SAPIENZA
UNIVERSITÀ DI ROMA

Sviluppo Sicuro applicativi e servizi

SAPIENZA
UNIVERSITÀ DI ROMA

Sommario

ACRONIMI

Acronimi e definizioni	
ABAC	Attribute Based Access Control - Sistema di controllo accessi basato sugli attributi, l'accesso a una risorsa è determinato dal controllo di diversi attributi, o combinazione di essi, assegnati agli utenti.
BC	Business Continuity - processi e procedure eseguite nell'ambito dell'organizzazione per assicurare l'operatività delle funzioni base durante e a seguito di un incidente e governare i diversi aspetti tecnico/amministrativi.
Dati Personali e particolari	"dati personali" sono definiti come qualsiasi informazione riguardante una persona fisica identificata o identificabile; "dati particolari" dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare 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.
MFA	Multi Factor Authentication -autenticazione a più fattori è quella tecnologia che permette di riconoscere, attraverso più di due metodi di autenticazione, la persona che effettua l'accesso ad un sistema
OWASP	Open Web Application Security Project un progetto open-source che ha l'obiettivo di realizzare linee guida, strumenti e metodologie per lo sviluppo di codice sicuro
PT	Penetration Test – processo operativo eseguito mediante simulazione di attacco per determinare criticità di un sistema.
RBAC	Role Based Access Control - Sistema di controllo accessi basato sui ruoli in cui le entità del sistema che sono identificate e controllate rappresentano posizioni funzionali in una organizzazione o processi.
Sistema	Applicazione/Servizio che deve essere disponibile agli aventi diritto in termini di esercizio e disponibilità dell'informazione.
SSL	Secure Sockets Layer protocollo crittografico delle comunicazioni
TLS	Transport Layer Security protocollo crittografico evoluto
VA	Vulnerability Assessment - processo finalizzato a identificare e classificare i rischi e le vulnerabilità del sistema informatico.

1. Scopo del documento

Il presente documento rappresenta un vademecum di carattere generale per la messa in sicurezza di applicativi e servizi *custom* sviluppati da Sapienza o da fornitori esterni con i quali è stipulato un contratto, a garanzia della protezione dei dati personali fin dalla progettazione e per impostazione predefinita, nel rispetto del GDPR Regolamento (UE) 2016/679 ed in linea con le indicazioni di "secure by design" e "privacy by design".

Il documento riporta in sintesi le regole ed i requisiti contenuti nelle linee guida per la progettazione dei servizi digitali e dei siti della PA, del rispetto ai principi di accessibilità ed usabilità i cui link ai documenti sono riportati in appendice.

In caso di acquisto del servizio di sviluppo è consigliato seguire inoltre le indicazioni contenute nelle linee guida per gli acquisti ICT per le Pubbliche Amministrazioni sintetizzate nel documento "Acquisto Sicuro" reperibile sulla pagina del Centro InfoSapienza nella sezione "sicurezza informatica".

2. Requisiti per lo sviluppo sicuro

La sicurezza delle applicazioni è funzionale alla protezione delle informazioni che esse trattano ed alla continuità dei servizi erogati. I dati devono essere accessibili solo agli utenti autorizzati nel rispetto dei ruoli prefissati e del principio di riservatezza. Devono essere messe in atto misure tecniche ed organizzative adeguate per proteggere i dati da accesso, uso, modifica, divulgazione, perdita, distruzione o danno accidentali, non autorizzati o illegali (GDPR Regolamento (UE) 2016/679- Considerando 39, 75, 77, 78, 79, 83, 87; Art. 5, 9, 32).
Nello sviluppo di un applicativo è fondamentale fare affidamento ed essere aderente ai contenuti delle **linee guida emanate da AGID per lo sviluppo del software sicuro nella pubblica amministrazione** i cui riferimenti, tra gli altri, sono reperibili nell'Appendice A.
La sicurezza insiste sulle diverse aree, infrastruttura e applicativa, trattate nello specifico nelle linee guida sopra richiamate e qui schematizzate nei punti fondamentali:

2.1. Infrastruttura, protezione server database e server backend

2.1.1. Isolamento dei servizi

Il server di database ed il server con la logica di backend, siano essi *on-premises*, nel cloud o in ambiente *containerizzato*, secondo le scelte progettuali applicative, è opportuno che siano situati in ambiente sicuro ed isolato, non raggiungibili da sistemi esterni all'architettura del servizio. I server su cui risiedono la logica di backend ed il server di database è opportuno che siano separati.
L'accesso ai dati contenuti nel server di database deve essere possibile dal solo server di backend, il server di database non deve essere consultabile in forma diretta ed esposto.

Per segmentare la rete si può far uso di: Private VLAN isolated; Suddivisione fisica della rete con la creazione di sottoreti fisiche separate utilizzando apparati di rete fisici; opportuna configurazione delle regole del Firewall su macchina locale e/o centralizzata.
In presenza di applicativi che non gestiscono categorie di dati personali o particolari è consentito fare uso di architetture iperconvergenti (logica di backend, front-end e database che risiedono sullo stesso nodo).

2.1.2. Ridondanza

Se il servizio richiede una disponibilità continuativa dell'accesso alle informazioni, per ridurre il rischio di interruzioni del servizio o di perdita di dati è opportuno ricorrere alla ridondanza dei server.
La ridondanza può essere attiva o passiva, secondo le scelte progettuali.
La ridondanza attiva implica l'utilizzo di due o più server che lavorano in modo coordinato consentendo di gestire le richieste bilanciandole tra i server ed in caso di guasto il server funzionante si assume l'intero carico. La ridondanza passiva implica l'utilizzo di un server di riserva che è pronto a entrare in funzione in caso di guasto o interruzione del servizio sul server principale.

2.1.3. Backup

Le attività di backup, delle macchine e dei dati, sono necessarie a garantire la protezione dei sistemi e delle informazioni ed il loro recupero in caso di indisponibilità o perdita. È opportuno provvedere al backup delle macchine server e delle informazioni secondo metodologie di backup full ed incrementali dei dati. La programmazione dell'attività di backup deve essere giornaliera. Deve essere prevista un'area di archiviazione dei backup protetta e non modificabile, con una copia off-line, ed un periodo di inalterabilità medio/lungo. E' indicato eseguire attività di verifica periodica sull'integrità delle copie di backup.

2.1.4. Controllo degli accessi amministrativi ai sistemi server

L'accesso per scopi amministrativi, e di gestione, alle macchine server su cui sono ospitate le logiche di backend, i front-end ed i database è opportuno che sia riservato alle sole utenze gestionali, preventivamente profilate. L'accesso ai sistemi deve essere permesso solo previa autenticazione e autorizzazione in base ai ruoli strettamente assegnati.
La gestione amministrativa del server di Database deve essere riservata al ruolo di DBA e non legata al livello applicativo.
Gli accessi da remoto devono essere garantiti attraverso protezione del canale di comunicazione ed autenticazione forte dell'utenza attraverso connessioni in VPN.

2.1.5. Sistema Operativo - versione stabile e aggiornamenti di sicurezza

Utilizzare una versione stabile del sistema operativo che sia supportata dal produttore/comunità e considerata affidabile per un utilizzo quotidiano.
Installare gli aggiornamenti di sicurezza rilasciati regolarmente per correggere le vulnerabilità del sistema operativo e prevenire gli attacchi informatici. È importante installare questi aggiornamenti il prima possibile per mantenere il sistema sicuro.
Monitorare le notifiche di sicurezza, il produttore del sistema operativo può inviare notifiche di sicurezza per avvisare gli utenti di eventuali problemi di sicurezza.

2.1.6. Monitoraggio, Detection e Remediation

È opportuno eseguire operazioni di monitoraggio, detection e remediation sui sistemi server di backend, frontend e di database, l'insieme di queste attività garantiscono la sicurezza dei sistemi. Il monitoraggio consiste nel controllare continuamente i sistemi ed il traffico di rete per identificare eventuali attività anomale o comportamenti potenzialmente dannosi. Questo può essere fatto attraverso tecnologie come sistemi di analisi dei log, IDS, SIEM, sonde su rete, agent installati sui server. La *detection* si verifica quando viene identificato un comportamento anomalo o una minaccia. Questo può essere fatto manualmente da un analista di sicurezza, eventuale supporto SOC, automaticamente da sistema EDR, AI, correlazione dei dati delle diverse fonti. La *remediation* consiste nel prendere le misure appropriate per contenere immediatamente la minaccia, eventuale supporto SOC di 2° livello, risolvere il problema identificato.

2.1.7. Analisi Vulnerabilità

L'utilizzo di tool, o supporto esterno per verifiche eseguite ad intervalli prestabiliti, è raccomandato per prevenire eventuali minacce attraverso l'analisi dei sistemi per ricercare eventuali vulnerabilità. Le potenziali vulnerabilità scoperte devono essere risolte con le opportune applicazioni di *patching* o attività sistemistiche evolutive.

2.1.8. Implementazione e conservazione dei log di sistema

È necessario effettuare la registrazione degli accessi e dei syslog dei sistemi server anche per identificare e risolvere eventuali problemi di sicurezza. Le sorgenti dei log possono essere i sistemi di protezione perimetrali, come i firewall, per la raccolta delle informazioni di traffico, i log di sistema dei server coinvolti nell'erogazione del servizio. Il periodo di conservazione deve essere corrispondente alle normative vigenti ed ai regolamenti di Sapienza che prevedono un periodo di 6 mesi per i log di amministratore di sistema.

2.2. Sviluppo applicativo

2.2.1. Ambienti separati per sviluppo, test e produzione

È necessario separare gli ambienti per lo sviluppo, test e produzione allo scopo di permettere di progettare ed implementare efficacemente le funzioni dell'applicativo, identificare e correggere le criticità prima che l'applicativo venga rilasciato in ambiente di produzione.
La separazione, inoltre, consente di mantenere la stabilità dell'ambiente di produzione, poiché eventuali le modifiche evolutive possono essere testate prima di essere rilasciate in produzione.

2.2.2. Accesso allo schema database

Le utenze applicative devono consentire l'accesso al solo schema del database per permettere le operazioni di DDL (Data Definition Language) per la creazione/modifica/inserimento degli oggetti del database dell'applicativo ed il controllo della sua struttura. L'utenza di DBA non deve essere disponibile all'area di sviluppo applicativo ed utilizzato per gli scopi funzionali dell'applicativo.

2.2.3. Utilizzo dei dati in fase di sviluppo, test e collaudo

In fase di sviluppo i dati utilizzati dovrebbero essere solo dati di esempio che non rappresentano i dati reali utilizzati dall'applicativo. Questo consente di garantire che i dati non vengano esposti ad accessi non autorizzati o utilizzati in modo improprio durante lo sviluppo.
Le fasi di test e collaudo applicativo, in caso siano disponibili dati preesistenti, è opportuno che vengano effettuate utilizzando una copia dei dati anonimizzati per la sicurezza delle informazioni e il rispetto della normativa della privacy. L'uso dei dati anonimizzati, consente agli sviluppatori di verificare il corretto funzionamento dell'applicativo utilizzando lo stesso schema di database e il set di dati rappresentativo senza compromettere la sicurezza dei dati reali.

2.2.4. Conformità ai parametri OWASP

È opportuno eseguire nello sviluppo dell'applicativo WEB le linee guida e le buone pratiche raccomandate dal progetto OWASP.
La conformità ai parametri OWASP e l'applicazione sistematica di queste procedure riduce considerevolmente il rischio di data breach causati da vulnerabilità dovute alla non alta qualità del codice mantenendo un elevato controllo della sicurezza. Alcune delle misure di sicurezza raccomandate da OWASP includono ad esempio: autenticazione sicura, autorizzazione limitate alle funzioni e dati nel rispetto dei ruoli

attribuiti, input validation, protezione dei dati particolari, aggiornamento continuo delle componenti, monitoraggio e registrazione degli eventi applicativi.

2.2.5. Implementazione e conservazione log applicativi

Configurare l'applicazione per la registrazione dei log; i log applicativi registrano le attività che avvengono all'interno dell'applicazione, come le richieste del client, le risposte del server, le eccezioni e gli errori. È necessario decidere quali informazioni registrare, selezionare le informazioni più rilevanti come ad esempio l'indirizzo IP del client, la data e l'ora della richiesta, le informazioni sulle transazioni e gli errori.

2.2.6. Utilizzo di componenti e librerie non deprecate

Verificare regolarmente la sicurezza delle componenti e delle librerie utilizzate, gli eventuali aggiornamenti di sicurezza e patch, attenzionare le segnalazioni relative a nuove vulnerabilità zero-day sulle componenti o le librerie utilizzate, utilizzare componenti e librerie che sono supportati attivamente dai loro sviluppatori e che hanno una comunità attiva e affidabile, evitare di utilizzare componenti e librerie che non sono supportati o che non sono più mantenuti.

2.3. Protezione dati e rispetto privacy

2.3.1. Accesso ai dati secondo modello RBAC o ABAC.

L’accesso alle informazioni è opportuno che sia garantito agli utenti secondo le autorizzazioni loro concesse ed esclusivamente per la visibilità ai dati permessi dai ruoli o attributi assegnati. I modelli adottabili per assegnare le autorizzazioni possono essere RBAC o ABAC.

2.3.2. Crittografia della base dati

I dati presenti all’interno dei server di database è opportuno che siano crittografati per prevenire l’accesso alle informazioni in caso di sottrazione della base dati stessa. La crittografia può essere realizzata attraverso le funzioni native dei sistemi di archiviazione o per mezzo di crittografia del dato realizzata dallo strato applicativo. La chiave di decriptazione deve essere esterna allo strato applicativo è conservata su aree del sistema accessibili solo ad utenze con elevati privilegi.

2.3.3. Pseudonomizzazione delle informazioni

In presenza di dati particolari, è opportuno adottare la pseudonomizzazione dei dati, questo processo mira a rendere anonimi i dati particolari, ma conservare comunque le informazioni necessarie per l'elaborazione. La separazione del dato particolare

dall'informazione dell'interessato è attuata dallo strato applicativo a livello di progettazione dello schema della base dati. L'associazione dell'identità dell'interessato al dato particolare è realizzabile tramite i valori archiviati in un database separato, o singola tabella separata che è accessibile esclusivamente ad utenti con elevati privilegi autorizzativi (GDPR Regolamento (UE) 2016/679- Considerando 26, 28, 29; Art. 32).

2.3.4. Anonimizzazione dei dati per scopi di test e collaudo

Per le attività di test e collaudo applicativo sulla base dati è opportuno effettuare copie dei dati su server di database separati da quelli in produzione rispettandone gli schemi. Le informazioni contenute all'interno delle copie devono essere preventivamente anonimizzate per consentire le operazioni di test eseguite anche da utenti non autorizzati al trattamento delle informazioni presenti. (GDPR Regolamento (UE) 2016/679- Art. 32 riservatezza)

2.3.5. Limitazione delle funzioni all'accesso ai dati.

Per il rispetto della privacy è opportuno programmare funzioni dell'applicativo che eseguano accesso alle informazioni per i dati strettamente necessari allo svolgimento delle attività previste dalla funzione stessa. L'accesso alle informazioni non necessarie e non correlate all'espletamento della specifica funzione espone l'applicativo a possibili violazioni della privacy.

2.3.6. Pubblicazione informative privacy e conservazione consenso

Prevedere l'esposizione e la conservazione delle informative sulla privacy, o l'indicazione esplicita del consenso espresso, per la raccolta e gestione dei dati, personali e particolari, degli interessati e le indicazioni sul trattamento dei dati effettuato dall'applicativo.
Il modello dell'informativa sulla privacy può essere reperito nel sito del Settore Privacy nella sezione "Informative".

2.4. Regole per lo sviluppo di siti internet e servizi digitali erogati da PA, Accessibilità degli strumenti informatici, Usabilità del servizio digitale

Le presenti indicazioni hanno lo scopo di definire e orientare la progettazione e la realizzazione dei siti internet e dei servizi digitali erogati dalle Pubbliche Amministrazioni, secondo quanto definito all'articolo 53 del CAD e le linee guida emanate da AGID.

2.4.1. Protezione del canale di comunicazione

Al fine di garantire autenticazione, integrità dei dati e confidenzialità tra le componenti del servizio le comunicazioni devono avvenire utilizzando il protocollo di comunicazione HTTPS (HTTP over TLS).
Il Transport Layer Security (TLS) è un protocollo che permette di stabilire un canale con le proprietà di integrità e riservatezza in senso crittografico tra un client e un server.

2.4.2. Accessibilità

Rendere accessibili a tutti gli utenti il contenuto, la struttura e il comportamento degli strumenti informatici, secondo i requisiti di legge come indicato nelle linee guida riportate nell'appendice A.

2.4.3. Affidabilità, trasparenza e sicurezza

Progettare e sviluppare servizi digitali che garantiscano la trasparenza delle informazioni e la sicurezza, nel rispetto della normativa EU e nazionale in materia di protezione dei dati personali.

2.4.4. Semplicità di consultazione ed esperienza d'uso

Progettare, realizzare e mantenere siti internet e servizi digitali utili e facili da usare, secondo una metodologia di progettazione centrata sull'utente

2.4.5. Monitoraggio dei servizi

Analizzare e migliorare l'esperienza d'uso dei siti/servizi digitali mediante la rilevazione qualitativa e quantitativa dei dati di fruizione

2.4.6. Interfaccia utente

Mettere a disposizione interfacce utenti semplici da utilizzare

2.4.7. Integrazione delle piattaforme abilitanti

Prevedere un'esperienza d'uso comune alle diverse procedure on line, si deve garantire l'accesso ai servizi digitali della PA con i sistemi di autenticazione previsti dal CAD (Spid, CIE, CNS).

2.5. Standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici

Mantenere l'aderenza alle linee guida per la sicurezza dell'interoperabilità tramite API (Application Programming Interface) dei sistemi informatici nello sviluppo di servizi digitali che richiedano transazioni digitali realizzate tra e verso le pubbliche amministrazioni.

Le Linee Guida contribuiscono alla definizione del modello di interoperabilità delle Pubbliche Amministrazioni (ModI).

2.6. Rilascio in produzione - Penetration Test (PT) e Vulnerability Assessment (VA) dell'applicativo prima del rilascio

In presenza di dati particolari gestiti dall'applicativo è opportuno attivare i processi di VA e PT per garantire che l'applicativo sia compliance ai criteri di sicurezza minimi prima del suo rilascio in produzione e non sia esposto ad eventuali vulnerabilità note. *Penetration Test* consiste nell'esecuzione di una simulazione di attacco all'applicativo per identificare eventuali punti deboli nell'applicativo e valutare la sua capacità di resistere a un attacco reale. *Vulnerability Assessment* consiste nell'analisi automatica del codice e dell'architettura dell'applicativo per identificare eventuali vulnerabilità di sicurezza e consentire la risoluzione di tali criticità.

2.7. Modalità di gestione e manutenzione

2.7.1. Ciclo di vita del software secondo il modello CI/CD

Il modello CI/CD è un processo di sviluppo software che prevede una continua integrazione e distribuzione del codice. È opportuno adottare e seguire le diverse fasi del modello: Sviluppo, i membri del team di sviluppo scrivono codice e lo inviano al repository di versione; Integrazione: il codice viene integrato nel repository principale e verificato automaticamente utilizzando un sistema test che consenta di effettuare test unitari, integrazione e test di accettazione; Deployment: se tutti i test sono superati, il codice viene distribuito in un ambiente di produzione; Monitoraggio: il codice in produzione viene monitorato per identificare eventuali problemi. Il modello CI/CD accelera il processo di sviluppo del software, garantendo la qualità del codice e la rapidità del deployment.

2.7.2. Accesso sicuro da remoto ai sistemi per attività amministrative e di gestione

Per garantire un accesso sicuro da remoto alle attività amministrative e di gestione è necessario utilizzare connessioni protette attraverso l'uso di VPN (Virtual Private Network), con accesso protetto da credenziali degli utenti profilati, è raccomandata

l'autenticazione a due fattori (2FA). L'accesso sicuro da remoto ai sistemi è un aspetto critico per la protezione dei dati e delle risorse applicative.

2.7.3. Aggiornamento di sicurezza periodici in produzione

L'aggiornamento periodico di moduli e librerie, dell'applicativo in produzione, dovrebbe essere programmato e automatizzato per garantire che sia eseguito in modo regolare e senza interruzioni.
E' importante verificare che gli aggiornamenti non interferiscano con il funzionamento dell'applicativo e che siano adeguatamente testati prima di essere installati in produzione al fine di evitare eventuali interruzioni del servizio legate a questi.

Appendice A – Documentazione di riferimento

Si raccomanda, a tutti coloro che sviluppano codice per la PA, di seguire le raccomandazioni:

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 - GDPR
  - https://www.garanteprivacy.it/regolamentoue

- Modello Informativa Privacy
  - https://www.uniroma1.it/it/pagina/settore-privacy

- "Le linee guida per lo sviluppo del software sicuro nella pubblica amministrazione".
  - https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro
    - Allegato 1- Linee Guida per l'adozione di un ciclo di sviluppo di software sicuro
    - Allegato 2 - Linee Guida per lo sviluppo sicuro di codice
    - Allegato 3 - Linee Guida per la configurazione per adeguare la sicurezza del software di base
    - Allegato 4 - Linee Guida per la modellazione delle minacce e individuazione delle azioni di mitigazione conformi ai principi del Secure/Privacy by Design

- "Misure minime di sicurezza ICT per le pubbliche amministrazioni".
  - https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

- "Le linee Guida sull'Accessibilità degli strumenti informatici"
  - https://www.agid.gov.it/it/design-servizi/accessibilita

- "Linee guida di design per i siti internet e i servizi digitali della PA"
  - https://www.agid.gov.it/it/design-servizi/linee-guida-design-servizi-digitali-pa

- Usabilità
  - https://www.agid.gov.it/it/design-servizi/usabilita

- Linee Guida Tecnologie e standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici
  - https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_tecnologie_e_standard_sicurezza_interoperabilit_api_sistemi_informatici.pdf

- CAD – Codice dell'Amministrazione Digitale
  - https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82

Appendice B – CheckList

Requisito	Dati Personali	Dati Particolari
2.1.1. Isolamento dei servizi	raccomandato	necessario
2.1.2. Ridondanza	necessario	necessario
2.1.3. Backup	necessario	necessario
2.1.4. Controllo degli accessi amministrativi ai sistemi server	necessario	necessario
2.1.5. Sistema Operativo - versione stabile e aggiornamenti di sicurezza	necessario	necessario
2.1.6. Monitoraggio, Detection e Remediation	necessario	necessario
2.1.7. Analisi Vulnerabilità	raccomandato	necessario
2.1.8. Implementazione e conservazione dei log di sistema	necessario	necessario
2.2.1. Ambienti separati per sviluppo, test e produzione	necessario	necessario
2.2.2. Accesso allo schema database	necessario	necessario
2.2.3. Utilizzo dei dati in fase di sviluppo, test e collaudo	raccomandato	necessario
2.2.4. Conformità ai parametri OWASP	raccomandato	necessario
2.2.5. Implementazione e conservazione log applicativi	necessario	necessario
2.2.6. Utilizzo di componenti e librerie non deprecate	necessario	necessario
2.3.1. Accesso ai dati secondo modello RBAC o ABAC	necessario	necessario
2.3.2. Crittografia della base dati	raccomandato	necessario
2.3.3. Pseudonomizzazione delle informazioni	raccomandato	necessario
2.3.4. Anonimizzazione dei dati per scopi di test e collaudo	raccomandato	necessario
2.3.5. Limitazione delle funzioni all'accesso ai dati.	necessario	necessario
2.3.6. Pubblicazione informative privacy e conservazione consenso	raccomandato	necessario
2.4.1. Protezione del canale di comunicazione	necessario	necessario
2.4.2. Accessibilità	necessario	necessario
2.4.3. Affidabilità, trasparenza e sicurezza	necessario	necessario
2.4.4. Semplicità di consultazione ed esperienza d'uso	necessario	necessario
2.4.5. Monitoraggio dei servizi	raccomandato	necessario
2.4.6. Interfaccia utente	necessario	necessario
2.4.7. Integrazione delle piattaforme abilitanti	necessario	necessario
2.5. Standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici	necessario	necessario

2.6 Rilascio in produzione - Penetration Test e Vulnerability Assessment dell'applicativo prima del rilascio	raccomandato	necessario
2.7.1. Ciclo di vita del software secondo il modello CI/CD	raccomandato	necessario
2.7.2. Accesso sicuro da remoto ai sistemi per attività amministrative e di gestione	necessario	necessario
2.7.3. Aggiornamento di sicurezza periodici in produzione	necessario	necessario