OEA | CICTE

Basado en el Modelo SIM3

CSIRTAmericas Baseline

Referencia de Madurez para CSIRTs de los Estados miembros de la OEA

CSIRTAmericas Network

UK Government

Open CSIRT Foundation

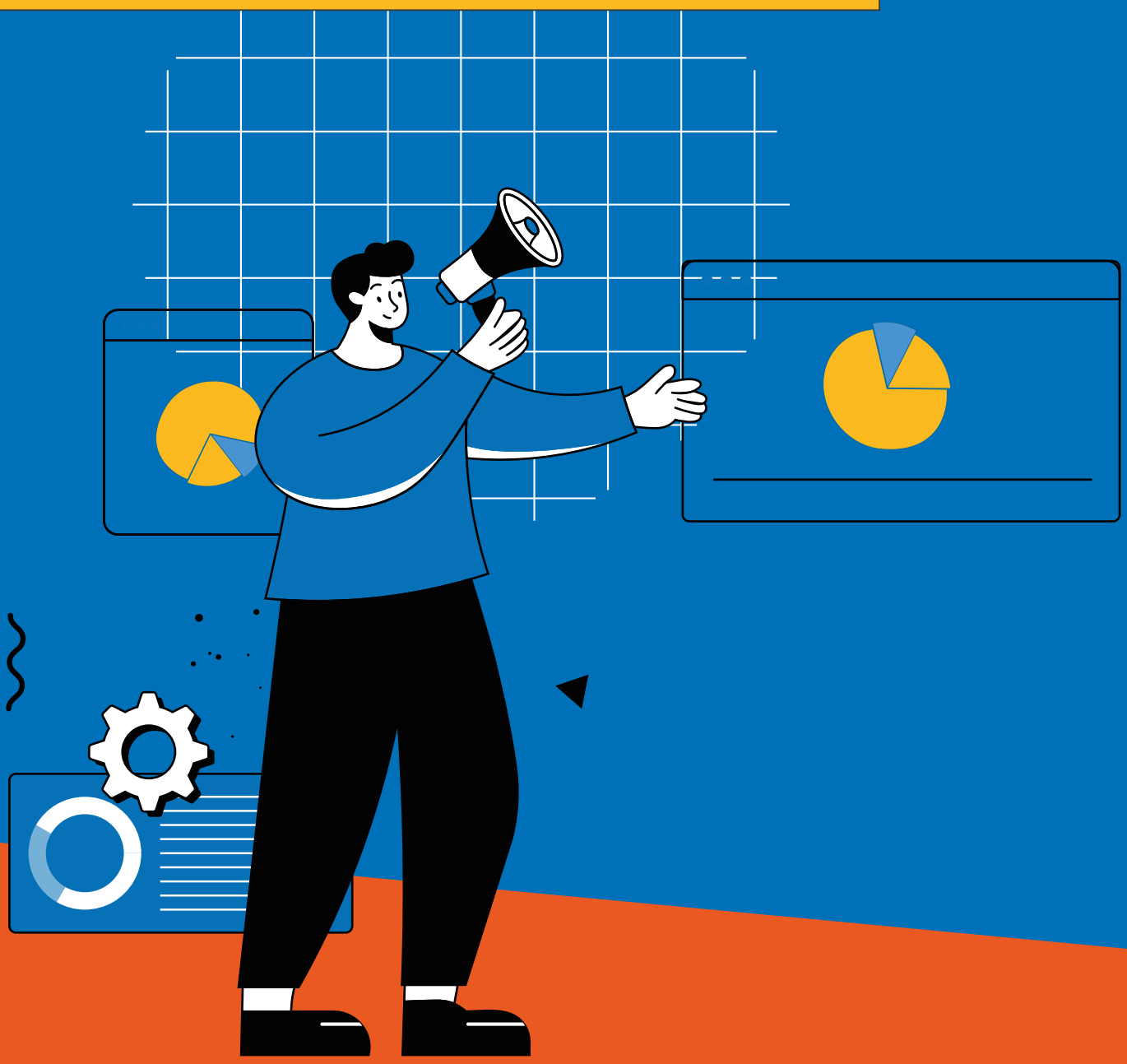
CSIRTs con madurez, Estados miembros más seguros

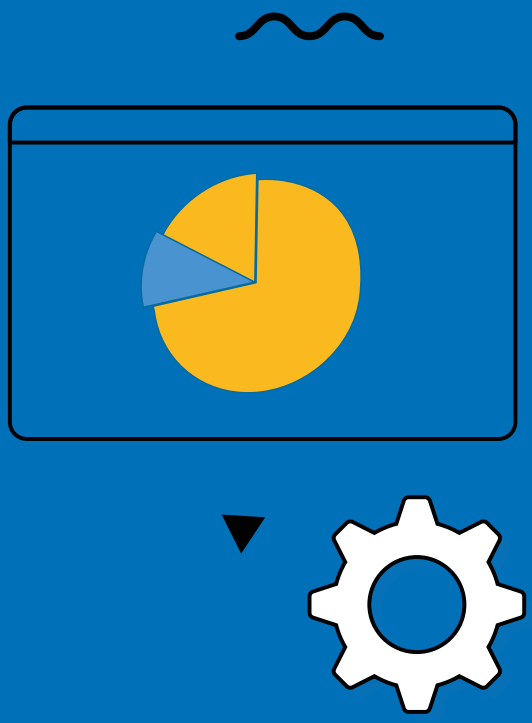
CSIRTAmericas Baseline

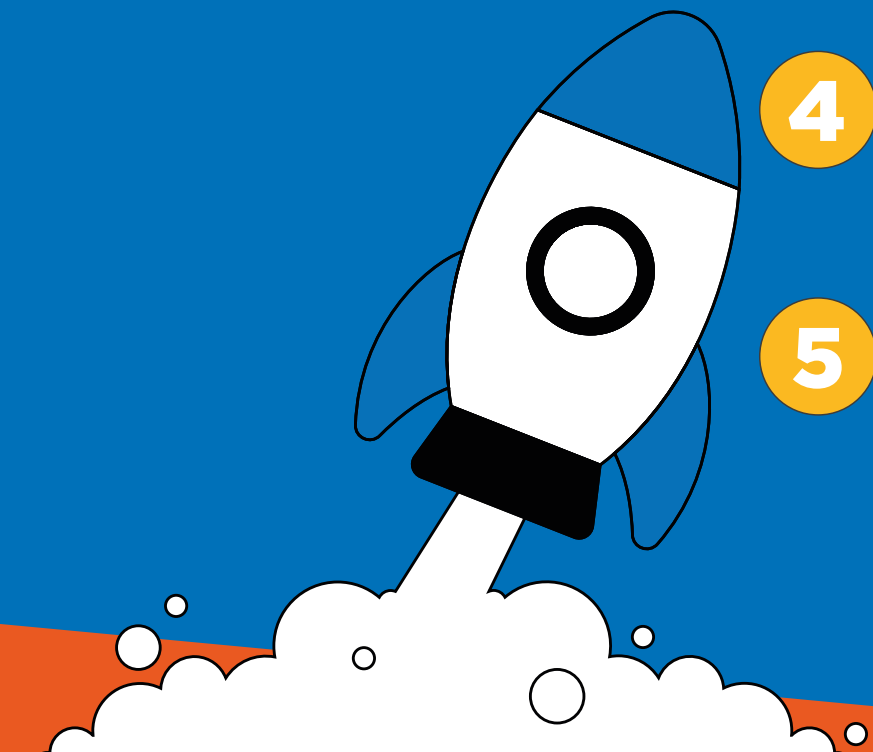
Referencia de **Madurez** para CSIRTs de los Estados miembros de la OEA

Basado en el Modelo SIM3

Tabla de Contenido







1. INTRODUCCIÓN

CSIRTAmericas[1] es la red de Equipos de Respuesta ante Incidentes Cibernéticos (CSIRT) gubernamentales de los Estados Miembros de la Organización de los Estados Americanos (OEA). Actúa como el impulsor principal de la Sección de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE) de la OEA en el fortalecimiento de las capacidades de respuestas ante incidentes cibernéticos de la región, promoviendo la cooperación y el intercambio efectivo de información entre los CSIRTs de la región, facilitando respuestas más rápidas y coordinadas frente a los incidentes cibernéticos.

En línea con este propósito, es fundamental evaluar de forma continua la madurez de un CSIRT para enfrentar los incidentes cibernéticos. La madurez es el estado en el que algo o alguien alcanza su desarrollo completo y funciona de manera estable y efectiva. En el caso de un CSIRT, se refleja en su estructura organizativa, su integración con la comunidad a la que sirve, la preparación de los miembros de su equipo, el uso eficiente de herramientas tecnológicas y la implementación de procesos claros para gestionar incidentes. Evaluar el nivel de madurez debe ser realizado con metodologías que impulsen su evolución, permitiendo identificar fortalezas y áreas de mejora, optimizar recursos, establecer prioridades estratégicas y garantizar que el equipo esté preparado para enfrentar un panorama de amenazas cibernéticas cada vez más complejo.

Este documento presenta el nuevo recurso de la red CSIRTAmericas: **"SIM3 CSIRTAmericas Baseline"**, una línea base de madurez desarrollada a partir del modelo SIM3[2], creado por Open CSIRT Foundation[3] (OCF), un modelo reconocido internacionalmente para evaluar la madurez de los equipos de seguridad. "CSIRTAmericas Baseline" sirve para que las organizaciones puedan evaluar de manera estructurada la preparación de sus equipos de respuesta a incidentes cibernéticos.

Objetivos principales

Actuar como una referencia para que cualquier CSIRT de los Estados Miembros de la OEA evalúen su nivel de madurez.

Para más detalles, consulte la Sección III.

Servir como requisito para que los CSIRTs gubernamentales puedan solicitar su incorporación a la red CSIRTAmericas.

Para más detalles, consulte la Sección IV.

Es importante destacar que el modelo SIM3 es aplicable a cualquier tipo de organización CSIRT[4], sin importar su naturaleza (pública o privada), tamaño o sector.

[1] CSIRTAmericas es la red de CSIRT gubernamentales de los Estados miembros de la OEA: www.csirtamericas.org
[2] SIM3: Modelo de Madurez para la Gestión de Incidentes de Seguridad. https://opencsirt.org/csirt-maturity/sim3-and-references/
[3] OCF: Open CSIRT Foundation. https://opencsirt.org/
[4] CSIRT, CERT, IRT, NCSC y otros son variaciones que pueden clasificarse como CSIRT.

2. **SIM3:** Modelo de Madurez de la Gestión de Incidentes de Seguridad

SIM3 es un modelo que permite medir el nivel de madurez de los equipos responsables de la gestión de ciberamenazas, vulnerabilidades e incidentes de seguridad. Este modelo es gestionado y desarrollado por la Open CSIRT Foundation (OCF).

SIM3 ofrece un enfoque simple y estructurado basado en parámetros clave para analizar áreas fundamentales como la organización, el factor humano, las herramientas y los procesos. Al seguir este enfoque, los equipos de seguridad pueden avanzar paso a paso en la mejora de su nivel de madurez. Además, el modelo permite reportar a la gerencia de manera clara y efectiva, destacando los problemas identificados y las áreas que requieren mejoras. Esto podría facilitar la justificación y priorización de recursos en términos de presupuesto, personal, capacitación y otros aspectos críticos para fortalecer las capacidades del equipo.

Actualmente, SIM3 está centrado en el **perfil CSIRT**; sin embargo, la OCF está trabajando en tres nuevos perfiles para los equipos SOC, ISAC y PSIRT. A continuación, se ofrece una breve descripción de estos equipos:

- **SOC (Security Operations Center):** Equipos encargados de detectar amenazas en curso que podrían convertirse en incidentes. Cuando estas amenazas alcanzan un nivel de gravedad significativo, se escalan a los responsables correspondientes para su gestión.

- **CSIRT (Computer Security Incident Response Team):** Equipos responsables de gestionar los incidentes de seguridad, ya sea de manera directa o a través de la coordinación. Por lo general, también se enfocan en la prevención y detección de amenazas.

- **ISAC (Information Sharing and Analysis Center):** Equipos especializados en recopilar, analizar y compartir información sobre amenazas, sin participar directamente en la gestión o coordinación de incidentes.

- **PSIRT (Product Security Incident Response Team):** Equipos que se centran en la gestión de vulnerabilidades y problemas de seguridad relacionados con los productos tecnológicos de la organización, trabajando en estrecha colaboración con los equipos de desarrollo.

Para los fines de este documento,
el enfoque se centra exclusivamente en el **perfil CSIRT**.

El modelo SIM3 abarca cuatro categorías fundamentales:

Organización, Aspectos Humanos, Herramientas y Procesos

Donde el proceso de evaluación consiste en 45 preguntas distribuidas entre estas categorías, diseñadas para medir el nivel de madurez. Para cada pregunta, se selecciona un nivel que varía desde 0 (desconocimiento o inexistencia del elemento evaluado) hasta 4 (procesos auditados y optimizados de manera continua).

OCF capacita formalmente a los auditores certificados[5] en la aplicación del modelo SIM3. Únicamente estos auditores certificados están autorizados para emitir certificados relacionados con auditorías y evaluaciones formales basadas en el estándar de la OCF. Además de su aplicación formal, el modelo SIM3 también puede ser utilizado como una herramienta de autoevaluación para organizaciones de cualquier tipo, tamaño o naturaleza. Este enfoque permite a las organizaciones identificar áreas de mejora y beneficiarse del proceso sin necesidad de cumplir con requisitos específicos o de una certificación formal.

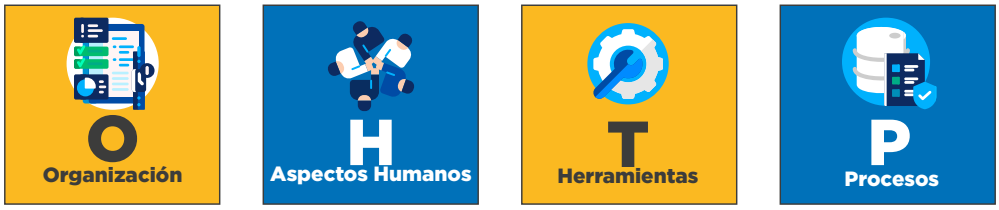
[5] Auditores SIM3 certificados: https://opencsirt.org/csirt-maturity/certified-auditors/

Elementos fundamentales

1) Parámetros de Madurez

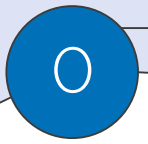
Parámetros son las variables que se miden con respecto a la madurez del CSIRT - hay 45 para el perfil CSIRT. Para más detalles, consulte la Sección III.

2) Categorías de Madurez

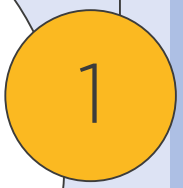


3) Niveles de madurez

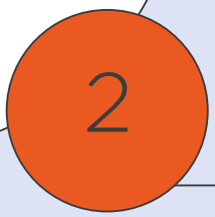
4 = explícito, auditado/ evaluado periódicamente por la autoridad de los niveles de gobernanzas superiores al jefe/gerente del CSIRT - sujeto a un proceso de control, auditoría, evaluación o aplicación periódicos.



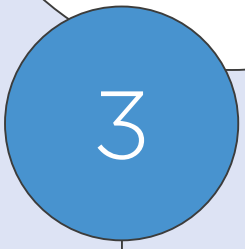
0 = no disponible / indefinido / desconocido - no se ha considerado todavía.



1 = implícito - conocido/ considerado, pero no escrito, "entre las orejas", lo que los expertos hacen de memoria sin base escrita ni herramientas.



2 = explícito, interno - escrito, pero no formalizado de ninguna manera, escritos informales, nivel de borrador.



3 = explícito, formalizado bajo la autoridad del jefe/ director del CSIRT o de un nivel superior - aprobado formalmente, sellado o publicado (abiertamente).

3. SIM3 CSIRTAmericas Baseline

SIM3 CSIRTAmericas Baseline es una referencia para medir el nivel de madurez de los CSIRTs en los Estados Miembros de la OEA. Fue desarrollada por la red CSIRTAmericas de la OEA/CICTE en colaboración con la Open CSIRT Foundation.

Una línea base (baseline) de SIM3 establece niveles mínimos de madurez (en una escala de 0 a 4) para un subconjunto o la totalidad de los parámetros de SIM3. También puede incluir requisitos o aclaraciones adicionales según el contexto. Estas líneas base se diseñan con fines específicos: por ejemplo, FIRST[6] tiene su propia línea base de SIM3 para su membresía, TF-CSIRT[7] en Europa utiliza TI-Certification para certificar equipos, y ENISA[8] ha desarrollado varias líneas base enfocadas en CSIRTs nacionales y sectoriales, y de manera similar, CSIRTAmericas ha establecido su propia línea base de membresía.

SIM3 CSIRTAmericas Baseline está adaptado a la realidad y desafíos específicos de los CSIRTs nacionales y sectoriales en América Latina y el Caribe. Su desarrollo se basó en la experiencia regional de equipos miembros de la red CSIRTAmericas con el conocimiento especializado de la Open CSIRT Foundation (OCF), creadora del modelo SIM3. Además, se basó en recursos clave, como la Guía Práctica para CSIRTS[9]y la Guía de Buenas Prácticas para establecer un CSIRT Nacional[10] de OEA/CICTE, junto con documentos relevantes de ENISA[11] y FIRST[12] sobre evaluación de madurez.

Evaluar los parámetros de SIM3 CSIRTAmericas Baseline representa una valiosa oportunidad para que los CSIRTs identifiquen áreas de mejora y fortalezcan sus capacidades de manera estructurada. Para maximizar este potencial, se recomienda una aplicación gradual que comience con autoevaluaciones internas e informales.

Proceso de aplicación recomendado:

•Autoevaluación inicial

El CSIRT realiza una autoevaluación exhaustiva utilizando la herramienta[13] en línea de Open CSIRT Foundation (OCF), que incluye un diagrama de radar para comparar el estado actual con los niveles requeridos y facilitar el seguimiento del progreso.

• Plan de mejora

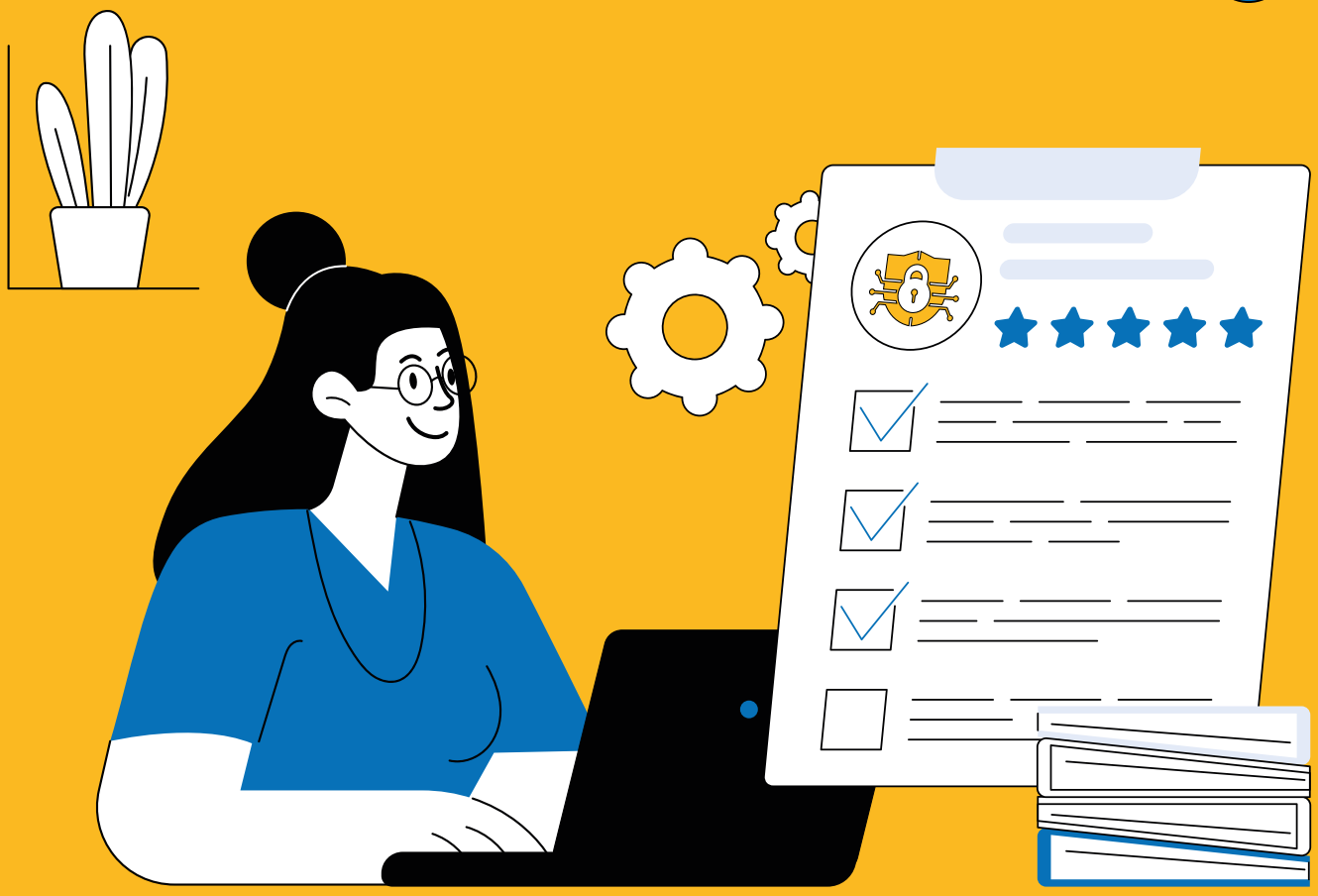
Basándose en los resultados de la autoevaluación, el CSIRT desarrolla un plan de acción con objetivos claros y plazos realistas para abordar las áreas de mejora identificadas. A medida que avanza en su plan de mejora, el CSIRT verifica los parámetros alcanzados.

• Validación de resultados

En el caso de autoevaluaciones, no es necesario contar con una línea de base, ya que el propósito principal es la mejora continua. En caso se requiera una constancia formal de evaluación o auditoría, esta debe ser realizada por auditores certificados por OCF, ya que son los únicos autorizados.

6. FIRST: Forum of Incident Response and Security Teams. https://www.first.org
7. TF-CSIRT: Trusted Introducer for CSIRTs. https://tf-csirt.org/
8. ENISA: European Union Agency for Cybersecurity. https://www.enisa.europa.eu
9. Guía práctica para CSIRTs, Vol. 2, Organización de los Estados Americanos, 2023. https://shares.csirtamericas.org/s/AqfMc7XYBmcRpZM/download/Guia-CSIRT%202023%20ESP%20V6.pdf
10. Guía de Buenas Prácticas para establecer un CSIRT Nacional, Organización de los Estados Americanos, 2016. https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2016%20-%20Buenas%20Practicas%20CSIRT.pdf
11. ENISA CSIRT Maturity Framework. https://www.enisa.europa.eu/topics/incident-response/csirt-capabilities/csirt-maturity
12. FIRST Membership Baseline. https://www.first.org/membership/process#annex-3
13. Herramienta en línea SIM3. https://sim3-check.opencsirt.org/#/

Comienza a usar la **“herramienta de evaluación CSIRTAmericas Baseline”** y evalúa la Organización, Aspectos Humanos, Herramientas y Procesos de tu CSIRT, **responde 45 preguntas**, eligiendo entre nivel 0 (desconoces su existencia o no tienes conocimiento) hasta nivel 4 (es un proceso auditado y optimizado continuamente)



3.1. Herramienta de Evaluación de CSIRTAmericas Baseline

Identificador de Parámetro SIM3	Nombre del Parámetro SIM3	Descripción	CSIRTAmericas Baseline	CSIRT Level
Organización				
O-1	Mandato	La asignación del CSIRT derivada de los niveles superiores de gobernanza.	**3**	
O-2	Comunidad	A quién van dirigidas las funciones del CSIRT: los «clientes» del CSIRT.	**3**	
O-3	Autoridad	Lo que el CSIRT está autorizado a hacer hacia su comunidad para cumplir con su función.	**3**	
O-4	Responsabilidad	Lo que se espera que el CSIRT haga hacia su circunscripción con el fin de cumplir con su función.	**3**	
O-5	Descripción del Servicio	Describe en qué consiste el servicio del CSIRT y cómo acceder a él. Aclaración: Un excelente punto de partida es el documento de FIRST 'FIRST Services Framework' que ofrece una definición exhaustiva y estructurada de todos los tipos de servicios que un CSIRT, ISAC o SOC (y en menor medida también PSIRT) puede ofrecer a su comunidad. La forma de utilizar este marco es partir del mandato de su equipo -y de los recursos que dispone- y, a continuación, seleccionar primero los servicios que debe prestar para cumplir su mandato, para pasar después a los que le gustaría prestar (pero para los que probablemente no disponga de recursos). Requisito mínimo: Contiene la información de contacto del CSIRT, las ventanas de servicio, una descripción concisa de los servicios ofrecidos y la política del CSIRT en materia de tratamiento y divulgación de la información. Disponible públicamente en inglés.	**3**	
O-6	Política de Medios Públicos	Describe la política del CSIRT sobre cómo tratar e interactuar con los medios de comunicación públicos.	**2**	

3.1. Herramienta de Evaluación de CSIRTAmericas Baseline

Identificador de Parámetro SIM3	Nombre del Parámetro SIM3	Descripción	CSIRTAmericas Baseline	CSIRT Level
Organización				
O-7	Descripción del Nivel de Servicio	Describe el nivel de servicio que se espera del CSIRT. Requisito mínimo: Especifica la velocidad de reacción a los reportes de incidentes entrantes, a los reportes de su comunidad y de los CSIRTs pares. Para estos últimos, lo mínimo que se espera es una reacción humana en un plazo de dos días laborables.	**3**	
O-8	Clasificación de Incidentes	Describe la disponibilidad y el uso de un esquema de clasificación aplicado a los incidentes registrados, que generalmente incluye una lista de categorías técnicas para asociar cada incidente o amenaza, , como por ejemplo si tiene las características de “spam”, “compromiso de raíz” o “DDoS”, etc. Aclaración: Las clasificaciones de incidentes suelen contener al menos «tipos» de incidentes o categorías de incidentes. Sin embargo, también pueden incluir la «gravedad» de los incidentes y potencialmente. Un esquema de clasificación popular de este tipo es la “Taxonomía de clasificación de incidentes de referencia” de ENISA.	**3**	
O-9	Participación en Sistemas de CSIRT	Describe el nivel de membresía del CSIRT en una cooperación de CSIRT bien establecida, ya sea directamente o a través de un CSIRT ‘ascendente’ del cual es cliente. Esto es necesario para participar e integrarse en las comunidades de CSIRTs transnacionales/ mundiales.	**2**	
O-10	Marco Organizativo	Une los parámetros del O-1 a O-9 en un documento marco coherente que sirva como el documento de control para el CSIRT. Requisito Mínimo: Describe la misión del equipo y los Parámetros O-1 a O-9 ya sea proporcionando referencias a documentos específicos o combinando los detalles requeridos en un solo documento.	**3**	
O-11	Política de Seguridad	Describe el marco de seguridad dentro del cual opera el CSIRT. Esto puede ser parte de un marco más grande, o el CSIRT puede tener su propia política de seguridad.	**2**	

3.1. Herramienta de Evaluación de CSIRTAmericas Baseline

CSIRTAmericas Baseline

Identificador de Parámetro SIM3	Nombre del Parámetro SIM3	Descripción	CSIRTAmericas Baseline	CSIRT Level
Aspectos Humanos				
H-1	Código de Conducta/ Práctica/Ética	Un conjunto de reglas o directrices para los miembros del CSIRT sobre cómo comportarse profesionalmente, potencialmente también fuera del trabajo. Aclaración: Por ejemplo, TI CCoP[14] o EthicsFIRST[15]. El comportamiento fuera del trabajo es relevante, porque se puede esperar de los miembros del CSIRT que se comporten de forma responsable también en privado cuando se trate de ordenadores y seguridad.	**2**	
H-2	Resiliencia del Personal	Cómo se asegura la dotación de personal del CSIRT durante enfermedades, vacaciones, salidas de personal, etc. Requisito mínimo: tres miembros del CSIRT (a tiempo parcial o a tiempo completo)	**2**	
H-3	Descripción del Conjunto de Habilidades	Describe las habilidades necesarias para los trabajos en el CSIRT. Aclaración: Un excelente punto de partida es el documento de FIRST 'CSIRT Roles and Competences' que parte del Marco de Servicios de FIRST (https://www.first.org/standards/frameworks/csirts/csirt_roles_competences), y luego trabaja hacia las habilidades/competencias necesarias para los diversos roles que dan vida a todo tipo de servicios a la comunidad.	**2**	
H-4	Desarrollo del Personal	Política de desarrollo profesional para capacitar a nuevos miembros y mejorar las habilidades de los existentes.	**2**	
H-5	Capacitación Técnica	Programa que permita al personal obtener formación técnica relacionada con el trabajo - como TRANSITS, FIRST, ENISA, OAS o formación similar de CSIRTs, o programas de formación comerciales (CERT/CC, SANS, etc.)	**1**	
H-6	Capacitación en Habilidades Blandas	Programa para que el personal reciba formación en competencias interpersonales, especialmente en comunicación (humana) y presentación.	**1**	
H-7	Redes Externas	Salir y reunirse con otros CSIRTs. Contribuir al sistema de CSIRT cuando sea posible.	**2**	

[14] TI CCoP: Trusted Introducer Code of Practice. https://www.trusted-introducer.org/TI-CCoP.pdf

[15] EthicsFIRST: Ethics Framework for Incident Response and Security Teams. https://ethicsfirst.org

3.1. Herramienta de Evaluación de CSIRTAmericas Baseline

Identificador de Parámetro SIM3	Nombre del Parámetro SIM3	Descripción	CSIRTAmericas Baseline	CSIRT Level
Herramientas				
T-1	Activos y Configuraciones de TI	Describe los activos (hardware, software, OT, etc.) utilizados habitualmente en la comunidad, incluidas sus configuraciones, para que el CSIRT pueda proporcionar asesoramiento específico sobre ellos.	**1**	
T-2	Lista de Fuentes de Información	De dónde obtiene el CSIRT su información sobre vulnerabilidades/amenazas/escaneo.	**2**	
T-3	Sistema(s) de Mensajería Consolidada(s)	Cuando todo el correo electrónico del CSIRT y otros tipos de mensajes (signal, threema, cable, etcétera) se mantienen en sistemas abiertos a todos los miembros del CSIRT, hablamos de sistema(s) de mensajería consolidado(s).	**3**	
T-4	Sistema de Seguimiento de Incidentes	Un sistema de gestión de tickets o software de flujo de trabajo utilizado por el CSIRT para registrar incidentes y rastrear su flujo de trabajo. Aclaración: RT(IR), OTRS, TheHive, sistemas de tickets de incidencias en general.	**1**	
T-5	Llamadas de Voz Resilientes	El sistema de llamadas de voz para el CSIRT es resistente cuando sus niveles de disponibilidad y tiempo de recuperación cumplen o superan los requisitos de servicio del CSIRT. Aclaración: Las llamadas de voz incluyen las llamadas telefónicas tradicionales (móviles y fijas), además de las llamadas de voz que utilizan herramientas de mensajería; el vídeo puede incluirse en las llamadas de voz. Los teléfonos móviles, con sus múltiples opciones de comunicación, son el mecanismo alternativo más sencillo para cuando el sistema telefónico de un equipo no funciona. Requisito mínimo: Mecanismo de emergencia en caso de interrupción del sistema de llamadas de voz.	**1**	
T-6	Mensajería Resiliente	El sistema o sistemas de mensajería disponibles para el CSIRT son resilientes cuando sus niveles de disponibilidad y tiempo de recuperación cumplen o superan los requisitos de servicio del CSIRT.	**1**	

3.1. Herramienta de Evaluación de CSIRTAmericas Baseline

Identificador de Parámetro SIM3	Nombre del Parámetro SIM3	Descripción	CSIRTAmericas Baseline	CSIRT Level
Herramientas				
T-7	Acceso a Internet Resiliente	El acceso a Internet disponible para el CSIRT es resiliente cuando sus niveles de disponibilidad y tiempo de reparación cumplen o superan los requisitos de servicio del CSIRT.	**1**	
T-8	Conjunto de Herramientas de Prevención de Incidentes	Una colección de herramientas destinadas a prevenir que ocurran incidentes en la comunidad. El CSIRT opera o utiliza estas herramientas o tiene acceso a los resultados generados por ellas. Aclaración: Por ejemplo, IPS, escaneo de virus, filtros de spam, escaneo de puertos. Si no es aplicable como para un CSIRT puramente coordinador, elija N/A y el parámetro se omitirá de la "puntuación".	**1**	
T-9	Conjunto de Herramientas de Detección de Incidentes	Una colección de herramientas destinadas a detectar incidentes cuando ocurren o están cerca de ocurrir. El CSIRT opera o utiliza estas herramientas o tiene acceso a los resultados generados por ellas. Aclaración: Por ejemplo, IDS, redes de cuarentena, análisis de flujo de red.	**1**	
T-10	Conjunto de Herramientas de Resolución de Incidentes	Una colección de herramientas destinadas a detectar incidentes cuando ocurren o están cerca de ocurrir. El CSIRT opera o utiliza estas herramientas o tiene acceso a los resultados generados por ellas. Aclaración: Por ejemplo, IDS, redes de cuarentena, análisis de flujo de red.	**1**	
Procesos				
P-1	Escalación a Nivel de Gobernanza	Proceso de escalación a la alta dirección para los CSIRTs que forman parte de la misma organización host (anfitriona) que su comunidad. Para comunidades externas: escalación a los niveles de gobernanza apropiado de los integrantes de su comunidad.	**3**	
P-2	Escalación a la Función de Prensa	Proceso de escalación a la oficina de prensa de la organización host del CSIRT.	**2**	
P-3	Escalación a la Función Legal	Proceso de escalación a la oficina legal de la organización host del CSIRT.	**2**	

3.1. Herramienta de Evaluación de CSIRTAmericas Baseline

Identificador de Parámetro SIM3	Nombre del Parámetro SIM3	Descripción	CSIRTAmericas Baseline	CSIRT Level
Procesos				
P-4	Proceso de Prevención de Incidentes	Describe cómo el CSIRT previene incidentes, incluyendo el uso del conjunto de herramientas relacionadas. Además, esto incluye la adopción de servicios proactivos como la emisión de avisos sobre amenazas/vulnerabilidades/ parches. Aclaración: Si no es aplicable, como para el caso de un CSIRT puramente coordinador, elige N/A como Nivel y el parámetro se omitirá de la «puntuación».	**2**	
P-5	Proceso de Detección de Incidentes	Describe cómo el CSIRT detecta incidentes, incluyendo el uso del conjunto de herramientas relacionadas.	**2**	
P-6	Proceso de Resolución de Incidentes	Describe cómo el CSIRT resuelve incidentes, incluyendo el uso del conjunto de herramientas relacionadas.	**2**	
P-7	Procesos de Incidentes Específicos	Describe cómo el CSIRT gestiona categorías específicas de incidentes, como phishing, DDoS o problemas de derechos de autor. Aclaración: puede ser parte de P-6.	**1**	
P-8	Proceso de Auditoría y Retro-alimentación	Describe cuál es el proceso para auditar/evaluar el CSIRT y la subsiguiente retroalimentación al equipo. El proceso de auditoría/evaluación puede tener una parte de autoevaluación interna del equipo, así como una auditoría independiente. Aquellos elementos que el CSIRT y su dirección consideran que no cumplen con los estándares, se tienen en cuenta para futuras mejoras. Aclaración: Por auditoría independiente se entiende cualquier tipo de auditoría no realizada por el propio equipo, sino que tiene lugar bajo la autoridad de niveles de gestión superiores. Este tipo de auditoría puede adoptar muchas formas: puede seguir siendo interna, por ejemplo, realizada por el CISO o en su nombre, o por un departamento de auditoría. O puede ser externa, por medio de un subcontratista, o como parte de un esquema de auditoría/evaluación dentro de una comunidad de CSIRT.	**2**	

3.1. Herramienta de Evaluación de CSIRTAmericas Baseline

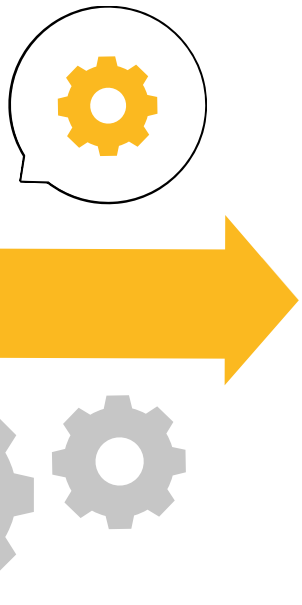
Identificador de Parámetro SIM3	Nombre del Parámetro SIM3	Descripción	CSIRTAmericas Baseline	CSIRT Level
Procesos				
P-9	Proceso de Contacto en Emergencias	Describe cómo contactar al CSIRT en casos de emergencia. Aclaración: A menudo, esto sólo disponible para otros equipos, socios o su comunidad en específico.	**2**	
P-10	Mejor Práctica de Presencia en Internet	Este proceso describe (1) la forma en que los alias genéricos de buzones de correo @ org.tld relacionados con la seguridad son gestionados por el CSIRT, o por las partes que saben cuándo deben informar al CSIRT; (2) la presencia en la web; y (3) la presencia en los medios sociales. Aclaración: El proceso debe tener en cuenta, para las tres áreas mencionadas: (1) el seguimiento por parte del CSIRT de al menos las direcciones de correo electrónico estándar cert@... y security@... - y se recomienda encarecidamente que se tenga en cuenta la norma RFC2142 y se garantice el seguimiento de los nombres de los buzones de correo pertinentes (postmaster y webmaster merecen especial atención). Y también, que quienes rastreen esos nombres de buzón, conozcan el CSIRT y sepan cómo transmitirles información. (2) una política web que garantice que toda la información relevante sobre el CSIRT esté actualizada y disponible para la circunscripción, y un subconjunto necesario que incluya RFC2350 (véase O-5) para el mundo.	**2**	
P-11	Proceso de Manejo Seguro de Información	Describe cómo el CSIRT gestiona los informes y/o la información confidencial sobre incidentes. También tiene relación con los requisitos legales pertinentes, incluida la legislación sobre privacidad, por ejemplo: GDPR (por sus siglas en inglés, General Data Protection Regulation). Requisito mínimo: El proceso debe apoyar el uso de TLP (por sus siglas en inglés Traffic Light Protocol).	**2**	
P-12	Proceso de Fuentes de Información	Describe cómo el CSIRT maneja las diversas fuentes de información disponibles para el CSIRT (según lo definido en la herramienta relacionada, si está disponible – ver T-2).	**1**	

3.1. Herramienta de Evaluación de CSIRTAmericas Baseline

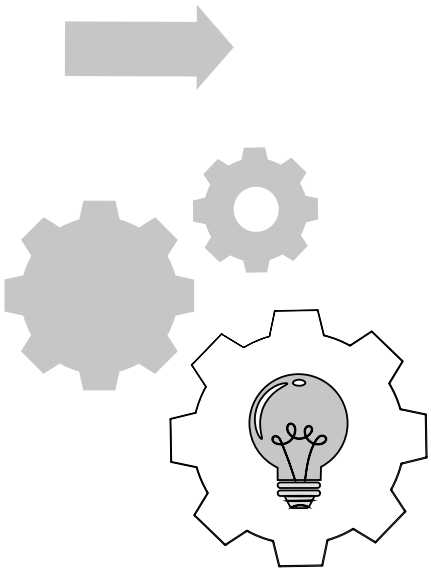
Identificador de Parámetro SIM3	Nombre del Parámetro SIM3	Descripción	CSIRTAmericas Baseline	CSIRT Level
Procesos				
P-13	Proceso de Difusión	Describe cómo el CSIRT llega a su comunidad, no en lo que respecta a los incidentes, sino a las relaciones públicas y la sensibilización. Este proceso debe permitir un canal bidireccional: los miembros de su comunidad objetivo también deben poder proporcionar información al equipo. Aclaración: Téngase en cuenta que la retroalimentación de la circunscripción al equipo (ascendente) es diferente de la retroalimentación mencionada en el proceso P-8, que es de la administración superior al equipo (descendente).	**1**	
P-14	Proceso de Informes de Gobernanza	Describe cómo informa el CSIRT a sus niveles superiores de gobierno. Este tipo de informes suele incluir estadísticas y gráficos. Aclaración: Si el CSIRT está situado dentro de una organización host, este proceso se refiere a los informes enviados a la dirección de la organización host, y/o al CISO, CSO o CIO, es decir, internamente. En el caso de un equipo nacional, se tratará de informar al ministro responsable, y posiblemente al parlamento.	**2**	
P-15	Proceso de Informes a la Comunidad	Describe lo que el CSIRT informa a su comunidad y/o más allá (potencialmente al mundo). Aclaración: Este tipo de informes puede variar desde concisos y genéricos, hasta más detallados, incluyendo estadísticas y gráficos (basados en su clasificación de incidentes, ver O-8). A veces - especialmente con CSIRT nacionales- adopta la forma de informes anuales de tendencias. También es válido elegir explícitamente informar sólo internamente y no a la circunscripción: en ese caso elija N/A y el parámetro se omitirá de la "puntuación".	**1**	
P-16	Proceso de Reuniones	Define el proceso de reuniones internas del CSIRT. Aclaración: Esto puede incluir reuniones en línea e híbridas	**1**	

3.1. Herramienta de Evaluación de CSIRTAmericas Baseline

Identificador de Parámetro SIM3	Nombre del Parámetro SIM3	Descripción	CSIRTAmericas Baseline	CSIRT Level
Procesos				
P-17	Proceso de Colaboración entre Pares	Describe cómo el CSIRT trabaja junto con CSIRTs pares y/o con su CSIRT "ascendente" - y también con pares entre otros tipos de equipos de seguridad como SOCs, PSIRTs, ISACs, etcétera. Aclaración: Un equipo par es un equipo de seguridad con el que existe un tipo especial de relación, basada en la pertenencia compartida a alguna comunidad o cooperación, o en acuerdos tipo MoU. Requisito mínimo: El proceso debe definir qué "pares" existen, y garantizar que con esos pares se establece una comunicación bidireccional de confianza.	**1**	

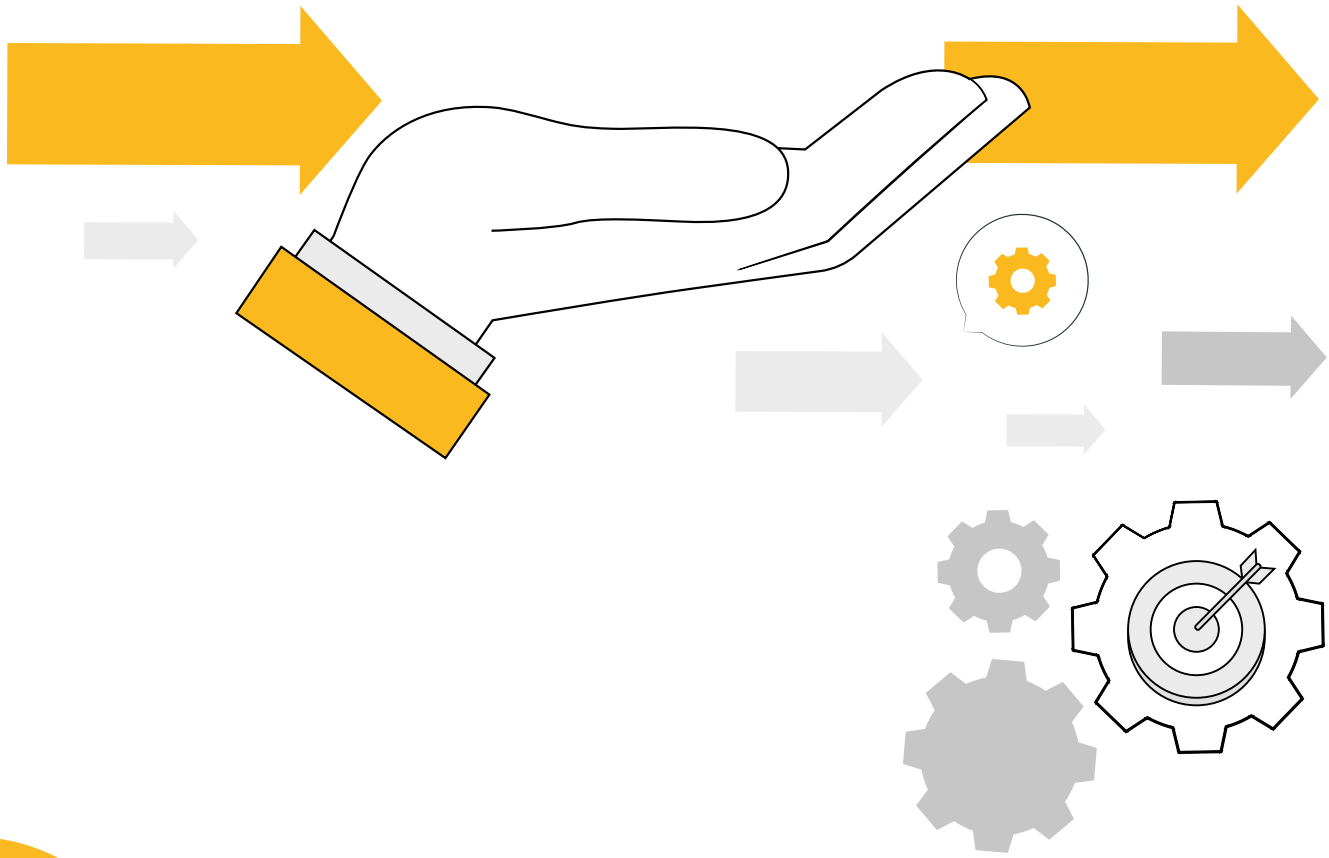


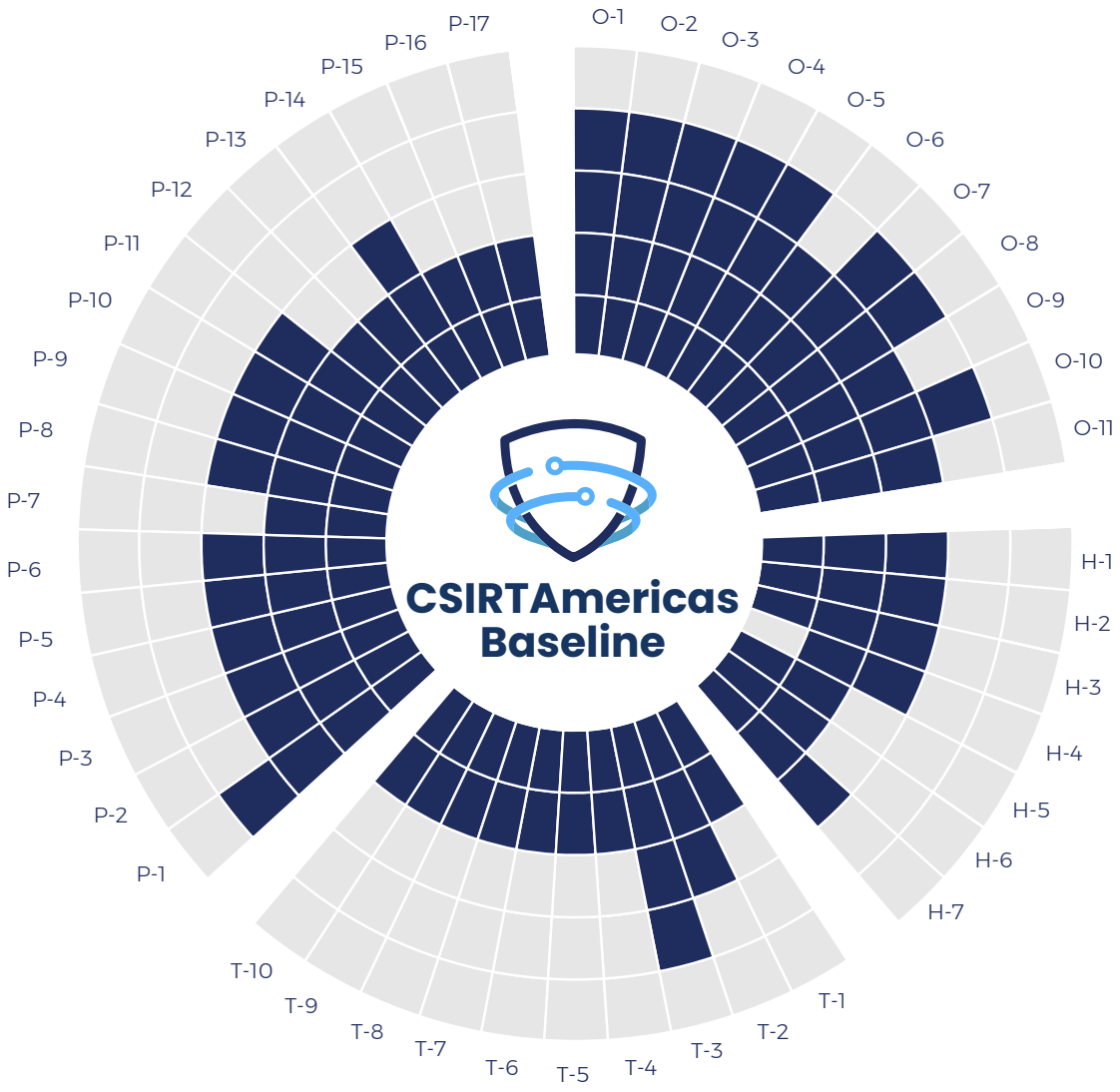
¿Qué revela la evaluación?



3.2. Diagrama de radar de CSIRTAmericas Baseline

A continuación, se presenta un diagrama de «radar» que refleja todos los Parámetros y Niveles requeridos para CSIRTAmericas Baseline, facilitando la comparación visual entre el estado actual del CSIRT y el estado requerido (CSIRTAmericas Baseline).



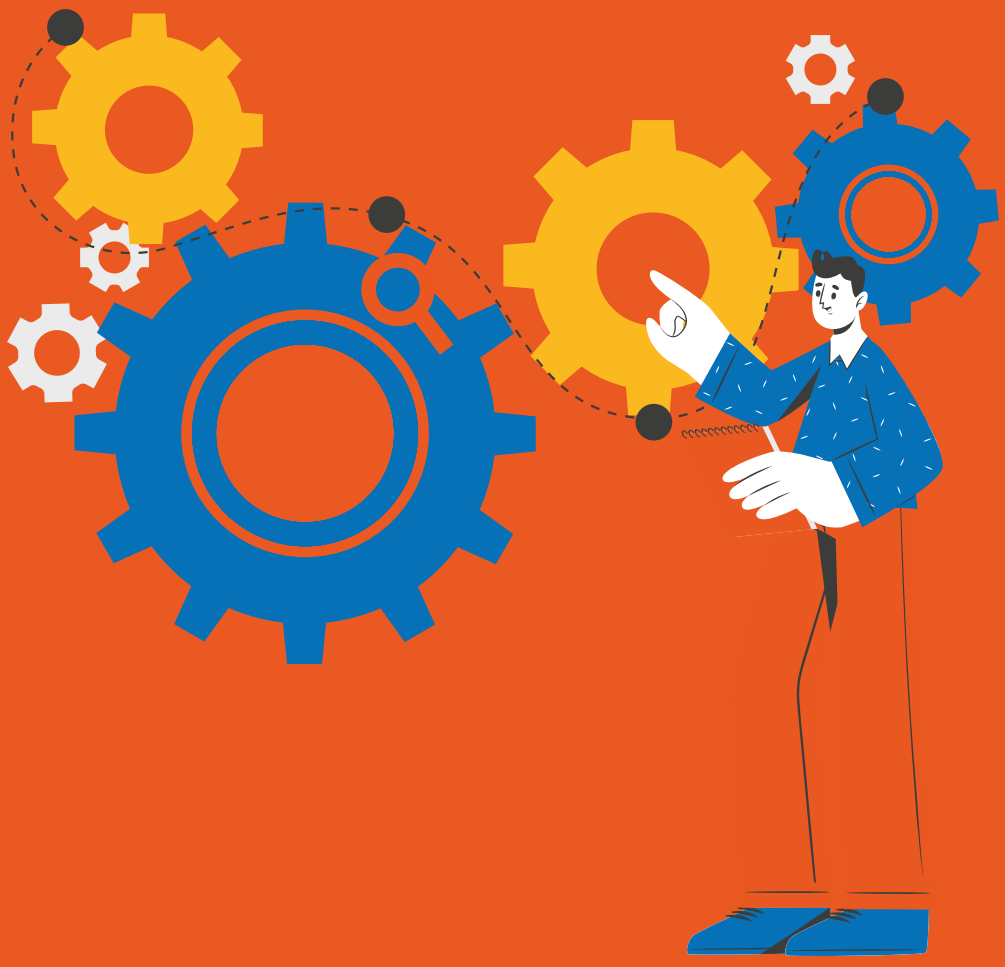


Fuente: Organización de Estados Americanos, 2024

Si eres un CSIRT gubernamental de un Estado Miembro de la OEA, esta información te puede interesar

4. PROCESO DE **ADHESIÓN A CSIRTAMERICAS**

Cumplir con SIM3 CSIRTAmericas Baseline forma parte de los requisitos para que un CSIRT gubernamental de un Estado Miembro de la OEA forme parte de la red CSIRTAmericas. Para más información, visite el sitio web de CSIRTAmericas: https://csirtamericas.org/es/supports/join



5. CRÉDITOS

Luis Almagro
Secretario General de la Organización de Estados Americanos

Equipo técnico de la OEA
Alison August Treppel
Kerry-Ann Barrett
Diego Subero
Carmen Quintos
Volker Esteves
Nelson Guanilo
Einar Lanfranco
Alejandro Sabolansky
Manuel Panero
Mariana Cardona

Open CSIRT Foundation (OCF)
Don Stikvoort

Contribuidores
Natalia Salazar
Carlos Leonardo
Elidier Moya

Diseño y diagramación
María Paula Lozano

Agradecimientos a

UK Government

CSIRTs con madurez, Estados miembros más seguros

OEA | CICTE

Basado en el Modelo SIM3

CSIRTAmericas Baseline

Referencia de Madurez para CSIRTs de los Estados miembros de la OEA

CSIRTAmericas Network | UK Government | SIM3 | Open CSIRT Foundation