



3 DEFINIZIONI E ACRONIMI

3.1 Definizioni

Vocabolo	Descrizione
Ambiente di produzione	Agglomerato di sistemi, dispositivi hardware ed applicazioni in cui il software viene installato nella sua forma definitiva al fine di soddisfare le richieste dell'operatore o dell'utente finale.
Ambiente di sviluppo	Agglomerato di sistemi, dispositivi hardware ed applicazioni in cui il software viene progettato e creato.
Ambiente di test	Agglomerato di sistemi, dispositivi hardware ed applicazioni in cui il software creato viene testato.
Autenticazione	Processo attraverso il quale un sistema, un utente o un programma tenta di confermare la sua identità ad un altro sistema o applicazione.
Autorizzazione	Processo di definizione dei privilegi, ruoli e permessi di un utente su un sistema o un'applicazione.
Batch Job	Processo di scambio dati o informazioni che intercorre automaticamente, in periodi temporali prestabiliti, tra due sistemi, applicazioni o componenti.
Dati critici	Dati che hanno una rilevanza preponderante per l'immagine e l'operato aziendale (esempio cartellini di traffico telefonico).
Dati giudiziari	I dati giudiziari sono quei dati personali in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti. Inoltre possono essere quei dati personali indicanti la qualità di imputato o di indagato.
Dati personali	Come da Regolamento UE 679/2016: "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".
Dati particolari	Come da Regolamento UE 679/2016: "dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".
Dati sensibili	Vedi definizione di "Dati particolari".
Eccezione	Occorrenza di una circostanza che altera o mira ad alterare il corso previsto o il normale operato di un sistema, di un'applicazione o di una sua componente.
Evento	Situazione riconducibile ad un'attività svolta o ad un'eccezione causata dall'utente, rilevante ai fini della sicurezza del sistema e dell'Information Security.
Identificazione	Meccanismo di convalida preventiva di un'azione.
Information Gathering & Disclosure	Processo relativo alla fuga di dati o informazioni, causato da bug o errori nel software.
Information Security	Insieme di controlli, policy, processi e procedure mirate a garantire la sicurezza delle informazioni in azienda.
Offuscatore	Software che converte il codice sorgente in forma difficilmente interpretabile o non interpretabile del tutto al fine di inibire l'utilizzo di tecniche di reverse engineering.
Organizzazione	Ente locale o centrale della Pubblica Amministrazione
Reverse Engineering	Processo mirato a scoprire i principi tecnologici di un'applicazione attraverso la sua analisi strutturale.



Vocabolo	Descrizione
Token	Valore generato per identificare univocamente una sessione interattiva.

Tabella 2 - Definizioni

3.2 Acronimi

Codice	Titolo
ACLs	Access Control List
AgID	Agenzia per l'Italia Digitale
API	Application Programming Interface
ASLR	Address Space Layout Randomization
ASVS	OWASP Application Security Verification Standard
BSIMM	Building Security in Maturity Model
CIO	Chief information officer
CLASP	Comprehensive and Lightweight Application Security Process
CVSS	Common Vulnerability Scoring System
DFD	Data Flow Diagram
DPA	Data Protection Authority
DPB	Data Protection Board
DPD	Data Protection Directive (95/46/CE)
DPIA	Data Protection Impact Analysis
DPO	Data Protection Officer
DREAD	Damage Potential, Reproducibility, Exploitability, Affected users, Discoverability
DS	Data Store
E	Entity
EDA	Ente di accreditamento
FIPP	Fair Information Practice Principles
FIPPs	Fair Information Practice Principles
FPFSD	framework for Privacy-Friendly System Design
GDPR	General Data Protection Regulation
HAZOP	Hazardous Operations
IOI	Item of Interest
IPSec	IP Security
LINDDUN	Linkability, Identifiability, Non Repudiation, Detectability, Disclosure of information, Content Unawareness e Policy and consent Non-compliance
MIC	Mandatory Integrity Control
MITM	Man In The Midle



Codice	Titolo
MLA	Multilateral Agreement
MPRA	Multilateral Privacy Requirements Analysis
MS –SDL	Microsoft’s Security Development Lifecycle
NIST	National Institute of Standards and Technology
OCSE	Organizzazione per la Cooperazione e lo Sviluppo Economico
OdC	Organismo di certificazione
OWASP	Open Web Application Security Project
OWASP-Proactive	OWASP Proactive Controls
P	Process
P.A.S.T.A	Process for Attack Simulation and Threat Analysis
PAR	Privacy Awareness Requirements
PbD	Privacy by Design
PE	Privacy Engineering
PETs	Privacy-Enhancing Technologies
PI	Personal Informations
PII	Personal Identifiable Information
PRET	Privacy Requirements Elicitation Technique
PriS	Incorporating Privacy Requirements into the System Design Process
ProPAn	Problem-based Privacy Analysis
ROI	Return On Investment
S.B.S.R.S.	Security Bulletin Severity Rating System
SAMM	Software Assurance Maturity Model
SDL	Security Development Lifecycle
SDLC	Software Development Life Cycle
SSDLC	Secure Software Development Life Cycle
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
SW	Software
TCP	Trasmission Control Protocol
UML	Linguaggio di modellazione Unificata
XSS	Cross-site scripting

Tabella 3 - Acronimi