Protocolo para el desarrollo de las acciones que se deben implementar ante una amenaza de un ataque a la ciberseguridad nacional

Versión: **001**	Fecha de elaboración: **06-05-2022**

Elaborado por:

Instituto Costarricense de Electricidad (ICE).

- ***Rayner García Villalobos***; Gerencia de Transformación Tecnológica
- ***Alejandro Picado Eduarte***, Gestión de Emergencias, Servicios de Gestión al Personal, Servicios Generales, Gerencia Operaciones y Logística (GOyL).

Comisión Nacional de Prevención del Riesgo y Atención de Emergencias (CNE).

- ***Walter Fonseca Bonilla,*** Coordinador de Planes y Operaciones de la CNE.
- ***Wilgen Saborío Córdoba,*** Jefe Unidad de Tecnologías de Información de la CNE.

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT)

- ***Raquel Cantillo Gamboa***; CSIRT-CR, Dirección de Gobernanza Digital, MICITT.
- ***Elídier Moya Rodríguez***; Departamento de Redes de Telecomunicaciones, MICITT.

Revisado y Aprobado por:

- ***Ministro del MICITT***; Sr. Carlos Enrique Alvarado Briceño

CARLOS ENRIQUE ALVARADO BRICEÑO (FIRMA)
PERSONA FISICA, CPF-01-1228-0078.
Fecha declarada: 16/05/2022 11:11:34 AM
Esta representación visual no es fuente
de confianza. Valide siempre la firma.

ÍNDICE

Prólogo

La **DIRECTRIZ N° 133-MP-MICITT** emitida el día 21 de abril del 2022, menciona: Que existe un conjunto de amenazas concretas derivadas del uso malicioso de las tecnologías digitales y de sus limitaciones y vulnerabilidades intrínsecas, cuyo fin último es lesionar la integridad individual en favor del crimen cibernético, lo cual lleva al Estado, con el fin de definir de manera integral el concepto de bienestar social, a extender su soberanía al especio tecnológico mediante las herramientas jurídicas y tecnológicas necesarias para garantizar espacios seguros en este entorno.

En el marco de estas amenazas y de los ataques cibernéticos de los cuales nuestro país ha sido víctima en este año, surge la necesidad de elaborar este Protocolo con la finalidad de compilar las responsabilidades y acciones del ente rector a nivel nacional y de las instituciones públicas y privadas, así como aquellas relacionadas con la protección de la sociedad civil.

Este documento está sujeto a ser actualizado periódicamente con el objeto de que responda en todo momento a las necesidades del país en esta materia.

1. OBJETIVO Y CAMPO DE APLICACIÓN

El objetivo del presente documento es que Costa Rica cuente con un Protocolo de nivel nacional que defina las acciones que se deben implementar en el nivel nacional, ante una amenaza de ataque cibernético.

Se compilan en este documento las responsabilidades de las diferentes instancias involucradas en esta materia y las líneas de acción generales construidas a partir del ente rector y de las instituciones participantes en la elaboración del documento, orientadas a salvaguardar la integridad de la información.

La aplicación de este documento va dirigido a la Administración Pública Central, la Administración Pública Descentralizada, las empresas del Sector Público, la Sociedad Civil y al ente rector, el MICITT.

Estos lineamientos son recomendaciones para todos los antes mencionados.

2. DOCUMENTOS Y LINEAMIENTOS DE REFERENCIA

Los documentos de referencia para la elaboración del presente protocolo son:

DIRECTRIZ N° 133-MP-MICITT**.** Emitida el 1 de abril del 2022**.**

GUÍA DE ACCIÓN ANTE UN INCIDENTE DE RANSOMWARE – V 2.0. Emitida por la Dirección de Gobernanza Digital del MICITT en el año 2020.

PROTOCOLO DE SEMÁFORO (TLP)MICITT-DGD-INF-005-2021. Emitida por el

Departamento de Respuesta a Incidentes de Seguridad Informática del MICITT el 04 de febrero del 2021.

3. DEFINICIONES Y ABREVIATURAS

Incidente de Seguridad Cibernética: Un evento de seguridad cibernética que se ha determinado que tiene un impacto en la organización, lo que provoca la necesidad de respuesta y recuperación. [1]

Evento de Seguridad Cibernética: Un cambio en la seguridad cibernética que puede tener un impacto en las operaciones de la organización (incluida la misión, las capacidades o la reputación).[2]

Riesgo: Una medida del grado en el que una entidad se ve amenazada por una circunstancia o evento potencial y típicamente una función de: (i) los impactos adversos que surgirían si ocurriera la circunstancia o el evento; y (ii) la probabilidad de que ocurra.[3]

Gestión del Riesgo: El proceso de identificar, evaluar y responder al riesgo.[4]

4. PRINCIPIOS

El MICITT, la Administración Pública Central y Descentralizada se comprometen a cumplir con los principios aceptados en el presente protocolo de buena conducta en el contexto de la amenaza cibernética que actualmente sufre nuestro país e incluso cuando las situaciones se tornen aún más difíciles.

A continuación, se presentan los principios en los cuales se basa el presente documento:

[1] Instituto Nacional de Estándares y Tecnología (2018). Marco para la mejora de la seguridad cibernética en infraestructuras críticas. doi: https://doi.org/10.6028/NIST.CSWP.04162018
[2] Instituto Nacional de Estándares y Tecnología (2018). Marco para la mejora de la seguridad cibernética en infraestructuras críticas. doi: https://doi.org/10.6028/NIST.CSWP.04162018
[3] Instituto Nacional de Estándares y Tecnología (2018). Marco para la mejora de la seguridad cibernética en infraestructuras críticas. doi: https://doi.org/10.6028/NIST.CSWP.04162018
[4] Instituto Nacional de Estándares y Tecnología (2018). Marco para la mejora de la seguridad cibernética en infraestructuras críticas. doi: https://doi.org/10.6028/NIST.CSWP.04162018

a) Rendición de cuentas
b) Transparencia
c) Comportamiento ético
d) Construcción colectiva con las partes interesadas
e) Respeto al principio de legalidad
f) Respeto a los derechos humanos

5. ALCANCE

El alcance del presente documento es definir las responsabilidades de los diferentes entes involucrados en las diferentes fases relacionadas con una amenaza de ciberseguridad.

6. ESTRUCTURA

El CSIRT será el ente encargado de ejecutar este protocolo. Según el Artículo 3º- del Decreto 37052-MICITT, el CSIRT-CR contará con un Consejo Director, que estará integrado de la siguiente manera:

- Ministro(a) de Ciencia y Tecnología o su representante, quien lo presidirá.
- 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

7. RESPONSABILIDADES

En el presente apartado se enumeran las principales responsabilidades de las instancias involucradas, de nivel nacional en la atención de una amenaza por ataque cibernético.

5.1 Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT).

Son responsabilidades de MICITT:

- Crear y emitir directrices de acatamiento obligatorio para las instituciones que pertenecen a la Administración Pública Central, e insta a las instituciones que pertenecen a la Administración Pública Descentralizada, respecto al tema de Ciberseguridad.
- Instruir e instar en el cumplimiento de las recomendaciones y medidas técnicas que emanen del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, por medio de la Dirección de Gobernanza Digital y el Centro de Respuesta de Incidentes de Seguridad Informática (en adelante CSIRT-CR), como ente coordinador de la ciberseguridad nacional, referentes a ciberseguridad y seguridad de la información, con el fin de mejorar las capacidades técnicas, de atención y de gestión de la ciberseguridad y seguridad de la información en las instituciones.
- Instruir e instar a realizar los procesos internos para promover de manera inmediata las acciones que favorezcan la resiliencia de la infraestructura tecnológica,
- Instruir e instar a autorizar a los contactos de ciberseguridad, equipos de tecnologías de la información, Centro de Respuesta de Incidentes de Seguridad Informática (CSIRTs internos) o grupos que en sus efectos se hayan creado para atender la ciberseguridad institucional, para que asistan a las actividades de formación, capacitación, u otra actividad que organice el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, por medio de la Dirección de Gobernanza Digital y el CSIRT-CR.
- Instruir e instar a que las alertas técnicas emitidas por el CSIRT-CR sean aplicadas, según corresponda en cada institución y sus sistemas.

Son responsabilidades del CSIRT como parte del MICITT:

- Instar a las instituciones del Sector Público para que tomen acciones con las recomendaciones enviadas en la Guía de acción ante un incidente de Ransomware.
- Instar a las instituciones del Sector Público para que utilicen el Protocolo de Semáforo en sus correos electrónicos y documentos.
- Emitir alertas técnicas con recomendaciones para las instituciones del Sector Público y Privado como parte del ente rector.
- Recibir de manera centralizada la información sobre los incidentes que ocurran en las instituciones, que afecten la confidencialidad, disponibilidad e integridad de servicios disponibles al público, o la continuidad de las funciones institucionales, o la suplantación de identidad de la institución en redes sociales, incluso aquellos incidentes que a lo interno de la institución se consideren bajo control.
- Recibir de manera centralizada información de todos los dominios de sitios web de las instituciones del Estado, para generar y validar los sitios web oficiales de sus instituciones.
- Definir los recursos disponibles para implementar este protocolo.
- Incorporar en las instancias de nivel nacional, designadas para el manejo de situaciones de ataque cibernético, los elementos necesarios para la consideración de la protección de la sociedad civil, lo que a información se refiere.

7.2 Administración Pública Central y Descentralizada

Son obligaciones de la Administración Pública Central y se recomienda a la Administración Descentralizada:

- Acatar las directrices emitidas por el ente rector, es decir el MICITT
- Atender las recomendaciones emitidas por el CSIRT del MICITT.
- Incorporar en su normativa interna los elementos necesarios para el cumplimiento del presente Protocolo.

- Definir los recursos disponibles para implementar este protocolo.

- Organizar las acciones con base en el Plan de Acción incorporado en este documento y referido a los siguientes cuatro ejes:
    - Eje Preventivo
    - Eje Detectivo
    - Eje Correctivo
    - Eje de Coordinación

7.3 Comisión Nacional de Prevención del Riesgo y Atención de Emergencias (CNE)

En caso de que la amenaza de ciberseguridad se materialice y evoluciones hacia una situación de emergencia nacional, la CNE tendrá la responsabilidad de:

- Asesorar al MICITT y a las autoridades de gobierno en materia de la atención de emergencias de nivel nacional, según las condiciones dadas en la Ley Nacional de Emergencias, Ley 8488, específicamente en los ejes correctivo y de coordinación.

8. MARCO GENERAL DE APLICACIÓN

En este apartado se detallan los ejes y las acciones primordiales, de cada uno de ellos, que los actores deben implementar.

A partir de estas acciones y de las responsabilidades, cada instancia debe desarrollar el o los procedimientos necesarios para ejecutar el presente documento.

Abarca los distintos ejes en los que tiene que existir coordinación entre las distintas entidades descritas en este documento, para asegurar los recursos informáticos, evitar, contener, mitigar y dar respuesta a los ataques de ciberseguridad o cibernéticos.

6.1 Eje Preventivo (Identificar y proteger recursos)

Se trata de acciones orientadas a comprender el riesgo de seguridad cibernética e implementar medidas adecuadas para la entrega de servicios críticos, para lo cual cada institución en el marco de sus propias responsabilidades debe:

1. Realizar periódicamente un diagnóstico y análisis de las vulnerabilidades existentes en los recursos informáticos. La periodicidad será definida por cada institución dependiendo de la sensibilidad de la información e infraestructura que deba proteger y en ningún caso excederá un plazo de 12 meses.
2. Realizar periódicamente un análisis de riesgos. La periodicidad será definida por cada institución dependiendo de la sensibilidad de la información e infraestructura que deba proteger y en ningún caso excederá un plazo de 12 meses.
3. Contar con un inventario actualizado de Software, Hardware, usuarios activos con sus roles y responsabilidades dentro de cada sistema de información institucional.
4. Identificar los controles requeridos para asegurar los recursos informáticos
5. Asignar los recursos presupuestarios para la adquisición y configuración y mantenimiento de los recursos en Ciberseguridad
6. Implementar programas de sensibilización y concientización sobre la Seguridad de la Información en las instituciones públicas y autónomas del estado.
7. Implementar los procesos y controles necesarios para asegurar la Disponibilidad, Integridad y Confidencialidad de los recursos de información.
8. Mantener un constante monitoreo de las redes de comunicación, tanto a nivel interno de la institución, como en aquellos canales de interacción con el usuario final.
9. Utilizar para la conexión remota a las redes institucionales Virtual Protocol Accesss (VPN), indispensable para el teletrabajo o las conexiones remotas.
10. Establecer Políticas de Respaldo de Información

11. Definir un equipo de Ciberseguridad en cada institución pública y órgano desconcentrado y autónomo, para ejercer las responsabilidades del tema de seguridad de la información tanto a nivel de establecimiento de políticas como de realizar las acciones operativas de aseguramiento de la información y acciones de contención ante ataques cibernéticos.
12. Implementar todas las alertas y medidas de ciberseguridad, cambio urgente masivo de contraseñas y protocolos de actuación, indicados por el CSIRT con el fin de disminuir las vulnerabilidades tecnológicas o contener oportunamente un ataque cibernético a nivel de las instituciones del aparato estatal y de la sociedad civil.
13. Promover y velar por el establecimiento de planes de contingencia en materia de seguridad de las tecnologías de la información y la comunicación en el sector público.
14. Establecer canales de comunicación entre los distintos equipos CSIRT de cada institución con el fin de fortalecer enlaces de comunicación y fomentar la colaboración interinstitucional.

8.2 Eje Detectivo (Monitoreo y detección de ataques)

Este eje detalla las acciones para el monitoreo de incidentes y eventos de seguridad cibernética; así como las acciones al momento en que se detectan estas; o bien la existencia de una amenaza cibernética.

Las acciones a seguir por parte de los involucrados en este documento son:

1. Informar al Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, a la Dirección de Gobernanza Digital y el Centro de Respuesta de Incidentes de Seguridad Informática (en adelante CSIRT-CR), cuando se compruebe que están teniendo un ataque cibernético, o que ha existido fuga de información como resultado de uno.
2. Coordinar con el Centro de Respuesta de Incidentes de Seguridad Informática (en adelante CSIRT-CR), lo requerido para afectos de lograr la

contención de los ataques y fortalecer tanto las herramientas de defensa y aseguramiento de los recursos de información.

3. Implementar, en la medida de sus posibilidades presupuestarias y de acuerdo con la infraestructura e información que deba proteger, sistemas de monitoreo y detección de ataques
4. Revisar regularmente las bitácoras de los sistemas de seguridad implementados (Firewall; Sistemas de identificación de intrusiones – IDS; Sistemas de Prevención de Intrusiones – IPS)

8.3 Eje Correctivo (Responder y recuperar)

Cuando ya se ha materializado la amenaza de ataque cibernético, las acciones a seguir son:

1. Realizar los procesos internos para promover de manera inmediata las acciones que favorezcan la resiliencia de la infraestructura tecnológica, incluyendo como mínimo actualizaciones permanentes de todos los sistemas institucionales, cambiar contraseñas de todos los sistemas institucionales (correos electrónicos, sistemas operativos, servidores, VPN, redes sociales, entre otros posibles), deshabilitar servicios y puertos no necesarios y monitorear la infraestructura de red, con el fin de garantizar que los eventos adversos relacionados con incidentes de ciberseguridad sean detectados, registrados y gestionados de forma que se pueda limitar el impacto de los mismos en cada institución o entidad.
2. Mapear conforme a la Ley General de Control Interno, a los ataques cibernéticos dentro de la valoración de riesgos de cada institución como una amenaza predominante que puede impactar infraestructuras estratégicas como los recursos informáticos
3. Coordinar conforme a la Valoración de Riesgos los Planes de Continuidad del Negocio y las acciones para garantizar disponibilidad de los servicios.

8.4 Eje coordinación

Finalmente se describen las acciones necesarias para la coordinación entre los actores a fin de garantizar una adecuada atención de la situación suscitada.

1. Participar en las acciones de capacitación y formación en temas de Seguridad de la Información y ataques cibernéticos que organice el MICITT y el CSIRT, relacionada con la atención y mejora en las capacidades de ciberseguridad y seguridad de la información
2. Coordinar el MICITT y CSIRT, sobre el diseño y aplicación de políticas, estrategias y lineamientos en la adquisición de bienes y servicios en materia de la seguridad de las tecnologías de la información y la comunicación, con los estándares que observen las normativas vigentes internacionales para la implementación y/o aplicación en el sector público en materia de aseguramiento de los recursos de información.
3. Establecer canales de comunicación entre los distintos equipos CSIRT de cada institución con el fin de fortalecer enlaces de comunicación y fomentar la colaboración interinstitucional, así como las lecciones aprendidas.
4. Incentivar, orientar y promover las iniciativas públicas y privadas conducentes a lograr un adecuado desarrollo del país en el campo de la seguridad de las tecnologías de la información y la comunicación, esfuerzos orientados a lograr una mayor protección del ciudadano.

7. COMUNICACIÓN

La comunicación del presente protocolo estará a cargo del MICITT y su réplica a cargo de las distintas áreas de comunicación de la Administración Pública Central y Descentralizada.

La vocería técnica y política del tema, puede estar a cargo de cualquiera de las siguientes opciones:

- ✓ Podría ser alguno de los miembros definido por el Consejo Director del CSIRT.
- ✓ Ministro(a) de Ciencia y Tecnología o su representante, quien lo presidirá
- ✓ 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.

Las acciones de comunicación para el cumplimiento del presente documento, seguirán, como mínimo, los siguientes objetivos:

a. Informar a lo interno las disposiciones y directrices emanadas, tanto por el ente rector como por las demás instancias aquí involucradas.
b. Divulgar el Plan de acción en todos sus ejes.
c. Difundir las recomendaciones técnicas emanadas de parte del MICITT.
d. Informar sobre las acciones específicas para dar continuidad a los servicios.

Tácticas:

- Información noticiosa.
- Campañas preventivas.
- Información para los clientes.
- Atención de los requerimientos informativos de los medios de comunicación

Productos:

- Comunicados de prensa
- Cuñas para radio

- Podcast.
- Mensajes SMS

Canales:

- Redes sociales
- Sitios web oficiales
- Correo electrónico
- WhatsApp
- Chat empresariales

8. APROBACIÓN, SEGUIMIENTO Y EVALUACIÓN

10.1 Aprobación

Este documento debe ser aprobado por el Sr. Ministro del MICITT. Sr. Carlos Enrique Alvarado Briseño.

10.2 Seguimiento

El seguimiento a la implementación del presente documento debe llevarse a cabo a través de las diferentes áreas rectoras y por parte de los equipos especializados, como el CSIRT o bien las oficinas de Tecnologías de Información de las distintas instancias aquí descritas.

10.3 Evaluación

La evaluación del cumplimiento del presente documento estará a cargo del MICITT, ente que debe definir los mecanismos para llevarla a cabo.