OSPEDALE POLICLINICO SAN MARTINO
Sistema Sanitario Regione Liguria
Istituto di Ricovero e Cura a Carattere Scientifico

PROCEDURA GENERALE PER LA VALIDAZIONE DEI SISTEMI INFORMATIVI CLINICO ASSISTENZIALI

Redazione
U.O. Information & Communication Technologies (ICT)
U.O. Governo Clinico e Organizzazione Ospedaliera
U.O. Gestione Rischio Clinico, Qualità, Accreditamento e URP

Acronimi

U.O. Unità Operativa
IO Istruzione Operativa
IOAZ Istruzione Operativa Aziendale
MOD Modulo
PQAZ Procedura Aziendale

Modifiche effettuate alla revisione precedente

Num. Rev.	Capitolo/Pag modificate	Descrizione tipo/natura della modifica
Rev. 0	-------	----------
Rev.		

1. GENERALITÀ – OGGETTO – SCOPO

La presente procedura aziendale ha l'obiettivo di definire la validazione dei principali applicativi aziendali, con relative modalità di audit trail, ai fini di garantire che le prestazioni richieste ai Sistemi Informativi dalle Unità Operative siano rispettate nei tempi e nella qualità definite a priori.
Tali procedure di validazione sono finalizzate a validare l'attività dei diversi sistemi informativi relativamente agli ambiti di competenza degli stessi ed inoltre verificare l'usabilità e l'integrità dei dati e la sicurezza degli accessi.

Inoltre, la procedura richiama l'Istruzione Operativa "IOAZHSI_0075 - Abilitazione applicativi aziendali", che ha lo scopo di descrivere il processo e i criteri con i quali il Policlinico procede alle abilitazioni e alle profilazioni di tutti gli utenti che, a vario titolo all'interno dell'Ospedale, svolgono attività che prevedono l'utilizzo degli strumenti informatici e degli applicativi aziendali (assistenza clinica, attività amministrativa, assistenza tecnica e informatica, attività di rendicontazione e controllo di gestione, ecc.).

Si richiama anche la procedura aziendale "PQAZHSI_0004 – Procedura di Emergenza in caso di indisponibilità dei sistemi informatici e telefonici", che ha lo scopo di riportare le procedure che si applicano nel caso in cui si verifichino guasti alla rete e alla fonia e ad apparati hardware, indisponibilità gravi delle procedure informatiche in uso presso il Policlinico San Martino, ovvero aggiornamenti hardware e software che comportino interruzioni prolungate dei servizi.

Infine è richiamata anche la procedura "IOAZHSI_0067 – Politiche di Backup", che definisce le politiche di backup dei dati, strutturate rispetto alla tipologia dei servizi erogati ed alla loro criticità, permettendo di non interrompere il servizio erogato.

2. RESPONSABILITÀ

L'aggiornamento di questa procedura è a cura dell'U.O. Information & Communication Technologies (ICT), dell'U.O. Governo Clinico e Organizzazione Ospedaliera e dell'U.O. Rischio Clinico, Qualità, Accreditamento e URP.
L'aderenza alle indicazioni contenute nella presente procedura è responsabilità di tutti gli operatori del Policlinico.

3. CONTENUTI

Procedure di validazione
Si definiscono in questo documento le procedure ed istruzioni da mettere in atto al fine di validare i principali applicativi aziendali, specificando le relative modalità di audit trail, ai fini dell'accreditamento dei sistemi informativi clinici.

I principali sistemi informativi individuati come maggiormente rilevanti ai fini della validazione sono i seguenti:

- **Sistema Informativo Ospedaliero (SIO Onesys)**
- **Sistema Informativo Radiologico (RIS Fenix)**
- **Sistema Informativo Cardiologico (CIS Suitestensa)**
- **Sistema Informativo Laboratorio (LIS TDSynergy)**
- **Sistema Informativo Trasfusionale (Emonet)**
- **Sistema Informativo di prescrizione e somministrazione farmaci (SOFIA)**
- **Sistema Informativo di preparazione farmaci antiblastici (Tera80)**

Di seguito le principali procedure ed istruzioni da seguire per le diverse aree:

1. **Organizzazione**:
   Le responsabilità dell'organizzazione aziendale sono inserite nel Documento Organizzativo di Unità Operativa.
   Le responsabilità dei fornitori degli applicativi aziendali sono invece descritte all'interno dei documenti contrattuali, con i relativi accordi sui livelli di servizio (SLA).
   I referenti dei vari applicativi aziendali hanno ricevuto una formazione adeguata per supportare gli utenti, in accordo con il fornitore, in caso di malfunzionamento del sistema ed esiste, per alcune fattispecie, anche un supporto diretto del fornitore per l'assistenza di primo livello (One.Sys e Sofia)

2. **Accordi**:
   Le responsabilità per il supporto software e hardware degli applicativi aziendali sono chiaramente definite all'interno dei documenti contrattuali, all'interno dei quali sono incluse anche le seguenti informazioni:
   - Responsabilità dei subappaltatori
   - Istruzioni per la documentazione degli eventi imprevisti,
   - Definizione del limite temporale per le azioni correttive da parte del supporto responsabile

   Inoltre, se i dati vengono trasferiti tra sistemi informatici diversi:
   - Sono descritti piattaforme e protocolli

- È obbligatorio comunicare reciprocamente i cambiamenti e gli eventi che possono influenzare l'informazione trasferimento incluso
- Le responsabilità per le diverse parti della catena tra i sistemi sono chiaramente definite all'interno dei documenti contrattuali, con i relativi accordi sui livelli di servizio (SLA).

Con riferimento al contratto di assistenza e manutenzione di uno specifico applicativo aziendale, viene incaricata la ditta attraverso l'atto di nomina a Responsabile trattamento dati personali.

3. **Documentazione del sistema**:
   La documentazione completa ed aggiornata di ogni sistema è disponibile sotto forma di manuali tecnici, manuali d'uso e guida per l'utente, con apposito numero di versione.
   La documentazione contiene misure per la gestione di malfunzionamenti.

4. **Manutenzione**:
   Le procedure operative standard per le misure da mettere in atto in caso di malfunzionamento o fermo totale dei sistemi applicativi sono disponibili all'interno degli specifici manuali applicativi.
   Inoltre, nella procedura aziendale "PQAZHSI_0004 – Procedura di Emergenza in caso di indisponibilità dei sistemi informatici e telefonici" sono state definite le indicazioni che si devono applicare nel caso in cui si verifichino guasti alla rete e alla fonia e ad apparati hardware, indisponibilità gravi delle procedure informatiche in uso presso il Policlinico San Martino, ovvero aggiornamenti hardware e software che comportino interruzioni prolungate dei servizi.
   È inoltre previsto un sistema di backup, secondo la procedura "IOAZHSI_0067 – Politiche di Backup", che definisce le politiche di backup dei dati, strutturate rispetto alla tipologia dei servizi erogati ed alla loro criticità, permettendo di limitare le possibili interruzioni dei servizi medesimi.
   Alcuni servizi critici sono inseriti in architetture che prevedono un sistema di Disaster Recovery atte a garantire la continuità pressoché assoluta del servizio.
   Di seguito la tabella degli applicativi principali, oggetto di validazione, con relativi riferimenti contrattuali, all'interno dei quali sono definiti gli accordi sui livelli di servizio (SLA) e le relative penali.

Applicativo	**Riferimenti contrattuali**
Sistema Informativo Ospedaliero (SIO Onesys)	Deliberazione n. 1640/2023
Sistema Informativo Radiologico (RIS Fenix)	Deliberazione n. 926/2023
Sistema Informativo Cardiologico (CIS Suitestensa)	Deliberazione n.552/2020
Sistema Informativo Laboratorio (LIS TDSynergy)	Deliberazione n. 232/2023
Sistema Informativo Trasfusionale (Emonet)	Deliberazione n. 1815/2023: Recepimento del contratto discendente da Accordo Quadro, Anno 2023 Nota prot. n° 50966/2023: Accordo Quadro 2023-2025 Nota prot. n° 57848/2023: Contratto discendente da Accordo Quadro, Anno 2023

Sistema Informativo di prescrizione e somministrazione farmaci (SOFIA)	Deliberazione n. 241/2022
Sistema Informativo di preparazione farmaci antiblastici (Tera80)	Deliberazione n. 1642/2023

5. **Modifiche**:
   Sono disponibili ambienti di Disaster Recovery e di test per i seguenti sistemi applicativi:

Applicativo	**Ambienti di DR e di test**
Sistema Informativo Ospedaliero (SIO Onesys)	Ambiente di DR + Ambiente di test
Sistema Informativo Radiologico (RIS Fenix)	Ambiente di DR + Ambiente di test
Sistema Informativo Cardiologico (CIS Suitestensa)	Ambiente di DR in testing + Ambiente di test
Sistema Informativo Laboratorio (LIS TDSynergy)	Ambiente in dismissione, a favore di una nuova piattaforma applicativa
Sistema Informativo Trasfusionale (Emonet)	Ambiente di test Ambiente in dismissione, a favore di una nuova piattaforma applicativa
Sistema Informativo di prescrizione e somministrazione farmaci (SOFIA)	Ambiente di DR + Ambiente di test
Sistema Informativo di preparazione farmaci antiblastici (Tera80)	Ambiente di test

Per quanto riguarda le procedure di validazione per ogni singola applicazione, a seguito di aggiornamenti, modifiche, nuove versioni nel sistema, si richiamano di seguito i riferimenti:

Applicativo	**Procedure di validazione/Piano di convalida**
Sistema Informativo Ospedaliero (SIO Onesys)	Qualifica del Sistema Informativo Ospedaliero (ONE.SYS).pdf Conservata agli atti della U.O. ICT
Sistema Informativo Radiologico (RIS Fenix)	Documento di qualifica e checklist di validazione in fase di redazione.
Sistema Informativo Cardiologico (CIS Suitestensa)	Documento di qualifica e checklist di validazione in fase di redazione.
Sistema Informativo Laboratorio (LIS TDSynergy)	Documento di qualifica e checklist di validazione in fase di redazione.
Sistema Informativo Trasfusionale (Emonet)	Già stato validato (da inserire riferimenti della procedura)
Sistema Informativo di prescrizione e somministrazione farmaci (SOFIA)	Documento di qualifica e checklist di validazione in fase di redazione. La Procedura di validazione dell'applicativo fa parte del Sistema di Gestione Integrato di Deenova. Nel dettaglio, si tratta della procedura PGI.ICT.02 "PROCEDURA DI VALIDAZIONE NUOVA VERSIONE SOFTWARE – ORBIT/SOFIA®".

	Si ricorda che SOFIA® è un Dispositivo Medico di classe 1 certificato ISO 13485
Sistema Informativo di preparazione farmaci antiblastici (Tera80)	Documento di qualifica e checklist di validazione in fase di redazione.

Tali procedure di convalida del software sono finalizzate a validare l'attività dei diversi sistemi informativi relativamente alle funzionalità di competenza ed inoltre verificare l'usabilità e l'integrità dei dati e la sicurezza degli accessi.

La procedura di validazione dei software comprende le seguenti macro-attività:

- analisi del rischio in cui si valutano gli elementi da validare con i relativi livelli di approfondimento in base alla quale si pianificata l'attività di validazione del singolo software
- illustrazione delle modalità di qualifica del software nelle varie fasi con definizione delle procedure di Installation Qualification, Operation Qualification e Performance Qualification.

Le principali fasi del piano di convalida, in aderenza a quanto previsto dalle "*Guideline on computerised systems and electronic data in clinical trials*" dell'European Medicines Agency (EMA), in relazione ai 3 item di Qualification, sono le seguenti:

1. Installation Qualification:
   È descritta in termini trasversali per quanto attiene le sottostanti procedure in appositi documenti agli atti della U.O. ICT

   a. installazione e collaudo
   b. backup
   c. materiale informativo
   d. training iniziale
   e. integrazione con sw
   f. privacy

   Per modalità di gestione backup, schema server-DR, formazione e schemi di integrazione la documentazione è conservata agli atti della U.O. ICT in apposita cartella di rete dedicata alla certificazione di qualità.

2. Operation Qualification
   È richiamata nei documenti di convalida del software dedicati a ciascuna applicazione critica e consiste nella verifica delle funzionalità principali e maggiormente critiche in relazione alla valutazione del rischio, attraverso l'uso di checklist/User Acceptance Tests (UATs) specifici per ciascuna applicazione.

3. Performance Qualification
   È richiamata nei documenti di convalida del software dedicati a ciascuna applicazione critica e consiste nella verifica delle principali integrazioni tra le applicazioni, ritenute maggiormente critiche in relazione alla valutazione del rischio, attraverso l'uso di checklist/User Acceptance Tests (UATs) specifici per ciascuna applicazione.

Per l'effettuazione della validazione vengono utilizzate checklist contenenti report di convalida dei test per un numero congruo di verifiche di validazione in relazione ai moduli applicativi oggetto di verifica.
Dato che le soluzioni applicative in questione risultano già installate ed operative, la modalità di convalida adottata è di tipo retrospettivo.
Nel caso di major release dei software validati verranno eseguiti nuovi test di validazione.

6. **Sicurezza informatica**:
   L'accesso ai locali server è protetto da misure di protezione fisica dei dati.
   È attivo un sistema di protezione antivirus.
   L'accesso al sistema informatico è protetto da credenziali di autenticazione nominali personali, distinte per i diversi ruoli (utente, amministratore di server, amministratore Active Directory).

   Il processo ed i criteri con i quali il Policlinico procede alle abilitazioni e alle profilazioni di tutti gli utenti che, a vario titolo all'interno dell'Ospedale, svolgono attività che prevedono l'utilizzo degli strumenti informatici e degli applicativi aziendali sono descritti all'interno dell'Istruzione Operativa "IOAZHSI_0075 - Abilitazione applicativi aziendali". Nello specifico, per abilitazione si intende la procedura con cui vengono rilasciate le credenziali di accesso all'utente, mentre per profilazione si intende la procedura che assegna ad ogni utente determinate funzionalità in relazione al ruolo svolto.

   È inoltre previsto un sistema di backup, secondo la procedura "IOAZHSI_0067 – Politiche di Backup", che definisce le politiche di backup dei dati, strutturate rispetto alla tipologia dei servizi erogati ed alla loro criticità, permettendo di non interrompere il servizio erogato.

   È stato attivato un sistema di rilevazione degli accessi ai server gestito attraverso SIEM e SOC esternalizzato.

   Audit Trail
   I sistemi garantiscono la tracciabilità dell'utente e forniscono la tracciabilità delle modifiche, attraverso lo strumento di audit trail, i cui dettagli sono riportati nelle procedure di qualifica rilasciate per ciascun software critico:

Applicativo	**Audit trail**
Sistema Informativo Ospedaliero (SIO Onesys)	Qualifica del Sistema Informativo Ospedaliero (ONE.SYS).pdf Conservata agli atti della U.O. ICT
Sistema Informativo Radiologico (RIS Fenix)	In fase di redazione.
Sistema Informativo Cardiologico (CIS Suitestensa)	In fase di redazione.
Sistema Informativo Laboratorio (LIS TDSynergy)	In fase di redazione.
Sistema Informativo Trasfusionale (Emonet)	Possiamo chiedere al fornitore di inviare documentazione già presente sui sistemi di audit trail esistenti (che certamente hanno essendo certificatI)
Sistema Informativo di prescrizione e somministrazione farmaci (SOFIA)	In SOFIA® a livello applicativo è presente un log puntuale per recuperare le informazioni di prescrizione e somministrazione di farmaci (col

	click sulle Unità di Prescrizione si richiama da applicativo il log). Altri log più approfonditi sono presenti a DataBase.
Sistema Informativo di preparazione farmaci antiblastici (Tera80)	In fase di redazione.

Per verificare la correttezza dei dati, inseriti manualmente oppure trasferiti da un altro sistema, si rimanda alle procedure interne delle Unità Operative, in conformità a quanto riportato nell'Istruzione Operativa aziendale "IOAZHQA_0709 - Il Sistema dei Doppi Controlli".

4. DOCUMENTI DI RIFERIMENTO/NORMATIVA/BIBLIOGRAFIA

- Codice dell'Amministrazione Digitale (CAD) - D. Lgs. N. 82/2005
- Linee Guida AgID per il Disaster Recovery delle Pubbliche Amministrazioni
- Direttiva UE 2016/1148 (NIS)
- Direttiva UE 2022/2555 (NIS2)