

# POLITICA PER LO SVILUPPO SOFTWARE SICURO

Al fine di mantenere un alto livello di *sicurezza dei software* prodotti, limitando eventuali disagi ai clienti ed eccessivi costi di manutenzione, **Mauden S.r.l.** si è dotata di procedure di *analisi, sviluppo, collaudo e rilascio* di tutti i propri applicativi.

In dettaglio, un progetto *software* dovrà prevedere un **ciclo di vita** (Figura 1) che includa le seguenti fasi:

- Requisiti
- Progettazione
- Implementazione
- Collaudo
- Rilascio
- Supporto



Figura 1 - Ciclo di Vita

## Requisiti

Definiamo con *Requisiti di sicurezza del software* quelle caratteristiche del *software* in grado di:

### 1. GARANTIRE:

- *Riservatezza*: ovvero l'accesso protetto e controllato ai dati
- *Integrità*: ovvero la consistenza e la correttezza dei dati
- *Disponibilità*: ovvero la possibilità di accesso ai dati nelle modalità previste

### 2. PREVENIRE

- *eventuali intrusioni effettuate da entità esterne al sistema*: ovvero attacchi malevoli effettuati tramite rete internet da parte di utenti remoti
- *eventuali intrusioni effettuate da entità interne al sistema*: ovvero accesso ai sistemi da parte di utenti non autorizzati
- *eventi accidentali*: ovvero utilizzo inappropriato del software o situazioni impreviste

## Progettazione

Prendere in considerazione la *sicurezza del software*, già dalle prime fasi di un progetto, è un principio indispensabile per lo sviluppo di sistemi sicuri.

La fase di progettazione dovrà tenere conto dei *requisiti del cliente* e dei *requisiti di sicurezza aziendali* sopra considerati. Per ogni progetto dovrà essere prodotta un'opportuna analisi dei requisiti al cui interno, oltre alle specifiche funzionali, dovranno emergere *i potenziali rischi del software e le relative soluzioni*.

Dal punto di vista della protezione, i fattori chiave su cui porre attenzione nella fase di progettazione sono:

1. i sistemi di login
2. la gestione attenta dei profili utente e dei relativi privilegi
3. l'utilizzo esclusivo di transazioni criptate tramite protocollo https
4. l'utilizzo esclusivo di transazioni gestite da token creati all'accesso e sottoposti a scadenza
5. l'utilizzo di sistemi di monitoraggio
6. l'utilizzo di sistemi di log
7. l'utilizzo di sistemi di backup

**Mauden S.r.l.** raccomanda l'utilizzo delle *piattaforme hardware e software già disponibili in azienda*, al fine di ereditarne i meccanismi di sicurezza già implementati e collaudati.

## **Implementazione**

---

Per ridurre i rischi, gli sviluppatori dovranno prestare particolare attenzione alla correttezza del codice e verificare la qualità del lavoro svolto, applicando gli standard di codifica e test.

In particolare, è necessario prestare la dovuta attenzione:

1. alla **normalizzazione** dei dati, per assicurarne la **consistenza**
2. agli **algoritmi di verifica** dei dati inseriti da interfaccia, per assicurarne la **correttezza**
3. all'**ottimizzazione del codice**, per assicurare la velocità di esecuzione

Durante la fase di implementazione il team è tenuto a implementare il codice *esclusivamente all'interno degli ambienti di sviluppo forniti dall'azienda* e nel pieno rispetto delle *regole di sicurezza*.

Inoltre:

- gli ambienti di **Sviluppo, Test e Produzione** dovranno sempre essere tenuti distinti
- eventuali *dati di produzione*, utilizzabili in sede di collaudo per ottenere la maggior verosimiglianza con i *sistemi di produzione*, dovranno sempre essere distrutti al termine del collaudo stesso
- Le modifiche apportate al codice sorgente dovranno essere approvate da uno sviluppatore senior diverso da quello che ha originariamente scritto il codice, attraverso l'apposito strumento "Pull Request" presente su DevOps.

## **Collaudo**

---

Nella fase di collaudo il *software* è completo dal punto di vista funzionale e comincia ad essere sottoposto ai test. A tale scopo dovrà sempre essere identificato un **Responsabile di Collaudo**, la cui figura *non dovrà mai coincidere* con quella di **Responsabile del Progetto**.

Il **Responsabile di Collaudo** verificherà:

- la conformità del *software* agli standard di sicurezza di **Mauden S.r.l.**
- la conformità del *software* ai requisiti richiesti dal cliente
- l'esistenza di eventuali anomalie del *software*
- il funzionamento delle procedure di rilascio

Al termine delle operazioni verrà redatto uno specifico documento di test che certificherà l'avvenuta esecuzione dello stesso e la cui **validazione**, da parte del **Responsabile di Collaudo**, sarà una condizione necessaria al rilascio definitivo della procedura.

## **Rilascio**

---

Il rilascio è una fase critica nel ciclo di vita del *software*.

Per affrontarla al meglio è necessario:

1. Sviluppare sempre *software* in grado di effettuare auto-aggiornamenti
2. Eseguire le operazioni di rilascio solo dopo aver concordato con gli organizzatori data, ora e durata prevista dell'intervento
3. Avvisare i clienti del ripristino del servizio
4. Eseguire le operazioni di rilascio, utilizzando esclusivamente procedure verificate in fase di collaudo
5. Prevedere, laddove le condizioni lo consentano, il rilascio di una **versione pilota del software**, al fine di effettuare una ulteriore messa a punto insieme ai responsabili del progetto presso il cliente, per prevenire eventuali vulnerabilità non emerse in fase di collaudo

## **Supporto**

---

Non essendo possibile garantire al 100% la fornitura di un *software* del tutto esente da vulnerabilità, nella fase immediatamente successiva al rilascio si dovrà prevedere un intervallo di tempo in cui il *software* sia monitorato con attenzione, al fine di rispondere il più velocemente possibile ad eventuali anomalie.

## **AGID - Linee guida per lo sviluppo di software sicuro**

---

Per tutto quanto non citato in questo documento, utilizziamo e mettiamo in atto quanto riportato nel documento ufficiale LINEE GUIDA PER LO SVILUPPO DI SOFTWARE SICURO (<https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro>).

L'Amministratore Delegato