la atención oportuna y la toma de decisiones enfocada en prevenir ataques cibernéticos.

2.15. Ante esta situación, 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 comprenden la revisión de los componentes externos 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 detectar

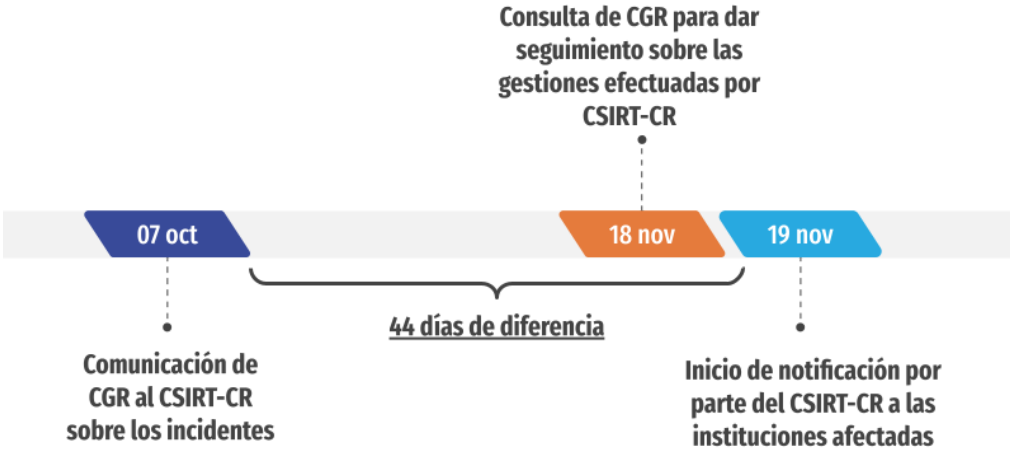
[2] Centro Criptológico Nacional (2022). Aproximación al marco de gobernanza de la ciberseguridad.

sitios web comprometidos por ataque defacement[3], datos cifrados por Ransomware[4] y exfiltración de información.

2.16. También el MICITT señaló que como parte de sus gestiones, realizó procesos para la emisión de alertas técnicas a las instituciones del sector público; no obstante, el Órgano Contralor revisó 197 de esas alertas, constatando que son de naturaleza distinta a los incidentes de ciberseguridad a los cuales hace referencia el Órgano Contralor. De lo observado, las alertas técnicas informan sobre posibles vulnerabilidades para que se tomen precauciones o acciones específicas sin que necesariamente se haya presentado un ciberataque. A diferencia, los incidentes a que hace referencia la Contraloría General, corresponden a cualquier suceso materializado que afecte a la confidencialidad, integridad o disponibilidad de los activos de información y por ende, la continuidad o reducción de la calidad de los servicios públicos.

2.17. Por otra parte, el Órgano Contralor comunicó al CSIRT-CR el 07 de octubre del 2022 la existencia de los incidentes citados anteriormente; sin embargo, las gestiones efectuadas por esta instancia para poner a las instituciones afectadas en conocimiento de los incidentes se realizaron hasta el 19 de noviembre, como resultado de una consulta efectuada el 18 de noviembre por la Contraloría General para verificar las acciones de seguimiento. Esto equivale a 44 días naturales entre el momento en que el CSIRT-CR tuvo conocimiento de los incidentes hasta que realiza la comunicación respectiva a las instituciones (ver figura n.° 4).

Figura n.° 4
Tiempo transcurrido entre la notificación de la Contraloría General sobre los incidentes y las actividades efectuadas por el CSIRT-CR para la atención



Fuente: Elaboración CGR.

[3] 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, ATT&CK).
[4] 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 transmites (Mitre.org)

2.18. Sobre esta situación, el MICITT señala que la comunicación sobre los incidentes se realizó inicialmente por vía telefónica con las instituciones respectivas. Cabe destacar que el Órgano Contralor no encontró evidencia de dicha comunicación y los seis de los siete incidentes se mantienen activos al momento de emisión del presente informe, situación que puede llegar a impactar la continuidad de los servicios públicos y ocasionar mayores afectaciones en términos de la seguridad de la información.

2.19. Adicionalmente, se determinó que el CSIRT-CR no cuenta con los mecanismos suficientes para recopilar información sobre los incidentes de ciberseguridad. En este sentido, los protocolos[5] establecidos para la gestión indican que en caso de que el incidente no pueda ser resuelto por la persona responsable en la institución afectada, se procede a reportarlo al Centro para su atención, y el enlace institucional de ciberseguridad enviará un formulario completo junto con la información y pruebas relevantes (archivos de registros, archivos sospechosos, entre otros) para efectuar un análisis más profundo del incidente reportado. No obstante, a la fecha las instituciones afectadas no cuentan con claridad sobre la información que se consideraría relevante para dar una atención ágil y oportuna, ya que de parte del CSIRT-CR no se han creado los formularios que permitan recolectar y estandarizar la información sobre los incidentes.

2.20. Además, se determinó que el CSIRT-CR no realiza una categorización de los incidentes de ciberseguridad según el nivel de criticidad, en aras de establecer un enfoque de priorización basado en riesgos. Esta situación se evidencia tanto en los ciberataques ocurridos durante el 2022, que fueron incorporados como parte del estado de emergencia, así como en los incidentes identificados por el Órgano Contralor en las pruebas de vulnerabilidad que fueron comunicados al MICITT el 07 de octubre del año en curso, los cuales en ambos casos no cuentan con un nivel de criticidad asignado.

2.21. Sobre el rol que ejecuta el MICITT, el CSIRT-CR se crea mediante el Decreto Ejecutivo n.° 37052-MICITT del 9 de marzo del 2012 con el fin de 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.

2.22. Acorde con buenas prácticas para establecer un CSIRT nacional señaladas por la OEA, los centros de respuesta de incidentes de ciberseguridad deben ofrecer servicios y soporte a un grupo en particular (comunidad objetivo) con la finalidad de prevenir, gestionar y responder a incidentes de seguridad de la información. Las personas que conforman los CSIRT suelen ser especialistas multidisciplinarios que actúan según procedimientos y políticas predefinidas, de manera que respondan, en forma rápida y efectiva, a incidentes de seguridad, además de coadyuvar a mitigar el riesgo de los ataques cibernéticos.

2.23. Las situaciones encontradas obedecen a que el nivel de preparación de este Centro no era el idóneo para hacer frente a la gestión de incidentes, situación que se visualiza en la desactualización de procedimientos que permitan procesos de detección y respuesta oportuna en los que se incluyan criterios de actuación, actividades, roles, responsables, plazos estimados, nivel de criticidad de los incidentes, mecanismos de control, coordinación y seguimiento, así como los mecanismos utilizados para recopilar la información de manera estandarizada y ágil. Adicionalmente,no se cuenta con un procedimiento en el que se indique la periodicidad y el tipo de monitoreo que debe realizar el personal del CSIRT-CR, según los múltiples incidentes que pueden afectar a las instituciones públicas.

[5] Protocolo de Gestión de Incidentes de Ciberseguridad" y su manual de apoyo, ambos de 2018, y el "Protocolo para el desarrollo de las acciones que se deben implementar ante una amenaza de un ataque a la ciberseguridad nacional" de mayo de 2022.

2.24. Como resultado de las debilidades descritas anteriormente, el sector público se enfrenta ante un riesgo elevado de que aún en un contexto de estado de emergencia, no se tenga claridad sobre la cantidad y magnitud de incidentes que actualmente han logrado vulnerar los sistemas informáticos, con el potencial de afectar la continuidad de los servicios públicos y la salvaguarda de la información.

Ausencia de un modelo de gestión en el CSIRT-CR acorde con las necesidades en materia de ciberseguridad

2.25. El Marco para la mejora de la seguridad cibernética en infraestructuras críticas[6] 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, las cuales son: Identificar, Proteger, Detectar, Responder y Recuperar (ver figura n.° 5).

Figura n.° 5
Etapas del Ciclo de Ciberseguridad

Fuente: Elaboración CGR.

2.26. Como parte de este ciclo de ciberseguridad, es de gran relevancia el rol que puede ejercer el CSIRT-CR en cada una de las etapas descritas, así como en el marco de la gobernanza de ciberseguridad, al ser el coordinador nacional en la materia para el sector público. Sin embargo, se determinó que el modelo de gestión del CSIRT-CR presenta limitaciones que impiden responder a las necesidades actuales y futuras en ciberseguridad en el sector público.

2.27. Al comparar las funciones del CSIRT-CR a cargo del MICITT, con otras entidades creadas bajo la misma figura de centros de respuestas a incidentes en la región latinoamericana, así como las buenas prácticas que define la Organización de los Estados Americanos (OEA), es posible identificar que dentro de las funciones que se le establece a este Centro mediante el Decreto Ejecutivo n.° 37052-MICITT, no se consideran suficientemente las actividades indispensables a desarrollar en las etapas del ciclo de ciberseguridad, tal es el caso de la detección, respuesta y recuperación ante incidentes (ver tabla n.° 1).

[6] 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

Tabla n.° 1
Análisis comparativo entre las funciones de los Centros de Respuesta a Incidentes de Ciberseguridad (CSIRT) de Latinoamérica

	CSIRT-CR	CHILE	COLOMBIA	URUGUAY	BUENAS PRÁCTICAS OEA
DETECTAR	-No se indican funciones de detección	-Monitoreo continuo a través de pruebas -Verificar el cumplimiento de normas y estándares -Registrar la totalidad de incidentes de ciberseguridad en el sector público	-Apoyar a todas las autoridades en la protección y detección ante incidentes	-Coordinar para la prevención, detección, manejo y recopilación de información sobre incidentes -Centralizar los reportes y llevar un registro de toda la información sobre incidentes	-Detectar amenazas o vulnerabilidades emergentes -Dar monitoreo y las alertas a través de la implementación de sistemas que ayudan a detectar eventos de seguridad
RESPONDER	-Concretar el equipo de expertos para prevenir y responder ante incidentes -Elaborar informes de incidentes para las instituciones que lo soliciten	-En respuesta a incidentes podrá disponer de acciones necesarias para asegurar la continuidad del funcionamiento de las redes y plataformas de los servicios públicos	-Apoyar a todas las autoridades en la respuesta y comunicación ante incidentes	-Asistir en la respuesta a incidentes de seguridad informática a los organismos estatales afectados.	-El principal rol del CSIRT es coordinar actividades de respuesta ante incidentes. -Un CSIRT se compone de personas cuyo trabajo es prevenir y responder a incidentes.
RECUPERAR	-No se indican funciones de recuperación	-No se indican funciones de recuperación	-Apoyar a todas las autoridades en la recuperación y aprendizaje ante incidentes	-Coordinar planes de recuperación de desastres y realizar un análisis forense del incidente de seguridad informática reportado.	-No se indican funciones de recuperación

Fuente: Elaboración CGR con base en el Decreto Ejecutivo n.º 37052-MICIT "Crea Centro de Respuesta de incidentes de Seguridad Informática CSIRT-CR", buenas prácticas para establecer un CSIRT nacional de la OEA y la normativa que respalda la creación de los CSIRT en Chile, Colombia y Uruguay.

2.28. En la **etapa de detectar**, se presenta un vacío en las funciones del CSIRT-CR en temas como el monitoreo, alertas y detección de eventos de ciberseguridad, y en la recopilación y registro de la información relevante sobre los incidentes de ciberseguridad ocurridos en el sector público. Sobre este último punto, en mayo de 2022 se publicó la Directriz n.° 133-MP-MICITT, en la que se instruye a la Administración Pública Central y se insta a la Administración Pública Descentralizada a comunicar los incidentes que ocurran en sus instituciones; sin embargo, debido a la naturaleza de esta norma, no existe un carácter vinculante que involucre a todo el sector público.

2.29. En la **etapa de respuesta**, las buenas prácticas señaladas por la OEA, establecen que a un CSIRT nacional le corresponde coordinar actividades de respuesta a incidentes como su rol principal, situación que en países de la región latinoamericana se incorpora mediante funciones de apoyo y asistencia de respuesta de incidentes. Si bien, mediante el Decreto Ejecutivo n.° 37052-MICITT se establece la potestad del CSIRT-CR para concretar el equipo de expertos que trabajará en responder ante incidentes, no se especifican las funciones mínimas que debe ejecutar este equipo.

2.30. Por su parte, en la **etapa de recuperación**, en el citado Decreto no se incorporan funciones para el CSIRT-CR; sin embargo, países como Colombia y Uruguay refieren a actividades enfocadas en apoyar en la recuperación y aprendizaje, coordinar los planes de recuperación y realizar análisis forense en la materia posterior a los incidentes.

2.31. Aún cuando la comparación efectuada entre centros de respuestas a incidentes de países en la región latinoamericana permite establecer un parámetro de referencia, el hecho de incorporar las etapas indispensables del ciclo de la ciberseguridad surge ante una necesidad creciente, que toma mayor relevancia por el aumento en ataques cibernéticos que han sufrido las instituciones públicas durante el 2022, los cuales inciden cada vez más en la continuidad de los servicios públicos y el resguardo seguro de la información.

2.32. En atención al principio de legalidad establecido en el artículo 11 de la Ley General de la Administración Pública, n.° 6227 del 2 de mayo de 1978 y sus reformas, la Administración Pública debe actuar sometida al ordenamiento jurídico y sólo podrá realizar aquellos actos o prestar servicios públicos que autorice dicho ordenamiento. Por su parte, en la citada ley se define mediante el artículo 4 que 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.

2.33. Además, el artículo 4 de la Ley de Promoción Desarrollo Científico y Tecnológico y Creación del MICITT, ley n.° 7169 del 26 de junio de 1990 y sus reformas, designa como parte de los deberes y responsabilidades del Estado, la función de 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.

2.34. A nivel de buenas prácticas, adicional a las mencionadas en el análisis comparativo, la OEA realiza una categorización de los servicios que brindan los CSIRT según el nivel de madurez, los cuales pueden cubrir servicios básicos, intermedios o avanzados (ver figura n.°6).

Figura n.° 6

Nivel de madurez de los servicios brindados por Centros de Respuesta a Incidentes de Ciberseguridad (CSIRT)

SOC: El Centro de Operaciones de Seguridad (Security Operations Center, por sus siglas en Inglés), es una central de seguridad informática que previene, monitorea y controla la seguridad en las redes y en Internet.

Fuente: Elaboración CGR con base en buenas prácticas para establecer un CSIRT nacional de la OEA.

2.35. La ausencia de un modelo de gestión que responda a las necesidades actuales y futuras e incorpore las etapas indispensables del ciclo de la ciberseguridad, obedece a que tanto este modelo como el marco normativo del MICITT que sustenta el funcionamiento del CSIRT-CR, se establecieron en 2012 y durante la última década se han mantenido estáticos, aún cuando la evolución de la ciberseguridad a nivel nacional e internacional ha tomado mayor relevancia y se posiciona como parte de las actividades cotidianas de las entidades encargadas de la prestación de los servicios públicos, para la salvaguarda de la información.

2.36. Si bien el CSIRT-CR durante los últimos años ha efectuado algunas acciones de monitoreo y generación de alertas, la carencia de un marco normativo que establezca el perfil de las acciones de detección, respuesta y recuperación, limitan la incidencia que puede tener el MICITT sobre el sector público en temas de ciberseguridad, lo cual es crítico principalmente considerando la necesaria capacidad que debe tener ese Ministerio de coordinar a nivel nacional acciones que permitan el mejoramiento general en materia de ciberseguridad una vez que se levante el estado de emergencia y estos temas deban ser gestionados mediante las competencias ordinarias de esa institución.

Falta de certeza acerca de la continuidad en la gestión de la ciberseguridad posterior al estado de emergencia

2.37. Para trascender del estado de emergencia hacia las actividades ordinarias de la Administración Pública en materia de ciberseguridad, debe prevalecer un enfoque preventivo, a efecto de capitalizar los aprendizajes y no reproducir las vulnerabilidades que motivaron el estado de necesidad y urgencia declarado.

2.38. Sin embargo, no existe certeza de cómo se garantizará la continuidad en la gestión de la ciberseguridad y la adquisición de licencias informáticas para proteger al sector público en su actividad ordinaria, aún cuando las necesidades urgentes que se han atendido con recursos del estado de emergencia van a continuar persistiendo en razón de la tendencia creciente a nivel nacional e internacional en ciberataques.

2.39. Si bien durante el estado de emergencia de ciberseguridad, así decretado, se le otorga al MICITT, en conjunto con la Presidencia de la República y la CNE, la función de coordinación para contener, solucionar y prevenir nuevos ciberataques, resulta evidente que este rol está delimitado por la temporalidad del estado de la emergencia. Como parte de estas acciones se han reforzado los recursos disponibles en el CSIRT-CR por un plazo máximo de un año en términos de recursos humanos y tecnológicos (ver figura n.° 7).

Figura n.° 7

Recursos humanos y tecnológicos aprobados por la Junta Directiva de la CNE para fortalecer al CSIRT-CR y al sector público en la atención del estado de emergencia de ciberseguridad

Fuente: Elaboración CGR tomando en consideración los Acuerdos N.° 167, 168, 169 y 171 aprobados por la Junta Directiva de la CNE, en la Sesión Ordinaria Nº 18-10-2022 del 06 de octubre del 2022.

2.40. En un contexto en el cual solamente el 18,7% de las instituciones públicas cuenta con mecanismos de protección ante amenazas de ciberseguridad[7], con la adquisición de herramientas informáticas donadas o financiadas con recursos del estado de emergencia se han logrado proteger hasta 184 instituciones públicas contra incidentes de ransomware y 167 instituciones en las que se protegen los servicios en la nube. Sin embargo persisten riesgos, debido a que posterior al vencimiento de estas licencias, la dinámica en el sector público retorna al escenario inicial, en el sentido de que la responsabilidad de realizar el proceso de adquisición recae sobre las propias instituciones públicas como parte de su actividad ordinaria. Además, en muchos casos previo al estado de emergencia no se le había dado prioridad a estas temáticas, incurriendo en vulnerabilidades en los sistemas de información.

2.41. Como parte de las gestiones efectuadas por el CSIRT-CR para coordinar el mejoramiento de la ciberseguridad, se remitió un correo electrónico a las instituciones públicas, comunicando que las licencias que inicialmente vencían el 19 de octubre de 2022 se ampliaron 12 meses adicionales en razón de la aprobación por parte de la Junta Directiva de la CNE, pero ante este vencimiento, el Centro reiteró la necesidad de que cada institución adquiera las herramientas tecnológicas para su gestión.

2.42. En relación con el marco normativo que regula las debilidades planteadas, la Constitución Política de la República define en su artículo 176 que la gestión pública se conducirá de forma sostenible, transparente y responsable, la cual se basará en un marco de presupuestación plurianual, en procura de la continuidad de los servicios que presta. Ante la relevancia que toma la ciberseguridad para garantizar la continuidad de los servicios públicos en la Administración Pública, resulta relevante dar sostenibilidad a las medidas de protección que permitan la mitigación de los riesgos asociados a la materia.

2.43. Por su parte, en el artículo 27 de la Ley General de la Administración Pública, n.° 6227, se establece que le corresponderá a los Ministros conjuntamente con el Presidente de la República las atribuciones que les señala la Constitución y las leyes, así como dirigir y coordinar la Administración Central y Descentralizada. Esta función de coordinación en el caso del MICITT se especifica en el Decreto Ejecutivo n.° 37052-MICITT, en el que se crea al CSIRT-CR con el fin de 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.

2.44. La situación descrita obedece a que la planificación del MICITT se ha centrado en atender la necesidades en el marco del estado de emergencia, principalmente a través de los planes de inversión, pero se ha dado poco énfasis en la necesaria transición de la gestión pública para gestionar la ciberseguridad como parte de las actividades ordinarias.

2.45. Al no haber garantía de la continuidad en las acciones para la gestión de la ciberseguridad en el sector público, se incurre en el riesgo de que una vez terminado el estado de la emergencia, se reproduzcan las vulnerabilidades en las infraestructuras tecnológicas que durante el 2022 limitaron la continuidad de los servicios públicos y el resguardo seguro de la información.

[7] Informe n.° DFOE-CAP-SGP-00003-2022, Seguridad de la información: Nivel de aplicación de prácticas en las instituciones públicas.

3. Conclusiones

3.1. Las acciones efectuadas por el MICITT y la CNE para la gestión de incidentes de ciberseguridad, tanto en el marco del estado de emergencia como en las actividades ordinarias a través del CSIRT-CR, cumplen parcialmente con lo establecido en el marco jurídico y técnico aplicable. Como parte de las acciones de cumplimiento destaca la aprobación del Plan General de la Emergencia y los respectivos planes de inversión, los cuales permitieron mejorar la capacidad del CSIRT-CR en términos de recursos humanos y tecnológicos adicionales para gestionar incidentes de ciberseguridad en el plazo del estado de emergencia. Además se presentan avances significativos en la formulación de la Estrategia Nacional de Ciberseguridad 2022-2027, la cual aún se encuentra en borrador.

3.2. No obstante, persisten debilidades que en el contexto del estado de emergencia de ciberseguridad se centran en la articulación entre MICITT y CNE, así como en la gestión de incidentes de ciberseguridad, la cual no se realiza de forma oportuna. Además, de cara a la consolidación de un marco de gobernanza en ciberseguridad, se determinó que el modelo de gestión del CSIRT-CR no responde a las necesidades actuales en la materia.

3.3. Bajo el entendimiento de que la gobernanza incluye la forma cómo surgen, operan y se dirigen las redes de coordinación entre los diferentes actores involucrados en la solución de problemas públicos, el país se encuentra ante un marco de gobernanza de ciberseguridad influenciado temporalmente por el estado de emergencia que se decretó para atender los ciberataques recibidos durante el 2022 en las instituciones públicas. Aún así, debe prevalecer un enfoque preventivo que permita una adecuada transición hacia la gestión de la ciberseguridad como parte de las actividades ordinarias de la gestión pública, a efecto de no reproducir las vulnerabilidades que se han evidenciado en la actualidad.

3.4. Como parte de los desafíos existentes, resulta indispensable consolidar un marco normativo que responda a las necesidades actuales y futuras en ciberseguridad, lo cual puede visualizarse desde dos vertientes principales. En primer lugar, el fortalecimiento del modelo de gobernanza en ciberseguridad, en el cual la posible ocurrencia de incidentes deba ser gestionada como parte de las actividades ordinarias de la Administración Pública, y no bajo el amparo de un entorno de estado de emergencia; y como segundo punto, la definición clara y formal de funciones, roles y responsabilidades, tanto del CSIRT-CR como ente coordinador y su articulación con las demás partes interesadas en el sector público.

4. Disposiciones

4.1. De conformidad con las competencias asignadas en los artículos 183 y 184 de la Constitución Política, los artículos 12 y 21 de la Ley Orgánica de la Contraloría General de la República, n.° 7428, y el artículo 12 inciso c) de la Ley General de Control Interno, se emiten las siguientes disposiciones, las cuales son de acatamiento obligatorio y deberán ser cumplidas dentro del plazo (o en el término) conferido para ello, por lo que su incumplimiento no justificado constituye causal de responsabilidad.

4.2. Para la atención de las disposiciones incorporadas en este informe deberán observarse los "Lineamientos generales para el cumplimiento de las disposiciones y recomendaciones emitidas por la Contraloría General de la República en sus informes de auditoría", emitidos mediante resolución n.° R-DC-144-2015, publicados en La Gaceta n.° 242 del 14 de diciembre del 2015, los cuales entraron en vigencia desde el 4 de enero de 2016.

4.3. Este órgano contralor se reserva la posibilidad de verificar, por los medios que considere pertinentes, la efectiva implementación de las disposiciones emitidas, así como de valorar el establecimiento de las responsabilidades que correspondan, en caso de incumplimiento injustificado de tales disposiciones.

A ALEJANDRO JOSÉ PICADO EDUARTE EN SU CALIDAD DE PRESIDENTE EJECUTIVO DE LA COMISIÓN NACIONAL DE PREVENCIÓN DE RIESGOS Y ATENCIÓN DE EMERGENCIAS Y A CARLOS ENRIQUE ALVARADO BRICEÑO EN SU CALIDAD DE MINISTRO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES O A QUIENES EN SU LUGAR OCUPEN LOS CARGOS

4.4. Establecer, formalizar e implementar de forma conjunta, ya sea para la Sala de Análisis de Situación Nacional o el mecanismo de coordinación interinstitucional que en adelante se determine, los objetivos, funciones, roles, responsabilidades, periodicidad de la coordinación, así como estrategia de ejecución de decisiones y su seguimiento, a fin de propiciar desde el nivel estratégico y operativo un trabajo proactivo por parte de las instituciones involucradas en la atención del estado de emergencia declarado mediante Decreto Ejecutivo n.° 43542. Remitir a la Contraloría General, a más tardar el 28 de abril de 2023, una certificación que acredite la elaboración y formalización de lo solicitado y al 31 de julio de 2023 un informe de avance de su implementación. (ver párrafos del 2.5 al 2.12).

A CARLOS ENRIQUE ALVARADO BRICEÑO EN SU CALIDAD DE MINISTRO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.5. Reformar, formalizar e implementar el marco normativo que regula el CSIRT-CR de manera que su modelo de gestión en materia de ciberseguridad incorpore al menos los roles y responsabilidades a lo largo del ciclo de la ciberseguridad, en las etapas de identificar, proteger, detectar, responder y recuperar. Remitir a la Contraloría General una certificación que acredite la reforma y formalización del marco normativo, a más tardar el 31 de agosto de 2023, así como un informe de avance de su implementación a más tardar el 30 de noviembre de 2023 (ver párrafos del 2.25 al 2.36).

4.6. Elaborar, formalizar e implementar un mecanismo en el que se incorporen las acciones requeridas por parte del MICITT para efectuar una transición de cara a la cesación del estado de emergencia declarado mediante el Decreto Ejecutivo n.° 43542, de tal forma que la gestión de incidentes de ciberseguridad pueda ser llevada a cabo como parte de las actividades ordinarias de la Administración Pública y el CSIRT-CR. Remitir a la Contraloría General una certificación que acredite la elaboración y formalización del mecanismo, a más tardar el 31 de julio de 2023, así como un informe de avance de su implementación a más tardar el 31 de octubre de 2023 (ver párrafos del 2.37 al 2.45).

A PAULA BRENES RAMÍREZ, EN SU CALIDAD DE DIRECTORA DE GOBERNANZA DIGITAL O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.7. Actualizar, formalizar e implementar procedimientos que permitan gestionar oportunamente los incidentes de ciberseguridad en el sector público, en los cuales se consideren al menos los criterios de actuación, actividades, roles, responsables, plazos estimados, nivel de criticidad de los incidentes, mecanismos de control, coordinación y seguimiento, así como los mecanismos utilizados para recopilar la información de manera estandarizada y ágil. Incluir como parte de los procedimientos, la periodicidad, acciones y el tipo de monitoreo que se deben realizar para la detección de incidentes, según la naturaleza de los incidentes que se puedan presentar. Remitir a la Contraloría General una certificación que acredite la elaboración y formalización de los procedimientos a más tardar el 31 de marzo de 2023, y una certificación mediante la cual se haga constar su respectiva implementación, a más tardar el 30 de junio de 2023 (ver párrafos del 2.13 al 2.24).

Firmado digitalmente por CAROLINA RETANA VALVERDE
Fecha: 2022-12-20 16:35

Licda. Carolina Retana Valverde
Gerente de Área

Firmado digitalmente por LIA MARIA BARRANTES LEON
Fecha: 2022-12-20 16:26

Licda. Lía Barrantes León
Asistente Técnico

CONTRALORIA GENERAL DE LA REPUBLICA
COSTA RICA

Firmado digitalmente por JOSE ROBERTO GONZALEZ CHAVES
Fecha: 2022-12-20 16:31

M.Sc. Jose Roberto González Chaves
Fiscalizador Asociado

Firmado digitalmente por MARIA VIRGINIA CAJIAO JIMENEZ
Fecha: 2022-12-20 15:59

M.Sc. María Virginia Cajiao Jiménez
Fiscalizadora

JRGC/LBL/pmt
Ci.: Archivo auditoría