REPÚBLICA DE CUBA
LA MINISTRA DE COMUNICACIONES

RESOLUCIÓN 73

POR CUANTO: El Decreto 360 "Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional", de 31 de mayo de 2019, regula en su Capítulo III lo referente a la seguridad de las Infraestructuras Críticas de las TIC, con la finalidad de contar con una estrategia de fortalecimiento y sostenibilidad.

POR CUANTO: Las Resoluciones 178 y 45 de 7 de Octubre del 2008 y 16 de marzo del 2010 respectivamente, ambas del Ministro de la Informática y las Comunicaciones establecían el Reglamento de Categorización de las Redes Propias de Datos y la creación de la Comisión Ministerial para el otorgamiento de la condición de Red Especial a las redes propias de datos.

POR CUANTO: El desarrollo e impulso de las Tecnologías de la Información y la Comunicación ha permitido automatizar y optimizar muchas de las actividades que se llevan a cabo en los organismos, e incrementar la dependencia de las infraestructuras que proporcionan servicios esenciales para una nación, a las Tecnologías de la Información y la Comunicación; el uso de los medios tecnológicos con fines delictivos alrededor del mundo, la utilización de nuevas tecnologías para generar amenazas en el ámbito del ciberespacio encaminadas a destruir infraestructuras, entidades públicas, sistemas financieros que podrían paralizar servicios esenciales para nuestro país y afectar la Administración Pública, la economía nacional, así como la Seguridad y Defensa del país.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas en el artículo145 inciso d) de la Constitución de la República de Cuba;

RESUELVO

ÚNICO: Aprobar el siguiente:

REGLAMENTO DE LAS INFRAESTRUTURAS CRÍTICAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Artículo 1. El presente Reglamento tiene por objeto establecer las disposiciones para la identificación y atención de las Infraestructuras Críticas de las Tecnologías de la Información y la Comunicación, en lo adelante TIC, para su protección.

Artículo 2. Este Reglamento es de aplicación para los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular.

Artículo 3. Las Infraestructuras Críticas de las TIC son aquellas que soportan los componentes, procesos y servicios esenciales que garanticen las funciones y la seguridad a los sectores estratégicos de la economía, a la Seguridad y Defensa Nacional y a los servicios que brinde la Administración Pública.

Artículo 4. La metodología para identificar en las organizaciones las infraestructuras críticas de las TIC se establece en el Anexo Único de esta Resolucion.

Artículo 5. La Dirección General de Informática del Ministerio de Comunicaciones, de conjunto con las unidades organizativas designadas de los ministerios de las Fuerzas Armadas Revolucionarias y del Interior, elabora y propone para su aprobación por el que suscribe, el Catálogo y el Plan Nacional de Protección de las Infraestructuras Críticas de las TIC.

Artículo 6. La Dirección de Ciberseguridad del Ministerio de Comunicaciones, de conjunto con la Oficina de Seguridad para las Redes Informáticas para desarrollar el Sistema Nacional de Protección de las Infraestructuras Críticas de las TIC, cumple con las funciones siguientes:

a) Proponer la actualización y custodiar el Catálogo de las Infraestructuras Críticas de las TIC, así como su Plan Nacional de Protección, y conciliar la información suministrada por las instituciones implicadas en el proceso;

b) estudiar los riesgos y las amenazas sobre los servicios esenciales y las instalaciones estratégicas;

c) asegurar los procedimientos de comunicación y los mecanismos de control y alerta a las entidades responsables de las Infraestructuras Críticas de las TIC.

Artículo 7. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular son los responsables de elaborar e implementar, así como mantener actualizado, en el ámbito de su competencia, el plan de protección de sus Infraestructuras Críticas de las TIC y controlar su aplicación.

Artículo 8. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular elaboran la estrategia de empleo de las telecomunicaciones/TIC a partir de la identificación de los activos esenciales para el cumplimiento de las misiones de sus Infraestructuras Críticas de las TIC.

Artículo 9. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular que tengan Infraestructuras Críticas de las TIC deben disponer de un equipo de respuesta a

incidentes computacionales, que se encargan de prevenir, gestionar y responder ante estos, de la constante evaluación del riesgo y de las medidas de protección, supervisión y control específicos.

Artículo 10. El jefe de la operación de las Infraestructuras Críticas de las TIC realiza en lo fundamental, las acciones siguientes:

a) Desarrollar mecanismos sistemáticos, para la gestión del riesgo, para que de forma permanente se gestione el ciclo completo o sea su evaluación, se determinen las medidas, se implementen controles y se identifiquen las amenazas;
b) concebir los recursos necesarios para garantizar la protección escalonada y razonable de las Infraestructuras Críticas de las TIC, así como diseñar e implementar los procedimientos para la seguridad de estas;
c) implementar las medidas generales de protección permanentes o de carácter temporal a adoptar para prevenir, proteger y reaccionar ante posibles afectaciones.

Artículo 11. El Sistema Nacional de Protección de las Infraestructuras Críticas de las TIC debe garantizar los elementos siguientes:

a) La coordinación y articulación de los esfuerzos entre los actores de este Sistema;
b) el control y la supervisión de la actividad que se realice a cada nivel en función de la seguridad y protección de las Infraestructuras Críticas de las TIC;
c) la actividad preventiva para enfrentar ciberamenazas y mitigar los riesgos que de ellas resulten;
d) el aviso oportuno y la respuesta efectiva ante incidentes;
e) el restablecimiento ante los daños producidos por incidentes de ciberseguridad.

Artículo 12. La Oficina de Seguridad para las Redes Informáticas del Ministerio de Comunicaciones, coordina con los ministerios de las Fuerzas Armadas Revolucionarias y del Interior, las actividades de prevención, evaluación, aviso, investigación y respuesta a las acciones que afecten el funcionamiento de las Infraestructuras Críticas de las TIC.

Artículo 13. Al producirse un incidente de ciberseguridad que afecte una infraestructura crítica el jefe de operación de la red reporta de inmediato a la Oficina de Seguridad para las Redes Informáticas, la que se encarga de activar al resto de las entidades especializadas para que accionen en correspondencia con el Modelo de Actuación establecido a esos fines.

Artículo 14. Las entidades responsables de las Infraestructuras Críticas de las TIC deben tener en cuenta que estas se exponen a determinadas amenazas y vulnerabilidades que pudieran provocar entre otras, la interrupción de las funciones y servicios esenciales que se prestan a través de estas y su repercusión negativa en la actividad económica, política o social, su efecto público y sobre el medio ambiente, de acuerdo a las particularidades de cada sector.

Artículo 15. Las Infraestructuras Críticas de las TIC requieren de la aplicación de medidas concretas de vigilancia, protección y reacción ante incidentes de seguridad; en ese sentido se adoptan por las entidades responsables las acciones siguientes:

a) Elaborar e implementar en los planes de inversiones acciones que garanticen el desarrollo y la modernización continua de las Infraestructuras Críticas de las TIC;
b) implementar Sistemas de Vigilancia Tecnológica para el mejoramiento continuo y la sostenibilidad de las telecomunicaciones/TIC que soportan los servicios;
c) implementar sistemas de monitoreo, supervisión y control integral de las operaciones en las Infraestructuras Críticas de las TIC para asegurar su vitalidad;
d) elaborar e implementar procedimientos para la protección contra programas malignos;
e) implementar mecanismos criptográficos compatibilizados con los ministerios de la Fuerzas Armadas Revolucionarias y del Interior para el intercambio de información y de credenciales de acceso a los servicios telemáticos que soportan la gestión de las Infraestructuras Críticas de las TIC;
f) diseñar aplicaciones y sistemas de trabajo que aseguren alta disponibilidad de los servicios que soporta;
g) evaluar las redes y aplicaciones informáticas que soportan las Infraestructuras Críticas de las TIC,
h) seleccionar al personal para gestionar las Infraestructuras Críticas de las TIC, y tener en cuenta su preparación técnica y profesional así como su idoneidad.
i) implementar seguridad a nivel físico y lógico en cada uno de los componentes de las Infraestructuras Críticas de las TIC;
j) instalar sistemas de medidas de protección técnica integral.

DISPOSICIONES FINALES

PRIMERA: Se faculta a la Oficina de Seguridad para las Redes Informáticas perteneciente al Ministerio de Comunicaciones para implementar las medidas que se requieran para dar cumplimiento a lo que se dispone por la presente Resolución.

SEGUNDA: Derogar el artículo 4 y el Capítulo IV de la Resolución 178 de 7 de octubre del 2008 y la Resolución 45 de 16 de marzo del 2010, ambas del Ministro de la Informática y las Comunicaciones.

COMUNÍQUESE a los directores generales de Informática y de la Oficina de Seguridad para las Redes Informáticas, del Ministerio de Comunicaciones.

NOTIFÍQUESE a los viceministros, a los directores generales de Comunicaciones y de Defensa y al director de Regulaciones, todos del Ministerio de Comunicaciones.

DÉSE CUENTA a los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular que tienen Infraestructuras Críticas de las TIC.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

Dada en La Habana, a los 17 días del mes de mayo de 2021.

Mayra Arevich Marín

LIC. MELBA PITA CALDERÓN, ESPECIALISTA SUPERIOR EN POLITICA EN FUNCIONES DE DIRECTORA JURÍDICA DEL MINISTERIO DE COMUNICACIONES
CERTIFICO: Que la presente Resolución es copia fiel y exacta del original que obra en los archivos de esta Dirección a mí cargo.
La Habana, 18 de mayo de 2021.

ANEXO ÚNICO

METODOLOGÍA PARA IDENTIFICAR EN LAS ORGANIZACIONES LAS INFRAESTRUCTURAS CRÍTICAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Esta metodología constituye el instrumento de trabajo de una organización, y tiene como propósito servir de guía para identificar los elementos o servicios esenciales de una Infraestructura Crítica, que estén soportados en las Tecnologías de la Información y la Comunicación (TIC), así como para hacer una caracterización de cada una de ellas desde el punto de vista de su seguridad.

Como resultado de la aplicación de la metodología se elabora un documento que contiene, para cada infraestructura crítica identificada, los elementos siguientes:

1. Descripción.
2. Organización a la que pertenece.
3. Ubicación.
4. Identificación de las funciones, servicios esenciales y vulnerabilidades en correspondencia con su misión.
5. Resultados del análisis de las consecuencias que podrían derivarse de una interrupción de las funciones y servicios esenciales.
6. Resultados del análisis de las amenazas a que se exponen.
7. Evaluación del grado de criticidad.

I. Identificación de las funciones, servicios esenciales y vulnerabilidades de las infraestructuras críticas en correspondencia con su misión.

a) Caracterizar de forma sintetizada la organización en la que se aplica la metodología.
b) Describir los servicios y funciones esenciales en los cuales las TIC son determinantes, en el sentido de que su funcionamiento inadecuado impide o degrada la ejecución del servicio o función.
c) Detallar, para cada servicio o función esencial, el papel de las TIC en su aseguramiento y sus interdependencias[1] con otros servicios o funciones identificadas.
d) Identificar y describir las vulnerabilidades que afectan las infraestructuras críticas.
e) Detallar, en el caso de las infraestructuras críticas de las TIC vinculadas a la automática y la industria, la forma en que se implementan las denominadas consolas de despacho para la gestión de la información proveniente de los sistemas SCADA; asimismo, explicar el esquema de despliegue de las redes vinculadas a procesos productivos y sus riesgos de convergencia con otras redes externas o directamente a Internet.

---

[1] Esta condición hace que se incremente su grado de criticidad, por lo que será un elemento a tener en cuenta en la valoración del impacto potencial de su interrupción.

f) En las infraestructuras de las TIC, en las organizaciones en que se incluyan elementos tecnológicos de Supervisión del Sistema de Comunicaciones y de Redes. de datos del país, este proceso se realiza de conjunto con el órgano del MININT responsabilizado con la supervisión.
g) En cada organización, el nivel superior se responsabiliza con la certificación del proceso de identificación y caracterización en sus niveles inferiores.

II. Análisis de las consecuencias de una interrupción de las funciones y servicios esenciales.

a) Determinar las funciones y servicios esenciales que no tienen alternativa de sustitución en caso de verse interrumpidas, el costo de la interrupción es demasiado alto o el tiempo requerido para su restitución es excesivo[2].
b) Identificar las consecuencias que podrían derivarse de la interrupción de las funciones y servicios esenciales, así como valorar la gravedad de su impacto de forma descriptiva (**bajo**, **medio**, **alto** y **muy alto**).
c) Evaluar el impacto que estas puedan tener en un área geográfica, la población y el medio ambiente.

III. Análisis de las amenazas a las que se expone la infraestructura crítica.

a) Identificar, a partir del papel de las TIC en las funciones y servicios esenciales descritos anteriormente (acápite **I**, inciso **b**), las amenazas potenciales que puedan afectar de alguna manera a las infraestructuras críticas referidas.
b) Describir el esquema implementado para protección contra códigos malignos en cada infraestructura crítica identificada.
c) Informar la cantidad de incidentes de ciberseguridad que han afectado las infraestructuras críticas y, de ellos, los originados por códigos malignos.
d) Determinar el riesgo que representan las amenazas identificadas para los elementos de las infraestructuras críticas, a partir de su valoración expresada en forma descriptiva (**bajo**, **medio**, **alto** y **muy alto**).
e) Describir el posible impacto de la materialización de cada amenaza y evaluar este (**bajo**, **medio**, **alto** y **muy alto**). Relacionar las posibles consecuencias.

IV. Evaluación del grado de criticidad de las infraestructuras críticas identificadas.

a) A partir de la probabilidad de materialización de las amenazas (riesgo) y el posible impacto estimado sobre estas, se determina el grado de criticidad resultante de las infraestructuras críticas (ver tabla 1).
b) Determinar las afectaciones de las infraestructuras críticas, a partir de los incidentes de ciberseguridad que han afectado su disponibilidad, como elemento concreto de la materialización de los riesgos identificados.

---

[2] A estas funciones y servicios les corresponderá el mayor impacto al valorar la gravedad de su interrupción. De igual forma se clasifica de excesivo el tiempo de restitución a partir de las normas y regulaciones establecidas por las autoridades facultadas a estos efectos, las que deben ser referenciadas adecuadamente durante el proceso de identificación de las infraestructuras críticas.

c) Calculo de la no disponibilidad de la infraestructura crítica a partir de la cantidad de incidentes y el tiempo de duración:

$$\left[\sum_{i=1}^{n}(Tiempo\ de\ no\ disponiblidad)_i\right]$$

n: Cantidad de incidentes de ciberseguridad en infraestructuras críticas

Tabla 1. Tabla para la determinación de la criticidad de las infraestructuras críticas.

Probabilidad (Riesgo)	Impacto	Grado de Criticidad Resultante
Baja	Bajo	Bajo
	Medio	Bajo
	Alto	Bajo
	Muy Alto	Medio
Media	Bajo	Bajo
	Medio	Medio
	Alto	Alto
	Muy Alto	Alto
Alta	Bajo	Medio
	Medio	Alto
	Alto	Alto
	Muy Alto	Muy Alto
Muy Alta	Bajo	Medio
	Medio	Alto
	Alto	Muy Alto
	Muy Alto	Muy Alto

V. Glosario de Términos.

a) **Amenaza:** Cualquier circunstancia o evento con un impacto potencial negativo, a partir de accesos no autorizados, destrucción, divulgación, modificación de datos y/o denegación de servicios.

b) **Criticidad:** Condición de crítico, en el sentido de valorar el impacto de la interrupción o afectación de una infraestructura sobre los servicios que soporta. El análisis de criticidad posibilita establecer la jerarquía o prioridades de procesos, sistemas y equipos, y crear una estructura que facilita la toma de decisiones acertadas y

efectivas, encauzar el esfuerzo y los recursos en áreas donde sea más importante o necesario mejorar la confiabilidad operacional en base a la situación actual.

c) **Función o Servicio Esencial:** La función o el servicio indispensable para el mantenimiento de las actividades sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.

d) **Interdependencias:** Dependencias recíprocas entre los sistemas. Implica una situación en la que estos son mutuamente responsables, y compartir principios de funcionamiento comunes o suscritos de forma conjunta con independencia de sus particularidades.

e) **Riesgo:** La posibilidad de que una amenaza particular impacte negativamente en un sistema, y ocasione la pérdida, daño o perjuicio (parcial/total) de todos o algunos de sus componentes, a través del aprovechamiento de una vulnerabilidad existente.

f) **Sistema SCADA:** Aplicación informática diseñada con la finalidad de controlar y supervisar procesos a distancia. Proporciona comunicación con los dispositivos de campo (controladores autónomos, autómatas programables, entre otros), permitir el control de forma automática y enviar la información generada en el proceso a diversos usuarios.

g) **Vulnerabilidad:** Debilidad en los procedimientos y configuraciones de seguridad de un sistema, así como los controles internos establecidos para su funcionamiento que puedan ser aprovechados en perjuicio de su disponibilidad.