GOBIERNO DE LA REPÚBLICA DE COSTA RICA COMISIÓN NACIONAL DE PREVENCIÓN DE RIESGOS Y ATENCIÓN DE EMERGENCIAS

PLAN GENERAL DE LA EMERGENCIA

CIBERATAQUES

DECRETO EJECUTIVO DE EMERGENCIA N°43542-MP-MICITT

JUNIO, 2022

Contenido

PRESENTACIÓN

El presente Plan General de la Emergencia responde a la disposición del Poder Ejecutivo de declarar el estado de emergencia, bajo el Decreto Ejecutivo N°43542 – MP – MICITT, los ciberataques que han afectado a las instituciones públicas desde el mes de abril del presente año, cuando se detectó el primer caso en el Ministerio de Hacienda.

El documento se elabora a partir de la información aportada por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), como ente rector en la materia y por las nueve instituciones que han sido afectadas hasta la fecha en la que se elabora este Plan.

La Ley N°8488, en el artículo N°38, brinda a las instituciones dos meses para elaborar el informe oficial de los daños, por lo que una vez vencido ese plazo se procede a la redacción de este Plan, con el detalle total de los daños y las propuestas de inversión que deben ser objeto de atención. Concluida esta tarea, corresponde a la Comisión Nacional de Prevención de Riesgos y Atención de Emergencias (CNE) la redacción del Plan.

En este documento se hace la sustentación de causa del fenómeno generador de la emergencia, se presenta la información de las acciones y las obras o acciones que proponen las instituciones para atender la emergencia, organizadas según las fases de primera respuesta, rehabilitación y reconstrucción, conforme lo dicta el artículo 30 de la mencionada Ley.

La aprobación y el control de ejecución del presente plan es una responsabilidad de la CNE, para lo cual le corresponde nombrar unidades ejecutoras a las instituciones afines a las competencias que se requieren para desarrollar las acciones que aquí se establecen.

1. BASE JURÍDICA

El presente Plan General de la Emergencia se elabora para la atención de la emergencia, por el Decreto N°43542 – MP – MICITT, del 11 de mayo del año 2022. El decreto se emite con fundamento en los artículos 140, incisos 3) y 18), 146 y 180 de la Constitución Política de Costa Rica, artículos 25 inciso 1), 27 inciso 1), 28 inciso 2), acápites b) y j) de la Ley Nº6227 del 2 de mayo de 1978, Ley General de la Administración Pública, la Ley Nº8488 del 11 de enero del 2006, Ley Nacional de Emergencias y Prevención del Riesgo, y la Ley Nº7169, Ley de Promoción del Desarrollo Científico y Tecnológico y Creación del MICIT.

Con la declaratoria del estado de emergencia entra en aplicación la condición de excepcionalidad que prevé el artículo 180 de la Constitución Política de Costa Rica para facilitar la disponibilidad de los recursos y los actos administrativos necesarios para atender la emergencia.

Dicho régimen de excepción está regulado por la Ley N°8488 que establece la competencia de conducción de las acciones por parte de la Comisión Nacional de Prevención de Riesgos y Atención de Emergencias (CNE). Igualmente, establece que, una vez firmado el decreto de declaratoria del estado de emergencia, con base en los reportes oficiales de los daños de todas las instituciones, la CNE debe elaborar el Plan General de la Emergencia, documento que brinda la explicación causal del evento generador de la emergencia, la estimación de los daños y pérdidas, la definición de las acciones, las obras necesarias para su atención, así como la estimación de los recursos.

Este Plan debe ser aprobado por la Junta Directiva de la CNE y su ejecución se realiza por medio de las instituciones públicas con competencia en cada uno de los conceptos incluidos, mismas que actúan como unidades ejecutoras de dicho plan. La organización de las acciones que se incluyen en el Plan se desarrolla en un mínimo de tres fases de atención: respuesta, rehabilitación y reconstrucción.

La ley también crea el Fondo Nacional de Emergencia que está bajo la administración de la CNE. A este fondo deben transferirse todos los recursos que van a ser usados bajo el régimen de excepción. No obstante, las instituciones pueden también desarrollar acciones bajo su propio presupuesto, pero sin aplicar el régimen de excepción aquí indicado. Todas las acciones y recursos empleados quedan bajo fiscalización de la CNE, que elabora informes periódicos de seguimiento y una vez concluida la ejecución del Plan, recomienda al Poder Ejecutivo emitir el decreto de cese del estado de emergencia. El tiempo máximo de ejecución del Plan, de acuerdo con la Ley, es de cinco años.

2. OBJETIVO

Desarrollar las acciones, obras y servicios necesarios para contener, solucionar y prevenir nuevos ataques en contra de los Sistemas de Información del Estado Costarricense, en específico de las instituciones que recibieron el ataque cibernético.

3. CARACTERÍSTICAS DE LA AMENAZA[1]

Con la aparición de internet y el desarrollo de los sistemas informáticos existe un nuevo espacio de interacción entre personas denominado “ciberespacio”, donde los roles de los diferentes agentes se construyen, evolucionan y cambian día a día” (Alonso García 2015, 18). En este espacio se comienzan a evidenciar los comportamientos delictivos en torno las herramientas y las operaciones cibernéticas, convirtiéndose estos en nuevas amenazas, denominadas de ciberdelincuencia y ciberterrorismo. Respecto al tema que corresponde al presente decreto, interesa entender y caracterizar la amenaza de ciberdelincuencia.

En la evolución y el crecimiento de los sistemas cibernéticos, los llamados ciberdelincuentes desarrollan técnicas y métodos para vulnerar los sistemas de seguridad, en algunos casos con mayor ventaja que las autoridades de Gobierno y dueños de empresas, con escasa preparación y conocimiento para atender el nuevo problema.

Los términos “cibercrimen”, “ciberdelito” o “ciberdelincuencia” describen de forma genérica la diversidad de ilícitos cometidos en el ciberespacio, los cuales tienen cuatro características específicas: “se cometen fácilmente; requieren escasos recursos en relación al perjuicio que causan; pueden cometerse en una jurisdicción sin estar físicamente presente en el territorio sometido a la misma; y se benefician de lagunas de punibilidad que pueden existir en determinados Estados, los cuales han sido denominados paraísos cibernéticos, debido a su nula voluntad política de tipificar y sancionar estas conductas” (Subijana Zunzunegui 2008, 171).

Entre los delitos de la ciberdelincuencia mejor tipificados están: el fraude, el robo, el chantaje, la falsificación y la malversación de caudales públicos. Más recientemente y en el contexto de diversos países, se están sumando figuras legales de otros tipos de delitos que también emplean las tecnologías de información y comunicación, tales como: el acoso electrónico, el descubrimiento y revelación de secretos, la interferencia ilegal de información o datos, los delitos contra la propiedad intelectual y los abusos con fines sexuales a través de internet u otros medios de telecomunicación a menores,

En el contexto de análisis actual de la delincuencia se afirma que esta naturaleza de delitos va en aumento y se tiene claro que por extremas que sean las medidas de seguridad que se adoptan, los sistemas informáticos siempre tendrán un punto débil por donde atacarlos, siendo cada vez más sofisticadas las herramientas y técnicas que tienen los delincuentes para ello. En tal sentido, se indica, la “inmunidad o blindaje” será siempre una aspiración y la seguridad completa no existe.

[1] El presente contenido se elabora con base en el artículo “Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad”, URVIO, Revista Latinoamericana de Estudios de Seguridad, núm. 20, pp. 80-93, 2017, Facultad Latinoamericana de Ciencias Sociales (FLACSO)

“Se estima que la industria del crimen cibernético vale más de 700 billones de dólares, aunque hay quienes dicen que su valor llega a rondar arriba de un trillón de dólares”. [2]

The Global Risks Report 2022 del World Economic Forum señala que para el 2020 se tuvo al nivel mundial un incremento del 435% en ransomware, además que el 95% de los problemas en ciberseguridad se debieron a factores humanos,

Fortinet señala[3] que las violaciones de datos resultaron en la exposición de 36 mil millones de registros en los primeros tres trimestres de 2020. El uso de malware aumentó un 358 % hasta 2020. Solo en julio del año 2020 se registró un aumento del 653 % en la actividad maliciosa, en comparación con el mismo mes del año 2019. Más del 90 % de las organizaciones de atención médica sufrieron al menos una brecha de ciberseguridad en los tres años anteriores, según el informe U.S. Healthcare Cybersecurity Market 2020.

Además, señalan que el delito cibernético le cuesta a las organizaciones $2.9 millones cada minuto, y las principales empresas pierden $25 por minuto como resultado de las filtraciones de datos, según la investigación de RiskIQ. Una investigación de IBM indique que se necesitan 280 días para encontrar y contener el ataque cibernético promedio, mientras que el ataque promedio cuesta $ 3,86 millones. El mercado global de ciberseguridad tendrá un valor de $ 403 mil millones para el año 2027, con una tasa de crecimiento anual compuesto (CAGR) del 12,5%, según Brand Essence Research. La firma señala que el mercado de la ciberseguridad tenía un valor de $ 176.5 mil millones en el año 2020. Los Estados Unidos tiene los costos de violación de datos más altos del mundo, con un costo promedio de ataque de $ 8.6 millones, según el informe “Costo de una violación de datos de IBM”.

De tal modo, el riesgo cibernético está presente siempre a pesar de políticas robustas en materia de seguridad y por su impacto tiene implicaciones en la dimensión económica, lo que teóricamente define a la actividad de la informática y la comunicación de datos (telemática) como parte de la “inteligencia económica, como el conjunto de acciones coordinadas de investigación, tratamiento y distribución de la información para tomar decisiones en el orden económico” (Olier Arenas 2013, 9). Las acciones de está naturaleza ocurren en el ámbito de economía nacional, en el ámbito de grandes negocios, pero también al nivel de sectores empresariales pequeños, dada la globalización, encadenamiento de los mercados y en ello, el uso de redes informáticas que además vinculan lo público con lo privado para la comunicación y las transacciones.

---

[2] Perspectivas Amenazas cibernéticas, Un peligro en constante evolución. Tomado de: https://www2.deloitte.com/ mx/es/pages/dnoticias/articles/amenazas-ciberneticas-peligro-en-constante-evolucion.html).

[3] Top Cybersecurity Statistics, Facts, and Figures for 2021 (fortinet.com). Tomando de: https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics

De acuerdo con Urueña Centeno (2015, 4-5) y el último informe de la Agencia europea para la Seguridad de las Redes y de la Información (ENISA), los instrumentos o técnicas que se utilizan para los ciberataques pueden hacer referencia a las quince amenazas más relevantes: Malware; ataques basados en el uso de la web; ataques basados en aplicaciones web; denegación de servicio; botnets; phishing; correo basura (spam); ransomware; amenaza interna; daños físicos, robos o pérdidas; kit de explotación de vulnerabilidades; violación de datos; robo de identidad; fuga de información; y ciberespionaje.

Sin dejar de tener presente que los delincuentes pueden hacer uso de cualquiera de estos instrumento o técnicas para atacar a personas, empresas e instituciones del país, el evento de ciberataque al que responde el presente decreto de emergencia está asociado al uso del ransomware. Este instrumento es un software malicioso que infecta y le da al atacante la posibilidad de bloquear el equipo informático y controlar los datos.

Se menciona que los ataques relacionados con este tipo de herramientas, que generalmente provienen de fuente externa, en muchas ocasiones operan con apoyo de agentes internos; se trata de una persona o agente, normalmente empleado o funcionario de una institución o empresa que tiene acceso a los programas informáticos de la organización para causar un incidente grave de seguridad. Estos constituyen parte de vulnerabilidad de los sistemas, una condición interna que hace más complejo el tratamiento del problema.

La posibilidad de robo o pérdida de material sensible es considerada como parte del riesgo que afecta la fuga de datos y robos de identidad. Si se tiene un conocimiento y habilidades especiales, se puede desarrollar un kit de explotación de vulnerabilidades de seguridad para tener una posición dominante sobre los competidores tanto económicos como institucionales; esas habilidades pueden proporcionar una brecha o violación de datos de carácter confidencial, robar la identidad, violar los datos correspondientes a registros personales, o realizar operaciones de espionaje cibernético a gran escala.

Un aspecto importante es considerar que los ciberataques son una expresión poderosa de desestabilización que presenta límites muy difusos entre delincuencia ordinaria y terrorismo, considerándose hoy como “la estrategia de guerra más poderosa” (Urueña Centeno 2015). De tal modo, incidentes que en apariencia son aislados y con un propósito delictivo inmediato, en su sumatoria y finalidad pueden tener un origen y una repercusión política más allá de la extorsión económica o del riesgo reputacional, lo que demanda un abordaje desde la perspectiva de la seguridad nacional. El análisis de las ciber amenazas en la perspectiva del terrorismo y de los actos de guerra, permite observar que las consecuencias más significativas de este tipo de delitos son efectivamente económicas y de imagen, pero no omite el impacto que tiene sobre los elementos sensibles de contenido de la información que se manipula, con riesgo del patrimonio y la vida de las personas.

A raíz de esto, el Consejo de Europa, en su convenio sobre la ciberdelincuencia promulgado el 23 de noviembre de 2001 en Budapest, engloba las actuaciones de ciberdelincuencia y tipifican las diversas actividades realizadas en el ciberespacio, dirigidas a diversos objetivos, que por su naturaleza pueden ser constitutivos de delito. Entre estas, se pueden citar: delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos (acceso ilícito, interceptación ilícita, interferencia en datos, interferencia en el sistema y abuso de dispositivos); delitos informáticos (falsificación informática o fraude informático); delitos relacionados con el contenido (pornografía infantil: producción, puesta a disposición, difusión, adquisición o posesión de la misma por medio de un sistema informático); y delitos relacionados con infracciones de propiedad intelectual y de derechos afines.

> ***"No existe un remedio fácil contra los ciberataques y el delito cibernético. Las características de apertura, alcance global e innovación sin permiso son fundamentales para el éxito de Internet. Sin embargo, estas mismas características hacen que sea más fácil y barato lanzar un ciberataque. Esto sin duda representa un desafío formidable para el futuro."***[4]

Adicional a lo anterior, la escasez mundial de talento cualificado en ciberseguridad agrava la tarea ya difícil de proteger contra el volumen creciente de amenazas avanzadas y sofisticadas; el CSIS (del inglés, Center for Strategic and International Studies, Centro de estudios estratégicos e internacionales) ha demostrado esto mediante un estudio para cuantificar la escasez de profesionales especializados en ciberseguridad en ocho países (Alemania, Australia, Estados Unidos, Francia, Israel, Japón, México y Reino Unido), para ello, han encuestado a los responsables de la toma de decisiones (TI), tanto del sector público como del sector privado, en relación con cuatro áreas clave del desarrollo de la plantilla en el ámbito de la ciberseguridad: gasto en seguridad, programas de formación, estrategias del empleador y políticas públicas. (McAfee, 2016)[5]

[4] Intenet Society: Las Amenazas Cibernéticas. Tomado de: https://future.internetsociety.org/2017/es/introduction-drivers-of-change-areas-of-impact/drivers-of-change/las-amenazas-ciberneticas/

5 La escasez de talento en ciberseguridad. Tomado de: https://www.mcafee.com/enterprise/es-mx/assets/executive-summaries/es-hacking-skills-shortage.pdf

4. DESCRIPCIÓN DEL EVENTO

De acuerdo con el informe del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), el ciberataque al Gobierno de Costa Rica es un ataque informático de índole extorsivo que se habría iniciado el domingo 17 de abril del 2022 en perjuicio de distintas instituciones públicas de la República de Costa Rica, incluido el Ministerio de Hacienda, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), el Instituto Meteorológico Nacional (IMN), la Radiográfica Costarricense Sociedad Anónima (RACSA), el Ministerio de Trabajo y Seguridad Social (MTSS), el Fondo de Desarrollo Social y Asignaciones Familiares (FODESAF) y la Junta Administrativa del Servicio Eléctrico Municipal de Cartago (JASEC), la Caja Costarricense del Seguro Social (CCSS).

El grupo de origen ruso Conti (también conocido como Wizard Spider, TrickBot, Ryuk, UNC1878 y Karakurt) se atribuyó el ciberataque (a excepción del caso de la CCSS que fue un incidente en sus redes sociales y en sus bases de datos que CONTI no se atribuyó) y solicitó un rescate de 10 millones de dólares estadounidenses a cambio de no liberar la información sustraída del Ministerio de Hacienda, la cual podría incluir información sensible como las declaraciones de impuestos de los ciudadanos y empresas que operan en Costa Rica.

Conti es una organización criminal de origen ruso dedicada a realizar ataques de ransomware por medio de la infección de equipos y servidores, sustrayendo archivos y documentos de servidores para luego exigir un rescate.

Conti es capaz de obtener acceso inicial sobre las redes de sus víctimas a través de distintas técnicas. Por ejemplo:

- Campañas de phishing especialmente dirigidas que contienen documentos adjuntos maliciosos (como un archivo Word) o enlaces. Estos adjuntos descargan malware como TrickBot, Bazar backdoor o incluso aplicaciones legítimas como Cobalt Strike que son utilizadas de forma maliciosa para realizar movimiento lateral dentro de la red de la víctima y luego descargar el ransomware.

- Explotación de vulnerabilidades conocidas sobre equipos que están expuestos a Internet.

- Ataques sobre equipos con el servicio de RDP (Protocolo de Escritorio Remoto) expuesto a Internet.

Todas las acciones realizadas por este grupo cibercriminal forman parte de un evento imprevisible que impidió el desarrollo de las labores habituales de servicios al público, de las instituciones del Estado involucradas, por medio de sus plataformas tecnológicas, siendo que las medidas existentes de ciberseguridad, ante las acciones de este grupo especializado de cibercrimen, hicieron inevitable la situación presentada. La Tabla 1, presenta las afectaciones reportadas al MICITT por las instituciones:

TABLA 1
Decreto de Emergencia N°43542 – MP - MICITT
Instituciones afectadas por los Ciberataques

INSTITUCIÓN	FECHA	INCIDENTE
Ministerio de Hacienda	17 de abril	• Exfiltración de información publicado sitio web del grupo cibercriminal CONTI • Cifrado de información • Afectación funcionalidad de sistemas informáticos
MICITT	18 de abril	• Defacement (modificación del sitio web) • Afectación de funcionalidad de sistemas informáticos
Instituto Meteorológico Nacional (IMN)		• Exfiltración de información publicado sitio web del grupo cibercriminal CONTI • Afectación de funcionalidad de sistemas informáticos
RACSA		• Exfiltración de información publicado sitio web del grupo cibercriminal CONTI • Afectación de funcionalidad de sistemas informáticos
Caja Costarricense del Seguro Social (CCSS)	20 de abril	• Robo de credenciales de RRSS • Ataque por medio de SQL inyección • Afectación de funcionalidad de sistema informático de Recursos Humanos de la CCSS • Exfiltración de información de una tabla con datos de bitácora, pero no datos sensibles
Ministerio de Trabajo y Seguridad Social (MTSS)	21 de abril	• Exfiltración de información publicado sitio web del grupo cibercriminal CONTI • Cifrado de información • Afectación funcionalidad de sistemas informáticos
Junta Administrativa del Servicio Eléctrico Municipal de Cartago (JASEC)	23 de abril	• Cifrado de información • Afectación funcionalidad de sistemas informáticos
Sede Interuniversitaria de Alajuela (SIUA)		• Exfiltración de información publicado sitio web del grupo cibercriminal CONTI • Afectación funcionalidad de sistemas informáticos
En las otras instituciones (Municipalidad de Golfito, Municipalidad de Turrialba, INDER, Municipalidad de Santa Bárbara, Municipalidad de Garabito, MEIC, Colegio Universitaria de Cartago, FANAL, Municipalidad de Alajuelita, CONAPE, Ministerio de Justicia y Paz) las medidas técnicas desplegadas logran detectar y contener el posible CONTI en sus sistemas.		

Fuente: MICITT, mayo, 2022.

En el caso del Ministerio de Hacienda y la Caja Costarricense del Seguro Social, el evento provocó que las plataformas digitales de estas instituciones fueran deshabilitadas por más de dos meses. Esta circunstancia generó una afectación directa en los usuarios de los servicios de estas instituciones, lo cual, considerando su relevancia en la prestación de servicios públicos, originó una grave afectación en toda la población nacional.

Podemos entonces decir que el estado resultante de estos ciberataques es la emergencia por el impacto inmediato que generó en los sistemas informáticos vinculados al funcionamiento de servicios críticos del Estado. Pero esto repercute también en una gran diversidad en la actividades económicas y sociales que afectan a toda la población, en donde se generan pérdidas por el encadenamiento con los servicios de Estado, en relación con temas como el comercio, la importación, la exportación, el pago de impuestos, la atención médica, en pago de servicios, entre otros; en una dimensión que de momento no puede ser estimada.

Si bien es afirmativo que existe una responsabilidad de prever y prevenir esta naturaleza de hechos mediante la aplicación de técnicas y la utilización de herramientas tecnológicas, en este caso estamos ante la presencia de una acción externa intencionada de la organización de ciberdelincuencia que generó una crisis de gran magnitud al nivel nacional, con repercusión significativa en la dinámica económica y social del país, en la prestación de servicios básicos y, en consecuencia, en el ejercicio de los derechos fundamentales de los habitantes y aún más allá de nuestras fronteras.

Por este motivo, más allá de la aplicación de técnicas y herramientas tecnológicas destinadas a la prevención de nuevos eventos, en la circunstancia actual impera la necesidad esencial de darle a estas técnicas y herramientas un uso destinado a la contención inmediata, consecuente un enfoque de respuesta que busca mitigar y evitar daños mayores, porque de no implementarse las medidas el impacto sería generalizado según reporte del MICITT. En tal sentido, las acciones que se vienen desarrollado desde la perspectiva de la contención y reactivación de los sistemas por parte de las instituciones afectadas ha sido la correcta porque contribuido a detener la propagación exponencial del evento hacia las demás instituciones gubernamentales, la empresa privada y la población en general.

Igualmente, se tiene presente que el evento de ciberataque al que alude esta declaratoria de emergencia tiene un primer episodio de materialización de daños que ha podido documentarse, pero es una situación en progreso, que implica mantener la alerta, la activación, así como la inminente necesidad de atender nuevos incidentes al amparo del estado de emergencia; esto resulta necesario hasta que las instituciones, vía el ejercicio ordinario de planificación y asignación de presupuesto, cuenten con la capacidad para atenderlo por sus propios medios; la medida tiene particular relevancia para el MICITT porque requiere el respaldo económico y operativo mientras genera condiciones óptimas para ejercer la labor de control y seguimiento a las amenaza relacionadas con le riesgo cibernético.

5. ACTIVACIÓN INSTITUCIONAL

La Dirección de Gobernanza Digital y el CSIRT-CR identificaron una publicación en la Dark Web, en el supuesto foro de publicaciones del Grupo CONTI. En dicha publicación se mencionaba que habían logrado tener acceso al Ministerio de Hacienda, por lo que se procedió a notificar al Ministerio de Hacienda para informar el incidente informático.

A partir de este evento el MICITT realiza el contacto con diversos países reconocidos en la atención de los ciberataques, entre ellos, España, Los Estados Unidos e Israel con la finalidad de recibir apoyo y asesoría

En el Consejo de Gobierno se expone la situación ante todos los jerarcas y se solicita aumentar los niveles de monitoreo y ciberseguridad de todas las instituciones. Adicionalmente, se crea la Sala de Situación Permanente de Alto Nivel con la finalidad de hacer el seguimiento a la emergencia; ésta sala quedó conformada por:

- Ministra de la Presidencia,
- Ministro de Hacienda,
- Ministro de Comunicación,
- Ministra de Ciencia, Innovación, Tecnología y Telecomunicaciones,
- Director y subdirector de inteligencia y Seguridad Nacional (DIS),
- Director de Gobernanza Digital (MICITT).

Posteriormente, el director de Gobernanza Digital del MICITT, junto con el coordinador del CSIRT-CR, con base en el Artículo 1 del Decreto Nº37052-MICIT, crearon un equipo de expertos en seguridad de tecnologías de información denominado “Equipo Técnico de Situación Nacional de Ciberseguridad”. El motivo de la creación de este grupo de trabajo es: “Identificar, gestionar y definir la ruta de implementación de las soluciones y cooperaciones en materia de ciberseguridad que el país ha recibido de diferentes países, agencias y empresas privadas, para lograr la mejor solución técnica posible ante esta situación nacional de ciberseguridad”. El equipo que mantenía reuniones permanentes se conformó de la siguiente manera:

- Banco de Costa Rica (BCR),
- Caja Costarricense del Seguro Social (CCSS),
- Comisión Nacional de Emergencias (CNE),
- Cybersec Cluster: En representación del sector privado,
- Dirección de Inteligencia y Seguridad Nacional (DIS),
- Instituto Costarricense de Electricidad (ICE),
- MICITT: director de Gobernanza Digital y el Coordinador del CSIRT-CR. Como coordinador del equipo,
- Organismo de Investigación Judicial (OIJ).

Se inicia un despliegue de instalación de una herramienta de protección perimetral en los ministerios, las infraestructuras críticas que no contaban con una protección de esta categoría y las instituciones descentralizadas del Estado costarricense, con el fin de crear una protección para poder identificar y contener cualquier amenaza en alguna otra institución pública.

En los días siguientes se realizan reuniones con el Viceministerio de Telecomunicaciones, la Dirección de Gobernanza Digital y el CSIRT-CR, con todos los operadores de internet y telecomunicaciones, para exponer la forma de trabajo del grupo cibercriminal “CONTI” y solicitar aumentar los niveles de monitoreo y seguridad en sus instituciones, así como la coordinación para la incorporación de indicadores de compromiso (IoC por sus siglas en inglés) para mitigar riesgos de instituciones públicas y el sector privado y otra reunión con el sector financiero del país, la Dirección de Gobernanza Digital y el CSIRT-CR para identificar posibles riegos en este sector, exponer la forma de trabajo del grupo cibercriminal “CONTI” y solicitar aumentar los niveles de monitoreo y seguridad en sus instituciones.

Adicionalmente, se crea un grupo de trabajo de análisis de información recolectada ante los diferentes eventos de ciberseguridad, conformado por:

- DIS,
- MICITT (Dirección de Gobernanza Digital y el CSIRT-CR),
- OIJ.

Luego de que el lunes 25 de abril el grupo de ciberdelincuentes realizara una publicación en su Blog en la Dark Web con una amenaza de hacia el sector empresarial de nuestro país, se realiza una convocatoria de alta prioridad con las principales cámaras empresariales, para explicar la situación nacional de ciberseguridad, el impacto de instituciones públicas hasta el momento y hacer un llamado para que todos sus miembros incrementen las medidas de monitoreo y de ciberseguridad, así como recomendaciones técnicas de las medidas por implementar a la brevedad posible. En esta reunión participaron:

- Cámara de Comercio de Costa Rica,
- Cámara de Industrias de Costa Rica,
- Cámara de Exportadores de Costa Rica,
- Asociación de Empresas de Zonas Francas de Costa Rica,
- Cámara Costarricense de Tecnologías de Información y Comunicación,
- Cámara de Info - Comunicación y Tecnología de Costa Rica,
- Cámara Costarricense de la Industria Alimentaria,
- Unión Costarricense de Cámaras y Asociaciones del Sector Empresarial Privado,
- Clúster de Ciberseguridad,
- Fedecámaras.

Además de estas acciones, se inicia el desarrollo de una propuesta de un “Protocolo para el desarrollo de acciones que se deben implementar ante una amenaza de un ataque a la ciberseguridad nacional”. Esta propuesta fue definida en el Equipo Técnico de Situación Nacional de Ciberseguridad y se creó un equipo de trabajo interinstitucional con participación de:

- CNE,
- CSIRT-CR del MICITT,
- ICE,
- Viceministerio de Telecomunicaciones del MICITT.

También el MICITT elaboró la Directriz N°133-MP-MICITT, aplicable a toda la administración pública, sobre la implementación de las medidas de seguridad que deben realizar de inmediato las instituciones para reforzar los mecanismos de seguridad.

Todas estas acciones se realizaron antes de que el Poder Ejecutivo decretara el estado de emergencia, mediante el Decreto N°43542-MP-MICITT. A raíz de este decreto y según las facultades que la Ley N°8488 le otorga a la CNE en la atención de emergencias declaradas, la CNE asume un rol más protagónico en la coordinación de las operaciones de emergencia.

Es así como, se establece por iniciativa de la CNE la Sala de Análisis de Situación Nacional (SASN), conformada por:

- Caja Costarricense del 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,
- Ministerio de Hacienda.

Al realizar las coordinaciones con el gobierno de España y el Centro Criptológico Nacional, este centro donó 100.000 licencias de microCLAUDIA para que fueran instaladas en las principales instituciones y equipos del país.

MicroCLAUDIA es una solución creada a partir del análisis de muestras de ransomware y de este análisis se desarrollan soluciones conocidas como vacunas que permiten detener la activación de las amenazas en los equipos cuando coincide con las condiciones registradas en la vacuna.

En los análisis realizados por el equipo de expertos españoles se desarrollaron varias vacunas para las variantes de ransonware que fueron puestas en nuestras infraestructuras.

Las actualizaciones de la herramienta se hacen por medio de conexión segura al sitio de microCLAUDIA en España y todas las instituciones tienen un acceso a una consola de administración para gestionar sus equipos y monitorear los mensajes que la herramienta les brinda.

A partir del momento en el que se comenzó la instalación e implementación de la herramienta y dentro del marco de la cooperación, el uso de microCLAUDIA en los equipos de usuario y servidores no tendrá costo por el período de un año; luego de eso deberá analizarse por parte de las instituciones la adquisición del software que permita la protección de los equipos. A continuación, se brinda el grado de avance de instalación del software en las instituciones del país:

TABLA 2
Decreto de Emergencia N°43542 – MP – MICITT
Avance de instalación del software microCLAUDIA, Al 06 de julio del 2022

Institución	Instalaciones
Comisión Nacional de Préstamos para la Educación (CONAPE)	121
CR Asamblea Legislativa	867
CR Autoridad Reguladora de los Servicios Públicos (ARESEP)	379
CR BANCO POPULAR	18
CR Caja Costarricense de Seguro Social (CCSS)	39206
CR Compañía Nacional de Fuerza y Luz (CNFL)	1866
CR Comisión Nacional de Prevención de Riesgos y Atención de Emergencias (CNE)	254
CR Agencia de Protección de Datos de los Habitantes (PRODHAB)	15
CR Comisión Reguladora de Turismo	24
CR Consejo de Seguridad Vial (CSV)	638
CR Consejo de Transporte Público (CTP)	114
CR Consejo Nacional de Concesiones (CNC)	2
CR Consejo Nacional de Investigaciones Científicas y Tecnológicas (CONICIT)	49
CR Consejo Nacional de Personas con Discapacidad (CONAPDIS)	112
CR Consejo Nacional de Vialidad (CONAVI)	409
CR Consejo Técnico de Aviación Civil (DGAC)	242
CR Contraloría General de la República (CGR)	720
CR Correos de Costa Rica	691
CR Cruz Roja Costarricense (CRC)	32
CR CSIRT del Poder Judicial	15449
CR Cuerpo de bomberos	96
CR Defensoría de los Habitantes de la República (DHR)	123
CR Dirección General de Migración y Extranjería (DGME)	607
CR Dirección General de Servicio Civil (DGSC)	189
CR Dirección General del Archivo Nacional (DGAN)	21

TABLA 2
Decreto de Emergencia N°43542 – MP – MICITT
Avance de instalación del software microCLAUDIA, Al 06 de julio del 2022

Institución	Instalaciones
CR Dirección Nacional de Desarrollo de la Comunidad (DINADECO)	93
CR Dirección Nacional de Notariado (DNN)	97
CR Empresa de Servicios Públicos de Heredia)	504
CR Fábrica Nacional de Licores (FNL)	14
CR Instituto Costarricense de Electricidad (ICE)	6954
CR Imprenta Nacional	102
CR Instituto Nacional de Desarrollo Rural (INDER)	658
CR Instituto Costarricense de Acueductos y Alcantarillados (AyA)	2745
CR Instituto Costarricense de Deporte y la Recreación (ICODER)	80
CR Instituto Costarricense de Ferrocarriles (INCOFER)	63
CR Instituto Costarricense de Investigación y Enseñanza en Nutrición y Salud (INCIENSA)	209
CR Instituto Costarricense de Pesca y Acuicultura (INCOPESCA)	169
CR Instituto Costarricense de Puertos del Pacífico (INCOP)	132
CR Instituto Costarricense de Turismo (ICT)	183
CR Instituto Costarricense Sobre Drogas (ICD)	138
CR Instituto de Fomento y Asesoría Municipal (IFAM)	177
CR Instituto del Café de Costa Rica (ICAFE)	180
CR Instituto Meteorológico Nacional (IMN)	120
CR Instituto Mixto de Ayuda Social (IMAS)	1109
CR Instituto Nacional de Aprendizaje (INA)	2923
CR Instituto Nacional de Estadística y Censos (INEC)	61
CR Instituto Nacional de Fomento Cooperativo (INFOCOOP)	77
CR Instituto Nacional de las Mujeres (INAMU)	369
CR Instituto Nacional de Seguros (INS)	3
CR Instituto Nacional de Vivienda y Urbanismo (INVU)	181
CR Instituto sobre Alcoholismo y Farmacodependencia (IAFA)	43
CR Junta Administrativa de Servicios Eléctricos de Cartago (JASEC)	199
CR Junta de Desarrollo Regional de la Zona Sur (JUDESUR)	1
CR Junta de Protección Social (JPS)	377
CR Laboratorio Costarricense de Metrología (LACOMET)	50
CR Consejo Nacional de Producción (CNP)	273
CR Junta de Administración Portuaria y de Desarrollo Económico de la Vertiente Atlántica (JAPDEVA)	142
CR Ministerio de Hacienda	2692
CR Ministerio de la Presidencia	269
CR Ministerio de Relaciones Exteriores	297

TABLA 2
Decreto de Emergencia N°43542 – MP – MICITT
Avance de instalación del software microCLAUDIA, Al 06 de julio del 2022

Institución	Instalaciones
CR Municipalidad de Turrialba	65
CR Ministerio de Economía y Comercio (MEIC)	287
CR Ministerio de Ciencia, Tecnología y Telecomunicaciones	177
CR Ministerio de Agricultura y Ganadería (MAG)	640
CR Ministerio de Ambiente y Energía (MINAE)	385
CR Ministerio de Comercio Exterior (COMEX)	134
CR Ministerio de Cultura y Juventud (MCJ)	26
CR Ministerio de Educación Pública (MEP)	3602
CR Ministerio de Gobernación y Policía	58
CR Ministerio de Justicia y Paz	1693
CR Ministerio de Obras Públicas y Transportes (MOPT)	1617
CR Ministerio de Planificación Nacional y Política Económica (MIDEPLAN)	218
CR Ministerio de Salud (MS)	1954
CR Ministerio de Seguridad Pública (MSP)	2652
CR Ministerio de Vivienda y Asentamientos Humanos (MIVAH)	152
CR Ministerio de Trabajo y Seguridad Social	613
CR Municipalidad de Abangares	34
CR Municipalidad de Alajuela	363
CR Municipalidad de Bagaces	5
CR Municipalidad de Buenos Aires	46
CR Municipalidad de Cartago	367
CR Municipalidad de Curridabat	131
CR Municipalidad de El Guarco	1
CR Municipalidad de Escazú	242
CR Municipalidad de Esparza	85
CR Municipalidad de Garabito	92
CR Municipalidad de Golfito	52
CR Municipalidad de Grecia	6
CR Municipalidad de La Unión	81
CR Municipalidad de Orotina	36
CR Municipalidad de Osa	6
CR Municipalidad de Paraíso	108
CR Municipalidad de Pococí	80
CR Municipalidad de Puntarenas	115
CR Municipalidad de Pérez Zeledón	1
CR Municipalidad de San José	844

TABLA 2
Decreto de Emergencia N°43542 – MP – MICITT
Avance de instalación del software microCLAUDIA, Al 06 de julio del 2022

Institución	Instalaciones
CR Municipalidad de San Rafael	7
CR Municipalidad de San Ramón	91
CR Municipalidad de Santa Cruz	54
CR Municipalidad de Santo Domingo	82
CR Municipalidad de Siquirres	39
CR Municipalidad de Tibás	84
CR Observatorio Vulcanológico y Sismológico de Costa Rica (OVSICORI)	37
CR Patronato Nacional de Infancia (PANI)	1519
CR Procuraduría General de la República (PGR)	386
CR Promotora del Comercio Exterior de Costa Rica (PROCOMER)	332
CR Radiográfica Costarricense, Sociedad Anónima (RACSA	661
CR Refinadora Costarricense de Petróleo (RECOPE	1796
CR Secretaría Técnica Nacional Ambiental (SETENA)	106
CR Servicio de emergencias 911	23
CR Servicio Fitosanitario del Estado (SFE)	245
CR Servicio Nacional de Salud Animal (SENASA)	146
CR Sistema Nacional de Bibliotecas (SINABI)	86
CR Instituto Mixto de Ayuda Social (IMAS), Sistema Nacional de Información y Registro Único de Beneficiarios del Estado (SINIRUBE)	55
CR Sistema Nacional de Radio y Televisión S.A. (SINART)	139
CR Sistema Nacional de Áreas de Conservación (SINAC)	423
CR Superintendencia de Telecomunicaciones (SUTEL)	71
CR Teatro Nacional (TN)	32
CR Teatro Popular Mélico Salazar (TPMS)	65
CR Tribunal Aduanero Nacional (TAN)	16
CR Tribunal Registral Administrativo (TRA)	75
CR Unión Nacional de Gobiernos Locales (UNGL)	4
Financiamiento Forestal (FONAFIFO)	157
CR Junta Administrativa del Registro Nacional (RN)	1425
CR Municipalidad de Liberia	15
TOTAL	**109.067**

Fuente: CSIRT-CR, MICITT.

Dada la gran cantidad de licencias donadas, el Centro Cripológico Nacional de España recomendó la instalación del Centro de Detección y Mitigación de Ransomware de microCLAUDIA en Costa Rica, esta tarea la coordinará el CSIRT-CR.

A lo anterior, debe sumarse el aporte de la empresa CISCO de licencias para la herramienta CISCO Umbrela. Se trata de 182 licencias que han sido distribuidas a las instituciones, incluidas municipalidades, ministerios, instituciones autónomas y adscritas.

Umbrela es una plataforma abierta y en la nube que ofrece protección activa ante la ciberdelincuencia y se integra fácilmente con los recursos de seguridad ya existentes en la compañía, para hacer frente a todas las amenazas, actuales y futuras, al analizar y aprender de los patrones de actividad de Internet. Gracias a ello, descubre automáticamente la infraestructura empleada para un ataque y puede bloquear de forma proactiva cualquier amenaza, sin que se vean afectados sistemas o usuarios.

Con Umbrella, se detectan ataques de phishing o infecciones de malware, identifica más rápidamente los dispositivos infectados y evita su contagio. Para ello, emplea el sistema de nombres de dominio (DNS), en el que se basa Internet para la asignación de direcciones IP, y aprovecha este mecanismo para atraer tráfico a su plataforma y luego asegurarlo. Así, cuando Umbrella recibe una solicitud DNS, utiliza su inteligencia en amenazas de seguridad para determinar si la solicitud es segura, maliciosa o supone un riesgo, lo que significa que el dominio contiene materia infecciosa; algún tipo de malware. Y, según el resultado de esta inspección, la conexión se permite, o no. (Tomado de: https://www.clase10.com/cisco-umbrella-primera-linea-de-defensa-en-internet/).

6. FASES DE ATENCIÓN DE LA EMERGENCIA

Como lo establece la Ley Nacional de Emergencias y Prevención del Riesgo, la atención de las emergencias se ejecutará en tres fases: Respuesta, rehabilitación y reconstrucción. En esta emergencia se ha seguido este patrón de atención por lo que a continuación se brindará detalle de todas las acciones realizadas en las primeras dos fases y lo que se planifica para la tercera fase.

Es importante mencionar que esta emergencia tiene la característica particular de estar en proceso de manifestación, con incidentes de ciberataque que siguen ocurriendo sin que algunas instituciones cuenten recursos suficientes para su control; por lo tanto, la CNE seguirá recibiendo reportes de las instituciones sobre daños, vinculados a la información que genera el monitoreo del CSIRT – CR. La expectativa es que en el siguiente ejercicio presupuestario las instituciones cuentes con los recursos y la planificación necesaria para hacer frente a la amenaza de ataque cibernético.

6.1. RESPUESTA

La ley define esta fase como el período en el que se desarrollan acciones inmediatas a la ocurrencia de una emergencia; procuran el control de una situación, para salvaguardar obras y vidas, evitar daños mayores, y estabilizar el área de la región impactada directamente por la emergencia.

Al respecto, y en el contexto de una emergencia de origen cibernético, la institución que es impactada por algún ataque es la que responde de manera inmediata para contenerlo y evitar que se propague a más sistemas de la organización. En términos generales, las acciones son:

- Desconexión de equipos de la red para hacer las revisiones respectivas,
- Identificación del punto de entrada del virus,
- Revisión de los equipos,
- Revisión y segmentación de la red,
- Revisión de respaldos,
- Instalación de herramientas de seguridad.

Todas estas acciones se ejecutan de manera reactiva en el momento en que se identifica un ataque a los sistemas; las mismas corresponden a un protocolo común de los departamentos de tecnologías de información de las instituciones, por lo que no se incurre en gastos adicionales de manera directa en esta fase de primera respuesta.

6.2. REHABILITACIÓN:

Esta fase se describe como las acciones orientadas a restablecer las líneas vitales y cualquier acción que contribuya a la recuperación de la autosuficiencia y estabilidad de la población y del área afectada por una emergencia.

Al igual que la fase anterior, muchas de las acciones que se ejecutan en esta fase se han realizado de manera autónoma por parte de las instituciones afectadas; en algunos casos el impacto fue menor y se restablecieron los servicios sin mayor contratiempo, en otros casos, el daño ha provocado la suspensión de diversos servicios esenciales a la población y por varias semanas, estas instituciones son el Ministerio de Hacienda y la Caja Costarricense del Seguro Social.

Las principales acciones que se identifican en esta fase son:

- Adquisición de herramientas de seguridad,
- Actualización de aplicaciones,
- Recuperación de bases de datos,
- Sanitización de los equipos,
- Formateo, reinstalación y reconfiguración de los equipos.

En el caso del Ministerio de Hacienda, la institución solicitó apoyo a la CNE para la adquisición de dispositivos USB que permitieran reinstalar aplicativos a los equipos de usuarios finales del Ministerio de manera más rápida, debido a la gran cantidad de equipos que se debía configurar. La CNE gestionó la compra de 100 dispositivos de estos y fueron entregados de manera inmediata al Ministerio, el costo de esta adquisición fue de ₡ 917.500.

TABLA 3
Decreto de Emergencia N°43542 – MP – MICITT
Gastos en la Fase de Rehabilitación, Ministerio de Hacienda

Descripción / Objeto	Monto (en millones colones)
Atención contingente de Sistema de Información para el Control Aduanero TICA (Financiado por PROCOMER)	₡15 000 000,00
Contratación CR-MOF-292346-NC-DIR, para atender la emergencia en el proceso de sanitización (limpieza) de los servidores (Contratación de la Empresa DELL, Fondos del Banco Mundial. Contratación CR-MOF-292347-NC. DIR)	₡423 481 774,32
Contratación CR-MOF-292347-NC-DIR: para implementar la plataforma de Tesoro Digital en modalidad CLOUD (Contratación de la Empresa Profesionales en Software Prosoft S.A - Fondos del Banco Mundial. Contratación CR-MOF-292347-NC-DIR. Este servicio estará en forma permanente)	₡438 319 080,00
Contratación “Adquisición de servicios de productividad segura, servicios online en la nube, servicios de monitoreo y respuesta de seguridad, servicios en la nube Azure y horas de servicio para el Ministerio de Hacienda, por demanda” (Fondos propios mediante el 0432022000-0009100001 con el Consorcio de GBM)	₡203 279 963,44
Implementar pago contingente para Integra 1 y 2 (564,5 horas, Fondos propios mediante el contrato 0432019000100115-00, con la empresa Grupo Asesor)	₡23 124 403,80

Descripción / Objeto	Monto (en millones colones)
Implementar Integra 2 en la nube ((498,5 horas, mediante el contrato 0432019000100115-00, con la empresa Grupo AsesoR. este servicio estará en forma permanente.)	₡20 420 753,40
TOTAL	**₡1 123 625 974,96**

Fuente: Oficio DTIC-384-2022, Ministerio de Hacienda, Dirección de Tecnologías de la Información y Comunicaciones. 05 de julio, 2022

Por parte de la Caja Costarricense del Seguro Social, la institución ha respondido con sus propios recursos para esta fase de atención y los gastos son de aproximadamente ₡10 000 000 000. Los gastos son diversos y se detalla en el siguiente cuadro:

TABLA 4
Decreto de Emergencia N°43542 – MP – MICITT
Gastos en la Fase de Rehabilitación, Caja Costarricense del Seguro Social

Descripción / Objeto	Monto (en colones)
Compra Directa 2021CD-000004-0001101150 para la adquisición de: "Servicio de Mantenimiento Plataforma Lenovo y Sistemas de Almacenamiento V7000" (aplicaciónArt. 208 RLCA al mantenimiento correctivo).	Sin costo adicional
Licitación Pública 2017LN-000002-1150 "Solicitud de alta disponibilidad para soportarsistema Centralizado de Recaudación SICERE y APEX, BDADMIN, MDI, MISE,PORTALRH, SCBM, SICSM, SIGC, SIGES" (aplicación Art. 208 RLCA al mantenimiento correctivo).	Sin costo adicional
Herramienta de multifactor de autentificación	₡600 000,00
Solución para administración de cuentas privilegiadas – PAM.	₡500 000,00
Licenciamiento EDR (Detección y respuesta a seguridad de equipos de usuario final)	₡1 000 000,00
Licitación Pública 2018LN-000002-1150 Servicios Profesionales en SeguridadInformática (aplicación Art. 208 RLCA al servicio contratado).	₡100 000,00
Servicio de Optimización de Equipos para la Comunicación LAN/WAN.	₡220 000,00
Switches Data Center SDN – ACI.	₡50 000,00
Licencias de Office 365 para completar aseguramiento de los ambientes de usuariosfinal	₡2 210 000,00
Sistema de respaldo (Bóveda) digital para aseguramiento de los respaldos deinformación de la plataforma.	₡700 000,00
Unidad de respaldo a cinta.	₡50 000,00
Servicios de Fábrica para plataformas DELL/EMC.	₡1 382 000,00
Otras compras de emergencia en sitios locales como parte de las labores asociadas alrestablecimiento de los sistemas de TI institucionales.	₡3 188 000,00
Total (Millones de colones)	**₡10 000 000,00**

* Estimado preliminar, sujeto a múltiples ajustes dependiendo de la evolución de laemergencia).

Fuente: Oficio GG-DTIC-3032-2022

En suma, esta fase ha tenido un costo de ₡11 124 543 474,96, lo cual se desglosa de la siguiente manera, según fuente de financiamiento:

TABLA 5
Decreto de Emergencia N°43542 – MP – MICITT
Gastos en la Fase de Rehabilitación: Según fuente de financiamiento

Fuente de Financiamiento	Monto
Fondo Nacional de Emergencias	₡917 500,00
	₡1 123 625 974,96
Recursos propios	₡10 000 000 000,00
Total	**₡11 124 543 474,96**

Fuente: Oficio GG-DTIC-3032-2022 y oficio CNE-UTI-OF-091-2022

6.3. RECONSTRUCCIÓN

Esta fase consiste en la ejecución de medidas finales que procuran la recuperación del área afectada, la infraestructura y los sistemas de producción de bienes y servicios, entre otros. En general, son acciones que contribuyen a estabilizar las condiciones sociales, económicas y ambientales de las áreas afectadas por una emergencia.

En este sentido, las acciones que proponen las instituciones se orientan a reforzar los mecanismos de seguridad informática, mediante la adquisición de herramientas de protección, detección y alerta de virus como el ransomware, equipo para asegurar la información mediante respaldos y contratación de servicios para el restablecimiento de una página web afectada.

En la Tabla 6, siguiente, se brinda más información sobre las medidas finales a implementar, con el fin de proteger los sistemas informáticos y reactivar los afectados de manera segura. Debe observarse que estas medidas aplican a las instituciones directamente afectadas por el ataque y responden al mandato del artículo 30 de la Ley N°8488, que señalan la posibilidad de realizar las obras bajo un enfoque preventivo, orientado a proteger los sistemas.

TABLA 6
Decreto de Emergencia N°43542 – MP – MICITT
Fase de Reconstrucción: Propuestas de Acciones por Unidad Ejecutora

Institución	Propuesta de Acciones	Monto
Ministerio de Hacienda	Adquisición de herramientas tecnológicas que permitan realizar una analítica de la red, identificar y bloquear ataque de malware, ransomware y cualquier tipo de nueva amenaza de Internet o a nivel interno y que permita también poder tener visibilidad completa de la actividad de todos los usuarios (y del rastro dejado por sus dispositivos), para bloquear cualquier amenaza. Adquisición de servicios de productividad segura, servicios online en la nube, servicios de monitoreo y respuesta de seguridad, servicios en la nube Azure y horas de servicio para sanitización de equipos faltantes.	₡1 049 388 494,63

TABLA 6
Decreto de Emergencia N°43542 – MP – MICITT
Fase de Reconstrucción: Propuestas de Acciones por Unidad Ejecutora

Institución	Propuesta de Acciones	Monto
Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT)	Implementar un nuevo sitio web bajo una versión de plataforma actualizada y segura que minimice ser nuevamente blanco de ataque. Herramientas para la defensa de aplicaciones web en forma inteligente y automatizada y de protección de correo electrónico. Equipo de respaldo de información y equipo para labores del CSIRT-CR. Contratación de personal temporal (por emergencia) para reforzar la capacidad de respuesta del CSIRT-CR. Pago de licencias de microCLAUDIA al Centro Criptológico Nacional de España.	₡641 475 400,00
Instituto Meteorológico Nacional (IMN)	Renovación de las licencias de Antivirus, EDR. Renovación de las licencias de los 3 FireWall que tiene el IMN. Renovación del certificado digital. Renovación del licenciamiento del sistema de respaldo Institucional. Renovación del contrato de licenciamiento de nuestra Base de Datos Oracle. Renovación de licencia para el clúster, que contiene vCenter Service.	₡66 000 000
Ministerio de Trabajo y Seguridad Social (MTSS)	Adquisición de Plataforma SIEM XDR opción incluyendo HW Appliance, licenciamiento de Cortex de PaloAlto, Kaspersky EDR Expert (700) + KATA para servidores (50), Web Application Firewall (WAF) (Hasta 1 Gb/seg)	₡345 000 000
Junta Administrativa del Servicio Eléctrico Municipal de Cartago (JASEC)	Contratación de consultoría experta en medios de almacenamiento (SAN) NetApp que permita realizar los análisis y recuperación de los datos críticos. Adquisición de un equipo Firewall para detectar y controlar el tráfico de datos de entrada y salida, actualizar las licencias de Microsoft Windows 2007 y 2010 por licenciamiento Windows más actual, actualización de la licencia ORACLE y adquirir dos licencias de tipo Enterprise.	₡164 000 000
Sede Interuniversitaria de Alajuela (SIUA)	Se requiere la obtención de al menos un servidor físico para poder implementar una solución SIEM/EDR en la SIUA. Compra de un equipo firewall-ng que permita identificar ataques DDoS, DoS, exploits, malware, aplicaciones no deseadas, brinde protección de correo, entre otros, se necesitan al menos un equipo con inteligencia contra amenazas y emparejamiento de firmas, para garantizar la seguridad y el acceso a los servicios públicos y privados del dominio siua.ac.cr.	₡28 500 000
TOTAL		**₡2,294,363,894.63**

Fuente: Sistema de Reportes de Daños, Pérdidas y Propuestas de Atención por Declaratorias de Emergencia Nacional, 2022.

Todas estas acciones están planteadas para que se realicen en un plazo máximo de un año a partir de la aprobación del presente Plan. Es importante indicar que, aunque estas propuestas se encuentran en el Plan, no significa que se encuentran aprobados y que se

cuenta con recursos para desarrollarlas. Las mismas deberán ser objeto del trámite de elaboración y aprobación de los planes de inversión, que estarán sujetas a revisión por profesionales y al contenido de recursos que el Gobierno logre destinar a esta emergencia.

Igualmente, se reitera que las licencias como microCLAUDIA y Cisco Umbrela aportas por las empresas dueñas sin costo para las instituciones y que se han instalado para protección de los sistemas, tienen vigencia de un año, por lo que es importante que el MICITT mantenga la comunicación con las instituciones para que realicen las previsiones presupuestarias que les permita asumir los costos de la protección, sea con estas herramientas o cualquier otra que resulte oportuna.

7. RECURSOS FINANCIEROS

Mediante los reportes de las instituciones involucradas en esta emergencia, se logra determinar que el costo de atención directa de esta emergencia es de **₡13 418 907 369,59,** tanto con recursos propios de las instituciones como con recursos del Fondo Nacional de Emergencias (FNE), en todas las fases de atención de la emergencia. A continuación, la Tabla 7 muestra el detalle de inversión que se requiere:

TABLA 7
Decreto de Emergencia N°43542 – MP – MICITT
Recursos Financieros: Según fuente de financiamiento

Institución	Fondo Nacional de Emergencias	Recursos Propios de las Instituciones
Fase de Rehabilitación		
Caja Costarricense del Seguro Social	₡0,00	₡10 000 000 000,00
Ministerio de Hacienda	₡917 500,00	₡1 123 625 974,96
Fase de Reconstrucción		
Ministerio de Hacienda	₡1 049 388 494,63	0,00
Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT)	₡641 475 400,00	0,00
Instituto Meteorológico Nacional (IMN)	₡66 000 000,00	0,00
Ministerio de Trabajo y Seguridad Social (MTSS)	₡345 000 000,00	
Junta Administrativa del Servicio Eléctrico Municipal de Cartago (JASEC)	₡130 000 000,00	₡34.000.000,00
Sede Interuniversitaria de Alajuela (SIUA)	₡28 500 000,00	
SUBTOTAL	**₡2 261 281 394,63**	**₡11 157 625 974,96**
TOTAL	**₡13 418 907 369,59**	

Fuente: Sistema de Reportes de Daños, Pérdidas y Propuestas de Atención por Declaratorias de Emergencia Nacional, 2022.

8. ORIENTACIÓN PARA LA EJECUCIÓN DE LA FASE DE RECONSTRUCCIÓN

La fase de reconstrucción puede ser ejecutada con recursos propios de las instituciones, es decir, con el presupuesto institucional bajo los mecanismos ordinarios, así como con recursos del Fondo Nacional de Emergencias, que corresponde a la vía de excepción (prevista en el artículo 180 de la Constitución Política y regulada mediante la Ley N°8488).

8.1. VÍA ORDINARIA

Las acciones que desarrollen las instituciones por esta vía no quedan exentas del control presupuestario ordinario, sin embargo, en la medida que estén identificadas en el Plan, se favorece la aplicación de medidas de tramitación más ágiles que las normales, en el tanto la CNE sea capaz de certificar que están destinadas a atender la emergencia. La CNE ejerce un seguimiento al nivel de resultados de dichas acciones, diferente al control directo que corresponde en el caso de la vía de excepción.

8.2. VÍA DE EXCEPCIÓN

Conforme el dictado de la Ley corresponde a las acciones y obras que serán ejecutadas con recursos trasladados al Fondo Nacional de Emergencia (FNE), para lo cual la Junta Directiva de la CNE hará el nombramiento de unidades ejecutoras. Estas deberán ser instituciones públicas con competencia en cada una de las áreas de acción que se requieren para atender.

Las unidades ejecutoras deben preparar los planes de inversión con sustento en los contenidos de este plan. Los planes de inversión deben ser aprobados por la Junta Directiva de la CNE a efecto de asignarle los recursos y están sujetos al ejercicio de fiscalización de la CNE. No obstante, la asignación de tales recursos estará sujeta a la disponibilidad, según el aporte de recursos que esta declaratoria de emergencia reciba.

La CNE, en apego al mandato del Art. 39 de la Ley 8488 está facultada para confirmar en el sitio la veracidad de los datos, así como la consistencia técnica de las acciones y obras que se proponen, para determinar que guardan relación con el fenómeno generador y sus efectos.

Las unidades ejecutoras que la CNE nombre están supeditadas al Reglamento de Unidades Ejecutoras y en tal caso, es obligación del jerarca de la institución que opera como tal, manifestar por escrito que su institución cuenta con la capacidad para cumplir esta función. También debe designar a la persona o equipo encargada de actuar como responsable de los proyectos, con funciones de enlace con la CNE para la presentación de los planes de inversión y los procesos licitatorios, de inspecciones de proyectos, informes de avances, trámite de órdenes de modificación, finiquitos, entre otros que se le demanden.

9. INSUMOS PARA EL CONTROL, SEGUIMIENTO Y EVALUACIÓN

De conformidad con las potestades que confiere la Ley N°8488, la CNE tiene la responsabilidad de desarrollar el control sobre el desarrollo de las obras o acciones por medio de la fiscalización a las unidades ejecutoras y de los planes de inversión que la Junta Directiva apruebe. Igualmente, en tanto el plan esté vigente, existe la responsabilidad de presentar informes de seguimiento a la Junta Directiva, realizar las inclusiones y tomar las decisiones oportunas para garantizar el cumplimiento. Para esto, a lo interno de la CNE se tienen las siguientes competencias:

TABLA 8
Decreto de Emergencia N°43542 – MP – MICITT
Competencias para el control, seguimiento y evaluación del Plan General de la Emergencia

Unidad	Proceso
La Unidad de Gestión de Procesos de Reconstrucción	Realizar la asesoría para la presentación de los planes de inversión por parte de las unidades ejecutoras (Según el Reglamento de Unidades Ejecutoras) y generar los insumos de información necesarios para el control y posterior seguimiento.
Unidad de Recursos Financieros	Llevar el control de la asignación y ejecución de los recursos de dinero.
Unidad de Desarrollo Estratégico del Sistema Nacional de Gestión del Riesgo	De conformidad con los procedimientos existentes, debe elaborar los informes de seguimiento de manera periódica, basados en la información que generen las unidades antes mencionadas. Es con base en estos informes y criterios técnicos acerca del nexo de causa que la Junta Directiva puede considerar la aprobación de las inclusiones o ampliación del Plan General.

Fuente: DESNGR, CNE, 2022.

10. ADENDAS AL PLAN GENERAL DE LA EMERGENCIA

La información que sustenta este plan proviene de las instituciones con competencia en la administración de la infraestructura, servicios o actividades, delimitado por Ley, por lo que se considera que se han recibido datos ciertos y oficiales.

El Artículo 41 de la Ley N°8488 le da a la Junta Directiva de la CNE la potestad para decidir sobre medidas complementarias que deban incorporarse o de modificación de los planes, basado en los informes periódicos que la Dirección Ejecutiva debe rendir. Por ello, se tiene la oportunidad de incluir o modificar información sobre daños y pérdidas vinculados al evento del ciberataque, sea que respondan a omisión, error material, dificultades técnicas que no han permitido identificarlos y reportarlos a tiempo y en el caso de este decreto, que se trate de hechos del mismo origen que todavía no se manifiestan. En tal caso, si bien las medidas hasta ahora contempladas están consideradas para ejecutarlas en un año, deberá considerarse acciones o inversiones para mayor tiempo, debiendo observarse la pertinencia en función del nexo de causalidad y la urgencia de las acciones u obras por realizar. Las solicitudes para estos hechos deben contar con toda la información pertinente del caso que lo justifique y presentarse a la Dirección Ejecutiva de la CNE.

11. CONSIDERACIONES RESPECTO A LAS ACCIONES DE LARGO PLAZO Y ENFOQUE ESTRATÉGICO

El estado de emergencia establecido mediante el Decreto N°43542 – MP – MICITT permite aplicar el régimen de excepción y cierto margen de flexibilidad de disposiciones ordinarias para atender la emergencia provocada por los eventos de ciberataques contra instituciones del Estado Costarricense. Las acciones, tal y como queda evidente en el presente plan, se orientan atender los sistemas informáticos, rehabilitar los servicios públicos afectados, reforzar la seguridad de estos; todo bajo condiciones satisfactorias que aseguren la continuidad de estos servicios sin que se repita, hasta donde es posible, un evento de esta naturaleza.

Sin embargo, a la luz del daño ocurrido, se genera la expectativa de adoptar medidas que van más allá de atender los sistemas y servicios afectados. El marco de la atención de la emergencia el paso que se ha dado al respecto ha consistido en la adopción o actualización de protocolos de seguridad para actuar defensivamente en caso de que una amenaza se haga latente, por ejemplo, con el uso de herramientas destinadas a proteger, sea porque las instituciones ya cuentan con estas o porque accedieron a las licencias de microCLAUDIA, aportadas por la empresa española Centro Criptológico Nacional, considerada una vacuna que permiten detener la activación de las amenazas en los equipos, lo mismo que la herramienta CISCO Umbrela, aportadas por la empresa CISCO.

Pero la seguridad de los sistemas informáticos es un tema complejo que supera el alcance de las medidas de respuesta que la actual emergencia ha permitido. Este contexto de emergencia sirvió para que el MICITT, con el apoyo del ICE, aplicara un formulario de diagnóstico a 226 instituciones que pone en evidencia condiciones disímiles de seguridad cibernética, en aspectos como el uso de herramientas y técnica, protocolos, respaldos, asesoría técnica, personal especializado, capacitación, aplicación de auditorías, monitoreo, aplicación y actualización de políticas, regulaciones de acceso, entre los múltiples aspectos que involucran la seguridad de los sistemas informáticos. De manera general y a modo de resumen, los hallazgos señalan lo siguiente:

TABLA 9
Decreto de Emergencia N°43542 – MP – MICITT
Hallazgos respecto a los sistemas informáticos del sector público

Informe de diagnóstico del sector público MICITT-DGD-INF-009-2022	• 188 instituciones no cuentan con personal especializado en ciberseguridad que administren los sistemas. • 28 instituciones tienen sistemas desarrollados por terceros, pero no contemplan aspectos de seguridad. • 41 instituciones no realizan copias de seguridad de los sistemas que tienen alojados por un tercero. • De los sistemas que se encuentran administrados por terceros el 28.8% (65 instituciones) no cuentan con un registro de la actividad que realizan los administradores en sus sistemas. • Existen 38 instituciones que no han implementado sistemas de protección y seguridad DNS.

	• 104 (46%) instituciones no poseen sistemas de protección EDR • 43.8%, 99 instituciones no han implementado doble factor de autenticación en sus sistemas. • 38.9%, 88 instituciones tienen sistemas operativos fuera de soporte, sin embargo, ese número es mayor ya que muchas indicaron que solo tenían unos pocos equipos, por lo que el porcentaje aumenta a casi un 50%. • 94 (41.6%) instituciones no han realizado auditorías de seguridad en sus servidores • 51 instituciones no tienen políticas definidas para las copias de seguridad. • 38.1% (86) instituciones no realizan pruebas de restauración de copias de seguridad realizadas. • 16.4% (37) instituciones no tiene configurado el sitio para evitar ataques de tipo SQL injection. • 42.9% (97) instituciones no cuentan con servicios innecesarios activos como SSH, FTP, telnet. • 32.3% (73) instituciones no han configurado un límite de accesos concurrentes para evitar ataques de denegación de servicios DDoS

Fuente: MICITT, 2022.

Con esta evidencia se pone de manifiesto que la normativa aplicable al tema de la seguridad desarrollada en la forma de disposiciones, lineamientos y recomendaciones de organismos como la Contraloría General de la República o el MICITT o por organismos internacional expertos en esta materia, no han significado en las instituciones estatales un cumplimiento estandarizado y un desarrollo de capacidades suficientes y similares para enfrentar la amenaza de la ciberdelincuencia. De tal modo, un decreto de emergencia destinado a la adopción de medidas contingentes no es suficiente para hacer un cambio significativo en la seguridad de los sistemas informáticos del Estado, es requerida una estrategia con metas claras de mejora que sea base para una inversión suficiente para el desarrollo de capacidades en seguridad. En la perspectiva de gestión de riesgo, se trata de la adoptación de un enfoque totalmente preventivo en el desarrollo y operación de los sistemas informáticos para reducir la vulnerabilidad, las pérdidas asociadas, evitar la interrupción y asegurar la continuidad de los servicios públicos.

En el ámbito de clasificación de las amenazas tecnológicas, se considera el desarrollo cibernético y la informática como parte de los temas emergentes de la “complejidad del riesgo” y parte de los nuevos retos que dominan la gestión del riesgo. Del estudio del MICITT se pone de manifiesto que la atención de esta problemática implica un proceso de planificación estratégica que aborde al menos las siguientes medidas:

- La inversión en herramientas de seguridad,
- La inversión en personal especialista y en capacitación regular,
- El desarrollo o mejora de sistemas de respaldo,
- El diseño y elaboración de protocolos de seguridad,
- El aprovechamiento de los recursos cibernéticos con proyectos que incluyan adecuados estándares de seguridad para los usuarios y administradores, con rutinas de control y actualización, entre otros.

Estas acciones que deben iniciar siendo parte una estrategia de mediano y largo plazo puede ser construida con un abordaje participativo y consensuado y debe servir para insertar las posibles soluciones en la planificación y el presupuesto ordinario de las instituciones, adoptar la seguridad de la información y la comunicación como una prioridad, donde la evaluación oportuna del riesgo asociado a la telemática, la cibernética y la informática contribuya a la aplicación de las medidas oportunas para su gestión.

El hito generado por la presente emergencia, pone en vigencia los alcances del Decreto Ejecutivo N°37052-MICITT, con el cual se crea el Centro de Respuesta de Incidentes de Seguridad Informática CSIRT-CR. Dicho Centro tiene las facultades suficientes para coordinar con los poderes del Estado, instituciones autónomas, empresas y bancos del Estado todo lo relacionado con la materia de seguridad informática y cibernética y concretar el equipo de expertos en seguridad de las tecnologías de la información que debe trabajar para prevenir y responder ante los incidentes de seguridad cibernética e informática que afecten a las instituciones gubernamentales.

Así mismo, el Decreto Ejecutivo N°43580-MP-PLAN asigna al Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) la rectoría en el tema de Tecnología.

Por lo expuesto, el MICITT es responsable de brindar la orientación estratégica para el accionar en esta materia, de acuerdo con las necesidades, prioridades y visión del Gobierno. A la vez, el CSIRT – CR cuenta con el Consejo Director que tiene entre sus competencias el diseño de políticas, estrategias y acciones en materia de seguridad cibernética e informática, así como elaborar programas nacionales en materia de seguridad de tecnologías de la información y la comunicación; también la tarea de promover la implementación de políticas y estrategias de seguridad cibernética de las instituciones gubernamentales, tomando en cuenta los estándares internacionales. Este Consejo está conformado por representantes de las siguientes instituciones:

- Ministro(a) de Ciencia y Tecnología o su representante, que lo preside,
- Ministro(a) de la Presidencia o su representante,
- Ministro(a) de Seguridad Publica o su representante,
- Fiscal General de la República o su representante,
- Ministro(a) de Relaciones Exteriores o su representante,
- Ministro(a) de Justicia y Paz o su representante,
- Presidente(a) de la Academia Nacional de las Ciencias o su representante.

Actualmente, el MICITT y las instituciones vinculadas al CSIRT – CR están en el proceso de construcción de la Estrategia Nacional de Ciberseguridad 2022-2027, la cual plasmará un esfuerzo conjunto y articulado entre todos los sectores del país, para así garantizar que los objetivos que se establezcan sean equilibrados, eficaces y acordes a la realidad y necesidad nacional, definiendo los principios generales que marcarán la pauta en esta materia.

Otra iniciativa que el MICITT está promoviendo es robustecer la ciberseguridad en el país, mediante la creación de un Centro de Operaciones de Seguridad (SOC), el cual permita monitorear en horario 24/7 las infraestructuras del sector público, para detectar posibles amenazas, anomalías o intentos de intrusión o ataque, para que el país pueda brindar una respuesta inmediata y minimizar las posibles consecuencias.

Este SOC debe ofrecer los siguientes servicios en materia de ciberseguridad:

- Servicios de prevención y gestión,
- Servicios de auditoría continua,
- Cibervigilancia,
- Servicio antiDDos,
- Servicios de detección de intrusiones,
- Servicio antirasomware,
- Servicio de correlación de eventos de seguridad,
- Servicio de detección de fuga de información,
- Servicios de respuesta a incidentes,
- Servicios de ciberinteligencia,
- Servicios de comunicación de vulnerabilidades,
- Servicios de asesoramiento en cumplimiento en normativa de ciberseguridad,
- Servicios de asesoramiento en concientización y capacitación en ciberseguridad.

La solución sustantiva para el fortalecimiento de las condiciones de ciberseguridad nacional es la implementación de la herramienta SOC de carácter nacional, este SOC debe estar instalado en el MICITT. Para lo cual el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones planteará los requerimientos específicos en esta materia para su respectivo financiamiento por la vía ordinaria.

REFERENCIAS BIBLIOGRÁFICAS

C10, CISCO Umbrella, Primera Línea de Defensa en Internet. Tomado de: https://www.clase10.com/cisco-umbrella-primera-linea-de-defensa-en-internet/)

Costa Rica, Leyes y decretos. (2022, 11 de mayo). Decreto N° 43542–MP-MICITT. Declaratoria de Emergencia por Ciberataques. Publicado en el alcance 94 de la Gaceta 86. San José, C.R.

Costa Rica, Leyes y decretos. (2006, 11 de enero). Ley No. 8488: Ley Nacional de Emergencias y Prevención del Riesgo. San José, C.R.: La Gaceta, No. 8

FORTINET. Top Cybersecurity Statistics, Facts, and Figures for 2021 (fortinet.com). Tomando de: https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics

Intenet Society: Las Amenazas Cibernéticas. Tomado de: https://future.internetsociety.org/2017/es/introduction-drivers-of-change-areas-of-impact/drivers-of-change/las-amenazas-ciberneticas/

McAfee. La escasez de talento en ciberseguridad. Tomado de: https://www.mcafee.com/enterprise/es-mx/assets/executive-summaries/es-hacking-skills-shortage.pdf

Santiago Gutiérrez, (Socio de Ciberseguridad en Deloitte México) Entrevista. Perspectivas Amenazas cibernéticas, Un peligro en constante evolución. Tomado de: https://www2.deloitte.com/mx/es/pages/dnoticias/articles/amenazas-ciberneticas-peligro-en-constante-evolucion.html).

Vicente Pons Gamón “Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad”, URVIO, Revista Latinoamericana de Estudios de Seguridad, núm. 20, pp. 80-93, 2017, Facultad Latinoamericana de Ciencias Sociales (FLACSO).

ANEXO UNICO: Reporte de Afectaciones y Medidas de Atención