Evaluación del nivel de madurez de un CSIRT Experiencia de CERTUNLP basada en SIM3

Francisco Javier Díaz[1], Paula Venosa[1,2], Gabriela Suarez[2], Mateo Durante[2], and Jeremías Pretto[2]

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

Abstract. En este artículo se describe el trabajo realizado en relación a la mejora contínua de procesos en CERTUNLP, basado en SIM3, modelo de madurez para CSIRTs. CERTUNLP [1] funciona en la Universidad Nacional de La Plata y es el primer CSIRT académico de la Argentina creado en 2008. El mundo de la ciberseguridad es muy dinámico, por lo cual se vuelve imprescindible para los equipos de respuesta a incidentes de seguridad, el mantenerse actualizados frente a los cambios y avances que se van presentando. También resulta necesario ajustar sus procesos para que éstos acompañen los cambios y los servicios se adecúen a las nuevas amenazas, tendencias y metodologías aplicadas. En este marco resulta de vital importancia contar con alguna metodología que facilite la mejora contínua. Para ello resulta útil empezar por evaluar el nivel de madurez del equipo. La madurez de un CSIRT es un indicativo del nivel de organización de su gobernanza y procesos, y del nivel de preparación del equipo y sus herramientas. La madurez puede medirse con el Modelo SIM3 (Security Incident Management Maturity Model) [2]. Realizar esta evaluación permite conocer fortalezas y debilidades, en función de estándares definidos por organizaciones referentes en la comunidad de CSIRTs.

Keywords: CSIRTs · Gestión de incidentes · SIM3 · Madurez de procesos · Automatización.

1 Intruducción

El trabajo aquí presentado describe la experiencia realizada en CERTUNLP con el objetivo de mejorar el nivel de madurez de sus procesos. CERTUNLP es el Centro de Respuestas de Incidentes de Seguridad de la Universidad Nacional de La Plata (UNLP) que ha operado de manera ininterrumpida desde el año 2008.

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 UNLP. El equipo presta 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 de seguridad

en aplicaciones, redes y servicios, el pentest de aplicaciones y servicios, el monitoreo de seguridad de redes y aplicaciones, y la capacitación y sensibilización en temáticas de ciberseguridad [1].

CERTUNLP funciona en el ámbito de la Universidad Nacional de La Plata y quienes lo integramos nos hemos formado en dicha casa de estudio y hemos impulsado el proyecto sumando alumnos, docentes e investigadores para ofrecer los servicios y hacer crecer al equipo. Sin embargo, nuestra situación actual no escapa a la realidad de escasez de talento humano calificado en materia de ciberseguridad, a nivel nacional, regional [3] y mundial, que hace que la demanda de la sociedad crezca, que nos cueste contar con recursos humanos y también retener a los mismos. Por dicha razón, resulta necesario contar con una estrategia para sostener el proyecto y mejorar los servicios que brindamos, y así continuar siendo referentes en nuestro ámbito y en las redes de las cuales formamos parte como LACNIC-CSIRTs [4], CSIRTAmericas [5] y subcomisión de Ciberseguridad del CIN [6].

2 Modelos de madurez

Un modelo de madurez es un conjunto de prácticas que representan niveles de progresión de las capacidades de una organización. Para medir la madurez de los procesos de negocio, se han diseñado modelos o marcos de referencia que funcionan como una guía para evaluarlos, detectar fallas y mejorar la forma en que los mismos se ejecutan en una organización [7]. Muchos modelos de madurez derivan de las sugerencias o requisitos de un marco de cumplimiento.

En el ámbito de los CSIRTs, la madurez es una indicación de qué tan bien un equipo de respuesta gestiona, documenta, realiza y mide su función. Su evaluación permite saber en qué punto se encuentra respecto a sus capacidades de atención de incidentes de seguridad y de protección de su comunidad objetivo. La madurez de un CSIRT puede medirse con el Modelo de Madurez de Gestión de Incidentes de Seguridad, también llamado SIM3 (acrónimo de las siglas en inglés de Security Incident Management Maturity Model) [2]. La organización "Open CSIRT Foundation" promueve actualmente su uso. Si bien existen otras metodologías como CERT-RMM (Computer Emergency Response Team - Resilience Management Model) [8] y/o guías como la ISO/IEC 27035 [9] y la NIST SP 800-61 [10], hemos elegido SIM3 por ser abierta y simple de aplicar.

SIM3 considera que un CSIRT es maduro cuando la calidad de sus servicios es estable y cuando el equipo cuenta con los recursos necesarios para ello. No considera la madurez respecto a la posesión de habilidades técnicas avanzadas o de la habilidad de manejar grandes volúmenes de incidentes.

SIM evalúa las capacidades de prevención, detección, resolución, control de calidad y retroalimentación en la gestión de incidentes de ciberseguridad. El modelo se compone de 44 parámetros (aspectos) organizados en 4 categorías relacionadas 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, representando las siguientes situaciones: a) Nivel

0: el parámetro en cuestión no está disponible, no fue definido o no fue discutido; b) Nivel 1: el parámetro en cuestión fue considerado pero no documentado; c) Nivel 2: el parámetro en cuestión se ha escrito parcial e informalmente para los fines del equipo pero no ha sido aprobado por la gerencia; d) Nivel 3: el parámetro en cuestión se ha escrito de manera formal y ha sido aprobado por el jefe del equipo; e) Nivel 4: el parámetro es auditado periódicamente por la autoridad de gobernanza que se encuentra por encima del jefe del CSIRT (obteniendo una retroalimentación externa al equipo).

La evaluación SIM3 puede ser realizada manualmente o a través de aplicaciones en línea como por ejemplo, la del propio Open CSIRT Foundation [2], o la implementación de ENISA [11]. 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. Estos grados globales, pueden utilizarse como una forma de acreditación para la membresía a una comunidad dada, como la CSIRT-Network impulsada por ENISA [11].

3 Evaluando el nivel de madurez de CERTUNLP

A fin de medir nuestro nivel de madurez, nos propusimos tomar SIM3 como marco de referencia y evaluar nuestra situación en cada uno de los dominios que este modelo propone. El objetivo que perseguimos al hacerlo es detectar fortalezas y debilidades del equipo a fin de afianzarnos como CSIRT para potenciar los servicios que prestamos.

La metodología que usamos fue que cada miembro del equipo hiciese una evaluación individual a conciencia de cada punto cubierto por SIM3, y luego discutimos cada uno de ellos en reuniones de las cuales participamos los 4 miembros del equipo, y donde se generó un espacio de discusión a partir del cual surgió, no sólo el nivel de madurez alcanzado en cada aspecto evaluado, sino también qué acciones concretas debemos llevar a cabo para superar ese nivel de madurez.

En el gráfico de la Fig. 1 puede apreciarse visualmente que las mediciones individuales no siempre coincidían y la "varianza" existente entre dichas mediciones y la consensuada. En algunos puntos, ello ocurría porque no todos tenemos el mismo conocimiento respecto al funcionamiento del equipo en relación a un aspecto en particular, y en otros porque variaba el criterio a la hora de evaluarlo. Por ello, podemos decir que el valor consensuado es el que más se acerca a la realidad y es el que tomamos como resultado de nuestra evaluación.

4 Conclusiones

La evaluación de SIM3 nos permitió identificar fortalezas y debilidades en nuestros procesos, qué áreas tenemos más maduras que otras, y qué nuevos servicios podemos prestar, facilitando así el crecimiento del equipo y la continuidad de nuestro CSIRT.

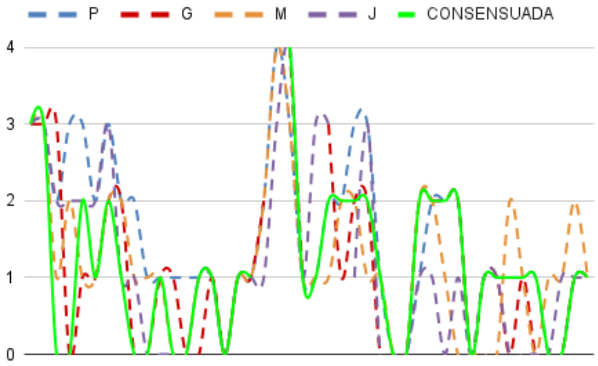

Fig. 1. Gráfico resultando de las evaluaciones individuales y consensuadas de SIM3 en CERTUNLP.

Como resultado de la evaluación, pudimos identificar que: a) tenemos muchos procesos que llevamos a cabo y tareas que hemos automatizado, pero que no hemos documentado y por ende no están formalizadas ni aprobadas; b) aspectos que no habíamos discutido (nivel 0 de madurez), eran debatidos en el momento de la evaluación, con lo cual nuestro nivel ya mejoraba a partir de dicho análisis; c) tenemos potenciales puntos de mejora, para los cuales dejamos registradas las tareas a implementar, quedando pendiente la planificación de objetivos que haremos luego de establecer el siguiente nivel de madurez que queramos alcanzar a corto, mediano y largo plazo; c) hoy en día no realizamos informes con estadísticas de los incidentes gestionados o vulnerabilidades reportadas, y consideramos que el incorporar dicha práctica presentando reportes a la dirección y a nuestra comunidad objetivo permitiría difundir nuestras acciones y visibilizar nuestro trabajo (siempre respetando la confidencialidad de la información que manejamos).

Creemos fehacientemente que trabajar aspirando a un siguiente nivel de madurez y adoptando esta evaluación como una práctica contínua, nos permitirá seguir desarrollándonos en diversos aspectos: a) Desde la perspectiva del equipo CERTUNLP, discutir y documentar nuestros procesos aumentará la coherencia del equipo, disminuirá la incertidumbre en las operaciones diarias, agilizará la incorporación de nuevo personal y mitigará su rotación; b) Como consecuencia de formalizar procesos podremos brindar una mejor atención a nuestra comunidad objetivo y apuntar a una futura certificación; c) Se podrá justificar o evaluar las direccionalidad de las inversiones en seguridad, ya que al permitir una comunicación constructiva con una autoridad de gobierno superior al jefe del CSIRT se podrá determinar si son necesarias mejores herramientas y procesos, más personas, más capacitaciones, etc.; d) Podremos mejorar nuestra visibilidad y cooperación con las redes de CSIRTs donde participamos, compartiendo datos estadísticos.

References

1. Sitio WEB CERTUNLP, recuperado el 20 de abril de 2023, de https://cert.unlp.edu.ar
2. SIM# Model and References, recuperado el 21 de abril de 2023, de https://opencsirt.org/csirt-maturity/
3. OEA (2023). Reporte sobre el desarrollo de la fuerza laboral de ciberseguridad en una era de escasez de talento y habilidades. Recuperado el 20 de abril de 2023, de: https://www.oas.org/es/sms/cicte/docs/Reporte_sobre_el_desarrollo_de_la_fuerza_laboral_de_ciberseguridad_en_una_era_de_escasez_de_talento_y_habilidades.pdf
4. LACNIC CSIRTs. CSIRTs de la Región. Recuperada el 24 de abril de 2023, de https://csirt.lacnic.net/csirts-de-la-region
5. Protegiendo a las Américas en el Ciberespacio. Recuperada el 24 de abril de 2023, de https://csirtamericas.org/
6. CIN Consejo Interuniversitario Nacional. Recuperada el 25 de abril de 2023, de https://www.cin.edu.ar
7. Paez, Gabriel & Rohvein, Claudia & Paravie, Diana & Jaureguiberry, Mario. (2018). Revisión de modelos de madurez en la gestión de los procesos de negocios. Ingeniare. Revista chilena de ingeniería. 26. 685-698. https://doi.org/10.4067/S0718-33052018000400685
8. Richard A. Caralli et all. (2016), CERT Resilience Management Model (CERT-RMM) Version 1.2. Software Engineering Institute.
9. Organización Internacional de Normalización. (2023). Information security incident management — Part 1: Principles and process (Norma ISO/IEC 27035-1: 2023)
10. Paul Cichonski (NIST), Thomas Millar (DHS), Tim Grance (NIST), Karen Scarfone (Scarfone Cybersecurity). (2012). SP 800-61 Rev. 2 Computer Security Incident Handling Guide.
11. CSIRTs Network. Recuperada el 27 de abril de 2023, de https://www.enisa.europa.eu/topics/incident-response/csirts-network