Optimización de un CSIRT Académico: SIM3 como punto de partida

Francisco Javier Díaz[1], Paula Venosa[1,2], Mateo Durante[2], María Agustina Echaniz[2], Ulises Cabrera[2], Agustín Paturlanne[2], and Jeremías Pretto[2]

[1] LINTI – Facultad de Informática - UNLP
{pvenosa, jdiaz}@info.unlp.edu.ar
[2] CERTUNLP - CeSPI - UNLP
{pvenosa, mdurante, maechaniz, ucabrera, apaturlanne, jpretto}@cert.unlp.edu.ar

Resumen En este artículo se presenta la experiencia de CERTUNLP y los logros obtenidos para aumentar el nivel de madurez en cada uno de los dominios del modelo SIM3. Este proceso se inició con la evaluación del CSIRT en 2022 e implicó la identificación de áreas clave para el fortalecimiento de la gobernanza, los servicios brindados y la capacidad técnica de nuestro equipo. A través de implementar estrategias concretas, como la optimización de procedimientos internos, el desarrollo de herramientas, la formación del equipo y la adopción de mejores prácticas alineadas con estándares internacionales, CERTUNLP logró elevar su nivel de preparación y respuesta frente a las amenazas emergentes. Actualmente contamos con una nueva versión de nuestro sistema de gestión de incidentes con más prestaciones y con un mecanismo de comunicación más eficiente, además de integrarse con otras herramientas que facilitan la prestación de nuestros servicios. Compartir este recorrido puede ser de utilidad para que otros equipos de respuesta de incidentes puedan trazar su propia hoja de ruta hacia una evolución de su nivel de madurez.

Keywords: CSIRT · SIM3 · Modelos de madurez · Herramientas de gestión de incidentes · Automatización de procesos.

1. Introducción

Este trabajo describe las acciones desarrolladas por el CSIRT Académico de la Universidad Nacional de la Plata (CERTUNLP) para mejorar la calidad de los servicios proactivos y reactivos brindados por nuestro equipo, a partir de una evaluación interna basada en SIM3 (Diaz y cols., 2023). Estas tareas incluyen el desarrollo de una nueva versión de nuestro sistema de gestión de incidentes, la implementación de nuevas herramientas, la documentación y mejora de procedimientos, y la incorporación de nuevas fuentes de información (feeds), entre otras.

Este proceso de mejora comenzó con la evaluación de aspectos relacionados a la gobernanza, las personas, las herramientas y los procesos de CERTUNLP, cuyos resultados fueron descriptos en (Diaz y cols., 2023). La identificación de oportunidades de mejora también se hizo en base a nuestra experiencia de más de 15 años en el ámbito de la ciberseguridad. El uso del modelo SIM3 como metodología no sólo posibilita que el proceso de evaluación sea ordenado y exhaustivo, sino que permite definir y llevar a cabo las tareas de mejora en forma ordenada y estableciendo prioridades que optimicen la labor del equipo.

Nuestro CSIRT tiene como misión la prevención, detección, mitigación e investigación de problemas e incidentes de seguridad, coordinando acciones para la protección de los usuarios y los servicios de la Universidad Nacional de La Plata (UNLP). El equipo ofrece distintos servicios a su comunidad objetivo, entre los que se encuentran la gestión de incidentes de seguridad y la asistencia para su resolución, el análisis y monitoreo de seguridad en aplicaciones, redes y servicios, y la capacitación y concientización en temáticas de ciberseguridad (CERTUNLP, s.f.-a).

CERTUNLP funciona en el ámbito de la UNLP desde el año 2008. Sus integrantes nos hemos formado y realizamos tareas de investigación y académicas en dicha casa de estudios, lo cual redunda en la optimización de los servicios que ofrecemos desde nuestro CSIRT. Al igual que otras organizaciones y proyectos, debemos enfrentarnos con la dificultad que existe para contar con recursos humanos calificados en materia de ciberseguridad y lograr su retención, lo cual se ha acentuado post pandemia (Organización de los Estados Americanos, 2022). Este es uno de los puntos claves a tener en cuenta a la hora de definir estrategias de gestión de nuestro CSIRT. Trabajar en el fortalecimiento de los servicios que brindamos, tener un rol activo en redes de colaboración como LACNIC-CSIRTs (LACNIC CSIRT, 2024), CSIRTAmericas (CSIRTAmericas, s.f.) y la subcomisión de Ciberseguridad del CIN (CIN — Consejo Interuniversitario Nacional, s.f.), y el esfuerzo en la formación del equipo y su participación en proyectos de investigación, son los pilares fundamentales de nuestra estrategia en este sentido.

2. Modelos de madurez

En el ámbito de los CSIRTs, la madurez es un indicador del grado de eficacia con el que un equipo lleva a cabo, organiza, registra, ejecuta y mide sus funciones. Para medir la madurez de un CSIRT se utiliza un conjunto de criterios y niveles progresivos, llamado modelo de madurez, donde cada nivel representa un estado más avanzado de madurez, eficiencia o efectividad.

Existen diversos modelos para medir la madurez de un CSIRT, entre ellos se encuentran SIM3 (acrónimo de las siglas en inglés de Security Incident Management Maturity Model) (Open CSIRT Foundation, s.f.),

CERT-RMM (Computer Emergency Response Team - Resilience Management Model) (Caralli y cols., 2016) y/o guías como la ISO/IEC 27035 (Organización Internacional de Normalización, 2023) y la NIST SP 800-61 (Cichonski y cols., 2012).

En nuestro caso hemos elegido SIM3, promovido por la Open CSIRT Foundation, por tratarse de una metodología abierta y de aplicación ágil.

SIM3 considera que un CSIRT es maduro cuando la calidad de sus servicios es estable y el equipo cuenta con los recursos necesarios para ello. Este modelo evalúa las capacidades de prevención, detección, resolución, control de calidad y retroalimentación en la gestión de incidentes de ciberseguridad.

El modelo se compone de 4 categorías o dominios, llamadas cuadrantes en la versión actual, que agrupan distintos aspectos relacionados a la organización del CSIRT, sus recursos humanos, las herramientas que utiliza y sus procesos. De cada parámetro se evalúa su nivel de madurez asignándole un valor entre 0 y 4.

La evaluación SIM3 puede ser realizada manualmente o a través de aplicaciones en línea como la del propio Open CSIRT Foundation (Open CSIRT Foundation, s.f.), o la implementación de ENISA (ENISA, s.f.). Como resultado de la evaluación se obtiene, además de los niveles de madurez de cada parámetro, un grado global de madurez para el CSIRT que puede resultar en básico, intermedio o avanzado.

Actualmente se encuentra definida una nueva versión, aún provisoria, de SIM3 (Stikvoort y cols., s.f.).

Varias organizaciones que agrupan y respaldan CSIRTs (organismos de coordinación, equipos de referencia, etc) tienen definido su perfil de SIM3. Entre estas organizaciones se encuentran el FIRST (Bernal Barzallo y cols., s.f.), ENISA (ENISA, s.f.), y recientemente la OEA (Organización de Estados Americanos, 2025), entre otras.

Un perfil define los requisitos de cumplimiento, especificando el nivel de madurez esperado para el CSIRT en cada uno de los parámetros evaluados en los distintos dominios. Los “perfiles” pueden ser utilizados para: (a) establecer en qué nivel de madurez se encuentra un CSIRT, (b) poder ser miembro de una comunidad en particular, (c) alcanzar una certificación, (d) ser auditados, etc.

3. Hacia la mejora del nivel de madurez de CERTUNLP

El dominio **Organización** se refiere al conjunto de personas, recursos, herramientas e infraestructura que trabajan juntos de manera planificada. Las metas de una organización están dirigidas por un conjunto de objetivos estratégicos específicos. Como SIM3 se centra en la madurez de la gestión de los incidentes de seguridad, hay que distinguir entre los objetivos estratégicos de toda la organización y los objetivos estratégicos

relacionados con la organización del CSIRT, responsable de gestionar los incidentes de seguridad (sim3, s.f.).

Aspectos Humanos alude a las personas que forman parte del equipo y trabajan para brindar los servicios descriptos en el dominio anterior. Todas las personas que contribuyen a los objetivos del CSIRT requieren educación técnica u orientada a la gestión de incidentes, además de aquella capacitación adicional como el análisis de malware o la forensia. En resumen, los parámetros incluidos en este cuadrante tratan sobre el "capital" humano de las personas que trabajan en el CSIRT (sim3, s.f.).

El dominio **Herramientas** tiene que ver con los programas, aplicaciones, servicios, e incluso equipamiento, que es utilizado por el personal mencionado en la sección anterior, para alcanzar los objetivos y ofrecer los servicios definidos en el dominio respectivo a la organización. Se refiere específicamente a las herramientas que permiten mejorar la gestión de los incidentes de seguridad, en términos de tiempo, calidad y/o con un mayor nivel de detalle. (sim3, s.f.).

Procesos trata sobre los conjuntos de acciones que son llevadas a cabo por el personal o por herramientas automatizadas con el fin de lograr un resultado específico en el marco de los servicios prestados por el CSIRT. Todos los procesos pueden caracterizarse por una serie de atributos. Mediante la aplicación de tales atributos también podemos determinar cuán exitoso es un proceso o cuán exitosa es una organización en la prestación de un servicio. En las organizaciones maduras los procesos son documentados, medibles y repetibles. Aquí, hablamos específicamente de aquellos procesos que apoyan la gestión de incidentes y cualquier otro servicio que ofrece el CSIRT y adoptamos el término "procesos" en el sentido más amplio de la palabra, de modo que en este área también encontrará procesos que a veces podrían ser etiquetados como "política" o de otra manera (sim3, s.f.).

3.1. Organización

En el caso del dominio de organización, lo referido a la misión (O1) y la comunidad objetivo (O2) se encontraban definidos en el sitio web de CERTUNLP (CERTUNLP, s.f.-a). Estos parámetros se hallaban en el nivel 3 en la primer evaluación y durante el proceso de mejora fueron formalmente definidos documentados y a partir de eso, periódicamente revisados, llegando así al nivel 4. Por su parte, al realizar la evaluación, los parámetros autoridad (O3) y responsabilidad (O4) se encontraban indefinidos; al concluir la mejora, estos parámetros se encuentran formalmente definidos en un documento, y son revisados periódicamente adquiriendo así el nivel 4. Asimismo, la descripción del servicio (O5) y la clasificación de incidentes (O8) se encontraban parcialmente documentadas; al finalizar la mejora estos parámetros se encuentran formalmente documentados y tienen revisión continua, por lo tanto se encuentran en nivel 4. Respecto a la política de medios públicos (O6) no estaba definida, por lo tanto se

incluyó un apartado en la política de manejo y divulgación de la información, obteniendo un nivel 2. Para continuar, la descripción del nivel de servicio (O7), y la integración con CSIRT existentes (O9), se encontraban en el nivel 1, es decir, definidas pero no documentadas; al concluir este proceso se encuentran en el nivel 4. Finalmente, el marco organizativo (O10) en la evaluación SIM3 mostraba el nivel 0, es decir, indefinido. Luego del proceso de mejora se encuentra en el nivel 4. En un principio este parámetro fue definido en un documento interno de servicios y luego fue modificado para cumplir con la RFC2350 (RFC 2350, s.f.).

Cuadro 1: Fortalecimiento del dominio Organización en CERTUNLP

Parámetro	**Estado base**	**Estado actual**	**Nivel base**	**Nivel alcanzado**
Mandato (O1)	Publicado en sitio web	Formalmente documentado	3	4
Comunidad (O2)	Publicado en sitio web	Formalmente documentado	3	4
Autoridad (O3)	No había sido discutido	Formalmente documentado	0	4
Responsabilidad (O4)	No había sido discutido	Formalmente documentado	0	4
Descripción del Servicio (O5)	Parcialmente documentado	Formalmente documentado	2	4
Política de Medios Públicos (O6)	No había sido discutido	Parcialmente documentado	0	2
Descripción del Nivel de Servicio (O7)	No había sido discutido	Formalmente documentado	0	4
Clasificación de Incidentes (O8)	Parcialmente documentado	Formalmente documentado	2	4
Participación en Sistemas de CSIRT (O9)	Definido pero no documentado	Formalmente documentado	1	4
Marco Organizativo (O10)	No había sido discutido	Formalmente documentado	0	4
Política de Seguridad (O11)	No había sido discutido	Formalmente documentado	0	4

3.2. Aspectos Humanos

En este dominio la mejora comenzó desarrollando un código de ética (H1), luego de la evaluación se encontraba en el nivel 1, dado que estaba definido pero no documentado, y al finalizar el proceso de mejora este parámetro se encuentra en el nivel 4. Asimismo, se desarrolló el documento de resiliencia del personal (H2) que indica cómo CERTUNLP se asegura la capacidad operativa del equipo durante vacaciones o enfermedad. Al comenzar este proceso no se encontraba definido, y al finalizar, se encuentra en el nivel 4. Por su parte, la descripción del conjunto de habilidades (H3) no se encontraba definida, pero durante este proceso de mejora se completó el equipo por lo tanto fue necesario definirla, sin embargo aún se encuentra en desarrollo el documento correspondiente. Como resultado, se pasó del nivel 0 al nivel 1.

Cuadro 2: Fortalecimiento del dominio Aspectos humanos en CERTUNLP

Parámetro	**Estado base**	**Estado actual**	**Nivel base**	**Nivel alcanzado**
Código de Ética (H1)	Definido pero no documentado	Formalmente documentado	1	4
Resiliencia del Personal (H2)	No había sido discutido	Formalmente documentado	0	4
Descripción del Conjunto de Habilidades (H3)	No había sido discutido	Definido pero no documentado	0	1

3.3. Herramientas

Al adentrarnos en este dominio se desarrolló la lista de fuentes de información (T2), en ella se especifica de dónde obtiene CERTUNLP la información sobre vulnerabilidades, amenazas, escaneo, e incidentes de la comunidad objetivo. Este parámetro, al iniciar la mejora, se hallaba en el nivel 0, debido a que las fuentes de información utilizadas eran conocidas pero no se habían definido formalmente ni documentado. Al finalizar se alcanzó el nivel 4, ya que es revisado periódicamente. Este documento es esencial, dado que contar con fuentes de información confiables es una de las bases para la operación eficaz de un CSIRT. Las fuentes de información permiten la detección temprana de amenazas, vulnerabilidades y campañas de ataque en curso, la calidad, actualidad y relevancia de estas fuentes inciden directamente en la capacidad del equipo para anticiparse

a incidentes y responder con rapidez y precisión, reducen el riesgo de falsos positivos y evitan la sobrecarga de análisis innecesarios, optimizando los recursos del equipo y fortaleciendo la toma de decisiones en contextos críticos.

Siguiendo con este cuadrante, se definió y documentó la mensajería resiliente (T6), pasando del nivel 1 al 4.

En relación al parámetro herramientas de gestión de incidentes (T4), Ngen (CERTUNLP, s.f.-c) es el sistema de gestión de incidentes desarrollado y utilizado por CERTUNLP. El mismo, originalmente implementado en PHP con Symfony, fue reimplementado en Python con React. Este proyecto de desarrollo se llevó a cabo durante varios años y su objetivo fue no sólo la actualización de la tecnología y el desacople del *backend* y *frontend*, sino también enriquecer su funcionalidad. En el transcurso del 2024 se realizó gradualmente la transición de uno a otro, para esto se utilizaron ambas versiones del sistema en simultáneo, duplicando la información para asegurar que ambos posean el seguimiento de los casos.

Respecto a la gestión de incidentes, con la nueva versión de Ngen se implementaron mecanismos más acordes para la clasificación y tratamiento de los eventos como utilización de taxonomías con tipos "vulnerabilidad" o "incidente", y reportes en cascada para evitar la repetición de plantillas utilizadas en el envío de notificaciones. Se definieron nuevas estructuras de seguimiento de "eventos", que permiten el seguimiento individual de acontecimientos en la comunidad objetivo del CSIRT con un correcto agrupamiento de los mismos en los llamados "casos", lo cual posibilita manejar en forma conjunta el estado y referencia de uno o múltiples incidentes y vulnerabilidades.

La nueva versión de Ngen fue desarrollada utilizando nuevas tecnologías para buscar una rápida inclusión de nuevos desarrolladores y permitir nuevas capacidades, como su integración con analizadores como Cortex (CERTUNLP, s.f.-b) y Kintun (StrangeBee, 2025). Estas herramientas nos permiten verificar la existencia de vulnerabilidades, descartar falsos positivos, enriquecer eventos, entre otros.

Kintun es un desarrollo propio que tiene como principal objetivo detectar vulnerabilidades y servicios específicos en puertos que pueden afectar a la comunidad objetivo o comunidades externas al CSIRT, y su acople con Ngen permite la verificación de existencia de eventos.

En el contexto de las herramientas de prevención y detección de incidentes, parámetros T8 y T9, se trabajó principalmente en el consumo de información proveniente de nuestro IDS de red (NIDS) Zeek. A partir de la información que el mismo recolecta podemos obtener gran cantidad de información referente a dominios, certificados SSL, resultado de consultas DNS, tráfico HTTP, etc.

La información proveniente del Zeek, junto a análisis continuos de conexiones a determinados servicios y tráfico DNS, etc, nos permite generar un catálogo de activos existentes en la comunidad objetivo a fin de poder

analizar debilidades, existencia de patrones, etc; y así prevenir actividades maliciosas antes de su ocurrencia.

Por último, dentro de las herramientas de prevención (T8) se desarrolló un sistema que unifica información de usuarios y contraseñas provenientes de filtraciones de datos publicados en sitios de la darkweb. Esta aplicación tiene como objetivo identificar posibles compromisos de cuentas de nuestra organización y alertar a los respectivos usuarios y administradores de sistemas, con el fin de prevenir incidentes que esta información pueda causar.

Cuadro 3: Fortalecimiento del dominio Herramientas en CERTUNLP

Parámetro	**Estado base**	**Estado actual**	**Nivel base**	**Nivel alcanzado**
Lista de Fuentes de Información (T2)	Definido pero no documentado	Formalmente documentado	1	4
Mensajería Resiliente (T6)	Definido pero no documentado	Formalmente documentado	1	4
Sistema de Seguimiento de Incidentes (T4)	Formalmente documentado	Formalmente documentado	4	4
Conjunto de Herramientas de Prevención de Incidentes (T8)	Parcialmente documentado	Parcialmente documentado	2	2
Conjunto de Herramientas de Detección de Incidentes (T9)	Parcialmente documentado	Parcialmente documentado	2	2

Si bien el parámetro T4 se encontraba en el máximo nivel, las funcionalidades descriptas en párrafos anteriores permitieron automatizar aún más el proceso de gestión de incidentes, agilizando el mismo y mejorando la comunicación con nuestra comunidad objetivo.

Por su parte, los parámetros T8 y T9 continúan en el nivel 2 puesto que el equipo se encuentra desarrollando nuevas herramientas de prevención y detección.

3.4. Procesos

Respecto al dominio de procesos, al realizar la evaluación el proceso de resolución de incidentes (P6), que describe la forma en que CERTUNLP resuelve los incidentes de forma genérica, incluyendo el uso del conjunto de herramientas relacionadas, y los procesos de incidentes específicos (P7) se encontraban parcialmente documentados, es decir en nivel 2, se documentaron formalmente los procesos y se revisan periódicamente, de esta manera se llegó al nivel 4. Asimismo, como resultado de la evaluación se obtuvo que, tanto el proceso de manejo seguro de la información (P11), que indica cómo CERTUNLP gestiona la información confidencial y refiere a los requisitos legales pertinentes, como el proceso de fuentes de información (P12), que describe cómo CERTUNLP maneja y utiliza las diversas fuentes de información disponibles, se encontraban definidos pero no documentados. A partir de ésto, se desarrollaron los documentos y se definió un proceso de revisión periódico para lograr alcanzar el nivel 4.

Cuadro 4: Fortalecimiento del dominio Procesos en CERTUNLP

Parámetro	**Estado base**	**Estado actual**	**Nivel base**	**Nivel alcanzado**
Proceso de Resolución de Incidentes (P6)	Parcialmente documentado	Formalmente documentado	2	4
Procesos de Incidentes Específicos (P7)	Parcialmente documentado	Formalmente documentado	2	4
Proceso de Manejo Seguro de Información (P11)	Definido pero no documentado	Formalmente documentado	1	4
Proceso de Fuentes de Información (P12)	Definido pero no documentado	Formalmente documentado	1	4

4. Resultados obtenidos

En esta sección se muestra, en forma gráfica, la evolución en la madurez de cada uno de los parámetros de SIM3 en los distintos dominios, producto del proceso de mejora relatado, considerando los perfiles de FIRST y OEA.

Para empezar, elegimos comparar nuestro nivel de madurez respecto al perfil de FIRST por tratarse de una organización de referencia mundial

para los equipos de respuesta de incidentes y una de las pioneras en prestar servicios a los CSIRTs, cuya membresía es valorada en nuestro ámbito. Los resultados puede observarse en Figura 1 y Figura 2.

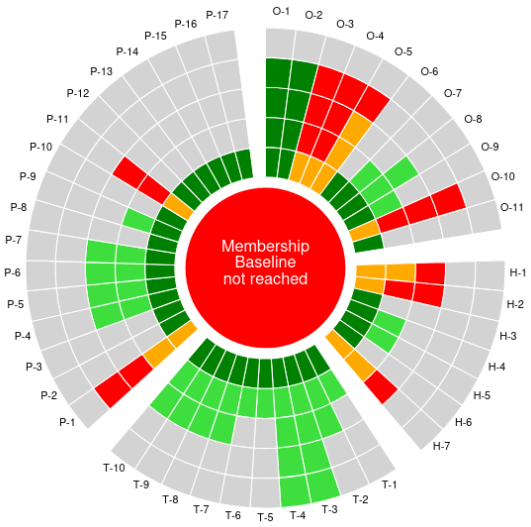

Figura 1: Estado de cumplimiento del perfil de FIRST en la evaluación de SIM3 (2022) de CERTUNLP

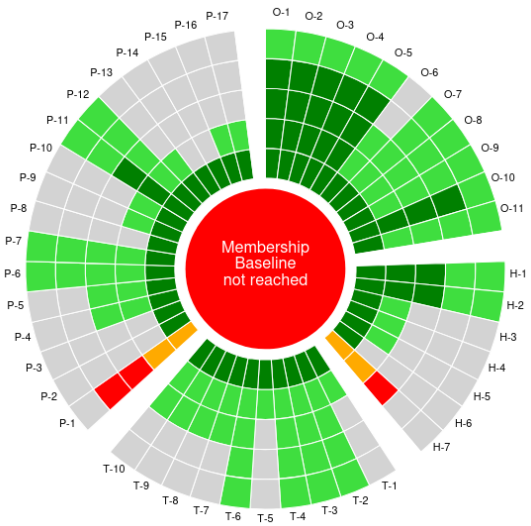

Figura 2: Estado de cumplimiento del perfil de FIRST en la evaluación de SIM3 (2025) de CERTUNLP

A su vez, analizamos la evolución de nuestro nivel de madurez teniendo en cuenta el perfil de la OEA, dado que somos miembros de CSIRTAmericas y participamos activamente en dicha comunidad. Si bien la OEA ha definido su perfil recientemente, es decir, no existía al momento de nuestra primera evaluación, mostramos en qué estado nos encontrábamos respecto su "perfil" de cumplimiento tanto en 2022 como en la actualidad, de manera que se pueda apreciar visualmente la mejora en los diferentes aspectos. Los resultados puede observarse en Figura 3 y Figura 4.

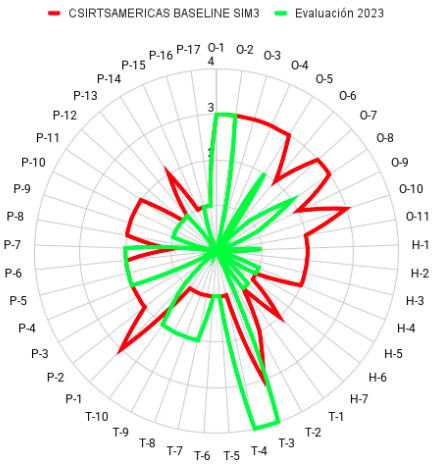

Figura 3: Estado de cumplimiento del perfil de OEA en la evaluación de SIM3 (2022) de CERTUNLP

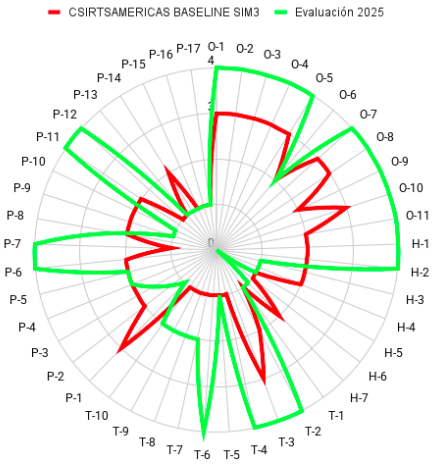

Figura 4: Estado de cumplimiento del perfil de OEA en la evaluación de SIM3 (2025) de CERTUNLP

5. Conclusiones

Así como la evaluación de SIM3 (Diaz y cols., 2023) nos permitió identificar fortalezas y debilidades en nuestros procesos, áreas que estaban más maduras que otras, y oportunidades de mejora; el proceso de fortalecimiento, descripto en este trabajo, hizo posible el crecimiento de nuestro equipo consolidando los servicios que brindamos a nuestra comunidad objetivo.

Durante este proceso trabajamos en la elaboración de la documentación de los procesos que teníamos automatizados pero no documentados, es decir, no se encontraban formalizados ni aprobados, lo cual nos permitió elevar el nivel de madurez en todos los dominios.

Como se puede ver en las secciones anteriores al alcanzar un mayor nivel de madurez en todos los cuadrantes, nuestro equipo de respuesta de incidentes se acercó al cumplimiento de los requisitos de los perfiles de SIM3 de FIRST y CSIRTAmericas de OEA. De todas maneras es necesario continuar trabajando en pos de alcanzar el siguiente nivel de madurez.

Llevar a cabo una evaluación continua, utilizando SIM3 como metodología para medirnos, nos permitirá seguir desarrollándonos en diversos aspectos: a) al consolidar una cultura de mejora continua, CERTUNLP contará con los mecanismos y la mentalidad enfocada en la evolución permanente y adaptándose al panorama de amenazas en constante cambio; b) con procesos de recopilación, análisis y gestión de la información, CERTUNLP podrá tomar decisiones más informadas y estratégicas en todos los aspectos de su operación; c) los procesos estarán definidos, automatizados y optimizados, esto se traduce en una respuesta a incidentes más rápida, una gestión de vulnerabilidades más efectiva y, en general, una operación de CERTUNLP mucho más fluida.

Referencias

Bernal Barzallo, P. F., y cols. (s.f.). *SIM3 Modelo de Madurez de CSIRTs.* Descargado 2025-04-09, de https://www.first.org/resources/papers/cali2022/FIRST-LACNIC-SIM3-Modelo-de-madurez-de-los-CSIRT-Paul-Bernal.pdf

Caralli, R., y cols. (2016). *CERT Resilience Management Model (CERT-RMM) Version 1.2* (Inf. Téc.). Software Engineering Institute.

CERTUNLP. (s.f.-a). *Cespi unlp.* Descargado 2025-04-08, de https://www.cert.unlp.edu.ar/

CERTUNLP. (s.f.-b). *GitHub - CERTUNLP/kintun: Restful Vulnerability Scanner.* Descargado de https://github.com/CERTUNLP/Kintun

CERTUNLP. (s.f.-c). *GitHub - CERTUNLP/ngen: Incident Response Management System.* Descargado 2025-04-14, de https://github.com/CERTUNLP/ngen/

Cichonski, P., y cols. (2012). *SP 800-61 Rev. 2 Computer Security Incident Handling Guide* (Inf. Téc.).

CIN — Consejo Interuniversitario Nacional. (s.f.). *Cin — consejo interuniversitario nacional.* Descargado 2025-04-14, de https://www.cin.edu.ar

CSIRTAmericas. (s.f.). *Csirtamericas.* Descargado de https://csirtamericas.org/

Diaz, F. J., y cols. (2023). Sacs. En *Memorias de las jaiio* (Vol. 9, p. 53-57). Descargado de https://revistas.unlp.edu.ar/JAIIO/article/view/18172/17840

ENISA. (s.f.). *Csirt maturity framework — enisa.* Descargado 2025-04-14, de https://enisa.europa.eu/topics/incident-response/csirt-capabilities/csirt-maturity

LACNIC CSIRT. (2024). *Lacnic csirt - csirts de la región.* Descargado 2025-04-03, de https://csirt.lacnic.net/csirts-de-la-region

Open CSIRT Foundation. (s.f.). *Csirt maturity – open csirt foundation.* Descargado 2025-04-08, de https://opencsirt.org/csirt-maturity/

Organización de Estados Americanos. (2025). *CSIRTAmericas Baseline, basado en el modelo SIM3.* Descargado 2025-04-08, de https://www.oas.org/ext/DesktopModules/MVC/OASDnnModules/Views/Item/Download.aspx?type=1&id=1191&lang=2

Organización de los Estados Americanos. (2022). *Reporte de la oea y cisco presenta acciones para ayudar a cerrar la brecha entre la oferta y la demanda de talento en ciberseguridad en latinoamérica.* Descargado 2025-04-09, de https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-069/22

Organización Internacional de Normalización. (2023). *Information secu-*

rity incident management — part 1: Principles and process [Norma ISO/IEC 27035-1: 2023].

RFC 2350. (s.f.). *RFC 2350: Expectations for Computer Security Incident Response* [IETF Datatracker]. Descargado de `https://datatracker.ietf.org/doc/html/rfc2350`

sim3. (s.f.). *sim3.* Descargado de `https://sim3-check.opencsirt.org/#/`

Stikvoort, D., y cols. (s.f.). *SIM3 v2 interim – Security Incident Management Maturity Model.* Descargado 2025-04-07, de `https://opencsirt.org/wp-content/uploads/2023/11/SIM3_v2_interim_standard.pdf`

StrangeBee. (2025). *Cortex — speed up analysis and make response easier.* Descargado de `https://strangebee.com/cortex/`