Una Estrategia de Medición y Evaluación como Soporte para la Gestión de Tecnologías de Información en el Estado

Autores

Covella, Guillermo; Fac. de Ingeniería, UNLPam, 110 nº 390, (L6360GLH) General Pico, La Pampa, Argentina; guillermo.covella@gmail.com

Dieser, Alexander; Fac. de Ingeniería, UNLPam, 110 nº 390, (L6360GLH) General Pico,La Pampa, Argentina; alexander.dieser@gmail.com

Olsina, Luis; Fac. de Ingeniería, UNLPam, 110 nº 390, (L6360GLH) General Pico, La Pampa, Argentina; olsinal@ing.unlpam.edu.ar

Abstract

Teniendo en cuenta la importancia de la gestión de activos de Tecnologías de Información en el Estado es necesario contar no solo con herramientas, sino también con estrategias para poder medir, evaluar, cambiar y mejorar. Es decir, contar con medios eficaces para obtener datos e información confiable para tomar decisiones. Se propone en este trabajo una solución a esa encrucijada, en base a una estrategia basada en métricas e indicadores gestionados como activos de la organización, con soporte en una ontología, un proceso y una metodología bien definidos, a efectos de una implementación factible y práctica. La idea subyacente es ofrecer un enfoque ingenieril, sistemático y sustentable a las áreas de medición y evaluación, que pueden contribuir tanto a procesos como a productos, o incluso artefactos intermedios de un desarrollo. Una prueba de concepto, basada en un caso de estudio sobre una aplicación Web de uso corriente en el ámbito universitario, se presenta como ilustración de la propuesta.

1. Introducción

Tanto los datos como la información son insumos básicos para diferentes procesos. Mientras que los datos suelen provenir de hechos, medidas, cálculos, fórmulas, etc., -que se organizan a menudo como conjuntos de datos y se representan en bases de datos-, la información es la interpretación significativa de datos para un propósito determinado, considerando el punto de vista de un usuario y el contexto en que se genera.

En el presente trabajo se argumenta que las métricas e indicadores son activos básicos de una organización para proporcionar datos e información adecuados para análisis, recomendación, control y seguimiento tanto de procesos como de productos de TI en el ámbito del Estado.

Con el objetivo de llevar a cabo sistemáticamente la medición y evaluación (M&E) de proyectos y programas, las organizaciones que gestionan Tecnologías de Información (TI) deben establecer claramente un conjunto de principios, actividades, métodos y herramientas para especificar, recoger, almacenar y utilizar las medidas confiables, los indicadores respectivos y sus valores.

Por otra parte, con el fin de hacer que el proceso de análisis y toma de decisiones sea más robusto, es necesario garantizar que las medidas y los valores de los indicadores sean repetibles y comparables entre los proyectos de la organización. En consecuencia, debe ser obligatorio almacenar no sólo datos de medición y evaluación, sino también métricas e indicadores con sus metadatos, como por ejemplo: método de medición, escala, tipo de escala, unidad, modelo de agregación de los indicadores y los niveles de aceptabilidad, entre otros.

De hecho, las métricas e indicadores deben ser vistos como diseñados y versionados “por producto” o recurso, y almacenados en un repositorio de la organización [10].

Particularmente, una métrica es la especificación de un proceso de medición que transforma un atributo de una entidad (la entrada) en una medida (es decir, datos, la salida) y el indicador elemental es la especificación clara de un proceso de evaluación, que tiene como entrada una medición de una métrica y produce un valor del indicador (es decir, información).

Sin embargo, mirando en la literatura reconocida [3, 8, 4, 5, 12] lo que significa una métrica o un indicador y cómo encuadran en un proyecto de M&E, así como cuestiones acerca de por qué, qué, quién, cuándo, dónde y cómo medir y evaluar son frecuentemente mal relacionadas y/o pobremente especificadas. Aún más, se observa frecuentemente la falta de un firme

consenso entre las bases terminológicas del área de M&E en diferentes normas reconocidas y publicaciones o, directamente la ausencia de términos relevantes [9].

En particular, se destacarán en este trabajo las especificaciones de métricas e indicadores para los atributos que pueden ser vulnerables con respecto a la característica de seguridad [4] para un sistema de información como entidad de destino.

Una vulnerabilidad es una debilidad inherente en un sistema objetivo que podría ser explotado por una fuente de amenaza. Los atributos más significativos de un sistema se pueden identificar, por ejemplo, con controles de seguridad que, o bien no se han aplicado o que, aunque se aplican, no disminuyen la debilidad [8]. Por lo tanto, la comprensión del nivel de seguridad alcanzado en función de la aceptabilidad de los indicadores relacionados con atributos vulnerables puede ayudar, a su vez, a la evaluación de la calidad y a la planificación de acciones de mejora.

La hipótesis subyacente es que cada atributo significativo asociado a la entidad evaluada (target entity) que será evaluado debe mostrar el máximo nivel de satisfacción de calidad, como un requisito no funcional elemental. Cuanto mayor sea el valor del indicador de calidad alcanzado por cada atributo, menor será la vulnerabilidad y por lo tanto, el impacto potencial.

En definitiva, las contribuciones particulares de este trabajo son: i) resaltar la importancia de agregar valor al área de soporte a la evaluación de seguridad de TI con métodos y estrategias de evaluación de calidad basadas en métricas e indicadores; ii) una discusión detallada sobre la especificación de métricas e indicadores como recursos para los procesos de M&E, haciendo hincapié en la importancia de registrar no sólo los conjuntos de datos e información, sino también los metadatos asociados de las necesidades de información, el contexto, los atributos, las métricas e indicadores con el fin de garantizar la repetitividad y consistencia dentro de los proyectos de la organización; y iii) la ilustración de métricas e indicadores de Seguridad, tomando un resumen de la realización de un caso de estudio. Estos recursos informativos son parte de una estrategia integrada llamada GOCAME (*Goal-Oriented Context-aware Attribute, Measurement and Evaluation*) [13, 14], que se puede utilizar para comprender y mejorar la calidad o la calidad de la capacidad de cualquier activo de una organización.

1.a. Importancia del Trabajo para el Interés Público

Hemos visto a lo largo de los últimos años como las TIC se han transformado no sólo en soporte operativo sino también en herramientas indispensables para la toma de decisiones en organizaciones de todo tipo. A tal punto puede afirmarse esto, que no se concibe hoy, y menos a nivel del Estado, prácticamente ningún proceso que no implique un soporte tecnológico/informático para su ejecución.

Asimismo, cuanto más relevantes son esos procesos, mayores prestaciones se esperan de los métodos y las herramientas que los soportan, de gran volumen o complejidad serán los datos que insume y significativo el aporte a las cadenas de valor en las que participen.

En este sentido, gestionar exitosamente procesos, métodos y herramientas complejos relacionados al gobierno de las TI, tal como se presentan en la actualidad, representa un desafío ineludible para la gerencia de cualquier organización estatal. Necesariamente, aunque no siempre en forma explícita, se debe lidiar con preguntas acerca de la calidad de los productos y servicios que se administran, contratan y proveen: ¿cómo -con qué calidad- son percibidos por los usuarios?, ¿se ajustan a los requerimientos actuales?, ¿adhieren a estándares?, ¿están actualizados en relación al marco legal?, ¿son interoperables?, ¿son vulnerables –inseguros-?.

Cuando estas preguntas se las hace un responsable informático en el Estado, las respuestas adquieren relevancia indiscutida para el interés público, no solo por la eficiencia que pueda exigirse en el manejo de los fondos públicos para su implantación y manejo, sino también en cuanto a la sustentabilidad de las soluciones con las que responda.

Se debe tener en cuenta, en ese sentido, que el Estado es administrador de áreas complejísimas que tienen que ver con la provisión de energía, transportes, educación, justicia, salud y seguridad, entre otras. También compite con grandes organizaciones financieras en el ámbito bancario, tiene el monopolio de la estrategia militar en todos los ámbitos y gestiona la información de miles de estudiantes, docentes, investigadores y administrativos en el ámbito universitario, por enumerar algunos ejemplos concretos.

El soporte de IT de los procesos que llevan adelante esas actividades necesariamente debe ser evaluado, comprendido y mejorado en la medida que el contexto y nuevos requerimientos lo demanden o, al menos, para mantenerse como referencia de organismos a los que controla y fiscaliza. En ese sentido, áreas clave como el desarrollo de software o la seguridad de la Información son importantísimos para el Estado y sensibles a la calidad de los procesos y recursos que se emplean para su realización e implementación.

Llegado a este punto se pueden tener en cuenta un conjunto de estándares de referencia: [3], [4], [5], [6] como punto de partida, porque, orientados por principios básicos de la gestión de la calidad, son bien conocidos y en muchos casos adoptados por organizaciones de referencia. En todos los casos, aunque cada uno en un formato particular, se presenta un área, capítulo o sección, destinado a medición y evaluación. Pero, lamentablemente, no siempre está claro cómo debe diseñarse e implementarse en concreto, y sólo excepcionalmente se ofrecen algunas métricas como ejemplos genéricos de referencia.

Complementariamente, algunos enunciados tradicionales sobre la gestión de la calidad tales como: “no se puede mejorar lo que no se puede comprender”, “no se puede controlar lo que no se puede medir”, “lo que no se controla no se puede gestionar”, etc., dan una pauta general de la importancia de medir, evaluar, comprender y mejorar en una gestión orientada a la calidad.

Ahora bien, cabe preguntarse no si ¿es posible contar con un marco de referencia, una metodología y una base conceptual que permitan responder de modo ingenieril a esas preguntas y desafíos, de manera que las respuestas resulten en procesos repetibles con información comparable y adecuadamente relacionada a los objetivos de la medición?, sino también ¿es factible afrontar ese desafío en el marco de la gestión de TI dentro del Estado?

A continuación se desarrolla una propuesta para responder a estos interrogantes, basada en una estrategia soportada por una base conceptual, métodos, herramientas y un ejemplo que facilita su interpretación e implementación. En la sección 2 se presenta un panorama general de la estrategia GOCAME, centrándose en su marco conceptual y el proceso para una mejor comprensión del modelado de las métricas e indicadores. La sección 3 muestra la especificación concreta de métricas e indicadores, en este caso para Seguridad, aplicadas a un caso de estudio del que se extrae una prueba de concepto. Más adelante, en la sección 4 se ofrecen las conclusiones y cierre de la propuesta. Finalmente se encuentran las referencias a la literatura considerada en la elaboración del trabajo.

2. Antecedentes

Medición y Análisis es un área de proceso para el estándar CMMI [3] para el nivel 2 de su representación por etapas. Constituye, considerando a CMMI un estándar de referencia para Ingeniería de Software, un ejemplo de la importancia que se le asigna a las mediciones y su interpretación como soporte para el análisis y la mejora, de casi todas las otras áreas de proceso.

Además, son necesarias estrategias bien definidas de M&E para sostener consistentemente programas y proyectos de medición, evaluación y análisis, de modo que éstos puedan aportar información apropiada para el cambio y la mejora. En [11] se analizan ampliamente dos estrategias integradas: GQM+Strategies [1] y GOCAME. Esta última basada en tres principios fundamentales: i) un marco conceptual soportado en una terminología bien definida; ii) un proceso de M&E; y iii) métodos y herramientas de evaluación

El primer principio de GOCAME parte de la idea que diseñar e implementar un proyecto o programa de M&E requiere un sólido marco conceptual. No es raro que las organizaciones revisen permanentemente sus programas de medición por falta de resultados consistentes, y lo hacen porque no se presta suficiente atención a la forma en que especifican, implementan y analizan los requerimientos no funcionales, las propiedades del contexto, las métricas y los indicadores relacionados. Para evitar esta situación es que se desarrolló oportunamente el marco de referencia C-INCAMI (*Contextual-Information Need, Concept model, Attribute, Metric and Indicator*) y sus componentes [10], basado en una ontología propia sobre métricas e indicadores [9].

El segundo principio de GOCAME se establece a partir un proceso bien establecido para garantizar la repetitividad en la realización de actividades y consistencia en los resultados. Un proceso prescribe un conjunto de fases, actividades, entradas, salidas, secuencias,

paralelismos, roles y puntos de control entre otras cosas. En [2] se propone un modelo de proceso para GOCAME, compatible tanto con los componentes como con la base conceptual de C-INCAMI.

El tercer principio de GOCAME se basa en métodos y herramientas, que pueden ser instanciados tanto desde el marco conceptual como desde el proceso. Mientras que las actividades describen 'qué' se debe hacer, los métodos especifican 'cómo' se deben realizar esas actividades, que, a su vez, pueden ser automatizadas por herramientas.

2.a. Perspectiva de la Estrategia GOCAME

GOCAME es una estrategia multipropósito para la definición y realización de proyectos de M&E, con un enfoque orientado a metas y sensible al contexto. Es una estrategia multipropósito porque, siempre que se instancien adecuadamente sus modelos de calidad, puede ser usada para evaluar no solo la calidad de distintas categorías de entes tales como producto, sistema y sistema en uso sino también otras, a un nivel de abstracción diferente, como proceso y recurso. Aún más, el foco de la evaluación puede variar: "calidad externa", "calidad de la capacidad", "costo", "costo/calidad", por ejemplo.

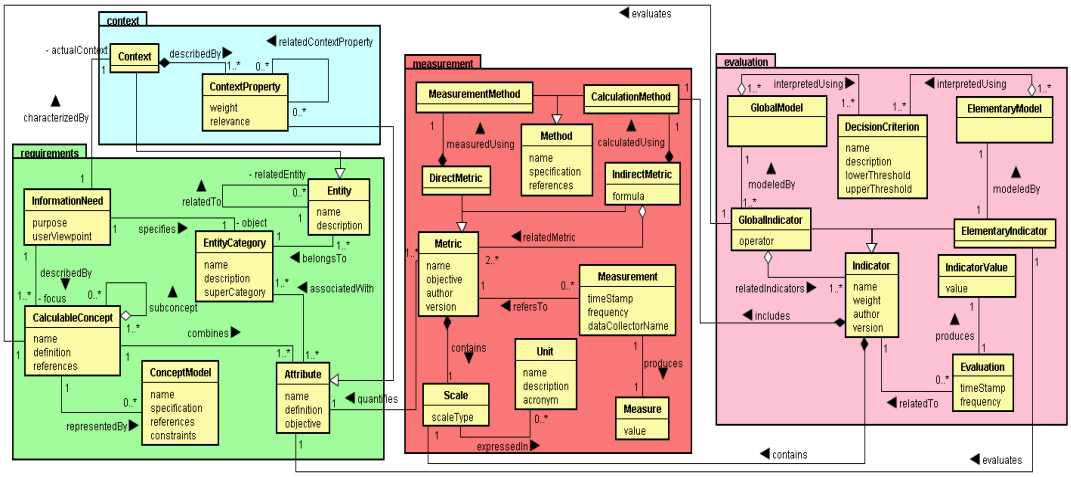

Figura 1. *Conceptos Principales y sus Relaciones para los componentes de Requerimientos, Contexto, Medición y Evaluación de C-INCAMI.*

Teniendo en cuenta el primer principio mencionado anteriormente, GOCAME tiene una base terminológica definida como una ontología desde donde surge el marco conceptual C-INCAMI. Este marco está estructurado en seis componentes: i) definición del proyecto de M&E, ii) especificación de requerimientos no funcionales, iii) especificación del Contexto, iv) diseño e implementación de la Medición, v) Diseño e implementación de la Evaluación y vi) especificación del análisis y la recomendación. Por razones de espacio se presentan a continuación sólo algunos componentes de la Figura 1 y algunos de sus términos (ver más detalles en [10]).

El componente de requerimientos no funcionales permite especificar la necesidad de información del cualquier proyecto de M&E. Identifica el propósito (comprender, predecir, mejorar, controlar) y el punto de vista del usuario (desarrollador, responsable de seguridad, gerente de riesgo, etc.), además se focaliza en un Concepto Calculable (por ej.: "seguridad", "confiabilidad", "calidad") y permite especificar la Categoría de Entidad a evaluar (por ej.: recurso, producto, producto en uso, etc.). Las hojas del modelo instanciado, llamado árbol de requerimientos, son Atributos asociados con una Categoría de Entidad. Debe aclararse que Necesidad de Información está definida como "Visión o entendimiento necesario para gestionar objetivos, metas, riesgos y problemas"; Categoría de Entidad está definida como "una categoría de objeto que puede ser caracterizada por la medición de sus atributos o propiedades", y Entidad como "un objeto concreto que pertenece a una categoría de entidad". Por último, Atributo es "una propiedad mensurable, concreta o abstracta, de una categoría de entidad".

Teniendo en cuenta el componente de Contexto (paquete `context` en la Fig. 1), un término clave es justamente Contexto, definido como "una clase especial de entidad representando el

estado de situación de una entidad, la cual es relevante para una necesidad de información". Se considera Contexto como una clase especial de Entidad, en la que se involucran entidades relevantes relacionadas tales como ciertos recursos, el ambiente empresarial o el proyecto de medición, entre otros. Para describir el contexto se emplean Atributos de las entidades relevantes, que permiten su cuantificación. Esos atributos se llaman Propiedades del Contexto (ver detalles en [7]).

El componente de la medición (paquete `measurement` en la Fig. 1) permite la especificación de métricas que cuantifican atributos. Para el diseño de una métrica es necesario definir tanto los métodos de Medición y Cálculo como la Escala a utilizar. Un método de medición es necesario para especificar una Métrica Directa, en cambio, para una Métrica Indirecta se emplea un método de cálculo. Una Medición produce una Medida. Medición está definido como "una actividad que usa la definición de una métrica para producir el valor de una medida ", Medida es "el número o categoría asignada al atributo de una entidad al realizar una medición", y la Métrica es "la medición o el método de cálculo definidos más la escala de medición asociada".

Consecuentemente, para diseñar una métrica directa se deben especificar claramente dos aspectos como metadatos: el método de medición y la escala. El Método de Medición (también llamado regla de conteo o procedimiento) está definido como "la secuencia lógica particular de las operaciones y posibles heurísticas especificadas para permitir la comprensión de la descripción de una métrica directa por medio de una medición". Escala es "un conjunto de valores con propiedades definidas". El tipo de Escala depende de la relación entre los elementos de la escala y determina el conjunto de operaciones matemáticas y técnicas estadísticas disponibles que pueden usarse para analizar los datos. Las escalas más comunes en el ámbito de la IS son: "nominal", "ordinal", "intervalo", "proporción" y "absoluta".

El componente de la Evaluación (paquete `evaluation` en la Fig. 1) incluye los conceptos y relaciones tendientes a especificar el diseño y la implementación de las evaluaciones elemental y global. Indicador es el término principal, que permite especificar cómo calcular e interpretar los atributos y conceptos calculables del árbol de requerimientos no funcionales. Hay dos tipos de indicadores: Indicadores Elementales e Indicadores Parciales/Globales. En el primer caso se trata de indicadores que permiten evaluar atributos, combinados en un modelo conceptual. Cada indicador elemental tiene un "modelo elemental" que provee una función de mapeo desde las medidas de la métrica a la escala del indicador. Así, la nueva escala es interpretada usando Criterios de Decisión previamente acordados y permite analizar el nivel de satisfacción alcanzado por cada requerimiento elemental, es decir por cada atributo. En el segundo caso se encuentran los Indicadores Parciales/Globales, que permiten evaluar requerimientos de nivel medio y alto, esto es características y sub-características en el modelo conceptual (por ej. el modelo para seguridad, de la Tabla I). Finalmente, el indicador global representa el grado de satisfacción global en obtener la información deseada para un propósito dado y bajo el punto de vista de un usuario predefinido.

En cuanto a su implementación, una Evaluación representa la actividad involucrada en un solo cálculo, siguiendo la especificación particular de un indicador –elemental o global-, produciendo un Valor de indicador. En la ontología de referencia Evaluación está definida como la "actividad que usa la definición de un indicador en términos de producir un valor del indicador", e Indicador (sinónimo: Criterio) como "el método de cálculo y la escala que, junto al modelo y al criterio de decisión, permiten obtener una estimación o evaluación de un concepto calculable con respecto a las necesidades de información definidas"; por último Criterio de Decisión (sinónimo de Nivel de Aceptabilidad) está definido como "umbrales, rangos o patrones usados para determinar la necesidad de una acción o profundizar una investigación, o bien describir el nivel de confianza en un resultado dado".

Teniendo en cuenta el segundo principio de GOCAME, su proceso general abarca las siguientes actividades principales: i) Definir Requerimientos No Funcionales; ii) Diseñar la Medición; iii) Diseñar la Evaluación; iv) Implementar la Medición; v) Implementar la Evaluación; y vi) Analizar y Recomendar. Estas actividades de alto nivel, como también secuencias, paralelismos, entradas y salidas se presentan en la Figura 2.

El proceso propuesto para M&E sigue un enfoque orientado a metas. Una vez que el proyecto ha sido creado, la primer actividad: Definir Requerimientos Funcionales, tiene una meta específica, un problema o riesgo como entrada y una Especificación No Funcional como salida

(la cual contiene un propósito de M&E, punto de vista, un foco, atributos y características instanciadas, e información contextual).

Luego, la actividad Diseñar la Medición permite identificar las métricas desde el repositorio de Métricas para cuantificar los atributos: la salida es un documento de Especificación de Métricas (con la descripción del método de medición, la escala y otros metadatos para cada especificación de métrica). Una vez que la medición fue diseñada, ya es posible realizar las actividades de diseño e implementación de la evaluación. La actividad de Diseño de la Evaluación permite identificar Indicadores con la idea de conocer el nivel de satisfacción alcanzado por los requerimientos elementales y globales.

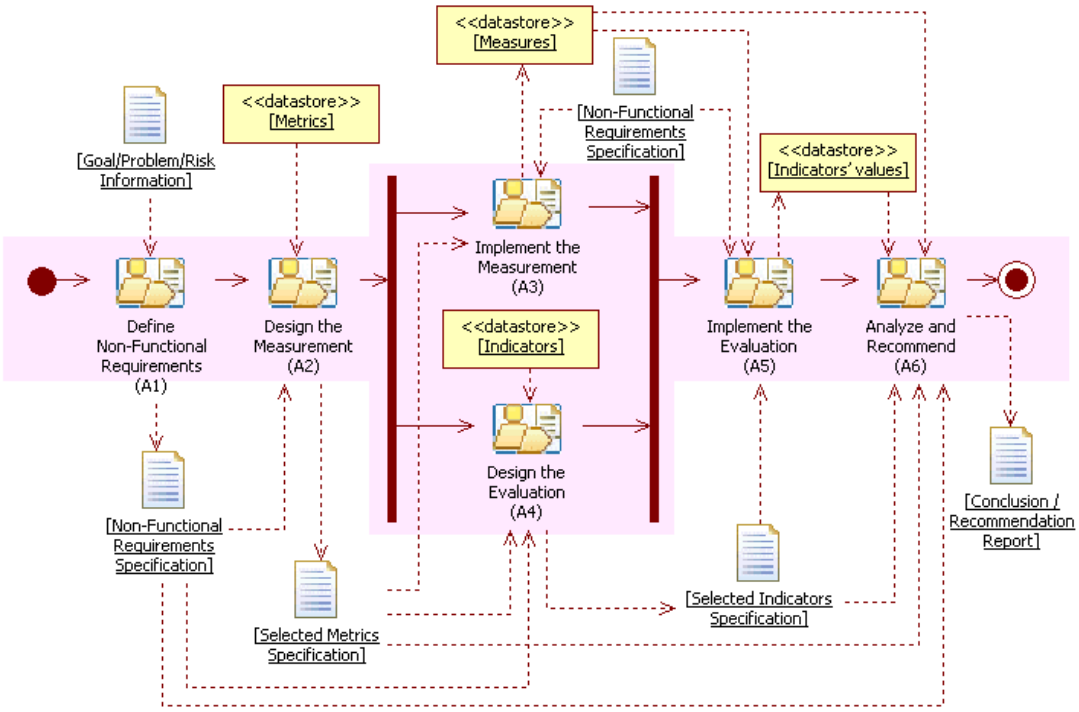

Figura 2. *Actividades de alto nivel del proceso de M&E en GOCAME.*

La actividad Implementar la Medición emplea las métricas seleccionadas para obtener las medidas que son almacenadas en el repositorio de Medidas. Luego se puede ejecutar la actividad de Implementar la Evaluación. Finalmente, la actividad Analizar y Recomendar tiene como entradas los datos de las medidas e indicadores, el documento de especificación de requerimientos y los metadatos de métricas e indicadores para poder producir un reporte sobre la Conclusión/Recomendación.

Considerando que el proceso de M&E incluye actividades tales como la especificación de un árbol de requerimientos, identificación de métricas, análisis y recomendación, etc., se ve necesario disponer de una metodología para integrar todos estos aspectos, así como también herramientas que los automaticen. Para lograr este objetivo se instancian, desde el proceso y el marco conceptual, la metodología WebQEM y su herramienta asociada denominada C-INCAMI_Tool [10].

3. Especificación de Métricas e Indicadores de Seguridad

Una de las contribuciones resaltadas en la sección introductoria es que tanto métricas como indicadores son activos organizacionales clave en la provisión de datos e información relevantes para analizar, recomendar, controlar y finalmente tomar decisiones.

Desde el punto de vista de la especificación, las métricas e indicadores pueden ser consideradas como productos diseñados, versionados y almacenados en repositorios organizacionales, para ser más tarde empleados en procesos de medición (A2 y A3) y evaluación (A4 y A5 en Fig. 2).

3.a. Características de Seguridad para una Aplicación. Una Prueba de Concepto

Se presenta a continuación una prueba de concepto a partir de un caso de estudio sobre la aplicación de GOCAME a Seguridad de una aplicación Web. En principio, para iniciar el proceso, se debe considerar la pregunta acerca de qué se debe medir y evaluar.

En este caso la entidad concreta (target entity) de estudio es un sistema de gestión de estudiantes ampliamente utilizado en el ámbito de la Facultad de Ingeniería de la UNLPam. Se trata de un sistema de información –desde el punto de vista de la Categoría de Entidad a la que pertenece. Ahora bien, ¿porqué debe ser evaluado? Principalmente por la necesidad de información que tiene un responsable de seguridad de la información, en relación a potenciales vulnerabilidades del sistema que, de materializarse, podrían inutilizar la información que gestiona y desacreditar a la institución ante su comunidad y las autoridades pertinentes. Por ejemplo, si un estudiante pudiera modificar notas ya asignadas, empleando un perfil ajeno, como el de un profesor.

En consecuencia, el propósito de la necesidad de información es primero entender el nivel de satisfacción alcanzado, particularmente en este caso se hablará de no vulnerabilidad teniendo en cuenta la característica de seguridad, desde el punto de vista de un administrador del sistema. Una vez comprendido el nivel actual de seguridad, el segundo propósito es mejorar el sistema allí donde se encuentren los indicadores con más bajo desempeño. O en otras palabras, reducir los riesgos que pueda generar la falta de seguridad del sistema.

La Figura 2 muestra como salida de la actividad A1, la especificación de requerimientos no funcionales. Por lo que la Tabla I representa el árbol de requerimientos instanciado para la característica Seguridad y sus sub-características: Confidencialidad (1.1), Integridad (1.2) y Autenticidad (1.3), todas prescriptas por el modelo de calidad externa de la ISO 25010 [4].

Tabla I. Especificación del Árbol de Requerimientos para 'Seguridad'

1. Security
1.1. Confidentiality
1.1.1. Authentication Schema Protectability
1.1.1.1. Authentication Schema Bypass
1.1.1.2. Login Schema Protectability
1.1.2. Session Data Protectability
1.1.2.1. Session Data Disclosure Protectability
1.1.2.2. Session Data Theft Protectability
1.2. Integrity
1.2.1. Cross-Site Scripting Immunity
1.2.1.1. Reflected Cross-Site Scripting Immunity
1.2.1.2. Stored Cross-Site Scripting Immunity
1.2.1.3. DOM-based Cross-Site Scripting Immunity
1.2.1.4. Cross-site request forgery Immunity
1.2.2. *Session Data Tampering Protectability*
1.2.3. *SQL Injection Immunity*
1.3. Authenticity
1.3.1. Session ID Protectability
1.3.1.1. Session ID Theft Protectability
1.3.1.2. Session ID Disclosure Protectability
1.3.1.3. Session ID Tampering Protectability
1.3.2. Session Impersonation Protectability
1.3.2.1. **Session Management Protectability**
1.3.2.1.1.Session ID Expiration
1.3.2.1.2.Session Expiration Due to Idle Timeout
1.3.2.1.3.Re-authentication Mechanism Availability
1.3.2.1.4.Session ID Regeneration Availability
1.3.2.1.5.Keep-me-logged-in Mechanism Availability
1.3.2.2. Session Non-Replay Protectability
1.3.2.3. Session Fixation Protectability
1.3.3. Password Protectability
1.3.3.1. Password Aging Policy
1.3.3.2. String Password Strength

En la Tabla II se definen las sub-características. Por ejemplo, Confidencialidad (Confidentiality (1.1)) representa "el grado en que un producto o sistema asegura que los datos son accedidos solamente por aquellos autorizados para hacerlo"

Adicionalmente, se ha identificado para 1.1 la sub-característica Session Data Protectability (1.1.2) definida como: "el grado en que un sistema asegura la confidencialidad de los datos proveyendo capacidades de protección al acceso". A su vez, se especificaron dos atributos mensurables para 1.1.1, tal como se muestran en itálica en la Tabla I.

Tabla II. Definición de la Característica 'Seguridad' y las sub-características asociadas

Calculable Concept	Definition
Security (1 enTabla I)	Grado en el que un producto o sistema protege información y datos de manera que las personas u otros productos que acceden lo hagan conforme sus niveles y tipos de autorización [4].
Confidentiality (1.1)	Grado en que un producto o sistema asegura que los datos son accedidos solamente por aquellos autorizados para hacerlo [4].
Authentication Schema Protectability (1.1.1)	Grado en que un sistema asegura la confidencialidad de los datos proveyendo capacidades de protección al acceso.
Session Data Protectability (1.1.2)	Grado en que un sistema asegura la confidencialidad de los datos proveyendo capacidades de protección a los datos de sesión.
Integrity (1.2)	Grado en que un sistema o producto protege de accesos no autorizados para su modificación a los programas o datos. Nota ISO [4]: Inmunidad ("el grado en que un producto o sistema es resistente a un ataque") está cubierto por integridad.
Cross-Site Scripting Immunity (1.2.1)	Grado en que un sistema asegura la integridad de los datos proveyendo capacidades de inmunizar contra ataques de tipo "Cross-Site"
Authenticity (1.3)	Grado en que puede probarse que la identidad de una persona un recurso es la que corresponde con quien dice ser [4].
Session ID Protectability (1.3.1)	Grado en que un sistema o producto está protegido contra el robo (ID-thieving) o adulteración (ID-tampering) del Id de sesión.
Session Impersonation Protectability (1.3.2)	Grado en que un sistema o producto asegura la protección contra la imitación de una sesión, proveyendo protocolos de manejo seguro de sesión.
Session Management Protectability (1.3.2.1)	Grado en el que la configuración de la gestión de sesiones de un producto o sistema satisface estándares de seguridad.
Password Protectability (1.3.3)	Grado en el que la configuración de la gestión de contraseñas de un producto o sistema satisface estándares de seguridad (por ej. fortaleza de las contraseñas o vencimiento de contraseñas).

Tabla III. Especificación de las Métricas Involucradas en la Cuantificación del Atributo 'Authentication Schema Bypass'

AttributeName: *1.1.1.1 Authentication Schema Bypass*
Indirect Metric:
Name: Ratio of Protected Pages Accessed via Forced Browsing **(%PPA)**
Objective: Determine the ratio between the number of successful attempts accessing protected pages by forced browsing and the total number of attempts performed.
Author: Covella G. and Dieser A. Version: 1.0
Reference: OWASP Testing Guide 2008 V3.0
Calculation Method:
Formula Specification: %PPA = (#PF / #TPP) * 100
Numerical Scale:
Representation: Continuous Value Type: RealScale Type: Proportion
Unit:
Name**:** Percentage Acronym**:**%
Related metrics:
Number of successful attempts to access protected pages by forced browsing **(#PF)**
Total number of attempts to access protected pages by forced browsing **(#TPP)**

Tabla III (continuación). Especificación de las Métricas Involucradas en la Cuantificación del Atributo 'Authentication Schema Bypass'

Attribute Name: Amount of successful attempts to access protected pages
Direct Metric
Name: Number of successful attempts to access protected pages by forced browsing **(#PF)**
Objective: The number of successful attempts bypassing the authentication schema for the protected page population using the forced browsing technique
Author: Covella G. and Dieser A. Version: 1.
References: OWASP TESTING GUIDE 2008 V3.0
Measurement method
Name: Direct page request
Specification: Using an unauthenticated browser session, attempt to directly access a previously selected protected page URL through the address bar in a browser. Add one per each successful access which bypasses the authentication schema.
Type: Objective.
Numerical Scale
Representation:Discrete ValueType: Integer ScaleType: Absolute
Unit
Name: Successful attempts Acronym: Sa

Attribute Name: Amount of attempts to access protected pages
Direct Metric
Name: Total number of attempts to access protected pages **(#TPP)**
Objective: The total number of protected pages (i.e. the given population) to be attempted for access by a given techniques.
Author: Covella G. and Dieser A. Version: 1.
Measurement method
Name:
Specification: Precondition: Log into the website with a valid user ID and password.
Browse the site looking for the population of protected pages within the "set of pages" subentity, which are those that must be accessed only after a successful login. Add one per each selected protected URL.
Type: Objective.
Numerical Scale
Representation:Discrete ValueType: Integer ScaleType: Absolute
Unit
Name:Protected pages Acronym:Pp

Para el ejemplo señalado en Tabla III, el objetivo del atributo es encontrar el grado en que puede ser evitado el esquema de autenticación previsto. Tiene esto que ver con que si bien la mayoría de las aplicaciones que gestionan datos sensibles requieren autenticación por parte de los usuarios, no todos los métodos proveen una seguridad adecuada. Aquí la plantilla de la métrica presenta el atributo, la métrica indirecta y las métricas directas relacionadas.

Una vez que los requerimientos no funcionales se han especificado, la siguiente actividad (A2) consiste en seleccionar las métricas significativas desde el repositorio de Métricas (ver Figura 2) para cuantificar atributos. Sólo una métrica debe ser asignada para cada atributo del árbol requerimientos. De este modo, la representación de la métrica como recurso informacional para las actividades A2 y A3 abarca metadatos tales como escala, tipo de escala, tipo de valor, especificación del método de cálculo/medición, herramienta, versión, autor, etc. Estos metadatos permitirán luego la repetitividad entre proyectos de M&E y la consistencia de los análisis posteriores. Una vez que se seleccionaron las métricas para la cuantificación de los atributos de la Tabla I, puede llevarse a cabo la siguiente actividad A4, que tiene que ver con el diseño de la evaluación.

Mientras que un indicador elemental evalúa el grado de satisfacción alcanzado por un requerimiento individual, esto es un atributo del árbol de requerimientos, un indicador parcial/global evalúa el nivel de satisfacción alcanzado por requerimientos parciales (nivel de sub características) o globales (nivel de características). Como ya se dijo en la sección 2.a,

indicador es el concepto clave para evaluación, y pueden ser tanto elementales como parciales/globales.

En la Tabla IV se especifica un indicador denominado "Performance Level of the Authentication Schema Bypass (P_ASB)". Este indicador elemental determina el nivel de satisfacción alcanzado por el atributo Authentication Schema Bypass, considerando los valores medidos de su métrica indirecta. A diferencia de las métricas, los indicadores poseen criterios de decisión para la interpretación de los datos, hecho que representa en última instancia información dentro del contexto. En la Tabla IV se emplean, por ejemplo, tres niveles de aceptabilidad, útiles para la interpretación de los valores de los indicadores empleando una escala de porcentaje, previo acuerdo entre los interesados. Un valor entre cero y ochenta [0-80] representa un nivel insatisfactorio y significa que se deben realizar "cambios con alta prioridad"; un valor entre ochenta y noventa y ocho (80-98] representa niveles marginales que significan que "deben llevarse a cabo acciones de mejora"; mientras que finalmente un valor entre noventa y ocho y cien (98-100] corresponde a niveles satisfactorios de aceptabilidad.

En relación a los metadatos de un indicador global, son similares a los mostrados para un indicador elemental. Pero en lugar de un modelo elemental tiene asociado un modelo global o uno de agregación. Un caso de modelo global es LSP (*Logic Scoring of Preference*). Se trata de un modelo de agregación multicriterio ponderado, con operadores especiales para modelar relaciones de simultaneidad (operadores C, de conjunción) y reemplazabilidad (D, de disyunción), tanto entre atributos como entre características y sub-características del árbol de requerimientos.

Tabla IV. Plantilla de Indicador Elemental usada para interpretar el atributo 'Authentication Schema Bypass'

Attribute: *Authentication Schema Bypass* **Coded:** 1.1.1.1

Elementary Indicator:
Name: Performance Level of the Authentication Schema Bypass **(P_ASB)**
Author: Covella G. and Dieser A.
Version: 1.0
Elementary Model:
Function Name: P_ASB function
Specification: the mapping is: P_ASB = 100 iff %PPA=0;
P_ASB = 90 iff %PPA< $\%PPA_{MAX}$;
P_ASB = 0 iff %PPA >= $\%PPA_{MAX}$
where %PPA is the indirect metric.
Decision Criterion:
[Acceptability Levels]
Name 1: Unsatisfactory
Description: indicates change actions must be taken with high priority
Range: if $0 \leq P\_ASB \leq 80$
Name 2: Marginal
Description: indicates a need for improvement actions
Range: if $80 < P\_ASB \leq 98$
Name 3: Satisfactory
Description: indicates no need for current actions
Range: if $98 < P\_ASB \leq 100$
Numerical Scale:
Representation: Continuous
Value Type: Real
Scale Type: Proportion
Unit:
Name: Percentage
Acronym: %

Finalmente, como resultado del proceso total de selección y diseño –actividades A1, A2 y A4 en la Figura 2-, se deben obtener los siguientes documentos: la especificación de requerimientos no funcionales, la especificación de métricas y la especificación de indicadores.

Cuestiones sobre **cuándo** y **dónde** se hacen estas actividades se relacionan en mayor medida en las actividades de Implementar la Medición y Evaluación. Particularmente, por cada

proyecto que se ejecuta de M&E, las actividades A3 y A5 producen como resultados valores de medidas e indicadores en momentos dados, conforme a tiempo y frecuencias predeterminados.

3.b. Valor agregado de la Estrategia basada en Métricas e Indicadores

Es importante remarcar nuevamente que las especificaciones de métricas e indicadores deben considerarse metadatos que deben estar vinculados -con el fin de garantizar la consistencia de análisis comparativos- a valores de medidas e indicadores (datasets) producidos por las actividades A3 y A5.

Supongamos que el mismo atributo del ejemplo Authentication Schema Bypass, puede ser cuantificado por dos métricas (recordar, sin embargo que sólo una puede usarse en cada proyecto de M&E). En un caso una métrica (M1), en el repositorio, es la ya especificada en la Tabla III, y la otra (M2) es una que tiene diferente método de medición y tipo de escala; por ej. M2 tiene asociada una escala de tipo ordinal con valores en el rango de 1 a 3, donde 3 representa la más alta dificultad para alcanzar el objetivo y 1 el más bajo. Luego de varios proyectos de M&E usando los mismos requerimientos no funcionales- o sea los mismos atributos y sub-características, todos los datos y conjuntos de datos de la medición son almacenados en el repositorio de Medidas (Fig. 2). En algunos proyectos fue usada la métrica M1 y en otros la M2 para cuantificar el atributo de referencia.

Consecuentemente, si los metadatos de los datos almacenados no están debidamente vinculados, por ej. el valor 3 que puede provenir de ambas métricas en proyectos distintos, la actividad A6 producirá un análisis inconsistente, principalmente por el hecho de que el valor 3, dependiendo del uso de la métrica, tiene escalas con distintas propiedades, recordando que cada tipo de escala determina el conjunto de operaciones matemáticas y técnicas estadísticas que se pueden usar para analizar datos y conjuntos de datos. Resumiendo, aun si el atributo es el mismo, ambas mediciones de la métrica no son comparables.

Por otro lado, considerando el indicador elemental mostrado en la Tabla IV, se observa que su especificación está hecha en función de niveles de satisfacción de calidad, de modo que el indicador de vulnerabilidad puede ser obtenido por la ecuación del modelo elemental. Recuérdese que la hipótesis subyacente es que cada atributo de seguridad a ser controlado en la entidad objetivo debería tener los más altos niveles de satisfacción de calidad, como un requerimiento no funcional elemental. Sin embargo, la plantilla del indicador elemental en la Tabla IV podría representar el nivel de vulnerabilidad, bajo la premisa de que cuanto más alto es el valor del indicador de calidad alcanzado por cada atributo, menor deberá ser el valor del indicador de vulnerabilidad.

4. Conclusiones

La primer contribución ofrecida en este trabajo tiene que ver con el valor agregado que pueden aportar los métodos y estrategias de M&E basados en métricas e indicadores a la gestión de la calidad de los procesos y los productos desempeñados y desarrollados en el Estado. La propuesta está ejemplificada con una prueba de concepto para seguridad de la información, sobre una aplicación Web de uso generalizado por la comunidad educativa de la Facultad de Ingeniería de la UNLPam. La puerta de entrada de esta propuesta está basada en la identificación de atributos de una entidad objetivo, los que pueden ser cuantificados por métricas e interpretados por indicadores.

Específicamente hablando de la prueba de concepto, ilustrada en la sección 3, representa un caso de cómo aplicar el enfoque presentado en áreas sensibles de TI. Aquí la necesidad de información detectada fue comprender el nivel de calidad alcanzado sobre la característica Seguridad de una aplicación Web, desde el punto de vista del administrador. Una vez comprendido el estado particular y general, el siguiente objetivo sería mejorar aquellos ítems relacionados con los indicadores que mostraron un bajo desempeño, de modo de mejorar la seguridad y reducir riesgos simultáneamente. Las mejoras deberán mostrar, en proyectos semejantes sucesivos, una mejora en la calidad de la aplicación desde el punto de vista de la Seguridad.

El segundo aporte tiene que ver con la consideración acerca de que *métricas e indicadores son también activos organizacionales básicos* para la provisión de datos e información para el análisis, la recomendación, el control y, finalmente, para la toma de decisiones. Nuestro aporte tiene que ver con una forma práctica, sustentable y repetible de llevar adelante un proceso que

provea estos activos a cualquier gerencia de TI en el ámbito público, con un soporte conceptual y empírico desarrollado íntegramente en una universidad pública por investigadores, docentes y becarios argentinos.

REFERENCIAS

[1] Basili V., Lindvall M., Regardie M., Seaman C., Heidrich J., Jurgen M., Rombach D., Trendowicz A. Linking Software Development and Business Strategy through Measurement, IEEE Computer, (43):4, pp. 57–65, 2010.

[2] Becker P., Molina H., Olsina L. Measurement and Evaluation as quality driver. In: ISI Journal (Ingénierie des Systèmes d'Information), Special Issue "Quality of Information Systems", Lavoisier, Paris, France, (15): 6, pp. 33-62. 2010.

[3] CMMI Product Team. CMMI for Development, Ver.1.3. CMU/SEI-2010-TR-033, USA, 2010.

[4] ISO/IEC 25010. Systems and software engineering – Systems and software product Quality Requirements and Evaluation (SQuaRE) – System and software quality models, 2011.

[5] ISO/IEC 27004. Information technology — Security techniques — Information security management — Measurement, 2009.

[6] ISO/IEC 15939. International Standard, Information technology - Software Engineering: Software Measurement Process, Geneva, Switzerland, 2002.

[7] Molina H.; Rossi G., Olsina L. Context-Based Recommendation Approach for Measurement and Evaluation Projects, In: Journal of Software Engineering and Applications (JSEA), Irvine, USA, (3): 12, pp. 1089-1106, 2010.

[8] NIST SP 800-30. Guide for Conducting Risk Assessments. Available at http://csrc.nist.gov/publications/PubsSPs.html, Set. 2011, accessed in March, 2013.

[9] NIST SP 800-55. Performance Measurement Guide for Information Security. Available at http://csrc.nist.gov/publications/PubsSPs.html, July 2008, accessed in March, 2013.

[10] Olsina L., Pesotskaya E., Covella G., Dieser A. Bridging the Gap between Security/Risk Assessment and Quality Evaluation Methods. In Pen-Drive of the 8th Central Eastern European Software Engineering Conference (CEE-SECR) Available at http://2012.secr.ru/talks/bridging-the-gap-between-security-risk-assessment-and-quality-evaluation-methods., Moscow, Russia, pp. 1-10. 2012

[11] Olsina L., Martín M. Ontology for Software Metrics and Indicators. In: Journal of Web Engineering, Rinton Press, USA, (2): 4, pp. 262-281. 2004.

[12] Becker P., Lew P., Olsina, L. Specifying Process Views for a Measurement, Evaluation, and Improvement Strategy. In: Advances in Software Engineering Journal, Academic Editor: Osamu Mizuno, Hindawi Publishing Co, V. 2012, 27 pg., DOI:10.1155/2012/949746. 2012.

[13] Olsina L., Papa F., Molina H. How to Measure and Evaluate Web Applications in a Consistent Way. Chapter 13 in Springer book, HCIS Series: Web Engineering: Modeling and Implementing Web Applications, Rossi G., Pastor O., Schwabe D. and Olsina L. (Eds), pp. 385-420, 2008.

[14] Olsina L., Lew P., Dieser A., Rivera B. Updating Quality Models for Evaluating New Generation Web Applications, In: Journal of Web Engineering, Special issue: Quality in new generation Web applications. Rinton Press, US, 11 (3), pp. 209-246. 2012.