Università degli studi di Salerno

***Corso di Laurea in Informatica***

******

***PROGETTO DI INGEGNERIA DEL SOFTWARE – System Design Document***

***“BUY & SEE”***

**Docente:**

Andrea De Lucia

# Studenti:

##### Nome Matricola

## Fabio Curci 0512103296

## Francesca Di Mauro 05121

## Francesco Ciampa 05121

## Anna Santoro 05121

**Indice**

1. Introduzione

1.1. Scopo del sistema

1.2. Obiettivi di design

1.2.1 Criteri di Performance

1.2.2 Criteri di Affidabilità

1.2.3 Criteri di Costi

1.2.4 Criteri di Manutenzione

1.2.5 Criteri per l’Utente Finale

1.3 Definizioni, acronimi e abbreviazioni

1.4 Riferimenti

1.5 Panoramica

1. Architettura del software corrente
2. Architettura del software proposto 3.1. Panoramica

3.2.Decomposizione del sistema

3.3.Mapping Hardware/Software

3.4.Gestione dei dati persistenti

3.5.Controllo degli accessi e della sicurezza

3.6.Controllo del software globale

3.7.Condizioni Boundary

3.7.1Avvio del sistema

3.7.2Terminazione del sistema

3.7.3Fallimento del sistema

1. Servizi dei sottosistemi

4.1 Gestione Autenticazione

4.2 Gestione Account

4.3 Gestione Registrazione

4.4 Gestione Prodotti

4.5 Gestione Utente

4.6 Gestione Fornitori

4.7 Gestione Store

1. Glossario

**1. Introduzione**

**1.1 Scopo del sistema**

**1.2 Obiettivi di Design**

**1.2.1 Criteri di Performance**

**1.2.2 Criteri di Affidabilità**

**1.2.3 Criteri di Costo**

**1.2.4 Criteri di Manutenzione**

**1.3 Definizioni, acronimi e abbreviazioni**

**1.4 Riferimenti**

**1.5 Panoramica**

1. **Architettura del software corrente**

**3. Architettura del software proposto**

**3.1 Panoramica**

**3.2 Decomposizione del sistema**

**3.3 Mapping Hardware/Software**

**3.4 Gestione dei dati persistenti**

Il sistema si avvela di un database di tipo relazionale che consente un accesso efficiente ai dati , brevi tempi di risposta e un ampio spazio di archiviazione. Inoltre , è garantito l’accesso concorrente ai dati affidabili , ovvero ne viene salvata una copia ed è possibile ripristinare lo stato del database in caso di danni software o hardware. Infine , i dati sono privatizzati , cioè il DBMS ne consente un accesso protetto , quindi utenti diversi con operazioni diverse possono accedere a diverse sezioni del database.

**3.5 Controllo degli accessi e della sicurezza**

La sicurezza ed controllo dei dati del database è garantita tramite l’utilizzo di username e password per ogni singolo utente , che verranno richieste per singolo accesso . Ogni tipo di utente , amministratore o gestore avrà a disposizione diverse interfacce grafiche , in modo che ogni utente possa accedere solo alle rispettive funzionalità che rientrano nella sua categoria di utenza.

**3.6 Controllo del software globale**

Il sistema fornisce funzionalità che richiede una continua iterazione da parte dell’utente , ragione per cui , il controllo del flusso globale del sistema è guidato dagli eventi.

**3.7 Condizioni Boundary**

**3.7.1 Avvio del sistema**

Il server deve essere sempre acceso altrimenti i client non possono richiedere funzionalità quali l’autenticazione e di conseguenza la condivisione dei documenti tra le postazioni dello stesso gruppo di lavoro e l’accesso ai documenti presenti nell’archivio.

**3.7.2 Terminazione del sistema**

Nella terminazione del sistema si ha un regolare Log-out. Per consentire la corretta terminazione del server , l’amministratore del sistema dovrà effettuare la procedura di terminazione , dopo la quale nessun client potrà connettersi al sistema.

**3.7.3 Fallimento del sistema**

1. Nel caso di guasti dovuti al sovraccarico del database con successivo fallimento dello stesso è prevista come procedura preventiva il salvataggio periodico dei dati sotto forma di codice SQL , per la successiva generazione del DB.
2. Nel caso in cui si verifichi un’interruzione inaspettata non sono previsti metodi che ripristinato lo stato del sistema precedente allo spegnimento non voluto.
3. Un altro caso di fallimento potrebbe derivare dal software stesso che causa una chiusura inaspettata dovuta ad errori commessi durante la fase di implementazione. Non essendo previste politiche correttive , l’unica operazione consentita in questa particolare situazione è la chiusura del sistema e il suo successivo riavvio.
4. Un altro caso di fallimento potrebbe essere dovuto ad un errore critico nell’hardware , contro il quale non è prevista alcuna contromisura.

**4. Servizi dei sottosistemi**

**4.1 Gestione Autenticazione**

**4.2 Gestione Account**

**5. Glossario**