Hacia la mejora continua con un Modelo de Madurez para evaluar CSIRT Coordinadores

Dora Alexandra Araque Cruz
Universidad de los Andes
Bogotá, Colombia
d.araquec@uniandes.edu.co

Angela Lizeth Luque Tovar
Universidad de los Andes
Bogotá, Colombia
al.luque@uniandes.edu.co

Luis Felipe Navas Pineda
Universidad de los Andes
Bogotá, Colombia
l.navas@uniandes.edu.co

Resumen— Se dice que lo que no se puede medir, no se puede mejorar. Esto aplica incluso para equipos de profesionales expertos en ciberseguridad. Diversas comunidades de investigadores han desarrollado marcos de referencia para mejorar el rendimiento de las capacidades de ciberseguridad, pero no todos son apropiados para equipos cada vez más jerárquicos y complejos que ofrecen servicios a grandes grupos de empresas de distintos sectores económicos. El objetivo del presente estudio es establecer una metodología de análisis para aplicar un modelo de madurez personalizado en equipos de coordinación de incidentes de ciberseguridad.

Palabras clave—*CSIRT, modelo de madurez, marco de referencia, SOC-CMM, SIM3, ENISA, CREST*

Contexto

Todas las organizaciones que se han encaminado por la transformación digital de sus procesos, independiente de su tamaño, deberían tener un equipo de profesionales encargados de la gestión de incidentes de seguridad de la información, propio o tercerizado.

A esos equipos se les denomina, por sus siglas en inglés, equipos CSIRT (Computer Security Incident Response Team) y todos coinciden en ofrecer servicios dirigidos a la prevención, detección, análisis, respuesta y/o reporte de incidentes, pero a su vez, todos difieren en su estructura, dependiendo de si sirven a una o varias organizaciones y de cómo se reparten las responsabilidades entre sus miembros.

Como a cualquier función de negocio, a un CSIRT se le puede medir su capacidad para mejorar continuamente en el conocimiento del equipo humano, la tecnología empleada para sus funciones y los procesos de trabajo. A esa medición se le llama modelo de madurez.

I. Definición del problema

Aunque existen diversos modelos de madurez, se observó que estaban diseñados para el modo de operación más frecuente, un **CSIRT centralizado**: está formalmente constituido, sirve a una sola organización y tiene roles dedicados para las operaciones del día a día. El presente artículo se centra en el desarrollo de un modelo de madurez adecuado para otro modo de operación, el **CSIRT coordinador**: formalmente constituido, sirve a grandes compañías o a instituciones de gobierno, se enfoca en la concienciación en ciberseguridad y en la administración global de los incidentes de ciberseguridad, no es operacional, sino que ofrece servicios al CSIRT centralizado que tenga cada organización.

Este modelo de madurez debe incluir indicadores realistas, que estén asociados con las actividades desempeñadas por analistas y líderes de servicios enfocados en la gestión de incidentes y en la coordinación de programas de ciberseguridad consolidados para empresas de un sector económico o con una postura de seguridad similar. Además, puede servir para evaluar y desarrollar planes de mejora para este tipo de equipos o como referencia en una fase previa de constitución de estos.

II. Propuesta

Los modelos de madurez existentes tienen sus ventajas y desventajas. Algunos cuentan con modos de calificación claramente identificados, otros son más subjetivos, y en general, permiten a las organizaciones medir si el ente que les presta los servicios está cumpliendo con la misión para la cual fue constituida, además de formar un programa de métricas formales para mejorar dichos servicios. Así que, el primer paso para el desarrollo fue la revisión de la literatura sobre este tema.

El segundo paso consistió en la selección de los modelos candidatos para ser modificados, combinados y analizar la relevancia de sus parámetros.

A. Objetivos

1) Objetivo general

Desarrollar un modelo de madurez específico basado en modelos de referencia para evaluar la eficacia y capacidad de respuesta de un CSIRT Coordinador en el ámbito de la ciberseguridad.

2) Objetivos específicos

- Identificar y analizar diversos marcos de referencia utilizados en la medición de modelos de madurez para CSIRT, con énfasis en aquellos aplicables a la función de coordinación.
- Seleccionar cuidadosamente marcos de referencia relevantes y aplicables que aborden de manera integral la medición de la madurez de un CSIRT Coordinador.
- Evaluar y depurar los marcos de referencia seleccionados, identificando los elementos específicos que contribuirán a la creación de un modelo personalizado para medir la madurez de un CSIRT Coordinador.

III. DESARROLLO DE LA SOLUCIÓN

En primera instancia, fue necesario entender que existen diversos términos para hacer referencia a un equipo de expertos en ciberseguridad que realizan alguna función en la gestión de incidentes y no hay un término universal. Así que era valioso incluir el término más común en la literatura para hacer la investigación de distintos modelos de madurez que evaluaran capacidades de estos equipos. Por esa razón, se determinó incluir marcos para equipos SOC, por sus siglas en inglés, Security Operations Center.

En segunda instancia, se hizo una investigación en fuentes abiertas de información de la entidad sin ánimo de lucro que consolida la constitución formal de múltiples equipos SOC y CSIRT en el mundo: el FIRST, la cual es el foro global de equipos de seguridad y de respuesta a incidentes. Este ente ha construido marcos de referencia del catálogo de servicios que ofrece un CSIRT y sus funciones, con el objetivo de crear, expandir y mejorar el portafolio de los equipos [2]. Sin embargo, no hace recomendaciones sobre capacidad, madurez o calidad del algún tipo particular de CSIRT, por lo que fue necesario ampliar la búsqueda.

En tercera instancia, se observó que existía ya literatura para evaluación de madurez de CSIRT nacionales, motivando aún más la creación de un modelo propio para el caso de estudio propuesto [3].

La primera referencia a un marco de madurez para un CSIRT es la publicada por **ENISA**, la agencia para ciberseguridad de la Unión Europea. A diferencia del FIRST, no sólo ofrece documentos especializados en la implementación de servicios, sino que también da recomendaciones de mejora, madurez y preparación de un CSIRT para aumentar el valor recibido por la comunidad objetivo (la empresa o grupo de empresas beneficiadas) [4]. Este marco está basado en un modelo, desarrollado por diversas comunidades de expertos, llamado SIM3 por sus siglas en inglés, Security Incident Management Maturity Model. Este marco tiene las siguientes características:

- Evalúa capacidades en 4 dominios: organizacional, humano, herramientas y procesos.
- Permite tanto una autoevaluación bajo la modalidad de encuesta, como la revisión entre pares de CSIRT.
- Tiene una escala de calificación que va de 0 a 4, con una indicación objetiva por pregunta, es decir, cada valor numérico tiene una explicación en contexto para guiar al evaluador sobre la justificación de esa calificación.

La segunda referencia a un marco de madurez fue el **SOC-CMM** [6]. Esta aparece como una de las 11 estrategias, según el MITRE, para crear un equipo de ciberseguridad de talla mundial: medir y mejorar el rendimiento [1]. Se caracteriza por ser una metodología de fuente abierta. Este marco tiene las siguientes características:

- Evalúa capacidades en 5 dominios: negocio, gente, procesos, tecnología y servicios.
- Está basado en la revisión de la literatura sobre conformación de equipos SOC y sus modelos organizacionales.
- Define 6 niveles de madurez, con indicación objetiva de calificación por pregunta, en la escala de 1 a 5.

La tercera y última referencia revisada en la literatura es una de las sugeridas por la entidad ISACA, que también publicó documentación con estrategias para la construcción de un equipo SOC efectivo [7]. Una de ellas consiste en una evaluación periódica de los servicios y madurez con el modelo **CREST**, entidad que acredita a más de 300 compañías que representan a la industria de ciberseguridad global [8]. Este modelo tiene las siguientes características:

- Se enfoca en la evaluación de capacidades en 3 fases del proceso de respuesta a incidentes: preparación, respuesta y seguimiento.
- Tiene una escala de calificación que va de 1 a 5. Sin embargo, tiene una asignación subjetiva de los valores, es decir, la respuesta a una pregunta puede ser: No, cumple parcial, mayoritaria o completamente.

Cabe destacar, finalmente, que existen otras autoevaluaciones de las capacidades de un equipo de ciberseguridad, pero fueron descartadas por pertenecer a fabricantes que no abordaron el problema de manera holística y sólo se enfocaron en el dominio tecnológico, como es la herramienta de autoevaluación de Microsoft.

Así pues, luego de revisar la literatura recomendada por entidades de ciberseguridad reconocidas, la selección de los 3 marcos de referencia para combinar, analizar y fusionar en un modelo acorde con el caso de uso planteado fue: ENISA, SOC-CMM y CREST. La metodología para realizar el análisis fue:

- Tome como base para el modelo personalizado el marco que tenga el sistema de calificación más amplio.
- Continúe con el modelo que arroje una mayor descripción en cada pregunta para asignar una calificación objetiva.
- Revise una a una todas las preguntas y agregue sólo aquellas que tengan un criterio de evaluación no repetido en el anterior modelo.
- Si la pregunta es alusiva a un servicio prestado por el CSIRT coordinador, inclúyala en el modelo, en el dominio de procesos.
- Si una pregunta proviene de un sistema de calificación con un rango menor, ajústelo.

En ese orden de ideas, el modelo base fue el del SOC-CMM, seguido por ENISA y finalmente, el CREST.

El modelo definitivo, utilizado para la evaluación de la madurez, tiene 4 dominios: negocio, personas, procesos y tecnología. Estos cuatro pilares o dominios son fundamentales en la gestión de mejora de productividad y transformación digital de un proceso tecnológico.

A. El dominio de negocio

El modelo SOC-CMM cuenta con 5 criterios de evaluación en el dominio de negocio, cada uno compuesto de la siguiente cantidad de preguntas o parámetros:

Criterio	Número de parámetros
Indicadores de negocio	5
Clientes	7
Carta de constitución	5
Gobierno	11
Privacidad y políticas	11

Este es un dominio que aplica de forma general a todo equipo de ciberseguridad porque, independientemente de los servicios ofrecidos, evalúa si está identificados, validados y documentados los indicadores de negocio del CSIRT, si se conoce cuál es la comunidad objetivo, es decir, las empresas o clientes beneficiarias de los entregables de cada servicio, si se socializa la misión, visión, roles y responsabilidades de los miembros del equipo en una carta de constitución, además de los elementos de gobierno y alineación con las políticas de seguridad de la información de las empresas beneficiarias. El uso de las preguntas, o parámetros, en este dominio no requirió adaptaciones enfocadas a un CSIRT coordinador y se mantuvieron todas las preguntas sin cambios. Sin embargo, al evaluar el modelo en la práctica con un equipo coordinador real, se recomienda asignar un peso (weighting) a cada dominio que facilite la identificación de relevancia, importancia y urgencia para los líderes de negocio.

B. El dominio de personas

Este dominio tampoco sufre modificaciones al adaptarlo a un escenario de CSIRT coordinador puesto que permite cuantificar la asignación del personal calificado en las responsabilidades e identificar escenarios de gestión del riesgo al involucrar contratistas o conocer cuáles son los planes de gestión de la capacidad en ausencia de uno de los miembros del equipo. Estos son los criterios de evaluación que incluye el SOC-CMM, con su cantidad de preguntas o parámetros:

Criterio	Número de parámetros
Empleados	10
Roles y jerarquía	10
Administración del personal	14
Administración del conocimiento	10
Entrenamiento y educación	9

En este dominio, el modelo de ENISA aportó una pregunta que no estaba en los otros dos modelos y es

global a cualquier equipo que ofrezca servicios, incluso de TI: el código de ética, práctica o conducta.

En cuanto al modelo CREST, como sus criterios de evaluación estaban enfocados a las fases que componen la gestión de incidentes, el análisis consistió en identificar aquellas preguntas que estuvieran asociadas al dominio del personal, en cualquier parte del proceso. De allí, se retomaron preguntas que evaluaron el empoderamiento y la capacidad de comunicación del personal con las partes interesadas: miembros de CSIRT subordinados, administradores de sistemas de información, otros mecanismos de cooperación y la alta dirección de las empresas beneficiarias.

C. El dominio de herramientas y tecnologías

En este dominio es donde hay grandes diferencias con el modo de operación tradicional de CSIRT centralizado. Se descartaron por completo los criterios de evaluación del SOC-CMM, pues evalúan las siguientes herramientas: SIEM, UEBA, NDR, EDR y SOAR, todas estas son propias de la gestión de un CSIRT subordinado. Este dominio es el que menos puede estandarizarse, puesto que cada CSIRT coordinador escoge el portafolio de servicios que ofrece hacia su comunidad objetivo, dependiendo de los indicadores de negocio. En función de los servicios, se definen las herramientas. Las funciones de coordinación pueden ser pasivas o activas. Las funciones pasivas son, por ejemplo: concienciación en ciberseguridad y coordinación global de los incidentes. Las funciones activas son, por ejemplo: análisis de código malicioso (*malware*), análisis forense e inteligencia de amenazas, entre otras.

Al revisar los criterios de evaluación de este dominio para el modelo ENISA, se identificaron dos herramientas comunes a un CSIRT coordinador y subordinado: el listado de recursos de TI y un sistema de seguimiento de incidentes.

El listado de recursos de TI es esencial en la fase de identificación de riesgos de una organización: si no se sabe qué activos se tienen, no se sabe qué es lo que se quiere proteger. Los activos comprenden el hardware, el software, las personas, los datos y todo aquello que constituya valor en la información de una organización. Si bien, un CSIRT coordinador no es responsable de las herramientas de administración de activos, debe haber un grado de madurez que evalúe su capacidad para tomar decisiones con la consulta de los activos, sea para acompañar al CSIRT subordinado en la evaluación de impacto durante la gestión de vulnerabilidades o en la generación de contexto de negocio ante el manejo de fuentes de inteligencia de amenazas.

El sistema de seguimiento de incidentes es fundamental para la labor de coordinación. Con este, de forma estructurada y organizada se registran los incidentes que requieren investigación con sus respectivas evidencias técnicas, se puede determinar si el incidente es confirmado o potencial y se coordinan todas las acciones para resolver el incidente.

En cuanto al modelo CREST, se identificaron otras 2 herramientas comunes para todo tipo de CSIRT: el sistema de administración de la documentación y la plataforma de colaboración y conocimiento, ambas fundamentales para:

- Crear una base de conocimiento.
- Reducir los tiempos de investigación de los analistas CSIRT.
- Centralizar las lecciones aprendidas de todos los procesos asociados al portafolio de servicios.

D. El dominio de procesos

Estos son los criterios de evaluación que incluye el SOC-CMM:

Criterio	Número de parámetros
Administración	8
Operaciones e instalaciones	6
Reportes y comunicaciones	13
Casos de uso	20
Ingeniería de detección y validación	18

Los tres primeros criterios fueron adoptados en su totalidad pues no dependen del modo de operación de un CSIRT. Este tipo de entes deben definir elementos como matrices RACI, catálogos de servicios, documentar procesos e implementar estrategias de socialización con las partes interesadas. El criterio de operaciones e instalaciones busca evidenciar los tipos de ejercicios técnicos que un CSIRT realiza como ejercicios de mesa de crisis, simulación cibernética, de red team y prácticas CTF o tipo “captura la bandera”, entre otras.

Los criterios de “Casos de uso” y de “Ingeniería de detección y validación” fueron descartados en su totalidad porque no pertenecen a la acción de coordinación, sino a labores que hace un CSIRT subordinado como la detección de eventos anómalos, su reporte y mitigación.

Este es el dominio que suscita más personalización a un caso particular de evaluación de un CSIRT coordinador, porque cada servicio ofrecido debe tener un

mapa de procesos, así que los 3 marcos de referencia cuentan con preguntas para procesos específicos: monitoreo de la seguridad, administración de incidentes de seguridad (prevención, detección, resolución), análisis forense, inteligencia de amenazas, caza de amenazas, administración de vulnerabilidades, administración de logs, reportes, etc.

E. Aplicación del modelo de madurez en un CSIRT coordinador de prueba

La metodología de análisis anteriormente descrita se implementó en un CSIRT coordinador cuyo catálogo de servicios es el siguiente: coordinación de incidentes, coordinación de gestión de vulnerabilidades, capacitación y generación de alertas y comunicados. La siguiente tabla ilustra la cantidad de preguntas o parámetros tomado de cada modelo por cada dominio:

Dominio	**Modelo**	**Número de parámetros**
Negocio	SOC-CMM	15
Negocio	ENISA	0
Negocio	CREST	0
Gente	SOC-CMM	5
Gente	ENISA	2
Gente	CREST	3
Tecnologías	SOC-CMM	0
Tecnologías	ENISA	1
Tecnologías	CREST	3
Procesos	SOC-CMM	14
Procesos	ENISA	6
Procesos	CREST	7

El modelo difiere en la cantidad de parámetros de las secciones anteriores porque el trabajo realizado para este caso de prueba buscaba dar prioridad a aquellas preguntas cuya acción de mejora no dependiera de ajustes en procedimiento o de documentación, sino en actividades que se pudieran automatizar, o que representen la formación de un plan de trabajo de implementación de una herramienta tecnológica.

Una vez seleccionadas las preguntas, el modelo se socializó con el jefe del CSIRT, quien procedió a asignar la calificación de cada una, tomando como referencia la escala del SOC-CMM, haciendo el ajuste de escala para el caso de una pregunta ENISA y asignando una puntuación subjetiva entre 0 y 5 para el caso de una pregunta CREST. Todos los resultados se grafican en un diagrama radial del estilo de la figura 1.

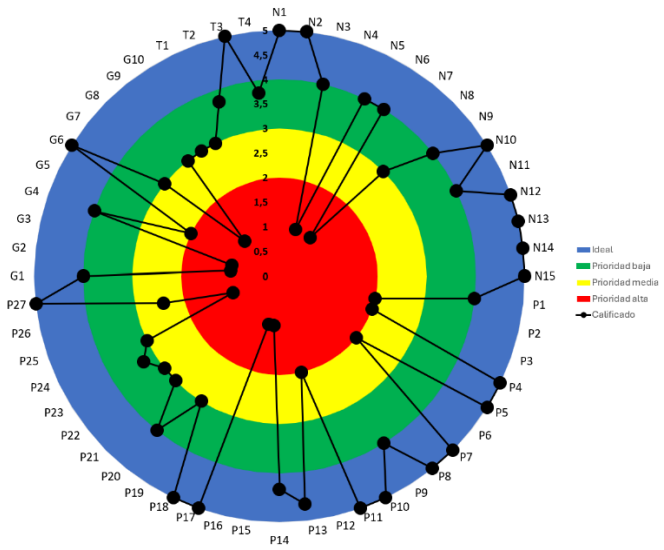

Fig. 1. Diagrama radial de un modelo de madurez para un caso de prueba.

Las calificaciones más bajas se sitúan más cerca del centro del círculo (el cero en la figura 1). Al tener los resultados finales de la evaluación, se asignaron 3 tipos de prioridad, así:

- Prioridad alta; calificaciones entre 0 y 2.
- Prioridad media: calificaciones entre 2 y 3.
- Prioridad alta: calificaciones entre 3 y 4.

Las preguntas con calificación entre 4 y 5 no iban a ser intervenidas con alguna acción de mejora. Luego, por cada pregunta según su prioridad se resolvieron las siguientes preguntas:

¿Mejorar este parámetro requiere presupuesto?

¿Cuál es el esfuerzo humano para subir la calificación de esta pregunta?

¿Se pueden idear y planear actividades de implementación técnica para mejorar este ítem?

¿Qué prioridad se le puede asignar a esta pregunta según los intereses de las empresas beneficiarias del CSIRT coordinador?

A partir de allí, el modelo fue la base para crear un plan de proyecto con actividades variadas, como la automatización de procesos, la implementación de herramientas de gestión, la documentación de los elementos de evaluación y la socialización de las iniciativas con las partes interesadas.

IV. Conclusiones

- Los procesos proactivos y reactivos para la gestión y respuesta a incidentes cuentan con marcos de referencia ampliamente estudiados y establecidos, los cuales permitieron una evaluación estructurada y clara del estado de madurez de un CSIRT coordinador y el establecimiento de prioridades muy bien justificadas para entrar a la etapa de mejora continua como parte del ciclo de vida de este tipo de entes.

- La definición, el análisis, el diseño, la implementación y la evaluación de este proyecto permitieron afianzar los conocimientos de dirección de un CSIRT en un escenario real, fuera del ámbito académico que se suele idealizar, pudiendo experimentar los retrasos propios de la operación por distintas razones.

- El desarrollo del proyecto facultó a los miembros del equipo para comprender la importancia de conocer cómo está estructurado un CSIRT, qué tipo de modelo organizacional usa, cuáles son sus desafíos y entender cómo los productos mínimos viables propuestos generan valor en los clientes del CSIRT.

- El ajuste de preguntas para el modelo de madurez de un CSIRT Coordinador no pretende ser una receta infalible de auditoría o evaluación para todos los equipos de ciberseguridad con este modo de operación, pero puede servir como referencia para que equipos nuevos o existentes sean conscientes de que existen estructuras formales que evalúan las capacidades y contribuyen a la mejora continua, siempre y cuando las adapten a su portafolio de servicios y a su contexto tecnológico.

V. Referencias

[1] Knerler, K., Parker, I., Zimmerman, C. *11 strategies of a world-class cybersecurity operations center pp. 74.*(2022). Mitre.

[2] *Marco de referencia de servicios CSIRT.* FIRST. https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1 (Disponible el 4 de diciembre de 2023).

[3] *Marco de referencia de madurez de un CSIRT global: estimulando el desarrollo y la mejora continua de CSIRT nacionales*. https://cybilportal.org/wp-content/uploads/2020/02/Global-CSIRT-Maturity-Framework_v2_april-2021.pdf pp. 3. (2021). Global Forum on Cyber Expertise.

[4] *Marco de referencia de madurez de un CSIRT.* ENISA. https://www.enisa.europa.eu/topics/incident-response/csirt-capabilities/csirt-maturity (Disponible el 4 de diciembre de 2023).

[5] *Herramienta de auto - evaluación SIM3v1*. ENISA. https://www.enisa.europa.eu/topics/incident-response/csirt-capabilities/csirt-maturity/csirt-survey (Disponible el 4 de diciembre de 2023).

[6] *Autoevaluación con SOC-CMM. https://www.soc-cmm.com/ (Disponible el 4 de diciembre de 2023).*

[7] Narayanan Kaliyaperumal, L. *The evolution of Security Operations and Strategies for Building an Effective SOC. ISACA. https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/the-evolution-of-security-operations-and-strategies-for-building-an-effective-soc* (Disponible el 4 de diciembre de 2023).

[8] *Introducción a quién es el CREST.* https://www.crest-approved.org/about-us/who-is-crest/ (Disponible el 4 de diciembre de 2023).