

## La misura della sicurezza

Il tema della misurazione in ambito ICT è un argomento sempre in maggiore espansione, che ormai riguarda diversi aspetti quali: applicazioni, architetture, processi, infrastrutture, ecc. I sistemi di misurazione e il dettaglio degli indicatori è evoluto nel tempo e oggi si può contare su standard per aspetti diversi quali: service level agreement, system performance, dimensioni, caratteristiche di qualità, ecc.

Queste misurazioni si collocano poi all'interno di metodologie e processi che permettono attività di controllo e miglioramento. Alcuni di questi approcci sono diventati degli standard ufficiali approvati da organismi internazionali, oppure de facto adottati da aziende di tipologia e dimensioni diverse.

Un'area in forte evoluzione, anche in quest'ambito, è quella relativa alla sicurezza. La sicurezza tocca argomenti diversi, quali i processi, le applicazioni, le architetture e le soluzioni generali. Gli indicatori anche in quest'area stanno evolvendo secondo le diverse direttrici. Esistono standard per la definizione delle caratteristiche di sicurezza dei processi quali BS7799 (ISO27001), per la valutazione dei rischi dei sistemi quali CRAMM, per la valutazione della sicurezza applicativa come OWASP (Open Web Application Security Project).

Uno degli elementi importanti nella sicurezza, e che è fortemente connesso con il lavoro dell'associazione,

è proprio nell'area applicativa e di sviluppo dei sistemi.

Le applicazioni sono il centro di ogni attività di business e ad oggi le possibilità di controllare e misurare l'uso delle applicazioni per migliorarne i livelli di sicurezza, l'aderenza agli standard e alle performance, è un argomento non ancora pienamente indirizzato con una visione completa. In quest'area c'è un impegno interessante della comunità OWASP, che mira alla ricerca di aspetti di insicurezza insiti nei sistemi software. Aree di interesse sono le applicazioni SOA, le applicazioni web, ecc.

Parallelamente, esistono studi e tecnologie che controllano e analizzano gli aspetti di sicurezza infrastrutturali e in quest'area si collocano strumenti di sicurezza perimetrale e di analisi degli eventi di sicurezza; spesso le informazioni raccolte sono tra loro correlate per avere una visione integrata delle diverse vulnerabilità o tentativi di attacco. Questo tipo di analisi introduce attività volte a determinare preventivamente il grado di efficacia, efficienza e robustezza delle contromisure e delle infrastrutture tecnologiche di sicurezza, rilevandone le eventuali inadeguatezze e fornendo le indicazioni necessarie alla stesura dei piani correttivi di intervento.

In termini generali la possibilità di misurare in modo univoco e oggettivi tali indicatori rappresenterebbe un importante risultato per valutare i livelli di sicurezza presenti in azien-

da. Da ciò emerge che iniziano ad esistere indicatori che cercano di fornire una visione integrata e una misura dei gradi di sicurezza, o vulnerabilità dei sistemi, dei software e delle soluzioni, intendendo per soluzione un sistema integrato HW-SW per erogare un servizio. Ma alla data ancora non emerge un reale standard nell'area delle metriche per il tema sicurezza.

In ambito ISO nell'SC27 ci sono gruppi di studio per lo sviluppo di standard in ambito sicurezza per l'area delle misurazioni. Obiettivo di queste iniziative è creare Security Metrics che possano essere comparate con i Security Objectives, e che possano nel tempo essere confrontate per valutare i rischi attuali e le evoluzioni e che permettano di misurare aspetti e requisiti quali:

- (corporate) governance;
- compliance con le leggi;
- stato dei livelli di aderenza a modelli di certificazione.

Inoltre tali indicatori, se opportunamente aggregati e analizzati, potrebbero fornire indicazioni al management sui livelli di esposizione al rischio dell'organizzazione, nonché sul Total Cost di un programma di sicurezza.

La possibilità di ricavare tali indicatori in maniera oggettiva permetterebbe tra l'altro:

- comparazione con benchmark;
- comparazione con best practice;
- analisi storica delle evoluzioni dei livelli di sicurezza;
- comparazione con possibili competitor, ecc.

Proprio per cogliere questa necessità di evoluzione e attenzione da parte del mercato, e considerando le finalità dell'associazione, è stato ideato un gruppo di lavoro che partirà per creare una base di conoscenza comune su questi argomenti e per poter fornire e raccogliere, come associazione, indicazioni sia dagli associati che dagli organismi interessati. L'evoluzione del gruppo di lavoro sarà riportata nelle prossime newsletter.

LOREDANA MANCINI  
PRESIDENTE [GUFPI-ISMA](http://www.gufpi-isma.org)



### Messaggio del GUFPI-ISMA

In un'epoca sempre più densa di messaggi via e-mail e di informazioni multimediali, sembra quasi antistorico voler dare una valenza informativa ad una semplice newsletter. Anche questa è però un'occasione di incontro "virtuale" tra persone che condividono tematiche analoghe in un ambito ICT oggetto da anni di un'inarrestabile e veloce trasformazione tecnologica, di cui è difficile fornire una fotografia statica che sintetizzi lo stato attuale.

La conoscenza digitale si sta estendendo a tutto lo scibile della conoscenza umana rappresentando, con opportuni standard, una garanzia conoscitiva di base delle generazioni future, più che un elemento di "digital divide".

I fattori di qualità di questa conoscenza, negli svariati aspetti del software, dei dati, della loro presentazione sul web, dell'integrazione tra sistemi diversi, della conservazione permanente, sono tutti in gioco e necessitano di sempre maggiori consapevolezza delle logiche del Knowledge Management e delle tecniche utilizzabili.

La rivoluzione in atto nel mondo del software riguarda, rispetto ai primordi, la maggiore centralità dei dati e

dell'utente, e presuppone anche un adeguamento culturale che porterà benefici nella direzione di una conoscenza digitale sempre più "usabile", "aggiornata", "integrata", "multimediale".

Anche le attività di misurazione dovranno adeguarsi all'evolversi delle tecnologie, condividendo nuovi schemi e semplificando gli attuali, all'insegna della produttività e della qualità dei servizi all'utente.

Con tale finalità pre-competitiva la nostra associazione promuove contributi, incontri e scambi di informazione sia nelle riunioni plenarie dedicate che in ambito pubblico della convegnistica di settore.

Ci auguriamo per il 2007 il proliferarsi di iniziative utili, secondo le esigenze di tutti, con ulteriori idee di quantificazione di quelle qualità essenziali del software e dei dati, che ci possono orientare verso la maggiore semplicità possibile di gestione degli eventi che andiamo ad automatizzare.

DOMENICO NATALE  
VICE PRESIDENTE [GUFPI-ISMA](http://www.gufpi-isma.org)

### Notizie

**Roma, 19 Gennaio 2007**

Si svolge l'esame **CFPS (Certified Function Point Specialist)** dell'IFPUG. Prossimo appuntamento in Italia a Maggio 2007.

**Roma, 2 Febbraio 2007**

Si terrà l'**Assemblea Ordinaria** del GUFPI-ISMA, aperta anche ai non-soci. Maggiori informazioni: [www.gufpi-isma.org](http://www.gufpi-isma.org).

**Vancouver, Aprile 2007**

Workshop IFPUG e Functional Sizing Summit, 2° edizione. Ulteriori informazioni: [www.ifpug.org](http://www.ifpug.org).

## Enti & Eventi



### EQUITY 2006

1<sup>st</sup> IEEE Conference on Exploring Quantifiable Information Technology Yields, 5-8 Febbraio, Amsterdam

**FASE 2007**, Fundamental Approaches to SW Engineering, 24 Mar. - 1 Aprile, Braga (Portogallo)

**SEPG 2007**, 19<sup>th</sup> SW Engineering Process Group Conf., 26-29 Marzo, Austin (Texas - USA)

**SE 2007**, Software Engineering 2007, 27-30 Marzo, Amburgo

**EASE 2007**, 11<sup>th</sup> Intl Conf. on Empirical Assessment in SW Engineering, 2-3 Aprile, Staffordshire (UK)

[www.gufpi-isma.org/eventi](http://www.gufpi-isma.org/eventi)

## CPC {COUNTING PRACTICES COMMITTEE}

Il Counting Practices Committee riunisce i membri del GUFPI-ISMA interessati al miglioramento della formulazione delle regole di conteggio dei Function Point e ad una loro omogenea interpretazione a livello interaziendale.

Linee Guida: di prossima pubblicazione la nuova versione del Manuale Operativo "Strategie di Acquisizione delle Forniture ICT" che è parte delle "Linee Guida sulla qualità dei beni e servizi ICT per la definizione e il governo dei contratti della PA" emanate dal CNIPA. Tale revisione, autonomamente governata dal CNIPA, espone l'approccio suggerito alle P.A. per l'uso dei Function Point nei

contratti di acquisizione di software custom ed è stata fortemente ispirata al documento GUFPI-ISMA sulle "Linee Guida Contrattuali per l'uso dei FP", già disponibile da Luglio 2006 sul sito dell'associazione. Nel primo semestre 2007 il CPC si propone di riallineare i documenti di riferimento pubblicati sulla materia, di raccogliere feedback di utilizzo dal mercato e di procedere nella eventuale estensione del documento GUFPI-ISMA.

Prassi di conteggio: La questione incentrata sulla presunta

identità di processi elementari che differiscono solo per l'esecuzione su media diversi (ad esempio video, stampante, sintetizzatore vocale etc.), oggetto di un recente ballottaggio da parte dell'IFPUG, si è conclusa con la decisione di approfondire lo studio di impatto e di censimento delle prassi utilizzate nel mondo prima di prendere una decisione definitiva. Il CPC GUFPI-ISMA ha già emesso tempo fa una propria linea guida che fa propria la scelta dell'identità.

Il coordinatore - ROBERTO MELI

[www.gufpi-isma.org/cpc](http://www.gufpi-isma.org/cpc)

## SBC {SOFTWARE BENCHMARKING COMMITTEE}

[www.gufpi-isma.org/sbc](http://www.gufpi-isma.org/sbc)

Il Software Benchmarking Committee riunisce i membri del GUFPI-ISMA interessati alle tecniche di standardizzazione usate per confrontare diverse performance, con particolare riferimento alla produttività e al costo unitario del SW.

Proseguono le ricerche affidate a vari sottogruppi e membri, in particolare sui temi seguenti:

- analisi discriminante aggiornata e ampliata sulla base del campione di progetti di sviluppo e manutenzione evolutiva ISBSG Benchmark 9;
- raccolta ragionata di fattori di impatto della produttività di sviluppo e manutenzione

del software, ausilio - per esempio - alla tassonomia contrattuale e alla costruzione di modelli di stima;

- "glossario del benchmarking", in italiano, ausilio all'utilizzo di database esistenti o alla definizione e raccolta di nuovi database "locali".

In occasione dell'assemblea plenaria dei soci del GUFPI-ISMA, prevista per il 2 febbraio p.v. il comitato riferirà sui progressi e sui primi risultati delle ricerche in corso.

Procede inoltre la collaborazione con l'ISBSG per l'evoluzione

dei questionari di raccolta dei dati metrici e progettuali per il benchmarking - in particolare per progetti di sviluppo e manutenzione evolutiva. Chi avesse esperienza di utilizzo di tale questionario e volesse fornire i propri spunti, può comunicarli ai coordinatori.

Per la cronaca, l'ISBSG ha superato la ragguardevole quota di 4'000 progetti di sviluppo e manutenzione raccolti nel proprio benchmark, di cui si attende la prossima pubblicazione.

I coordinatori  
DOMENICO NATALE & LUCA SANTILLO

## Da leggere



S. Maguire (ed.),  
J. McCarthy, S. McConnell  
*Software Engineering Classics*  
Microsoft Press, 1998

J.R. Meredith, S.J. Jr. Mantel,  
*Project Management: A Managerial Approach, 6<sup>th</sup> Edition with Microsoft Project® & Crystal Ball®*  
John Wiley & Sons, 2006

GUFPI-ISMA  
*Metriche del software, Esperienze e ricerche*  
FrancoAngeli, 2006  
[www.gufpi-isma.org/libro](http://www.gufpi-isma.org/libro)

[www.gufpi-isma.org/bibliografia](http://www.gufpi-isma.org/bibliografia)

## Presi in rete



What Is Testing  
<http://www.whatistesting.com/>  
A Tester's Paradise

ZPG Measurement Resources  
<http://www.zigonperf.com/resources.html>  
Improve Employee Performance

Sticky Minds  
<http://www.stickyminds.com/measurementandreporting.asp>  
Measurement & Reporting Zone

R.S. Pressman & Associates, Inc.  
<http://www.rspa.com/reflib/Index.html>  
Downloadable Reference Library

Altri siti: [www.gufpi-isma.org/links.htm](http://www.gufpi-isma.org/links.htm)

## SMC {SOFTWARE MEASUREMENT COMMITTEE}

[www.gufpi-isma.org/smc](http://www.gufpi-isma.org/smc)

Il Software Measurement Committee riunisce i membri del GUFPI-ISMA interessati alla ricerca e al confronto dei vari possibili metodi di misurazione e metriche del software proposti e/o usati in ambito nazionale e internazionale.

Nel secondo trimestre 2006 sono stati pubblicati in Area Soci due technical report relativi al lavoro su ERP/COTS (Bibliografia ragionata, Guida Misure e Metriche), a conclusione dei lavori sul tema.

Si avvia quindi un nuovo lavoro sull'argomento ampiamente dibattuto della qualità della documentazione prodotta nell'

ambito dello sviluppo del software. Il ciclo di vita si compone di diversi processi, al termine dei quali è solitamente prodotta la documentazione dei risultati delle attività svolte. Scopo dell'analisi sarà individuare misure utili a valutare la documentazione prodotta dal progetto software. Ci si orienterà sui documenti prodotti nell'ambito dei processi primari dell'Ingegneria del Software, tralasciando al momento la documentazione generata dai processi organizzativi o di supporto. Due i sotto-obiettivi previsti:

- 1) Costruire un Modello di Qualità della documentazione con misure specifiche, con verifica di applicabilità su una selezione di "documenti tipo";
- 2) Introdurre il miglioramento continuo con l'appraisal Documentation Maturity Model, per determinare profili campione anche attraverso il mapping con ISO, CMMI/SPICE, IEEE, ecc.

Al termine dei lavori si prevede di rendere disponibili ai soci:

- il Modello di Qualità della documentazione di progetto;
- le Linee guida per la produzione di documenti validi secondo tale modello.

I coordinatori  
LUIGI BUGLIONE & CLAUDIO GRANDE

I soci beneficiano di sconti e documenti riservati. Per ulteriori informazioni: [info@gufpi-isma.org](mailto:info@gufpi-isma.org).