SIM3

Modelo de madurez de CSIRTs

Ing. Paul F. Bernal Barzallo, Mg.
Ing. Ernesto Pérez Estévez, Mg.
csirt@cedia.org.ec

Introducción

- La madurez busca identificar una organización bien cimentada, que se caracteriza por:
  - Brindar buenas condiciones al personal que trabaja en el equipo.
  - Contar con herramientas bien gestionadas y documentadas.
  - Tener procesos bien validados y que se revisan periódicamente.
- Un modelo de madurez busca medir la habilidad de una organización para mejorar, en el caso de los CSIRTs, sus capacidades de gestión de incidentes de seguridad y mejora del nivel de protección de su comunidad objetivo.

Métricas

- Para evaluar la madurez de un CSIRT es necesario definir métricas, que son las propiedades a tener en cuenta en la evaluación del equipo junto con las medidas asociadas a las mismas.
- Existen múltiples formas y modelos de métricas para evaluar la evolución y madurez de un equipo. Las que se elijan deben ser adecuadas para el equipo que se está evaluando. También deben ser claras y simples de medir para lograr una evaluación confiable.
- La evaluación de madurez puede ser realizada por un tercero o por el propio CSIRT.

SIM3

- SIM3 = **Security Incident Management Maturity Model.**
- Promovido por la Open CSIRT Foundation, permite medir la madurez de un CSIRT la cual es un indicativo de qué tan bien un equipo gobierna, documenta, ejecuta y mide su función.
- Es el modelo más usado y aceptado en la comunidad global.
- Su simplicidad permite que se ejecute de forma periódica, según las necesidades de cada equipo, generando un reporte que puede compartirse.

SIM3: Parámetros

Categoría	Número de parámetros	Niveles de madurez
Organizacional	10	0 = no disponible 1 = implícito 2 = explícito, interno 3 = explícito, formalizado por la autoridad del CSIRT 4 = explícito, evaluado regularmente por la alta gerencia, incluyendo un lazo de retroalimentación activa
Aspectos Humanos	7	
Herramientas	10	
Procesos	17	

Asignación de niveles

- Para determinar la madurez evaluamos los parámetros asignándole a cada uno el nivel de cumplimiento en el que se encuentra en cada equipo, siguiendo los niveles de madurez descritos en el modelo.
- SIM3 es un modelo neutral, en general no tiene ni busca condiciones preestablecidas. Por ejemplo, el término “formalizado” no significa “firmado y sellado”, entendiéndose que las organizaciones pueden tener formas y procesos diversos de formalización. Aunque hay excepciones para algunos parámetros.
- Quienes requieren de SIM3 pueden plantear requisitos, como por ejemplo: criterios de membresía, marcos de auditoría, certificaciones, etc.
- No hay nada malo en no conocer o tener algo en cierto nivel. Esto es parte del trabajo con SIM3, el que podemos detectar dónde podemos mejorar.

Descripción de niveles

0 = no disponible / indefinido / desconocido

1 = implícito (conocido / considerado pero no escrito, "entre las orejas")

2 = explícito, interno (escrito pero no formalizado de ninguna manera)

3 = explícito, formalizado bajo la autoridad del jefe del CSIRT (sellado o publicado)

4 = explícito, auditado con autoridad de niveles de gobierno por encima del nivel superior del CSIRT (sujeto a proceso de control / auditoría / cumplimiento)

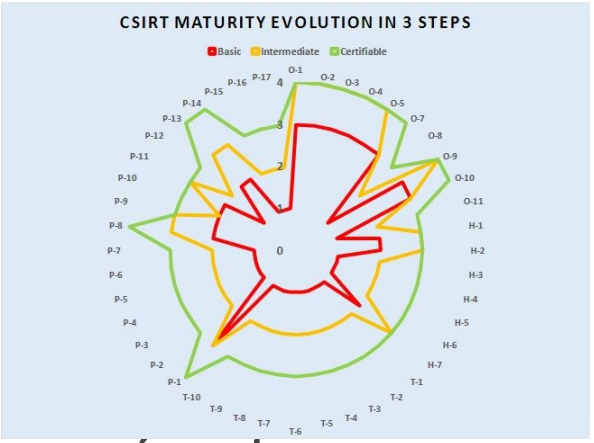
Descripción de niveles

Para que estos cinco niveles sean aún más claros, echemos un vistazo a lo que se debe agregar para pasar de un nivel al siguiente:

- 0 ➔ 1: adición de consideración – "lo hacemos/conocemos, somos conscientes de esto"
- 1 ➔ 2: adición de una descripción escrita – "lo tenemos escrito, así es como lo hacemos"
- 2 ➔ 3: adición de responsabilidad – "lo tenemos normado, esto es lo que estamos obligados a hacer"
- 3 ➔ 4: adición de mecanismo de control - "y así es como nos aseguramos de que suceda"

Evaluación

Como resultado de la evaluación se obtiene, adicionalmente a los niveles de madurez medidos en cada parámetro, un grado global de madurez, expresado en 3 niveles posibles:



- Básico,
- Intermedio y
- Avanzado

La evaluación puede ser manual, armando una matriz de parámetros y niveles de cumplimiento que luego se usa para establecer el grado de madurez del equipo. O en forma automática utilizando alguna aplicación, como la propia Open CSIRT Foundation o la de ENISA, disponibles en línea.

SIM3 para continuidad del CSIRT

Una vez realizada una evaluación, se pueden determinar los parámetros que se pueden trabajar para mejorar el estado de madurez, en base a alguna de estas 3 estrategias:

- **Tradicional.** Implica incrementar la madurez por parámetro, recorriendo la lista de los 44 e irlos cumpliendo. El objetivo general es llenar o cumplir la RFC2350.

- **Mejorado 1.** Además de la RFC2350, escribir al menos los siguientes documentos:
  - Marco de trabajo organizacional, cubriendo la mayor cantidad de parámetros O, además de algunos H y P.
  - Política de contratación de personal, cubriendo la mayoría de parámetros H, y
  - Manejar el resto de la forma tradicional (por parámetro).

- **Mejorado 2.** Escribir un Manual de Madurez del CSIRT, cubriendo todos los parámetros. No se debe olvidar la RFC2350.

Parámetros Organizacionales (10)

O-1: MANDATO La asignación del CSIRT derivada de la alta gerencia.

O-2: COMUNIDAD OBJETIVO: A quién van dirigidas las funciones del CSIRT

O-3: AUTORIDAD: Lo que el CSIRT puede hacer hacia su público objetivo para cumplir con su función.

O-4: RESPONSABILIDAD: Lo que se espera que haga el CSIRT con su público objetivo para cumplir su función.

O-5: SERVICIO Describe los servicios del CSIRT y cómo contactar al CSIRT

O-7: NIVEL DE SERVICIO: Describe el nivel de servicio que se espera del CSIRT.

O-8: CLASIFICACIÓN DE INCIDENTES: La disponibilidad y aplicación de un esquema de clasificación de incidentes a los incidentes registrados. Las clasificaciones de incidentes generalmente contienen al menos tipos de incidentes o categorías de incidentes. Pueden incluir la "gravedad" de los incidentes.

Parámetros Organizacionales (10)

O-9: INTEGRACIÓN EN SISTEMAS CSIRTs EXISTENTES: Describe el nivel de pertenencia del CSIRT a una cooperación CSIRT bien establecida, ya sea directamente o a través de un CSIRT "superior" del cual es consumidor / cliente. Necesario para participar e integrarse en los sistemas CSIRT transnacional / mundial.

O-10: MARCO ORGANIZATIVO: Se incluye O-1 a O-9 en un documento de marco de trabajo coherente que sirve como documento de control para el CSIRT.

O-11: POLÍTICA DE SEGURIDAD: Describe el marco de seguridad dentro del cual opera el CSIRT. Esto puede ser parte de un marco más amplio o el CSIRT puede tener su propia política de seguridad.

Parámetros Humanos (7)

H-1: CÓDIGO DE CONDUCTA / PRÁCTICA / ÉTICA: Conjunto de reglas o pautas para los miembros del CSIRT sobre cómo comportarse profesionalmente, potencialmente también fuera del trabajo.

H-2: RESILIENCIA DEL PERSONAL: Cómo se asegura el personal del CSIRT durante enfermedades, vacaciones, personas que se van, etc.

H-3: DESCRIPCIÓN DEL PROGRAMA: Describe las habilidades necesarias para realizar las labores asignadas

H-4: ENTRENAMIENTO INTERNO: Capacitación interna (de cualquier tipo) disponible para capacitar a nuevos miembros y mejorar las habilidades de los existentes.

Parámetros Humanos (7)

H-5: FORMACIÓN TÉCNICA EXTERNA: Programa que permite al personal obtener capacitación técnica externamente, como TRANSITS, Capacitación EFC CEDIA, Capacitación ENISA CSIRT ó programas como CERT/CC, SANS, etc.

H-6: ENTRENAMIENTO (EXTERNO) EN COMUNICACIÓN: Programa para permitir que el personal reciba capacitación externa en comunicación/presentación (humana).

H-7: REDES EXTERNAS: Salir y conocer otros CSIRT. Contribuir al sistema CSIRT cuando sea posible.

Parámetros Herramientas (10)

T-1: LISTA DE RECURSOS DE TI: Describe el hardware, software, etc., que se usa comúnmente en la circunscripción, de modo que el CSIRT pueda brindar asesoramiento específico.

T-2: LISTA DE FUENTES DE INFORMACIÓN: ¿De dónde obtiene el CSIRT su información de vulnerabilidad / amenaza / escaneo?

T-3: SISTEMA DE CORREO ELECTRÓNICO CONSOLIDADO: Cuando todo el correo de CSIRT se mantiene en un repositorio abierto a todos los miembros de CSIRT, es correo electrónico consolidado.

T-4: SISTEMA DE SEGUIMIENTO DE INCIDENTES: Sistema de notificación de problemas o software de flujo de trabajo utilizado por el CSIRT para registrar incidentes y rastrear su flujo de trabajo.

T-5: TELÉFONO RESILIENTE: El sistema telefónico disponible para el CSIRT es resiliente cuando su tiempo de actividad y los niveles de servicio de reparación cumplen o superan los requisitos de servicio del CSIRT.

Parámetros Herramientas (10)

T-6: CORREO ELECTRÓNICO RESILIENTE: Correo electrónico del CSIRT es resiliente, sus niveles de servicio de tiempo de actividad y tiempo de reparación cumplen los requisitos de servicio del CSIRT.

T-7: ACCESO A INTERNET RESILIENTE: El acceso a Internet para el CSIRT es resiliente, sus niveles de servicio de tiempo de actividad y tiempo de reparación cumplen los requisitos de servicio del CSIRT.

T-8: CONJUNTO DE HERRAMIENTAS PARA PREVENCIÓN DE INCIDENTES: Herramientas destinadas a prevenir que ocurran incidentes en la circunscripción. El CSIRT opera o utiliza estas herramientas o tiene acceso a los resultados generados por ellas.

T-9: CONJUNTO DE HERRAMIENTAS PARA DETECCIÓN DE INCIDENTES: Colección de herramientas destinadas a detectar incidentes cuando suceden o están cerca de suceder. El CSIRT opera o utiliza estas herramientas o tiene acceso a los resultados generados por ellas.

T-10: CONJUNTO DE HERRAMIENTAS PARA RESOLUCIÓN DE INCIDENTES: Conjunto de herramientas destinadas a resolver incidentes una vez que han ocurrido. El CSIRT opera o utiliza estas herramientas o tiene acceso a los resultados generados por ellas.

Parámetros Procesos (17)

P-1: ESCALAMIENTO AL NIVEL GERENCIAL: Proceso de escalamiento a la alta gerencia para los CSIRT que forman parte de la misma organización. Para comunidades objetivo externas: escalamiento a niveles de gerencia de público objetivo

P-2: ESCALAMIENTO A LA FUNCIÓN DE PRENSA: Proceso de escalamiento a la oficina de prensa de la organización anfitriona del CSIRT.

P-3: ESCALAMIENTO A LA FUNCIÓN LEGAL: Proceso de escalamiento a la oficina legal de la organización anfitriona del CSIRT.

P-4: PROCESO DE PREVENCIÓN DE INCIDENTES: Describe cómo el CSIRT previene incidentes, incluido el uso del conjunto de herramientas relacionadas. Además, esto incluye la adopción de servicios proactivos como la emisión de avisos de amenazas/vulnerabilidades/parches.

P-5: PROCESO DE DETECCIÓN DE INCIDENTES: Describe cómo el CSIRT detecta incidentes, incluido el uso del conjunto de herramientas relacionadas

Parámetros Procesos (17)

P-6: PROCESO DE RESOLUCIÓN DE INCIDENTES: Describe cómo el CSIRT resuelve incidentes, incluido el uso de las herramientas relacionadas.

P-7: PROCESOS ESPECÍFICOS DE INCIDENTES: Describe cómo el CSIRT maneja categorías específicas de incidentes, como suplantación de identidad o problemas de derechos de autor. Aclaración: puede ser parte de P-6.

P-8: PROCESO DE AUDITORÍA/RETROALIMENTACIÓN: Describe cómo el CSIRT evalúa su configuración y operaciones mediante autoevaluación, evaluación externa o interna y un mecanismo de retroalimentación posterior. Aquellos elementos que el CSIRT y su gestión consideren no conforme a los estándares se consideran para mejoras futuras.

P-9: PROCESO DE ALCANZABILIDAD EN EMERGENCIAS: Describe cómo llegar al CSIRT en casos de emergencia. Aclaración: A menudo, solo está disponible para otros equipos.

P-10: MEJORES PRÁCTICAS DE E-MAIL Y PRESENCIA WEB: Forma en que el CSIRT maneja alias de buzón de correo genéricos y relacionados con la seguridad o las partes que saben cuándo informar al CSIRT. Describe la presencia en la web.

Parámetros Procesos (17)

P-11: PROCESO PARA MANEJO SEGURO DE LA INFORMACIÓN: Describe cómo el CSIRT maneja los informes y/o la información confidencial de incidentes. También influye en los requisitos legales locales. Aclaración: este proceso apoya el uso de TLP para compartir información.

P-12: PROCESO DE FUENTES DE INFORMACIÓN: Describe cómo el CSIRT maneja las diversas fuentes de información disponibles para el CSIRT (como se define en la herramienta relacionada, si está disponible, ver T-2).

P-13: PROCESO DE DIVULGACIÓN: Describe cómo el CSIRT llega a su comunidad objetivo, no en lo que respecta a incidentes, sino en lo que respecta a las relaciones públicas y sensibilización.

P-14: PROCESO DE INFORMACIÓN: Describe cómo el CSIRT informa a la gerencia y/o al CISO de su organización anfitriona, es decir, internamente.

Parámetros Procesos (17)

P-15: PROCESO DE ESTADÍSTICAS: Describe qué estadísticas de incidentes, según su clasificación de incidentes (ver O-8), el CSIRT divulga a su comunidad objetivo y/o más allá.

P-16: PROCESO DE REUNIÓN: Define el proceso de reunión interna del CSIRT.

P-17: PROCESO PEER-TO-PEER: describe cómo funciona el CSIRT junto con los CSIRT pares y/o con su CSIRT "superior".

Ejercicio de ejemplo

https://sim3-check.opencsirt.org/

Taller

Ingresar a **https://sim3-check.opencsirt.org/**

Proponerse validar el estado de nuestro CSIRT para ingresar a la membresía de FIRST