# Conectar los marcos internacionales, coordinar la respuesta:

*una hoja de ruta para el fortalecimiento de los CSIRT en América Latina*

DOI: 10.29236/sistemas.n180a9

**Resumen**

La respuesta a incidentes cibernéticos requiere capacidades técnicas, responsabilidades institucionales claras y recursos que permitan sostener la operación. Para América Latina, uno de los desafíos consiste en traducir los marcos internacionales disponibles en decisiones acordes con las necesidades y condiciones de cada país. Este artículo examina, mediante una revisión documental, las aportaciones de la Unión Internacional de Telecomunicaciones, el Global Forum on Cyber Expertise, FIRST, NIST, la Open CSIRT Foundation, ENISA y la Organización de los Estados Americanos al establecimiento, la operación y la evaluación de los equipos de respuesta a incidentes de seguridad informática (CSIRT). El análisis distingue las funciones de estos instrumentos y propone una articulación que conecta mandato, comunidad atendida, servicios, gestión del riesgo, madurez y sostenibilidad. A partir de esta lectura, se plantea una hoja de ruta organizada en tres fases: mandato y diagnóstico; servicios y operación; y madurez, cooperación y aprendizaje. La propuesta constituye una orientación adaptable que requiere diagnóstico y validación en cada contexto. Se sostiene que la utilidad de los marcos debe comprobarse mediante procedimientos ejecutables, ejercicios, registros y seguimiento de mejoras. Su contribución reside en facilitar que el conocimiento técnico se convierta en una respuesta coordinada, verificable y sostenible.

**Palabras claves**

CSIRT; respuesta a incidentes; gobernanza; madurez; América Latina.

## Introducción

La gestión de incidentes cibernéticos plantea una pregunta que resulta familiar para quienes diseñan, administran o protegen sistemas informáticos: ¿cómo convertir una recomendación general en una capacidad que funcione bajo presión? En el ámbito de la práctica un procedimiento adquiere valor cuando puede ejecutarse con los recursos disponibles y producir resultados verificables. En la respuesta a incidentes ocurre algo semejante. La existencia de una guía, una plataforma o un equipo formalmente constituido es un punto de partida, su éxito depende de cómo se articulan las personas, los procesos y las decisiones que permiten atender una afectación real (Killcrece et al., 2003).

Este artículo examina los principales marcos internacionales relacionados con el establecimiento, la operación y la evaluación de Equipos de Respuesta a Incidentes de Seguridad Informática, conocidos como CSIRT. El propósito es identificar sus aportaciones y discutir cómo pueden orientar el desarrollo de capacidades en América Latina. Para ello, se realiza una revisión documental de instrumentos publicados por la Unión Internacional de Telecomunicaciones (ITU), el Global Forum on Cyber Expertise (GFCE), FIRST, la Agencia de la Unión Europea para la Ciberseguridad (ENISA), la Open CSIRT Foundation, el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) y la Organización de los Estados Americanos (OEA).

La selección responde a la complementariedad de estos instrumentos. Algunos orientan la creación y el respaldo institucional de una capacidad nacional, otros permiten organizar servicios, integrar la respuesta a la gestión del riesgo o evaluar la madurez de un equipo (Ethembabaoglu,2026). Esta diversidad importa porque los problemas de implementación también son distintos: definir quién coordina un incidente no equivale a seleccionar una herramienta de monitoreo. Y disponer de especialistas no garantiza que existan procedimientos para compartir información o autorizar medidas de contención.

La revisión se organiza alrededor de cuatro preguntas: 1) ¿Qué problema busca resolver cada marco? 2) ¿A qué tipo de organización o equipo se dirige? 3) ¿Qué decisiones permite orientar? 4) ¿Qué ajustes requiere su aplicación en América Latina? Estas preguntas permiten examinar la utilidad de los instrumentos sin asumir que todos son equivalentes. Un catálogo de servicios, un modelo de madurez y una guía para establecer un CSIRT cumplen funciones relacionadas,

aunque diferentes. Su adopción conjunta exige comprender esas diferencias y definir una secuencia de aplicación.

También, es necesario precisar la unidad a la que se aplican las recomendaciones. Un CSIRT nacional puede ejercer funciones de coordinación entre instituciones, uno gubernamental puede concentrarse en entidades de la administración pública y uno sectorial puede atender necesidades compartidas por operadores de una industria. En cada caso cambia la comunidad atendida, esta delimitación determina qué reportes recibe el equipo, qué servicios ofrece y cuáles son los límites de su responsabilidad (Alghamdi, 2020).

Desde esta perspectiva, el artículo propone una lectura de los marcos orientada a decisiones institucionales y operativas. Para los profesionales esto implica relacionar cada recomendación con una necesidad concreta: establecer un canal de reporte, clasificar incidentes, documentar un procedimiento, verificar contactos o evaluar la capacidad de recuperación. Para los responsables de política pública, implica vincular esas tareas con atribuciones, presupuesto y mecanismos de coordinación.

El análisis no presenta una medición original de la madurez de los países latinoamericanos. Las recomendaciones que se desarrollan constituyen una propuesta de adaptación derivada de las fuentes examinadas. Su aplicación requiere un diagnóstico del contexto nacional o sectorial, así como validación mediante ejercicios y revisión de resultados. Y se destaca que la pertinencia de un marco debe juzgarse por su contribución a resolver problemas identificados, considerando los recursos y las responsabilidades de quienes lo utilizarán.

## 1. Por qué la respuesta es una cuestión de gobernanza

Cuando se identifica una intrusión, la atención suele concentrarse en las preguntas técnicas: cómo ingresó el atacante, qué sistemas comprometió y qué acciones permitirían contenerlo. Son preguntas indispensables. Sin embargo, conforme el incidente afecta servicios, proveedores o instituciones adicionales, aparecen otras decisiones igualmente relevantes: quién puede desconectar un sistema, quién informa a las entidades afectadas, qué información se comparte y qué autoridad determina cuándo debe escalarse la respuesta. La gobernanza se hace visible precisamente en estas decisiones (Kazeem, 2026).

Para comprender su importancia, pensemos en un escenario hipotético. Un proveedor de servicios digitales detecta actividad maliciosa en una plataforma utilizada por varias instituciones públicas. Su equipo técnico identifica indicios de compromiso, pero desconoce si puede comunicar detalles a todos los

clientes. Una entidad decide suspender conexiones, otra mantiene la operación porque el servicio resulta indispensable. Mientras tanto, el CSIRT nacional recibe información incompleta y carece de contactos actualizados para coordinar una evaluación conjunta. Aunque existen especialistas y herramientas, la respuesta encuentra obstáculos en las relaciones entre organizaciones.

Este escenario ilustra que la capacidad de respuesta incluye acuerdos sobre autoridad, responsabilidades y circulación de información. El GFCE (2017) sitúa la función nacional de respuesta dentro de la estructura institucional de ciberseguridad y destaca la necesidad de definir su mandato y su comunidad atendida. A su vez, NIST (2025) incorpora la respuesta a incidentes en la gestión del riesgo organizacional, vinculándola con decisiones que deben prepararse antes de que ocurra una afectación.

En este artículo la gobernanza de la respuesta se entiende como el conjunto de reglas, responsabilidades y mecanismos de coordinación que permite convertir información técnica en acciones institucionales.

Para los miembros de un CSIRT, esto tiene consecuencias muy concretas. Una recomendación de aislamiento necesita un responsable que pueda autorizarla, una alerta requiere un destinatario capaz de actuar y una recuperación demanda criterios para determinar si el servicio puede restablecerse con un riesgo aceptable. La eficacia técnica depende, en parte, de que estas decisiones estén previstas y puedan tomarse oportunamente (Boeke, 2018).

Una primera condición es la claridad del mandato. El CSIRT debe conocer a quién atiende, qué servicios presta y qué competencias corresponden a otras entidades. Coordinar la respuesta técnica no supone asumir automáticamente funciones de investigación penal, inteligencia o dirección de una crisis nacional. Esas actividades pueden relacionarse durante un incidente, pero requieren atribuciones y procedimientos específicos. Delimitar sus interfaces ayuda a reducir duplicidades y evita que las decisiones dependan exclusivamente de acuerdos informales entre personas (Kasim et al., 2023).

Una segunda condición es la confianza. Compartir información sobre un incidente puede revelar vulnerabilidades, datos sensibles o fallas de operación. Por ello, los actores necesitan saber quién tendrá acceso, para qué utilizará los datos y en qué condiciones podrá transmitirlos. Los canales de cooperación deben ofrecer protección y previsibilidad. Cuando estos acuerdos son claros, la información puede circular con mayor utilidad para el análisis y la coordinación (West-Brown et al., 2003).

Por último, la sostenibilidad constituye una tercera condición. Los contactos cambian, las herramientas requieren mantenimiento y los equipos necesitan formación continua. Un presupuesto que cubre únicamente la instalación inicial deja sin resolver la continuidad de la capacidad. La guía de la OEA (2023) sobre un modelo de negocio sustentable permite abordar esta dimensión mediante la planificación de servicios, recursos y respaldo institucional.

Para América Latina, estas consideraciones sugieren que la adaptación de los marcos internacionales debe comenzar por identificar quién decide, quién ejecuta y quién coordina en cada escenario relevante. Una matriz de responsabilidades, un directorio verificado y procedimientos de escalamiento pueden parecer entregables modestos frente a una plataforma avanzada, pero permiten utilizar mejor las capacidades existentes. Su valor debe comprobarse mediante ejercicios: si una alerta llega a la persona adecuada, si las autorizaciones se obtienen a tiempo y si las instituciones pueden actuar de manera coordinada. Así, la gobernanza se convierte en una condición operativa de la respuesta y en un criterio para evaluar su funcionamiento.

## 2. ITU y la construcción de la capacidad nacional

Establecer una capacidad nacional de respuesta a incidentes cibernéticos supone organizar una función que pueda operar de manera continua, atender a una comunidad definida y coordinarse con otras instituciones. La ITU ha promovido este proceso mediante orientaciones y mecanismos de cooperación, con especial atención a los países que necesitan desarrollar sus capacidades iniciales. Sus resoluciones reconocen la importancia de crear y mejorar equipos nacionales de respuesta, así como de facilitar la cooperación entre ellos (ITU, 2022a, 2022b).

La aportación de la ITU & World Bank (2025) puede comprenderse desde una pregunta práctica: ¿qué necesita un país para convertir la respuesta a incidentes en una capacidad institucional? La respuesta requiere relacionar la estrategia nacional de ciberseguridad con una estructura organizativa, personal preparado, procedimientos y recursos. Desde esta perspectiva, el equipo nacional forma parte de un sistema de gestión del riesgo en el que participan autoridades públicas, operadores de servicios, empresas y comunidades técnicas.

Esta orientación tiene una consecuencia inmediata: las decisiones sobre infraestructura deben derivarse de una definición previa de funciones. Antes de seleccionar plataformas de monitoreo, análisis o intercambio de información, conviene establecer qué servicios ofrecerá el equipo y qué problemas necesita resolver. Si su tarea princi-

pal es coordinar incidentes que afectan a diversas instituciones, necesitará mecanismos de comunicación y escalamiento diferentes de los que utiliza un equipo dedicado a proteger una sola red. La arquitectura técnica debe corresponder al alcance institucional de la operación.

El punto de partida es delimitar la comunidad atendida. Un CSIRT nacional puede asumir responsabilidades de coordinación para el país, aunque su capacidad de intervención directa se concentre inicialmente en determinadas entidades o servicios. Precisar esa diferencia permite comunicar expectativas realistas: qué incidentes recibe, a quién proporciona asistencia y en qué condiciones solicita apoyo de otros equipos. La amplitud del mandato debe guardar relación con los recursos disponibles y con la distribución de responsabilidades dentro del Estado (Dubois & Tatar, 2022).

En ese sentido, el enfoque de la ITU resulta valioso porque permite situar la creación del equipo dentro de una estrategia de desarrollo de capacidades. Cada país necesita identificar qué recursos ya existen y cuáles requieren articulación. Universidades, proveedores, entidades financieras y organismos públicos pueden disponer de conocimientos y equipos que contribuyan a la respuesta nacional. Reconocer esas capacidades ayuda a definir dónde conviene crear servicios y dónde resulta más útil establecer acuerdos de coordinación (Kamariotou & Kitsios).

La continuidad también debe formar parte del diseño. El equipo necesita mantener conocimientos, actualizar procedimientos y conservar relaciones de cooperación aun cuando cambien sus integrantes. Esto requiere presupuesto recurrente, formación y respaldo institucional. Una capacidad nacional adquiere mayor consistencia cuando sus funciones se documentan, sus servicios se prueban y sus resultados permiten justificar decisiones de mejora.

## 3. GFCE y el mandato de un CSIRT nacional

Una de las decisiones más importantes al establecer un CSIRT nacional es definir su mandato. Aunque puede parecer un asunto administrativo, determina aspectos esenciales de la operación: a quién atiende el equipo, qué servicios presta, qué autoridad tiene para coordinar y cómo se relaciona con otras instituciones. Las buenas prácticas del GFCE (2017) sitúan esta definición dentro de la estrategia y la estructura nacional de ciberseguridad, vinculándola con las necesidades y los riesgos del país.

El mandato puede entenderse como un acuerdo institucional sobre la función del equipo. Para que sea útil, debe responder preguntas que cualquier operador encontrará du-

rante un incidente: ¿quién puede solicitar asistencia?, ¿qué información debe proporcionar?, ¿qué acciones puede realizar el CSIRT?, ¿cuándo debe escalar el caso? y ¿qué decisiones corresponden a otras autoridades? La precisión de estas respuestas reduce incertidumbre y facilita que los especialistas actúen dentro de responsabilidades reconocidas (Hidalgo-Guijarro, 2023).

En ese sentido, el mandato funciona como una definición del alcance del servicio. Permite relacionar solicitudes con capacidades y establecer límites que protegen la operación. Un equipo responsable de coordinar alertas nacionales no necesariamente administra los sistemas afectados ni puede ordenar su desconexión. Por ello, necesita procedimientos que conecten sus recomendaciones con las personas que tienen autoridad sobre esos sistemas. La claridad institucional permite que el análisis técnico se convierta en una decisión ejecutable.

Las buenas prácticas del GFCE (2017) también destacan la importancia de fundamentar la capacidad nacional en una evaluación de riesgos. Este principio ayuda a evitar que el diseño responda únicamente a modelos disponibles o a oportunidades de financiamiento. Si el diagnóstico identifica dificultades de coordinación entre sectores, la prioridad puede ser establecer contactos y procedimientos compartidos. Si revela una comunidad con escasa capacidad para analizar incidentes, podría ser necesario desarrollar servicios de asistencia técnica, las decisiones deben guardar relación con problemas identificados.

Otro componente del mandato es su relación con funciones cercanas, como la investigación de delitos, la inteligencia, la regulación y la gestión de crisis. Un incidente puede activar varias de ellas, pero cada una responde a atribuciones y objetivos propios. El CSIRT necesita saber cuándo coordinarse con esas autoridades y en qué condiciones compartir información. Definir estas interfaces favorece una respuesta coherente y ayuda a evitar solicitudes que excedan sus competencias (Nowikowska, 2021).

Esta delimitación es especialmente relevante para construir confianza. Una organización que reporta un incidente necesita comprender cómo se utilizará la información y quién podrá acceder a ella. Si las reglas son ambiguas, puede retrasar la notificación o proporcionar datos insuficientes.

En cambio, condiciones claras de confidencialidad, protección y uso permiten establecer relaciones de cooperación más previsibles. El mandato debe acompañarse de procedimientos que hagan operativas esas condiciones (GFCE, 2017).

En América Latina, la adaptación requiere considerar la estructura institucional de cada país. En un sistema federal, caso de países como México, Argentina y Brasil, puede ser necesario acordar responsabilidades entre autoridades nacionales y subnacionales. Cuando los servicios esenciales dependen de operadores privados, la coordinación exige mecanismos que faciliten su participación. Estos ejemplos muestran que una función nacional debe diseñarse a partir de relaciones concretas, sin suponer que una misma ubicación administrativa resolverá todas las necesidades (Scholta et al., 2025).

El respaldo institucional debe, además, permitir que el equipo mantenga su capacidad a lo largo del tiempo. Un mandato amplio sin personal, presupuesto o acuerdos de cooperación genera expectativas difíciles de cumplir.

Por ello, resulta conveniente vincular cada responsabilidad con servicios definidos y recursos disponibles. La revisión periódica permite ajustar el alcance conforme cambian los riesgos y se desarrollan nuevas capacidades.

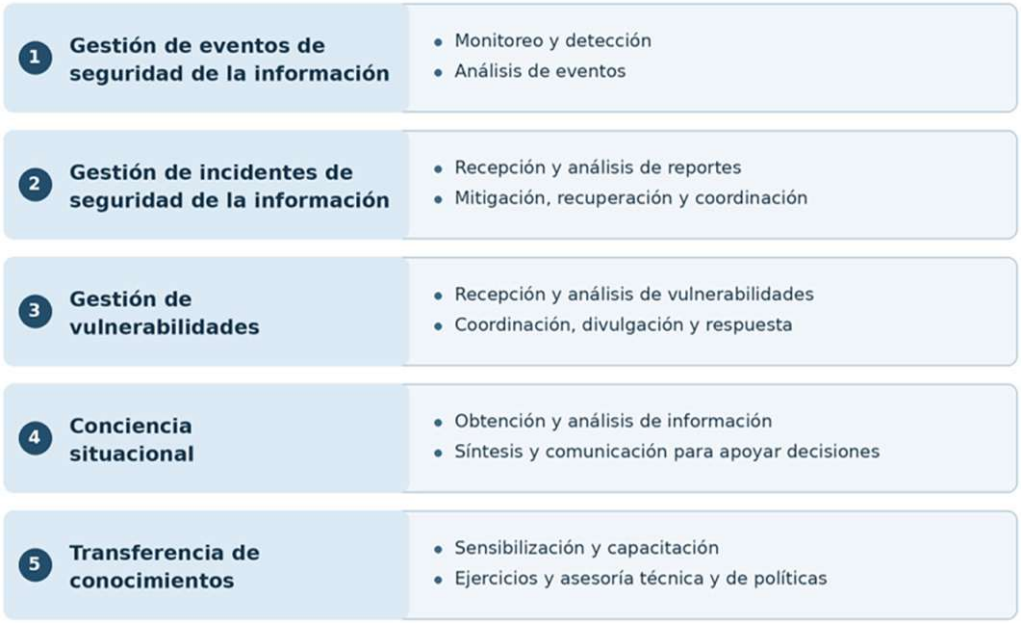
## 4. FIRST y el catálogo de servicios

Una vez definidos el mandato y la comunidad atendida, surge una pregunta operativa: ¿qué servicios puede ofrecer el equipo y qué necesitan sus usuarios? El *CSIRT Services Framework* de FIRST (2020) permite organizar esta discusión mediante un lenguaje común para describir servicios, funciones y actividades. Su utilidad consiste en ayudar a los equipos a definir su trabajo y comunicarlo de manera comprensible a otras organizaciones.

El marco agrupa los servicios en cinco áreas: 1) gestión de eventos de seguridad de la información, 2) gestión de incidentes, 3) gestión de vulnerabilidades, 4) conciencia situacional y 5) transferencia de conocimientos. Estas áreas permiten relacionar la observación de actividad potencialmente maliciosa con el análisis, la coordinación y el aprendizaje. No constituyen una obligación de implementar todos los servicios: cada equipo debe seleccionar los que correspondan a su mandato, a los riesgos de su comunidad y a sus recursos (Núñez-Agurto, 2022).

Esta estructura ayuda a distinguir actividades que suelen confundirse, un evento es una observación que requiere interpretación; un incidente supone una afectación o amenaza que demanda atención. Recibir registros, correlacionar alertas y coordinar la contención son tareas relacionadas, pero requieren procesos y responsabilidades diferentes. Separarlas permite identificar dónde se interrumpe el flujo de trabajo: en la detección, en el análisis o en la capacidad de convertir un hallazgo en una acción (Tanczer et al., 2018).

**Figura 1. Áreas de servicios de un CSIRT según FIRST.**




**Fuente:** Elaboración propia con base en FIRST (2020).

La gestión de vulnerabilidades introduce otra dimensión. El equipo puede identificar debilidades, analizar su relevancia, comunicar recomendaciones y colaborar en su tratamiento. Sin embargo, la responsabilidad de corregir una configuración o instalar una actualización puede corresponder al administrador del sistema, al proveedor o al fabricante. El catálogo debe aclarar qué apoyo proporciona el CSIRT y qué acciones espera de las organizaciones atendidas (FIRST, 2020).

La conciencia situacional permite integrar información para comprender el entorno de amenazas y apoyar decisiones. Su valor depende de seleccionar datos pertinentes y transformarlos en conocimiento utilizable. Una alerta sobre una vulnerabilidad, por ejemplo, resulta más útil cuando identifica los sistemas potencialmente afectados, explica las condiciones de explotación y ofrece recomendaciones acordes con la comunidad destinataria. El volumen de información distribuida no equivale, por sí mismo, a la calidad del servicio.

Por su parte, la transferencia de conocimientos reconoce que la respuesta también necesita formación, ejercicios y aprendizaje compartido. Los especialistas pueden utilizar los incidentes atendidos para mejorar procedimientos y desa-

rrollar capacidades en las instituciones de su comunidad. Esta función adquiere relevancia cuando los usuarios tienen diferentes niveles de preparación y requieren orientación para reportar, conservar información o aplicar medidas iniciales.

## 5. NIST y la integración de la respuesta al riesgo

Definir servicios permite ordenar el trabajo del equipo, pero la respuesta a incidentes necesita conectarse con las decisiones de la organización. En este punto son útiles herramientas como el *Cybersecurity Framework 2.0.* Su aportación consiste en vincular la preparación, la detección, la respuesta y la recuperación con actividades continuas de gobernanza y mejora (NIST, 2024).

Esta orientación amplía la mirada sobre el incidente, una intrusión puede comprometer información, interrumpir procesos o afectar servicios que dependen de proveedores externos. Para decidir cómo responder, los especialistas necesitan comprender la importancia de los activos afectados y las consecuencias de las medidas propuestas. La decisión de aislar un sistema, por ejemplo, debe considerar tanto la posibilidad de propagación como el efecto que su desconexión

**Figura 2. Respuesta a incidentes y gestión del riesgo en NIST.**




**Fuente:** Elaboración propia con base en NIST (2024).

tendría sobre la operación (Nelson et al., 2025).

NIST relaciona las funciones de gobernar, identificar y proteger con la preparación y la reducción del riesgo, mientras que detectar, responder y recuperar concentran actividades vinculadas con el manejo de incidentes. La mejora continua conecta estas funciones mediante aprendizajes que deben incorporarse a la gestión organizacional.

Ello permite comprender la respuesta como una capacidad que se prepara antes del incidente y se revisa después de su atención (Hajializadeh & Imani, 2021).

Este enfoque se traduce en preguntas concretas. ¿Existe un inventario suficientemente actualizado? ¿Se conocen las dependencias del servicio? ¿Los registros disponibles permiten investigar una afectación? ¿Está definido quién autoriza una medida de contención? ¿Las copias de respaldo pueden restaurarse en condiciones aceptables? Las respuestas condicionan el margen de actuación del equipo cuando ocurre un incidente y deben revisarse como parte de la preparación.

La relación con la continuidad operativa es especialmente importante. Recuperar un sistema requiere comprobar que puede volver a prestar su función y que las condiciones que permitieron el incidente han sido atendidas hasta un nivel de riesgo aceptado por la organización. Por ello, los especialistas deben coordinarse con responsables de procesos, administradores, proveedores y directivos. La recuperación combina verificación técnica con decisiones sobre prioridades y disponibilidad del servicio (Meçaj, 2026).

Esta arquitectura de gobernanza puede ilustrarse mediante un escenario hipotético de ransomware en una institución hospitalaria. El equipo técnico identifica equipos comprometidos y recomienda restringir conexiones. La decisión debe considerar qué sistemas sostienen la atención médica, cuáles pueden suspenderse y qué alternativas operativas existen. El análisis técnico necesita información sobre procesos críticos y autoridades para actuar. Este ejemplo muestra por qué la preparación debe involucrar a quienes administran el riesgo y la continuidad de la institución.

La comunicación forma parte también de la arquitectura de gobernanza. Durante un incidente, distintas personas necesitan información diferente: los operadores requieren instrucciones técnicas; los directivos, una valoración de impacto y opciones; y los usuarios afectados, orientación sobre la situación y las acciones que les corresponden. Definir responsables y canales ayuda a evitar mensajes contradictorios y permite actualizar la información conforme avanza la investigación (NIST, 2025).

El aprendizaje posterior también necesita traducirse en cambios. Identificar que una alerta se atendió tarde o que un contacto estaba desactualizado aporta valor cuando conduce a corregir el procedimiento, ajustar responsabilidades o capacitar al personal. La revisión debe examinar las condiciones que favorecieron el incidente y las dificultades encontradas durante su manejo. Así, los resultados de la respuesta retroalimentan la gestión del riesgo.

## 6. SIM3 y ENISA para medir madurez

Después de definir el mandato, organizar los servicios e integrar la respuesta a la gestión del riesgo, corresponde examinar qué tan consistente es el funcionamiento del equipo. La madurez permite abordar esta cuestión mediante criterios que relacionan las capacidades declaradas con su organización y ejecución. Por lo que esta dimensión representa una oportunidad de identificar qué procesos funcionan de manera previsible, cuáles dependen de esfuerzos individuales y dónde conviene concentrar las mejoras (Lee et al., 2024).

El *Security Incident Management Maturity Model*, conocido como SIM3 y promovido por la *Open CSIRT Foundation,* organiza la evaluación en cuatro dimensiones: 1) organización, 2) personas, 3) herramientas y 4) procesos. Estas dimensiones permiten examinar aspectos que van desde el mandato y las responsabilidades hasta la preparación del personal y la documentación de las actividades.

Su utilidad consiste en ofrecer una estructura para valorar el desarrollo del equipo y orientar decisiones de mejora (Open CSIRT Foundation, 2010)
.
La dimensión organizacional permite revisar si el equipo cuenta con una función reconocida y responsabilidades definidas. La relativa a las personas examina condiciones necesarias para desempeñar el trabajo, como conocimientos y formación. Las herramientas proporcionan soporte a la operación, mientras que los procesos permiten realizar actividades de manera consistente. La relación entre estas dimensiones explica por qué una capacidad técnica avanzada puede resultar insuficiente cuando existen dificultades de coordinación o procedimientos poco claros.

Por otra parte, ENISA desarrolló un modelo de evaluación de madurez para CSIRT nacionales y gubernamentales que incorpora SIM3 y otros referentes sobre capacidades. Su aportación consiste en relacionar los criterios de evaluación con una metodología que ayuda a examinar el desarrollo de los equipos. Estos instrumentos pueden utilizarse para establecer una línea de base y orientar revisiones posteriores, considerando el contexto y las funciones de la organización evaluada (ENISA, 2019).

**Figura 3. Dimensiones de madurez de SIM3 y proceso de mejora.**




**Fuente:** Elaboración propia con base en Open CSIRT Foundation (2010).

En este punto, es necesario distinguir entre autoevaluación, revisión externa y certificación. Una autoevaluación permite identificar brechas y organizar acciones; una revisión externa aporta una perspectiva adicional sobre los resultados; y una certificación responde a requisitos y procedimientos específicos.

Completar un diagnóstico interno no acredita automáticamente el cumplimiento de un esquema de certificación. Precisar estas diferencias evita atribuir a los resultados un alcance mayor del que poseen (Yesina & Holubnychyi).

La evaluación adquiere utilidad cuando se acompaña de evidencia. Un procedimiento escrito muestra que existe una instrucción, pero los registros de ejercicios y casos atendidos permiten examinar cómo se aplica. Del mismo modo, un directorio de contactos necesita pruebas de actualización y disponibilidad.

Para fines de mejora interna, conviene relacionar cada capacidad evaluada con documentos, registros o actividades que ayuden a comprender su funcionamiento. Esta es una recomendación de aplicación del modelo, cuyo detalle

debe ajustarse al propósito de la evaluación.

En América Latina, SIM3 y ENISA pueden ayudar a definir prioridades alcanzables sin exigir que todos los equipos recorran una trayectoria idéntica. Un CSIRT con recursos limitados podría comenzar por mejorar la documentación y la cobertura de sus servicios. Otros, con procedimientos establecidos, podrían concentrarse en ejercicios intersectoriales o revisión entre pares. La comparación resulta más útil cuando considera el mandato, la comunidad atendida y las condiciones de operación.

## 7. La OEA como puente de adaptación regional

Los marcos internacionales ofrecen criterios para diseñar y evaluar capacidades, pero su aplicación requiere comprender el entorno institucional donde operarán. La OEA aporta una perspectiva especialmente pertinente para América Latina y el Caribe mediante sus guías para CSIRT y sus iniciativas de cooperación. Su contribución permite relacionar las recomendaciones técnicas con preguntas sobre planificación, recursos y sostenibilidad.

La *Guía práctica para CSIRTs: Un modelo de negocio sustentable*, publicada en 2023, desarrolla esta dimensión. El término "modelo de negocio" debe entenderse aquí como una forma de organizar la propuesta de servicios, la comunidad atendida, los recursos y las relaciones que sostienen al equipo. Para un CSIRT público, la cuestión central es cómo mantener una función útil y viable a lo largo del tiempo (OEA, 2023).

Esta perspectiva permite abordar una dificultad frecuente en el diseño de capacidades: la diferencia entre financiar la instalación y sostener la operación. El establecimiento de un equipo puede requerir infraestructura, herramientas y contratación inicial, pero su continuidad implica formación, mantenimiento, actualización de procedimientos y disponibilidad de personal. La planificación necesita considerar estos compromisos desde el inicio y vincularlos con los servicios que se espera prestar.

La guía también ayuda a relacionar los servicios con las necesidades de la comunidad. Un equipo puede identificar numerosos problemas de ciberseguridad, pero necesita decidir cuáles puede atender directamente y cuáles requieren cooperación. Esta definición permite organizar prioridades y comunicar límites. Cuando el catálogo de servicios corresponde a la capacidad disponible, los usuarios tienen mayor claridad sobre la asistencia que pueden solicitar y las responsabilidades que conservarán durante el incidente (OEA, 2023).

La dimensión regional añade otra oportunidad, los incidentes pueden involucrar proveedores, infraestructura y organizaciones situados

en diferentes países. Las redes de cooperación facilitan el contacto entre equipos y crean espacios para intercambiar conocimientos y desarrollar capacidades. Sin embargo, su utilidad operativa depende de que los participantes sepan qué información compartir, por qué canales y en qué condiciones de protección. La cooperación necesita procedimientos que permitan utilizar oportunamente lo recibido (Aguilar Antonio, 2023).

La adaptación requiere reconocer diferencias entre países y sectores. Las prioridades de un equipo que coordina instituciones públicas pueden diferir de las de uno que atiende operadores financieros o universidades. Por ello, resulta conveniente utilizar las guías como instrumentos de planificación y revisión, incorporando el diagnóstico de necesidades y las condiciones locales. El objetivo es construir servicios que puedan prestarse de manera continua y mejorar mediante aprendizaje compartido.

Desde esta perspectiva, la cooperación regional puede apoyar ejercicios conjuntos, revisión de procedimientos y formación especializada. Sus resultados deberían traducirse en capacidades observables: contactos que funcionan, información que puede intercambiarse y

**Figura 4. Modelo de sostenibilidad de un CSIRT según OEA (2023).**




**Fuente:** elaboración propia con base en OEA (2023).

acciones correctivas que se completan. Esta propuesta permite evaluar el valor de los marcos por su contribución al funcionamiento de los equipos y a la coordinación de la respuesta en América Latina (Lima & Soares, 2021; Aguilar Antonio, 2021)

## 8. Una arquitectura complementaria de los marcos

Los instrumentos examinados permiten organizar la gestión de incidentes desde distintos niveles de decisión. Algunos orientan el establecimiento de una capacidad nacional; otros ayudan a definir servicios, integrar la respuesta al riesgo o evaluar el desarrollo de los equipos. Su complementariedad ofrece una base para construir una hoja de ruta en la que cada recomendación responda a una necesidad identificada y se traduzca en responsabilidades, recursos y procedimientos.

La tabla 1 sintetiza estas aportaciones. La última columna presenta propuestas de aplicación para América Latina, cuya pertinencia debe contrastarse con el diagnóstico de cada país o sector.

La articulación puede comenzar con las orientaciones de la ITU y el GFCE para definir el propósito de la capacidad nacional, su comunidad atendida y sus relaciones institucionales. Estas decisiones establecen el alcance dentro del cual se seleccionarán los servicios. Posteriormente, FIRST permite describir qué hará el equipo, mientras NIST ayuda a relacionar ese trabajo con la importancia de los activos y servicios que deben protegerse. Finalmente, SIM3 y ENISA aportan criterios para revisar el desarrollo de la capacidad y la OEA permite examinar cómo sostenerla mediante planificación y recursos.

Esta secuencia constituye una propuesta analítica en este artículo. Sin embargo, no se emite mencionar que no representa una metodología conjunta oficialmente adoptada por los organismos mencionados. Su utilidad consiste en ordenar preguntas que suelen abordarse por separado: quién coordina, qué servicios se prestan, cómo se toman decisiones y qué evidencia permite evaluar los avances.

La aplicación tampoco necesita seguir una trayectoria rígida. Un ejercicio puede mostrar que el catálogo de servicios excede los recursos disponibles o que el mandato deja dudas sobre quién autoriza una medida. En ese caso, la evaluación permite volver a las decisiones de diseño y corregirlas. La relación entre planificación, operación y aprendizaje hace posible que los marcos acompañen el desarrollo del equipo conforme cambian sus necesidades (NIST, 2025; ENISA, 2019).

Para América Latina, se propone organizar esta adaptación en tres fases: 1) Mandato y diagnóstico; 2) Servicios y operación; y 3) Madurez, cooperación y aprendizaje.

**Tabla 1. Aportaciones de los marcos internacionales a la gestión de incidentes cibernéticos.**

| Organismo e instrumento | Función principal | Ámbito de aplicación | Aplicación propuesta para América Latina |
|---|---|---|---|
| **ITU \| Orientaciones para capacidades nacionales** | Orientar el establecimiento de capacidades de respuesta y su vinculación con la estrategia nacional. | Nacional. | Definir funciones iniciales, recursos y relaciones de coordinación. |
| **GFCE \| Buenas prácticas para CSIRT nacionales** | Precisar mandato, comunidad atendida y respaldo institucional. | Nacional e interinstitucional. | Acordar responsabilidades y mecanismos de cooperación entre actores. |
| **FIRST \| CSIRT Services Framework** | Organizar y describir los servicios del equipo. | Equipos nacionales, sectoriales e institucionales. | Seleccionar una cartera de servicios acorde con necesidades y recursos. |
| **NIST \| SP 800-61 Rev. 3** | Integrar la respuesta a incidentes en la gestión del riesgo. | Organizacional. | Vincular la operación técnica con prioridades institucionales y recuperación de servicios. |
| **Open CSIRT Foundation \| SIM3** | Evaluar madurez en organización, personas, herramientas y procesos. | Equipos de gestión de incidentes. | Identificar brechas y dar seguimiento a mejoras. |
| **ENISA \| Modelo de evaluación de madurez** | Orientar la evaluación de capacidades de CSIRT nacionales y gubernamentales. | Nacional y gubernamental. | Adaptar criterios de diagnóstico y revisión al mandato de cada equipo. |
| **OEA \| Guía práctica para CSIRTs, volumen 2** | Orientar la planificación y sostenibilidad de los equipos. | CSIRTs de América Latina y el Caribe. | Relacionar servicios, costos recurrentes y respaldo institucional. |

**Fuente:** elaboración propia.

Cada fase debe producir resultados verificables y considerar la sostenibilidad desde el inicio. El criterio de avance será la capacidad de ejecutar las funciones acordadas, documentar dificultades y completar mejoras. Las siguientes secciones desarrollan esta propuesta.

### 8.1 Primera fase: mandato y diagnóstico

La primera fase busca establecer qué capacidad necesita desarrollarse, a quién atenderá y cómo se relacionará con las instituciones existentes. Su producto principal es una definición compartida del alcance de la respuesta, respaldada por un diagnóstico de riesgos y recursos.

Esta orientación retoma las buenas prácticas del GFCE (2017) sobre el mandato nacional y las recomendaciones de planificación de la ITU (2025) y la OEA (2023).

**Figura 5. Articulación de marcos internacionales para definir, desarrollar y sostener una capacidad nacional de gestión de incidentes.**




**Fuente:** elaboración propia.

El diagnóstico debe comenzar por identificar las funciones y los servicios cuya afectación tendría consecuencias relevantes. Para ello, conviene examinar qué procesos dependen de sistemas digitales, qué proveedores intervienen y quién administra los activos. La información permitirá reconocer necesidades de coordinación y asistencia técnica. El nivel de detalle debe corresponder al alcance del equipo: un CSIRT nacional necesita una visión de actores y dependencias estratégicas, mientras uno institucional requiere mayor precisión sobre su infraestructura.

También, es necesario mapear las capacidades disponibles. Pueden existir equipos gubernamentales, sectoriales, académicos o empresariales que reciben reportes, analizan amenazas o atienden incidentes. El diagnóstico debe identificar qué hacen, a qué comunidad sirven y cómo se comunican. Esta revisión permite reconocer oportunida-

des de cooperación y evita diseñar servicios que dupliquen funciones sin una justificación operativa.

A partir de esa información, el mandato debe precisar la comunidad atendida, los servicios iniciales y las responsabilidades de coordinación. Del mismo modo, necesita establecer cómo se relacionará el equipo con autoridades reguladoras, responsables de infraestructura, organismos de investigación y gestores de crisis. Cuando varias instituciones intervienen, resulta conveniente acordar criterios de escalamiento y reglas para compartir información sensible. Una matriz de responsabilidades puede ayudar a documentar estas relaciones, siempre que las instituciones involucradas reconozcan su contenido y lo mantengan actualizado.

Por último, la evaluación de recursos completa el diagnóstico. Es necesario revisar perfiles profesionales, disponibilidad, formación, herramientas y presupuesto recurrente. Esta información permite ajustar las expectativas y priorizar servicios que puedan sostenerse. La planificación debería considerar costos de mantenimiento y continuidad, además de los necesarios para iniciar la operación (OEA, 2023).

Como propuesta de implementación, esta fase puede cerrar con cuatro entregables: 1) Un mandato aprobado, 2.) Un mapa de actores y capacidades, 3) Un directorio verificado de contactos y responsabilidades y 4.) Un plan inicial de recursos vinculado con los servicios prioritarios. Estos productos se plantean como instrumentos de trabajo y deben adaptarse a los mecanismos administrativos de cada país.

### 8.2. Segunda fase: servicios y operación

Con el mandato definido y las capacidades identificadas, la siguiente fase consiste en convertir los acuerdos institucionales en servicios que puedan prestarse de manera consistente. El equipo debe establecer cómo recibirá reportes, qué información analizará, cuándo solicitará apoyo y cómo comunicará los resultados. El marco de FIRST (2020) proporciona una referencia para organizar esta cartera, mientras las recomendaciones de NIST (2025) permiten relacionar su ejecución con la gestión del riesgo y la continuidad de los servicios.

La selección inicial debe responder a las necesidades de la comunidad atendida. Un equipo puede comenzar con recepción y clasificación de reportes, análisis inicial, coordinación de respuesta y difusión de alertas. La combinación dependerá del diagnóstico previo y de los recursos disponibles. Lo relevante es que cada servicio tenga destinatarios, responsables y condiciones de prestación claramente establecidos (FIRST, 2020).

Es importante que estas condiciones deben expresarse en procedi-

mientos utilizables. El canal de reporte necesita indicar qué datos se solicitan, cómo se protege la información y qué respuesta puede esperar el remitente. La clasificación requiere criterios para valorar severidad, impacto y urgencia. El escalamiento debe identificar qué circunstancias activan la intervención de otros equipos o autoridades. Estas definiciones facilitan el trabajo cotidiano y permiten reconocer dónde aparecen demoras o decisiones ambiguas.

La operación también necesita distinguir entre asistencia técnica y responsabilidad sobre los sistemas. El CSIRT puede analizar un caso y recomendar medidas, mientras la entidad afectada conserva la autoridad para ejecutarlas sobre su infraestructura. Cuando el incidente involucra a varias organizaciones, los procedimientos deben conectar esas responsabilidades mediante contactos y mecanismos de coordinación previamente acordados (FIRST, 2020; NIST, 2025).

Antes de considerar concluida esta fase, conviene probar los servicios con ejercicios y revisar casos atendidos. La verificación debería mostrar que los reportes llegan al canal previsto, se clasifican mediante criterios compartidos y se asignan a responsables identificados. También, debe permitir comprobar que las recomendaciones se comunican a quienes pueden actuar y que las dificultades quedan documentadas.

Como resultado, esta fase debe producir una cartera de servicios publicada, procedimientos de atención probados y registros que permitan revisar su funcionamiento. La madurez posterior se apoyará en esta evidencia: un equipo puede evaluar y mejorar con mayor precisión cuando conoce cómo ejecuta sus servicios y dónde encuentra obstáculos.

### 8.3. Tercera fase: madurez, cooperación y aprendizaje

Cuando los servicios comienzan a operar, la prioridad es examinar su consistencia y convertir la experiencia en mejoras. La tercera fase articula evaluación de madurez, cooperación y aprendizaje. Su propósito es identificar qué capacidades funcionan, cuáles requieren ajustes y cómo puede sostenerse su desarrollo mediante revisión periódica y colaboración con otros equipos.

SIM3 y el modelo de ENISA ofrecen referencias para establecer una línea de base y examinar dimensiones organizacionales, humanas, tecnológicas y procedimentales. La evaluación debe considerar el mandato y la comunidad atendida, de modo que los resultados puedan interpretarse en relación con las responsabilidades reales del equipo.

Las brechas identificadas deben traducirse en acciones específicas y alcanzables (Open CSIRT Foundation, 2010.; ENISA, 2019).

Esto implica relacionar cada hallazgo con evidencia de operación. Si el diagnóstico señala dificultades de escalamiento, conviene revisar los registros de casos y ejercicios para identificar sus causas. Si muestra dependencia de determinadas personas, puede ser necesario documentar conocimientos y establecer sustituciones. La evaluación adquiere utilidad cuando permite decidir qué cambiar y cómo verificar que la modificación funciona.

La cooperación amplía las posibilidades de aprendizaje y asistencia. Los equipos pueden intercambiar conocimientos, contrastar procedimientos y participar en ejercicios conjuntos. Sin embargo, estos vínculos requieren contactos reconocidos, condiciones de protección de la información y claridad sobre la asistencia disponible. La pertenencia a una red debe acompañarse de relaciones operativas que puedan activarse cuando resulte necesario. En América Latina, los ejercicios intersectoriales y transfronterizos pueden ayudar a identificar dificultades que una institución no observaría por sí sola. Un escenario que afecte a un proveedor compartido, por ejemplo, permite revisar cómo circulan las alertas, cómo se concilian prioridades y qué información necesita cada participante.

Los resultados deberían conducir a correcciones documentadas y a una prueba posterior de los cambios.

El aprendizaje también procede de los incidentes reales. La revisión posterior debe examinar qué permitió detectar el problema, qué decisiones facilitaron la contención y qué condiciones retrasaron la recuperación. Su finalidad es mejorar capacidades y procedimientos mediante una comprensión compartida de lo ocurrido. Las acciones acordadas necesitan responsables y seguimiento para que los hallazgos se incorporen a la operación (NIST, 2025).

Los indicadores pueden apoyar este proceso si se interpretan con cautela. Es posible observar contactos verificados, servicios probados, tiempos de clasificación y acciones correctivas completadas. Sin embargo, una variación aislada no explica todo el desempeño. Un incremento de reportes puede reflejar mayor visibilidad o confianza en el equipo; una reducción del tiempo de atención puede depender de cambios en la complejidad de los casos. Conviene combinar mediciones con revisión cualitativa de los resultados.

Como propuesta de aplicación, esta fase debe generar una evaluación de madurez, un plan de mejora y evidencia de seguimiento. La periodicidad dependerá de los riesgos, los recursos y los cambios de la organización. También será necesario revisar el mandato o la cartera de servicios cuando los ejercicios y la experiencia revelen nuevas necesidades.

Esta tercera fase constituye un ciclo continuo. La evaluación puede mostrar que deben modificarse acuerdos institucionales de la primera fase o procedimientos de la segunda. La hoja de ruta permite así conectar diseño, ejecución y revisión. Su valor para América Latina reside en ofrecer una secuencia adaptable que convierta las orientaciones internacionales en capacidades comprobables y sostenibles.

## Conclusiones

Los marcos internacionales examinados ofrecen aportaciones complementarias para desarrollar la gestión de incidentes cibernéticos en América Latina. Su utilidad depende de traducir las orientaciones en decisiones sobre mandato, servicios, recursos y evaluación. La articulación permite relacionar el diseño institucional con la operación técnica y revisar los resultados mediante evidencia de funcionamiento.

La hoja de ruta propuesta organiza estas contribuciones en tres fases: 1) Mandato y diagnóstico; 2) Servicios y operación; y 3) Madurez, cooperación y aprendizaje. La primera establece el alcance y reconoce las capacidades disponibles. La segunda convierte los acuerdos en procedimientos y servicios probados. La tercera evalúa su consistencia y utiliza la experiencia para corregirlos. La relación entre fases permite revisar decisiones anteriores conforme cambian los riesgos y las necesidades.

Para los profesionales técnicos la principal implicación es que la respuesta necesita conectar el conocimiento técnico con responsabilidades institucionales claras. Detectar una afectación, recomendar una medida y recuperar un servicio exige información sobre prioridades, dependencias y autoridades.

Los marcos ayudan a organizar estas relaciones cuando su aplicación se acompaña de ejercicios, registros y seguimiento de mejoras.

Para los responsables de política pública, la propuesta destaca la importancia de sostener las capacidades más allá de su establecimiento inicial. La continuidad requiere personal, formación, mantenimiento y acuerdos de cooperación. La amplitud de los servicios debe corresponder a recursos que permitan prestarlos de manera consistente y a un mandato reconocido por las instituciones participantes.

América Latina puede utilizar los marcos internacionales para ordenar prioridades y desarrollar capacidades sobre recursos existentes.

El avance será observable cuando los reportes lleguen a quienes pueden atenderlos, las decisiones se coordinen dentro de atribuciones reconocidas y las lecciones se conviertan en mejoras verificables. Esa relación entre orientación, ejecución y aprendizaje constituye el fundamento de la hoja de ruta propuesta.

## Referencias


Aguilar Antonio, J. M. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. *Estudios Internacionales, 53*(198), pp. 169–197. https://doi.org/10.5354/0719-3769.2021.57067

Aguilar-Antonio, J.M. (2023), The Need for a Multistakeholder Approach in Cybersecurity for National Security. Available at SSRN: https://ssrn.com/abstract=4900235

Alghamdi, S. M., Win, K., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. Comput. Secur., 99, 102030. https://doi.org/10.1016/j.cose.2020.102030

Boeke, S. (2018). National cyber crisis management: Different European approaches. *Governance, 31*, 449-464. https://doi.org/10.1111/gove.12309

Dubois, E., & Tatar, U. (2022). Mitigating Global Cyber Risk Through Bridging the National Incident Response Capacity Gap. *International Conference on Cyber Warfare and Security.* https://doi.org/10.34190/iccws.17.1.66

Ethembabaoglu, A., Kadenko, N. I., Angelova, Y., Zhauniarovich, Y., Van Wegberg, R., Parkin, S., & Van Eeten, M. (2026). "Tell Them They Are a Responsible Entity, Not a Customer": Understanding Practitioner Challenges in Sector CSIRTs. *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems.* https://doi.org/10.1145/3772318.3790613

European Union Agency for Cybersecurity [ENISA] (2019). *ENISA CSIRT maturity assessment model.* https://www.enisa.europa.eu/publications/study-on-csirt-maturity

European Union Agency for Cybersecurity [ENISA] (2020). *Driving the global ecosystem of incident response capabilities: New studies now available.* https://www.enisa.europa.eu/news/enisa-news/driving-the-global-ecosystem-of-incident-response-capabilities-new-studies-now-available

Forum of Incident Response and Security Teams [FIRST] (2020). *CSIRT services framework* (Version 2.1). https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

Global Forum on Cyber Expertise [GFCE] (2017). *GFCE global good practices: National computer security incident response teams (CSIRTs).* https://thegfce.org/wp-content/uploads/2020/06/NationalComputerSecurityIncidentResponseTeamsCSIRTs-1.pdf

Hajializadeh, D., & Imani, M. (2021). RV-DSS: Towards a resilience and vulnerability- informed decision support system framework for interdependent infrastructure systems. *Comput. Ind. Eng.*, 156, 107276. https://doi.org/10.1016/j.cie.2021.107276

Hidalgo-Guijarro, J. (2023). Equipo de respuesta ante incidentes informáticos para la seguridad de la información (CSIRT-UPEC). *SATHIRI.* https://doi.org/10.32645/13906925.1200

International Telecommunication Union [ITU] & World Bank (2025). *Guide to developing a national cybersecurity strategy: Strategic engagement in cybersecurity* (3rd ed.). https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.03-2025-PDF-E.pdf

International Telecommunication Union [ITU] (2022a). *Resolución 58 (Rev. Ginebra, 2022): Fomento de la creación de equipos nacionales de respuesta a incidentes informáticos, en particular en los países en desarrollo.* https://www.itu.int/pub/T-RES-T.58-2022/es

International Telecommunication Union [ITU] (2022b). *Resolución 69 (Rev. Kigali, 2022): Facilitación de la creación de equipos nacionales de respuesta a incidentes informáticos, en particular en los países en desarrollo, y de la cooperación entre ellos.* https://www.itu.int/pub/D-RES-D.69-2022

Kamariotou, M., & Kitsios, F. C. (2023). Information Systems Strategy and Security Policy: A Conceptual Framework. *Electronics.* https://doi.org/10.3390/electronics12020382

Kassim, S. R. M., Li, S., & Arief, B. (2023). Understanding How National CSIRTs Evaluate Cyber Incident Response Tools and Data: Findings from Focus Group Discussions. *Digital Threats: Research and Practice, 4,* 1 - 24. https://doi.org/10.1145/3609230

Kazeem, L. O., Adedayo-Ajayi, V., Ajakwe, S., & Fiyinfoluwa, O. (2026). Incident Response in Cybersecurity: A Systematic Review. *Asian Journal of Current Research.* https://doi.org/10.56557/ajocr/2026/v11i411074

Killcrece, G., Kossakowski, K., Ruefle, R., & Zajicek, M. T. (2003). Organizational Models for Computer Security Incident Response Teams (CSIRTs). https://doi.org/10.21236/ada421684

Lee, G.-S., Kim, S., Lee, I., Brown, S., & Carbajal, Y. A. (2024). Adapting cybersecurity maturity models for resource-constrained settings: A case study of Peru. *The Electronic Journal of Information Systems in Developing Countries, 91.* https://doi.org/10.1002/isd2.12350

Lima, A. G. M., & Soares, C. O. (2021). Análisis de las ciberacciones y la ciberorganización en la OEA. *Hemisferio Revista del Colegio Interamericano de Defensa.* https://doi.org/10.59848/21.1207.hv7n3

Meçaj, J. (2026). Enhancing Business Cybersecurity Through Integrated Defense and Incident Response: A Comparative Decision Framework. *International Journal of Advanced Computer Science and Applications.* https://doi.org/10.14569/ijacsa.2026.0170166

National Institute of Standards and Technology [NIST]. (2024). *The NIST cybersecurity framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile* (NIST Special Publication 800-61 Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3

Nowikowska, M. (2021). The Main Tasks of the Network of Computer Security Incident Response Teams in the Light of the Act on the National Cybersecurity System in Poland. *Cybersecurity in Poland.* https://doi.org/10.1007/978-3-030-78551-2_15

Nuñez-Agurto, D., Ron, M., Carrera, E. V., Tapia, F., Cruz, H., Recalde, L., & Fuertes, W. (2022). Design of an Academic CSIRT – A Proposal Based on Strategic

Planning Principles. *Emerging Research in Intelligent Systems.* https://doi.org/10.1007/978-3-030-96043-8_23

Open CSIRT Foundation (2010). SIM3 model & references. Recuperado el 6 de octubre de 2026, de https://opencsirt.org/csirt-maturity/sim3-and-references/

Organización de los Estados Americanos [OEA]. (2023). *Guía práctica para CSIRTs: Un modelo de negocio sustentable* (Vol. 2). https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/Guia-CSIRT%202023%20ESP%20Digital.pdf

Scholta, H., Halsbenning, S., & Niemann, M. (2025). A coordination perspective on digital public services in federal states. *Gov. Inf. Q., 42*, 101984. https://doi.org/10.1016/j.giq.2024.101984

Tanczer, L., Brass, I., & Carr, M. (2018). CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy. *Global Policy*. https://doi.org/10.1111/1758-5899.12625

West-Brown, M., Stikvoort, D., Kossakowski, K., Killcrece, G., Ruefle, R., & Zajicek, M. T. (2003). Handbook for Computer Security Incident Response Teams (CSIRTs). https://doi.org/10.1184/r1/6574055.v1

Yesina, M., & Holubnychyi, D. (2023). CERT-UA assessment based on the CSIRT ENISA Maturity Model. *Radiotekhnika.* https://doi.org/10.30837/rt.2023.2.213.04

***Juan Manuel Aguilar Antonio.*** *Profesor - investigador en la Facultad de Estudios Superiores Aragón de la Universidad Nacional Autónoma de México (UNAM). Es miembro del Sistema Nacional de Investigadores (SNI), nivel Candidato (2024-2027). Realizó dos estancias posdoctorales en el Centro de Investigaciones sobre América del Norte (CISAN-UNAM) con proyectos centrados en ciberseguridad, inteligencia artificial y tecnologías emergentes. En 2026 recibió el reconocimiento de Xiangshan Young Fellow del 13th Beijing Xiangshan Forum. Fue Becario Fulbright-García Robles para el periodo 2025-2026. Es egresado de los programas "Cyber Policy Development" (2019) y "Combating Transnational Threat Networks in the Americas" (2023) del William J. Perry Center, en la Universidad de la Defensa Nacional, en Washington D.C.*

*Desde 2013 ha impartido conferencias y clases en instituciones de seguridad pública de los estados de Chihuahua, Tamaulipas, Jalisco, Estado de México y Guanajuato. En la Escuela Superior de Guerra (ESG), el Centro de Estudios del Ejército y la Fuerza Aérea (CEEFA), la Policía Cibernética de la Ciudad de México (CDMX). El Centro Superior de Estudios Navales (CESNAV) de la Armada de México, de la Secretaría de Marina (SEMAR) y el Instituto Mexicano de Estudios Estratégicos en Seguridad de la Defensa Nacional (IMEESDN), y el Centro Nacional de Inteligencia (CNI).*

*En el ámbito internacional ha impartido clases como mentor senior en el Colegio Interamericano de Defensa (CID), ha sido consultor para la Florida International University (FIU), el U.S. Southern Command, el Instituto de Estudios Estratégicos de Australia (ASPI), la Iniciativa Global contra la Delincuencia Organizada (GITOC) y el Proyecto de Desarrollo e Integración de Mesoamérica. Así como orador en el Foro de Gobernanza Internet (IGF) de la Organización de las Naciones Unidas (ONU) y expositor en Global Conference on Cyber Capacity Building (GC3B) del Global Forum on Cyber Expertise (GFCE). Cuenta con múltiples publicaciones en Journals y/o Revistas Académicas Indexadas de Estados Unidos, México, Colombia, Costa Rica, Chile, Ecuador, España, Guatemala, Colombia y Brasil.*