

LINEE GUIDA PER L'ADOZIONE DI UN CICLO DI SVILUPPO DI SOFTWARE SICURO

SOMMARIO

1	INTRODUZIONE	6
1.1	SCOPO	6
1.2	STRUTTURA DEL DOCUMENTO	6
2	RIFERIMENTI	7
2.1	DOCUMENTI DI RIFERIMENTO	7
3	DEFINIZIONI E ACRONIMI	8
3.1	DEFINIZIONI	8
3.2	ACRONIMI	8
4	ESIGENZE E AMBITI DI APPLICAZIONE	10
4.1	IL PANORAMA DELLE VULNERABILITÀ APPLICATIVE	10
4.2	SVILUPPO APPLICAZIONI SICURE	11
4.3	SECURITY TOOLS	14
5	ANALISI DELLE INIZIATIVE E DEGLI STANDARD	18
5.1	INIZIATIVE INTERNAZIONALI	18
5.1.1	<i>Open Web Application Security Project (OWASP)</i>	18
5.1.2	<i>Common Criteria (CC)</i>	20
5.1.3	<i>IEEE Computer Society</i>	21
5.1.4	<i>International Organisation for Standardization (ISO)</i>	22
5.1.5	<i>International Society of Automation (ISA)</i>	24
5.1.6	<i>Software Assurance Forum for Excellence in Code (SAFECODE)</i>	26
5.1.7	<i>SANS Software Security Institute (SANS SSI)</i>	27
5.1.8	<i>Web Application Security Consortium (WASC)</i>	28
5.1.9	<i>Institute For Software Quality (ifSQ)</i>	29
5.2	INIZIATIVE EUROPEE	30
5.2.1	<i>Networked European Software and Services Initiative (NESSI)</i>	30
5.2.2	<i>Piattaforme Nazionali NESSI</i>	31
5.2.3	<i>OWASP Local Chapters</i>	33
5.2.4	<i>Motor Industry Software Reliability Association (MISRA)</i>	36
5.2.5	<i>European Space Agency (ESA)</i>	37
5.3	INIZIATIVE US	38
5.3.1	<i>CERT Secure Coding</i>	38
5.3.2	<i>Software Assurance Metrics and Tool Evaluation (SAMATE)</i>	39
5.3.3	<i>Common Weakness Enumeration (CWE)</i>	41
5.3.4	<i>Common Attack Pattern Enumeration and Classification (CAPEC)</i>	43
6	LA SICUREZZA IN TUTTE LE FASI DEL CICLO DI SVILUPPO DEL SOFTWARE	45
6.1	SECURE SDLC	45
6.2	RISK ASSESSMENT	46
6.2.1	<i>Tool per l'analisi del rischio</i>	49
6.3	REQUISITI	50
6.3.1	<i>Linguaggi per la specifica dei requisiti</i>	50
6.3.2	<i>Tool per la specifica dei requisiti</i>	53
6.4	PROGETTAZIONE	54
6.4.1	<i>Secure Design Languages</i>	54
6.4.2	<i>Software Design Tools</i>	54

6.5	IMPLEMENTAZIONE.....	55
6.5.1	<i>Software Implementation Tools</i>	55
6.6	VERIFICA	57
6.6.1	<i>Software Verification Tools</i>	57
6.7	VALIDAZIONE.....	61
6.7.1	<i>Software Release Tools</i>	62
6.8	SUPPORTO	63
6.8.1	<i>Software Response Tools</i>	63
6.9	CATALOGO SECURITY TOOLS.....	66
6.10	TRAINING E FORMAZIONE.....	66
6.10.1	<i>Secure Coding in C and C++</i>	67
6.10.2	<i>Writing Secure Code - C++</i>	67
6.10.3	<i>Writing Secure Code - Java (J2EE)</i>	68
6.10.4	<i>Foundstone (Mcafee) Courses</i>	68
6.10.5	<i>Threat Modeling</i>	68
6.10.6	<i>Writing Secure Code - ASP.NET (C#)</i>	69
6.10.7	<i>Oracle Courses</i>	69
6.10.8	<i>Developing Secure Java Web Services, Java EE 6</i>	69
6.10.9	<i>MySQL and PHP - Developing Dynamic Web Applications</i>	70
6.10.10	<i>Google Gruyere</i>	71
6.10.11	<i>OWASP Training Courses</i>	71
7	CERTIFICAZIONI PROFESSIONALI	72
7.1	GIAC SECURE SOFTWARE PROGRAMMER (GSSP) CERTIFICATION	72
7.2	INTERNATIONAL COUNCIL OF E-COMMERCE CONSULTANTS (EC-COUNCIL) CERTIFICATIONS.....	72
7.3	CERTIFIED ETHICAL HACKER (CEH)	73
7.4	CERTIFIED SECURITY ANALYST (ECSA).....	73
7.5	CERTIFIED SECURE PROGRAMMER (ECSP)	73
7.6	CERTIFIED SOFTWARE SECURITY LIFECYCLE PROFESSIONAL (CSSLP) AND CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP)	74
7.7	CERTIFICAZIONI ISACA (CISA, CISM, CRISC)	75
7.8	INTERNATIONAL SECURE SOFTWARE ENGINEERING COUNCIL (ISSECO)	76
8	SECURE SOFTWARE DEVELOPMENT LIFE CYCLE (SSDLC): ANALISI DELLE METODOLOGIE E DEI PROCESSI	78
8.1	LIFE CYCLE & MATURITY MODELS	78
8.1.1	<i>Software Assurance Maturity Model (SAMML)</i>	78
8.1.2	<i>Systems Security Engineering Capability Maturity Model (SEE-CMM)</i>	79
8.1.3	<i>Building Security In Maturity Model (BSIMM)</i>	80
8.2	ANALISI DEI PROCESSI SSDLC	82
8.2.1	<i>McGraw's Secure Software Development Life Cycle Process</i>	82
8.2.2	<i>Microsoft Software Development Life Cycle (MS SDL)</i>	83
8.2.3	<i>Appropriate and Effective Guidance for Information Security (AEGIS)</i>	84
8.2.4	<i>Secure Software Development Model (SSDM)</i>	85
8.2.5	<i>Aprville and Pourzandi's Secure Software Development Life Cycle Process</i>	85
8.2.6	<i>Secure Software Development Model (SecSDM)</i>	86
8.2.7	<i>Software Security Assessment Instrument (SSAI)</i>	86
8.2.8	<i>Hadawi's Set of Secure Development Activities</i>	86
8.2.9	<i>Comprehensive, Lightweight Application Security Process (CLASP)</i>	87
8.2.10	<i>Secure Software Development Process Model (S2D-ProM)</i>	87
8.2.11	<i>Team Software Process for Secure Software Development (TSP Secure)</i>	87
9	LINEE GUIDA PER L'ADOZIONE DI UN CICLO DI SVILUPPO SOFTWARE SICURO	89
9.1	DEFINIZIONE DEI REQUISITI DI SICUREZZA.....	90

9.1.1	Identificazione degli strumenti a supporto	92
9.2	PROGETTAZIONE DI APPLICAZIONI SICURE	93
9.2.1	Identificazione degli strumenti a supporto	93
9.3	IMPLEMENTAZIONE DI APPLICAZIONI SICURE	94
9.3.1	Identificazione degli strumenti a supporto	94
9.4	VERIFICA DELLA SICUREZZA DELLE APPLICAZIONI.....	97
9.4.1	Identificazione degli strumenti a supporto	98
9.5	SUPPORTO PER LA MANUTENZIONE DI APPLICAZIONI SICURE.....	98
9.5.1	Identificazione degli strumenti a supporto	99
10	LINEE GUIDA PER L'IMPLEMENTAZIONE DELLA PRIVACY BY DESIGN NEL SDLC.....	100
10.1	INTRODUZIONE E CONCETTI BASE	100
10.1.1	Principi della Privacy.....	100
10.1.2	Obiettivi di protezione	103
10.1.3	Privacy by design	104
10.1.4	Data protection Impact Assessment.....	105
10.1.5	Flusso informativo del trattamento.....	110
10.1.6	Privacy Implementation Strategy	111
10.2	CICLO DI VITA DELLO SVILUPPO SOFTWARE NELL'AMBITO DEL GDPR.....	111
10.3	IMPLEMENTAZIONE DELLA STRATEGIA NELLE FASI DI SVILUPPO DEL SOFTWARE	114
10.3.1	Scopo	114
10.3.2	Le fasi di implementazione della Engineering Privacy by Design.....	114
10.4	INTEGRAZIONE DELLA ENGINEERING PRIVACY BY DESIGN NEL SOFTWARE LIFE CYCLE PROCESS.....	115
APPENDICE 1.	CATALOGO SECURITY TOOLS	116
APPENDICE 2.	VALUTAZIONE STRUMENTI.....	128
A.	CHECKMARX	128
B.	CODEDX.....	132
C.	SONARQUBE	134
11	BIBLIOGRAFIA	137

LISTA DELLE TABELLE

Tabella 1 - Documenti di Riferimento.....	7
Tabella 2 - Definizioni	8
Tabella 3 - Acronimi	9
Tabella 4 - Struttura del Catalogo Security Tool	66
Tabella 5 - Principi generali della privacy	101
Tabella 6 - I sette principi della Privacy by Design	105
Tabella 7 - Tipologie di trattamento che rappresentano un rischio elevato	107
Tabella 8 - Esempi di attributi per indentificare una persona	109
Tabella 9 - Fasi dell'Engineering Privacy by Design.....	114

LISTA DELLE FIGURE

Figura 1 - Andamento delle vulnerabilità per anno [Fonte: https://www.cvedetails.com]	11
Figura 2 - Il costo degli attacchi	12
Figura 3 - Defence-in-Depth model for IT	13
Figura 4 - OWASP Top 10 - 2017	14
Figura 5 - Augment the life cycle with security tools.....	16
Figura 6 - Una porzione dell'albero di classificazione CWE	42
Figura 7- CWE Top 25 [Fonte: https://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html]	43
Figura 8 - Secure development activities.....	45
Figura 9 - Modello fasi SSDLC	45
Figura 10 - Esempio di Schema di Risk Assessment.....	47
Figura 11 - Gestione del rischio nel ciclo di vita del Software	48
Figura 12 - Cyber Risk Management di AgID – Report dei rischi per categoria di minaccia	49
Figura 13 - Input e Output della fase Final Review - Secure Release.....	62
Figura 14 - SAMM Structure	79
Figura 15 - BSIMM SSF	81
Figura 16 - Training practice BSIMM.....	82
Figura 17 - Microsoft SDL.....	83
Figura 18 - Input e Output della fase Risk Assessment.....	92
Figura 19 - Input e Output della fase Threat Modeling Attack Surface Analysis	93
Figura 20 - Input e Output della fase Static Analysis	94
Figura 21 - Report di Checkmarx.....	96
Figura 22 - Interfaccia CodeDx.....	96
Figura 23 - Info Security Product Guide 2016 : Recensione CodeDX.....	97
Figura 24 - SonarQube	97
Figura 25 - Input e Output della fase Dynamic Analysis	98
Figura 26 - Continuous Security	99
Figura 27 – Esempio di flusso di valutazione necessità DPIA.....	106
Figura 28 - Esempio di flusso informativo del trattamento.....	111
Figura 29 - Integrazione della Engineering privacy by design nel Software Life Cycle Process	115

1 INTRODUZIONE

1.1 Scopo

Scopo del presente documento è fornire le linee guida per intraprendere un processo di sviluppo del software “sicuro”, nel corso di tutte le fasi SDLC, attraverso l’identificazione e l’implementazione di opportune azioni di sicurezza.

1.2 Struttura del documento

Il presente documento è articolato come di seguito:

- **Esigenze e Ambiti di Applicazione**, come nasce l’esigenza dello sviluppo di software sicuro.
- **Analisi delle iniziative e degli standard**, analizza lo scenario nazionale e globale fornendo una vista delle iniziative e dei risultati prodotti in termini di: metodi e modelli, standard best practices, strumenti. L’analisi dello scenario ha consentito la creazione del *Catalogo dei Security Tools*.
- **Secure Software Development Life Cycle (SSDLC): Analisi delle metodologie e dei processi**, analizza i diversi metodi e modelli SDLC esistenti, con l’obiettivo di identificare le caratteristiche che rendono un ciclo di sviluppo software sicuro ed efficace.
- **La sicurezza in tutte le fasi del ciclo di sviluppo software** è un approfondimento sulle fasi SDLC poiché, tradizionalmente, gli aspetti di sicurezza non sono mai considerati con sufficiente attenzione fin dall’inizio del SDLC stesso.
- **Training e formazione**, focalizza l’attenzione sul fatto che molti degli attuali problemi di sicurezza derivano da errori di progettazione e/o di implementazione, risolvibili solo disponendo di personale formato e consapevole.
- **Certificazioni professionali**, è un elenco delle principali certificazioni riconosciute in ambito InfoSec.