Linee Guida per le attività tecniche di progettazione, sviluppo, installazione, distribuzione e manutenzione di servizi informatici

Sommario

1. Introduzione

Il presente documento ha lo scopo di raccogliere un insieme di suggerimenti, raccomandazioni e prescrizioni da osservare nell'intero ciclo di vita dei servizi e delle forniture relativi al software, durante le fasi di progettazione, sviluppo, installazione, distribuzione e manutenzione.

Questo documento è vincolante laddove ricorrono i termini DEVE / DEVONO / DOVRÀ / DOVRANNO, o le proposizioni soggettive introdotte da È NECESSARIO (CHE).

Opzionali sono, invece, le indicazioni precedute da È CONSIGLIABILE, È PREFERIBILE, PREFERIBILMENTE, che possono essere oggetto di attribuzione di uno specifico punteggio in sede di gara.

Le linee guida sono suddivise per macro-argomento.

2. Progettazione

2.1. Definizione delle modalità di interazione del fornitore con l'ente

La presente sezione si riferisce ai fornitori che operano per l'ente al fine di erogare:

- software il cui codice sorgente è proprietà dell'ente committente;
- servizi informatici commissionati dall'ente, anche in corso di esecuzione di un contratto;
- servizi informatici sui quali l'ente si appoggia per erogare servizi digitali agli utenti.

Quando l'attività prevede la realizzazione o la modifica di codice sorgente, allora È NECESSARIO CHE:

- Il codice sorgente abbia il repository Git ospitato all'interno del sistema Gitlab dell'ente
- Siano attivate VPN nominali a scadenza predefinita, che consentano le attività richieste (la VPN è associata ad una persona fisica e ha una scadenza prefissata coerente con le attività pianificate)
- Sul sistema Gitlab vengano attivati gli accessi nominali tramite i quali è consentito al fornitore operare sul progetto specifico.

Le modalità di svolgimento delle attività tecniche richieste devono rispettare il seguente flusso:

Numero	Titolo	Descrizione	In carico a
0	Definizione piano di test	Fornitore e committente definiscono il piano di test, in base a caratteristiche, moduli e componenti interessati dal rilascio	Fornitore/ Committente
1	Rilascio in Git	Il Fornitore esegue il rilascio del codice prodotto sul repository Git e contestualmente avverte il committente mediante notifica mail. La mail DEVE allegare la dettagliata documentazione richiesta al par. 3.1. del presente documento.	Fornitore
2	Valutazione preliminare	Se i test svolti dal fornitore, o la relativa descrizione, vengono ritenuti insufficienti o poco significativi, si transisce immediatamente allo stato "Attività fallita".	Committente

3	Deploy (Test)	Il Fornitore esegue la distribuzione di una versione specifica su ambiente di Test. Contestualmente avverte il committente mediante notifica mail.	Fornitore
4	Test Funzionali	Il Committente esegue le verifiche funzionali di quanto presente su ambiente di Test e informa il Fornitore dell'esito dei test mediante notifica mail.	Committente
5	Deploy (Prod.)	Il Fornitore esegue la distribuzione di una versione specifica su ambiente di Produzione. Contestualmente avverte il committente mediante notifica mail.	Fornitore
6	Completata	Il Committente controlla che quanto presente su ambiente di Produzione sia coerente con la distribuzione richiesta e informa il Fornitore dell'esito della verifica mediante notifica mail.	Committente
7	Attività fallita	Nel caso di esito negativo dell'attività precedente, è necessario attivare le azioni e le misure necessarie per correggere l'anomalia e permettere di risolvere il problema. Il Fornitore invia una mail al Committente relativa alle misure e azioni da attuare.	Fornitore/ Committente

2.2. Riuso del codice sorgente

Deve essere chiarito in fase di progettazione se il codice sorgente da realizzare sarà oggetto di pubblicazione e possibile riuso.

In generale, è buona norma realizzare il codice sorgente in modo che esso sia riusabile *by default*, ma se già in fase di progettazione è stato definito che sarà messo a "riuso", tanto più saranno rafforzate le misure necessarie a rendere il codice sorgente "riusabile".

A tal proposito È NECESSARIO:

- soddisfare le linee guida di Agid, in materia di "acquisizione e riuso di software per le pubbliche amministrazioni" (https://www.agid.gov.it/it/design-servizi/riuso-open-source/linee-guida-acquisizione-riuso-software-pa);
- assicurare che eventuali variabili di ambiente, username, password, stringhe di collegamento a database, ed ogni altro eventuale dato sensibile non sia incluso nei file pubblici del codice sorgente;
- assicurare che il codice sorgente sia corredato della documentazione tecnica necessaria per poterne comprendere l'utilizzo e le peculiarità, effettuarne l'installazione e la configurazione, poterne effettuare diagnosi relative a malfunzionamenti;
- soddisfare i criteri di sicurezza nello sviluppo del codice sorgente, come indicato nella sezione 3.2 Sicurezza del Codice Sorgente.

Nel contesto dell'ente, si definisce che comunque i progetti sono salvati sul repository interno del Comune di Firenze.

Nel caso che si abiliti il riuso, è attivo un repository pubblico che contiene i progetti, (si veda come riferimento la pagina Github del Comune di Firenze https://github.com/ComuneFI) dove tenere aggiornato il codice sorgente mediante meccanismi di *mirroring* (si veda la documentazione di Gitlab relativa al Mirroring, https://docs.gitlab.com/ee/user/project/repository/mirror/).

Per l'accesso in modifica al repository pubblico è necessario ottenere i privilegi su un utente personale.

2.3. Architettura del prodotto

La seguente sezione si applica nel caso di attività tecnica volta alla realizzazione di una soluzione software.

La progettazione dell'architettura della soluzione software deve tenere in considerazione, oltre agli aspetti indicati nelle altre sezioni di questo documento, anche la possibilità di mettere a riuso e a disposizione dell'ente i componenti realizzati.

Per questo motivo la progettazione dell'architettura deve prevedere, ove possibile, una separazione fra lo strato applicativo e lo strato di accesso ai dati.

In particolare, devono essere riutilizzate le API già realizzate e disponibili sui cataloghi dell'ente (WSO2) e nazionali (PDND); nel caso si sviluppino nuove API, esse DEVONO essere pubblicate e documentate sul catalogo dell'ente.

Lo strato applicativo crea, aggiorna e legge le informazioni disponibili tramite accesso alle API e dovrà evitare ogni accesso diretto ai database se non motivato da vincoli stringenti.

Per l'utilizzo, la realizzazione e la pubblicazione di API si prendano come riferimento le Linee Guida di Interoperabilità del Comune di Firenze, allegate al presente documento.

Le indicazioni precedenti sono da ritenersi valide anche nel caso di deploy su infrastruttura CST (Centro Servizi Territoriali), gestito da Silfi s.p.A., nel seguito indicata con il suo marchio Firenze Smart. In questo secondo caso sono da considerare anche le linee guida di Firenze Smart per il deploy su infrastruttura CST, reperibili al seguente indirizzo: http://www.lineacomune.it/requisiti-dispiegamento-servizi-cst

2.4. Metodi di condivisione della documentazione

Per quanto riguarda la condivisione di documentazione, sia tra solo personale interno che con personale esterno, il fornitore DEVE catalogare i documenti secondo quattro diverse **categorie**:

- Documentazione progettuale
- Documentazione tecnica
- Manualistica
- Documenti interni

Si identificano inoltre alcuni **processi** che È NECESSARIO coprire per poter gestire correttamente la documentazione:

- Condivisione snella e dinamica della documentazione durante la fase di esecuzione del progetto;
- Registrazione della documentazione finale di progetto o relativa al raggiungimento di milestone intermedie per fini di archiviazione e aderenza alle norme di documentazione ISO;

- Archivio delle procedure tecniche di routine, utili per ritrovare soluzioni già applicate o per analisi interna.

Si evidenziano infine alcuni **punti di attenzione** che DEVONO essere tenuti in considerazione:

- Permettere la rapida ricerca di documentazione ed evitare la dispersione di documentazione all'interno di mail;
- Uniformare le modalità di condivisione dei documenti;
- Non creare vincoli di "lock-in" su piattaforme specifiche.

A fronte della catalogazione dei documenti, dell'analisi dei processi e dei punti di attenzione, si conclude di utilizzare PREFERIBILMENTE i seguenti strumenti per soddisfare le esigenze sopra indicate:

Processo	**Strumento**
Condivisione nella fase di esecuzione del progetto	Microsoft Sharepoint
Registrazione della documentazione di milestone e/o finale	Cartelle condivise dell'ente aderenti alla normativa ISO
Archivio procedure tecniche	WikiMedia

2.5. Integrazione con servizi SIT

Quando viene progettato un nuovo servizio/applicativo è raccomandato, nel caso siano utilizzate informazioni georeferenziate, individuare se è necessaria l'interazione con i servizi del SIT. Nel caso in cui esista questa possibilità, cioè se i dati trattati dall'applicativo hanno una valenza di tipo geografico, chi sviluppa deve confrontarsi con la P.O. Risorse Dati, Open Data, SIT per individuare la strategia di integrazione migliore.

A disposizione di chi sviluppa ci sono due strumenti principali che sono:

a. Geoserver che è un sistema che consente la condivisione dei dati spaziali in diversi formati sia raster che alfanumerici.
b. Geoflorentia che è un'interfaccia Web GIS che consente di fare ricerche e selezioni geografiche sul territorio di Firenze.

I documenti descrittivi dei due sistemi sono allegati al presente. In base alle esigenze applicative si potrà scegliere tra le due soluzioni. Con Geoserver è possibile accedere a dati geografici attraverso i formati:

- WMS, che consente di avere immagini raster nei formati AtomPub, GIF, GeoRSS, GeoTiff, GeoTiff 8-bits, JPEG, JPEG-PNG, KML (compressed), KML (network link), KML (plain), OpenLayers, OpenLayers 2, OpenLayers 3, PDF, PNG, PNG 8 bit, SVG, Tiff, Tiff-8bits, UTF-Grid.
- WFS, che consente di avere dati alfanumerici nei formati CSV, GML 2, GML 3.1, GML 3.2, GeoJSON, KML, Shapefile.

I servizi di cui sopra vengono esposti in modo diverso in base alla propria tipologia. I dati in formato raster vengono esposti all'esterno tramite il software GEOWEBCACHE che consente il caching dei servizi di mappa. All'interno è previsto l'utilizzo della cache integrata dentro Geoserver. Il software Geofence è deputato all'implementazione delle policy di accesso ai dati sia in intranet che in internet. I formati alfanumerici vengono preferibilmente esposti attraverso l'API manager di WSO2 preferendo il formato GeoJSON.

Visto che le banche dati sono in continua evoluzione per avere un elenco completo dei dataset disponibili rivolgersi alla P.O. Risorse Dati, Open Data, SIT per avere l'elenco aggiornato.

Con Geoflorentia è possibile, attraverso una chiamata http, ricevere risultati interrogando le banche dati del SIT. Attraverso l'interfaccia messa a disposizione dall'applicativo è possibile effettuare interrogazioni su cartografia secondo le entità geometriche di base (punto, linea, polilinea), il sistema restituisce una risposta http che sarà elaborata dall'applicativo chiamante.

Una volta ottenute, attraverso uno dei sistemi proposti, le informazioni geografiche, l'applicativo può integrare le informazioni nelle banche dati del SIT nelle modalità che verranno stabilite caso per caso.

2.6. Gestione dei dati su file system e policy di retention

Viste le finalità delle presenti linee guida, in questo contesto si farà riferimento ai log cosiddetti *applicativi*, ovverosia quelli prodotti da un applicativo durante il suo funzionamento per tracciare le operazioni eseguite, di tipo automatico, oppure generate da una qualsiasi interazione, sia essa di tipo uomo-macchina che machine-to-machine (ad es. Applicativi che richiamano API).

Con l'entrata in vigore del GDPR, infatti, i log file si sganciano dalle esigenze di controllo dell'operato degli amministratori di sistema, acquisendo secondo il principio di *accountability* (letteralmente "principio di responsabilizzazione") più ampia portata nell'ottica di protezione dei dati personali. Si pone, infatti, in capo al titolare del trattamento l'onere di provare la conformità della propria struttura organizzativa e procedurale alla normativa in ambito *privacy*.

Pertanto, il fornitore DOVRÀ rendere disponibili i log applicativi al sistema di *log management* utilizzato dall'ente, una volta individuato, capace di tracciare, conservare e analizzare le informazioni riguardanti le operazioni compiute sui sistemi e che impattano direttamente sui dati personali. A questo proposito, si riporta che è attualmente in fase di valutazione l'integrazione dei sistemi di logging con uno stack ELK (Elastic-Logstash-Kibana) che faciliti la gestione e l'interrogazione di questa base dati così eterogenea e variegata.

Secondo quanto stabilito dall'Autorità Garante per la Protezione dei dati personali i log file devono rispondere alle seguenti caratteristiche:

- completezza;
- inalterabilità;
- verificabilità.

Ciò premesso, è evidente come i log file rappresentino uno strumento fondamentale al fine di garantire la sicurezza dell'infrastruttura informatica e la lecita gestione dei dati personali, in quanto capace di "fotografare" le operazioni compiute sui sistemi informatici e quindi sui dati personali.

Pertanto, una corretta organizzazione e gestione è fondamentale per il perseguimento dei fini suddetti.

Partendo dalla struttura delle singole righe dei file di log, si riporta di seguito un set minimo di informazioni che il fornitore DEVE riportare:

- IP chiamante
- Userid
- Data
- Operazione/funzionalità richiamata
- Esito operazione
- Identificativo unico (per esempio il session ID)
- …

È CONSIGLIABILE la suddivisione per categorie:

- Info
- Debug
- Error

È CONSIGLIABILE la rotazione e successiva storicizzazione con base temporale da definire in sede di commessa, valutata sulla base delle effettive necessità.

La nomenclatura da rispettare per ogni file di log DEVE permettere una rapida e corretta individuazione di quanto ricercato; pertanto, sarà rispettato il pattern:
YYYY-MM-DD-log-<nome-applicativo>-<[se pertinente:]modulo-applicativo><tipologia-log>

I file di log seguiranno a tutti gli effetti le regole applicate ai documenti informatici, pertanto DEVE essere prevista la suddivisione in “live documents” da mantenere sui sistemi e “cold documents”

Ciò vale soprattutto nei casi in cui debbano essere soddisfatte le regole di conservazione secondo norma vigente. Per quanto concerne i periodi dell’eventuale conservazione, a parte quelli dettati da normativa, verrà effettuata una valutazione in sede di definizione progettuale, ovverosia in fase di elaborazione del Piano di Progetto Definitivo.

I log derivanti da sistemi e sensori seguiranno, per quanto possibile e compatibilmente con le possibilità tecniche degli stessi, le stesse regole stabilite nel presente documento.

L’accesso ai log avverrà sempre ed esclusivamente in modalità di lettura, con opportuna configurazione delle utenze, per evitare eventuali alterazioni e/o manomissioni, pena la decadenza dell’effetto probatorio.

2.7. Modalità di integrazione con Single Sign-On (SSO)

Il Comune di Firenze utilizza un Active Directory centralizzato per autenticare gli utenti aziendali e abilitarli all’utilizzo della postazione locale. Si è pertanto pensato di utilizzare lo stesso meccanismo anche per gli applicativi web, centralizzando in tal modo l’identità dell’utente. Il fornitore DEVE attenersi alle seguenti indicazioni.

Il meccanismo di autenticazione centralizzato si avvale di un url di autenticazione, denominato “login-url”, settato in modo da poter essere interrogato dall'applicativo chiamante. L’operazione di controllo dell’avvenuta autenticazione può avvenire in 2 modalità:

1. Modalità http semplice (CGI)
2. Modalità web service (SOAP)

Nel caso che l'applicativo abbia necessità di gestire documenti presenti nel sistema di gestione documentale dell'ente (Alfresco) è possibile chiamare un servizio di SSO per richiedere l'autenticazione al documentale. Anche in questo caso sono previste 2 modalità di servizio:

1. Modalità http semplice (CGI)
2. Modalità web service (SOAP)

Per consentire il logout dell'utente bisognerà richiamare un'altra url.

Per tutti i dettagli implementativi si rimanda alla documentazione completa presente in \\condivisioni\CONDIVISE\SISTEMI_Informativi\PROGETTI\SSO\MTO PSQ 8.5-4 Specifiche integrazione SSO.pdf

2.8. Modalità di integrazione con Servizi di Autenticazione Firenze Smart

Gli eventuali servizi di autenticazione SPID, CIE e CNS da attivare sul servizio software oggetto delle attività tecniche devono avvalersi dei servizi forniti da Firenze Smart.

Per usufruire dei servizi di autenticazione SPID, CIE e CNS, forniti da Firenze Smart, è necessario seguire le specifiche fornite sulla pagina http://www.lineacomune.it/requisiti-dispiegamento-servizi-cst nella sezione "Integrazione Identity Server WSO2".

I servizi di autenticazione si basano sulla piattaforma WSO2 e implementano il protocollo Oauth 2.0.

Per accendere i servizi di autenticazione su un nuovo servizio software, è necessario prima mettersi in contatto con Firenze Smart e procedere alla richiesta di attivazione.

3. Sviluppo

3.1. Validazione e test del prodotto

L'insieme dei test eseguibili comprende quanto segue:

- Test automatici da eseguire a fronte di ogni rilascio. Nel caso sia stata attivata una procedura automatica di CI/CD presso la piattaforma del committente, che prevede anche l'esecuzione dei test automatici, non è necessario fornire documentazione apposita, in quanto sarà la stessa procedura automatica che procederà o meno con i passaggi successivi nel caso di superamento / non superamento dei test automatici. In ogni caso, ne va fornita evidenza all'ente.
- Test di validazione del software dal punto di vista della sicurezza (vedi anche sezione 3.2 Sicurezza del codice sorgente).
- Test funzionali volti a verificare la correttezza del prodotto rispetto ai requisiti.
- Test di accessibilità in conformità ai livelli richiesti nelle linee guida sull'accessibilità di AGID (https://www.agid.gov.it/it/design-servizi/accessibilita/linee-guida-accessibilita-strumenti-informatici).

- Test di utilizzo del prodotto sotto stress (concorrenza dell'utilizzo, operazioni massive sul servizio, …).

Il committente e il fornitore condividono, prima di ogni rilascio, un piano dei test che DEVE essere applicato **dal fornitore stesso** al prodotto realizzato. Il piano di test potrà essere, di volta in volta, più o meno esaustivo a seconda delle componenti e delle funzionalità interessate.

Una volta che il personale incaricato del fornitore ha completato le attività di test pre-rilascio, rilascia altresì la documentazione che attesta il superamento dei test concordati, eventualmente integrati da ulteriori test che il fornitore abbia ritenuto necessari. In quest'ultimo caso, non è obbligatorio attestarne il superamento.

3.2. Sicurezza del codice sorgente

Le attività di realizzazione di codice sorgente DEVONO tenere in considerazione le misure necessarie per assicurarne, oltre alla correttezza, anche la sicurezza.

L' Agid pubblica ed aggiorna le linee guida per lo sviluppo di software sicuro, corredandole di allegati per quanto attiene ai seguenti ambiti:

- Linee guida per l'adozione di un ciclo di sviluppo di software sicuro (Allegato A);
- Linee Guida per lo sviluppo sicuro di codice (Allegato B);
- Linee Guida per la configurazione per adeguare la sicurezza del software di base (Allegato C);
- Linee Guida per la modellazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del Secure/Privacy by Design (Allegato D).

Il personale incaricato della realizzazione del software DEVE aver visionato le linee guida e rispettare ed applicare quanto di interesse per le attività coinvolte; DEVE inoltre assicurarsi di essere aggiornato con l'ultima versione disponibile pubblicata da Agid.

Le linee guida sono reperibili al seguente indirizzo:
https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro

4. Distribuzione

4.1. Procedure automatiche di build e distribuzione

La parte di distribuzione di un prodotto è un aspetto cruciale per la corretta erogazione di servizi funzionanti e aderenti a criteri imposti di continuità di servizio.

Le operazioni di distribuzione eseguite da un operatore umano, sebbene svolte con la necessaria attenzione, sono soggette a possibili errori e richiedono spesso delle attività ripetitive a basso valore aggiunto.

Per questi motivi È PREFERIBILE implementare un processo di build e distribuzione completamente automatico e basato sulle moderne pratiche del CI/CD.

La procedura automatica di build e distribuzione sarà realizzata considerando le caratteristiche seguenti:

- La procedura automatica DOVRÀ avviarsi in base ad eventi che si verificano sul codice sorgente (push di codice sorgente, creazione di un tag, chiusura di una merge request, …) e in accordo con quanto stabilito con il committente;
- La procedura automatica POTRÀ contenere l'esecuzione di batterie di test automatici sul prodotto sviluppato (si veda anche sezione 3.1 relativa alla "Validazione e test del prodotto");
- La procedura automatica DOVRÀ creare una build del software e orchestrare la sua distribuzione sui vari ambienti di sviluppo e test per i relativi controlli, prima di procedere alla distribuzione in produzione;
- La procedura automatica DOVRÀ interrompere la propria elaborazione in caso di fallimento di ogni step preliminare alla distribuzione del servizio, così da permettere una diagnosi ed un intervento da parte del personale incaricato;
- La procedura automatica POTRÀ richiedere una conferma da parte di un operatore umano del committente per la distribuzione sull'ambiente di produzione
- La procedura automatica DOVRÀ tenere in considerazione le linee guida OWASP DevSecOps (https://owasp.org/www-project-devsecops-guideline/), assicurandosi di soddisfare almeno i punti: secrets management, linting code, static application security testing (SAST), dynamic application security testing (DAST), Container vulnerability testing, privacy.

BENEDETTO FEMIA
Comune di Firenze
09.09.2022 12:13:31 GMT+01:00