H.I.T.
Health Information Technology

SAAS PRODUCT SPECIFICATION

MODULO GRC VERSIONE 1.1
PER
EOS MODULI VERSIONE 2

2023

Via di Tor Vergata, 440/B – 00133 Roma
06 94288371 – 06 9495335
info@hit.srl

ELENCO DELLE REVISIONI

Ed.	Rev.	Motivazione	Data
1	1	Prima emissione per versione software 2 – sostituisce integralmente vecchie PS “GRC Console Rev.04” e “GRC App Rev.02”	04-08-2021
1	2	Seconda emissione per versione software 2 – Aggiornamento di funzionalità e migrazione a nuova infrastruttura cloud	11-05-2022
1	3	Aggiornamento dei loghi aziendali	26-05-2023

INDICE

IL SISTEMA: DESCRIZIONE GENERALE

La piattaforma informatica **EOS Moduli** è un Sistema software web modulare orientato all'informatizzazione e digitalizzazione dei processi in ambito Sanitario ed Industriale, con particolare attenzione all'**archiviazione della documentazione di processo**.

La piattaforma è strutturata in **differenti Moduli**, ognuno dei quali implementa l'informatizzazione di un processo secondo linee guida e/o normative regionali, nazionali o europee. Tali Moduli sono indipendenti tra loro, ma interconnessi grazie ad una sofisticata **architettura tecnica condivisa** per la gestione degli accessi utente al sistema e la memorizzazione dei dati inseriti. Tale architettura permette agli utenti di accedere alle informazioni presenti in differenti Moduli tramite delle credenziali uniche (Single Sign-On) e di rendere visibili e/o trasferire dati comuni da un Modulo all'altro, incrementando notevolmente l'efficienza nella gestione di più processi in contemporanea.

Il sistema ne prevede l'utilizzo da parte di una Organizzazione esclusivamente tramite la concessione di una o più licenze con durata pluriennale.

Il software è progettato e di proprietà della società H.I.T. – HEALTH INFORMATION TECHNOLOGY S.R.L. (di seguito **HIT**).

Infrastruttura cloud

La piattaforma **EOS Moduli** è ospitata in un Datacenter locato in Italia su di un servizio di Infrastruttura Virtuale qualificata AgID, progettata sulla base dei seguenti standard:

- Standard gestionali
  - ISO/IEC 20000, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 22301
- Standard di progettazione
  - ITIL V3, TM Forum (TMF_CEM 17.5 *Customer Experience Management Frameworks*, TMF_SID 16.0 *Information Frameworks*), TMF_eTOM 16.0 (Business process Frameworks), ISO 9001, PMI 5.0, SIX SIGMA green belt, SOC 1/2
- Standard tecnici
  - CSA STAR Gold Certification, Common Criteria Evaluation Assurance Level 3+, Payment Card Industry Data Security Standard, Trusted Cloud Service (TRUCS) certifications in 16 domains, TÜV Trusted Cloud Service, Trusted Cloud Data Protection Profile, PSA security certification.

Le risorse a disposizione dell'infrastruttura sono dedicate, ed un Load Balancer si occupa di bilanciare le richieste verso le risorse a disposizione. Un servizio di backup giornaliero permette di recuperare da eventuali perdite di dati più o meno accidentali mentre un servizio di Replica in Disaster Recovery a sincronizzazione oraria giornaliera su di un Datacenter locato in altra città offre garanzie di ritorno all'operatività della piattaforma in tempi rapidi, anche a fronte di eventi problematici di grande impatto sul Datacenter principale.

Requisiti minimi client

L'accesso alla piattaforma **EOS Moduli** può essere effettuato da un qualsiasi dispositivo (computer desktop o smartphone/tablet) dotato di browser Google Chrome o Mozilla Firefox aggiornati all'ultima versione disponibile (*).

Si consiglia in ogni caso l'accesso tramite una postazione computer con monitor ad alta risoluzione (Full-HD 1920x1080) per via della mole di informazioni presenti sullo schermo e browser Google Chrome per la massima compatibilità e sicurezza.

NOTA(*): *Si considera una connessione ad internet attiva con banda bidirezionale da almeno 1 Mbit/s stabile come pre-requisito.*

Descrizione delle licenze

Per l'utilizzo della piattaforma **EOS Moduli** è previsto un meccanismo di licenze basato sulla concessione di una licenza singola pluriennale rinnovabile per ciascun Presidio/Sede Operativa di una Organizzazione, esclusivamente in **modalità SaaS** (Software as a Service), con due differenti tipologie di Licenze selezionabili: **Standard** (per piccole realtà) e **Manager** (per grandi Organizzazioni).

La tipologia di licenza Manager è dedicata alle Organizzazioni più strutturate che intendono gestire in totale autonomia gli aspetti di accesso al portale ed elenchi anagrafici; di seguito sono elencate le differenze funzionali tra le tipologie di licenze previste:

FUNZIONALITÀ DIPENDENTI DA TIPO LICENZA	LICENZA STANDARD	LICENZA MANAGER
ANAGRAFICA AZIENDE/PRESIDI	✗	✓
ANAGRAFICA REPARTI IN PRESIDI	✗	✓
ANAGRAFICA UTENTI	✗	✓
ANAGRAFICA ACCESSI UTENTE AL SISTEMA	✗	✓
CREAZIONE ACCESSI UTENTE AL SISTEMA – IN AUTONOMIA (SYSTEM ADMINISTRATOR)	✗	✓
CREAZIONE ACCESSI UTENTE AL SISTEMA – SU RICHIESTA	✓	✗
CREAZIONE ACCESSI UTENTE AL SISTEMA PER PRESIDIO	✓	✓
CREAZIONE ACCESSI UTENTE AL SISTEMA PER REPARTO (*)	✗	✓
INTEGRAZIONE FUNZIONALE CON DATI DA ALTRI MODULI (*)	✓	✓
PERSONALIZZAZIONE PARAMETRI NOTIFICHE (*)	✗	✓
PERSONALIZZAZIONE MAPPATURA TIPOLOGICA DOCUMENTI INCREMENTALE (*)	✗	✓
PERSONALIZZAZIONE GRAFICA BANNER DASHBOARD	✗	✓
NUMERO DI PRESIDI LICENZIABILI	**1-7**	**≥ 3**

(*) la funzionalità potrebbe non essere disponibile per tutti i Moduli

Per le licenze Standard, la funzionalità relativa al *System Administrator* è svolta esclusivamente da HIT.

IL SISTEMA: STRUTTURA

Ogni modulo della piattaforma **EOS Moduli** condivide una struttura di fondo composta dall'**architettura** di accesso al sistema e dalle funzionalità garantite al profilo utente speciale di Tipologia/Ruolo **System Administrator**.

Architettura di accesso al sistema

L'architettura di accesso alla piattaforma **EOS Moduli** garantisce per-design:

- accesso al sistema ai soli utenti specificatamente abilitati tramite un meccanismo di login basato su credenziali univoche;
- accesso ai dati di sistema definito dal concetto di **Visibilità**: accesso ad un range di dati specifico per ciascuna utenza per ciascun modulo, limitato a quanto definito in fase di creazione del profilo utente dal *System Administrator* e basato su **Tipologia + Presidi o Reparti**;
- accesso alle funzionalità di sistema definito dal concetto di **Ruolo**: disponibilità di un set predeterminato di funzioni per ciascuna utenza per ciascun modulo, limitato a quanto definito in fase di creazione del profilo utente dal *System Administrator* in base alla selezione del **Ruolo**, ognuno associabile ad una o più combinazioni di *Visibilità*;
- accesso a tutte le capacità (definite dal *System Administrator*) per ciascun utente su ogni modulo con una unica coppia di credenziali (email +password→Single Sign-On) e possibilità di cambiare in tempo reale il proprio *Ruolo* in ogni modulo (se previsto in base alle definizioni effettuate dal *System Administrator*).

Il primo set di credenziali viene generato automaticamente dal sistema all'atto della creazione del profilo utente; è imposto il cambio password al primo accesso per motivi di sicurezza.

L'accesso al sistema è protetto mediante connessioni crittografate (https).

Si garantisce piena compliance con il Regolamento generale per la protezione dei dati personali n. 2016/679.

Profilo utente System Administrator

Di seguito vengono dettagliate le funzionalità riservate al profilo utente di tipologia **System Administrator**. Per ogni sezione, è indicato l'elenco di *Ruoli* per cui la suddetta viene resa disponibile.

Menu Amministrazione→Presidi

RUOLI: SYSTEM ADMINISTRATOR

Sezione dedicata alla gestione dell'anagrafica di Aziende e relativi Presidi per i quali è possibile inserire dati nel sistema.

Il numero massimo di Presidi inseribili è equivalente al numero di Presidi considerati per il calcolo della licenza nel contratto con HIT. In caso di contratti multipli, ha valore il numero minimo di Presidi considerati nel singolo contratto tra tutti i contratti in essere.

Sono previste le seguenti funzionalità:

1. Inserimento Azienda
2. Modifica Azienda
3. Eliminazione Azienda

1.Inserimento Azienda

Permette di inserire i dati necessari al sistema per la registrazione in anagrafica di una Azienda (Ragione Sociale) e un suo primo Presidio.

2.Modifica Azienda

Permette di modificare i dati previsti per una Azienda e/o un Presidio, inserire un nuovo Presidio per l'Azienda o eliminare un Presidio esistente (*).

3.Eliminazione Azienda

Permette di eliminare una Azienda dall'anagrafica e tutti i suoi Presidi (*); per confermare l'operazione è richiesta l'immissione della propria password personale.

***NOTA(*):** Una qualsiasi operazione di eliminazione non può essere completata se agli elementi considerati sono ancora associati dei dati nel sistema.*

Menu Amministrazione→Reparti

RUOLI: SYSTEM ADMINISTRATOR

Sezione dedicata alla gestione dell'anagrafica dei Reparti di cui sono composti i Presidi per i quali è possibile inserire dati nel sistema.

Sono previste le seguenti funzionalità:

1. Inserimento Reparto
2. Modifica Reparto
3. Eliminazione Reparto
4. Associazione Reparto

1.Inserimento Reparto

Permette di inserire i dati necessari al sistema per la registrazione in anagrafica di un Reparto.

2.Modifica Reparto

Permette di modificare i dati previsti per un Reparto.

3.Eliminazione Reparto

Permette di eliminare un Reparto dall'anagrafica (*).

4.Associazione Reparto

Permette di effettuare le associazioni tra un Reparto ed i Presidi delle Aziende, indicando quel Reparto in quali Presidi è presente.

NOTA(*): *L' operazione di eliminazione non può essere completata se al Reparto sono ancora associati dei dati nel sistema.*

Menu Amministrazione→Utenti

RUOLI: SYSTEM ADMINISTRATOR

Sezione dedicata alla gestione dell'anagrafica degli Utenti per i quali è possibile inserire dati nel sistema.

Sono previste le seguenti funzionalità:

1. Inserimento Utente
2. Modifica Utente
3. Eliminazione Utente

1.Inserimento Utente

Permette di inserire i dati necessari al sistema per la registrazione in anagrafica di un Utente.

2.Modifica Utente

Permette di modificare i dati previsti per un Utente.

3.Eliminazione Utente

Permette di eliminare un Utente dall'anagrafica.

Menu Amministrazione→Gestione accessi

RUOLI: SYSTEM ADMINISTRATOR

Sezione dedicata alla gestione degli accessi al sistema da parte degli utenti.

Sono previste le seguenti funzionalità:

1. Inserimento Nuovo Accesso
2. Modifica Accesso
3. Disabilitazione Accesso
4. Riabilitazione Accesso
5. Reset credenziali di Accesso

1.Inserimento Nuovo Accesso

Permette di inserire i dati necessari al sistema per garantire un nuovo accesso ad un utente, che sia già registrato in anagrafica utenti oppure no. I dati richiesti per l'accesso sono:

- Dati generali dell'utente o selezione di un utente esistente in anagrafica
- *Tipologia* di profilo, che può essere selezionato a scelta tra:
  - *System Administrator*
  - *Unit User* (utente di unità/Presidio)
  - *Subunit User* (utente di subunit/Reparto)
- *Visibilità* sui dati per l'accesso (elenco di Presidi o Reparti)
- *Ruolo* per ogni singola informazione di *Visibilità*

Al termine della procedura è possibile inviare le credenziali di accesso auto-generate dal sistema all'indirizzo email inserito per l'utente.

2. Modifica Accesso

Permette di modificare i dati di un accesso.

3. Disabilitazione Accesso

Permette di disabilitare un accesso al sistema. L'operazione è reversibile.

4. Riabilitazione Accesso

Permette di riabilitare un accesso al sistema precedentemente disabilitato.

5. Reset credenziali di Accesso

Permette di effettuare il reset delle credenziali per un accesso di sistema; delle nuove credenziali verranno generate ed inviate all'indirizzo email indicato nei dati di accesso.

IL MODULO: DESCRIZIONE GENERALE

IL MODULO GRC: DESCRIZIONE GENERALE

Modulo GRC (Gestione Rischio Clinico)

Il **modulo GRC (Gestione Rischio Clinico)**, parte della piattaforma **EOS Moduli**, è il modulo software per l'informatizzazione del processo di gestione del rischio clinico di strutture sanitarie e socio-sanitarie secondo quanto specificato nelle seguenti linee guida/normative:

- Requisiti di autorizzazione all'esercizio;
- Linee guida AGENAS per i Manuali di Accreditamento;
- Legge 24/2017 (Gelli-Bianco).

Il processo informatizzato prevede l'invio da parte degli operatori sanitari (preventivamente abilitati) di segnalazioni di eventi avversi o possibili eventi avversi (con l'apposita WebApp) che gli utenti del modulo potranno leggere e poi processare con il sistema integrato di classificazione, valutazione e gestione di azioni correttive a chiusura del processo.

Con il **modulo GRC** si intende introdurre una gestione innovativa, concreta e responsabile del procedimento: la semplicità di utilizzo, la rapidità di segnalazione ed inserimento dei dati e la flessibilità dell'accesso via web permette un processo cooperativo tra tutti gli attori coinvolti nella gestione del rischio clinico.

Le capacità di analisi statistica integrate permettono la tenuta sotto controllo dello stato di avanzamento del processo di gestione degli eventi avversi in ogni momento, ed i grafici che verranno inseriti permetteranno di monitorare il progresso nel tempo nella gestione degli stessi.

IL MODULO: SPECIFICHE

Funzionalità

Le funzionalità del **modulo GRC** sono specificate nei paragrafi successivi. Per ogni sezione o funzionalità è indicato l'elenco di *Ruoli* per cui la suddetta viene resa disponibile. I dati visualizzati dal singolo utente sono sempre in funzione della *Visibilità* e del *Ruolo* specificato dal *System Administrator* in fase di creazione del suddetto profilo utente.

Elenco ruoli

Nella tabella successiva sono elencati i *Ruoli* disponibili per gli utenti che devono accedere al modulo:

DENOMINAZIONE RUOLO	DENOMINAZIONE BREVE	DESCRIZIONE GENERALE
RESPONSABILE DI GESTIONE	RDG	Visualizzazione dell'elenco degli utenti con accesso al modulo, gestione delle opzioni di configurazione del modulo (ove previste) e gestione completa del processo di valutazione e chiusura delle segnalazioni di eventi avversi
SUPPORTO DI GESTIONE	SDG	Supporto al ruolo RDG per la gestione parziale delle attività del processo di valutazione e chiusura delle segnalazioni di eventi avversi
GESTORE PRIVACY	PRI	Gestione del procedimento di pseudonimizzazione dei dati inseriti nelle segnalazioni di possibili eventi avversi a monte del processo di valutazione
SUPERVISORE	SUP	Sola visione/lettura dei dati nel modulo

Configurazione

RUOLI: RESPONSABILE DI GESTIONE

Sezione dedicata alla configurazione di eventuali parametri di funzionamento del modulo, nonché alla visualizzazione del riepilogo degli utenti che hanno diritto di accesso allo stesso su cui ha visibilità un utente.

Sono previste le seguenti funzionalità:

1. Visualizzazione riepilogo accesso utenti
2. Configurazione codici operatore per invio segnalazioni

1.Visualizzazione riepilogo accesso utenti

RUOLI: RESPONSABILE DI GESTIONE

Permette la visualizzazione di tabelle di riepilogo degli utenti che hanno accesso al modulo, con il dettaglio dei relativi Presidi/Reparti e *Ruoli*.

2.Configurazione codici operatore per invio segnalazioni

RUOLI: RESPONSABILE DI GESTIONE

Permette la creazione di appositi Codici Operatore da utilizzare obbligatoriamente nella WebApp di invio Segnalazione di possibile evento avverso da parte degli operatori individuati dall'Organizzazione. Ogni codice può essere associato alle informazioni di Presidio (in cui si verifica l'evento), Reparto (in cui si verifica l'evento) e Qualifica del segnalatore.

Resoconto Segnalazioni

RUOLI: RESPONSABILE DI GESTIONE, SUPPORTO DI GESTIONE, GESTORE PRIVACY, SUPERVISORE

Sezione dedicata al riepilogo dello stato di avanzamento nella gestione di ciascuna segnalazione di evento avverso non ancora chiusa su cui ha visibilità un utente.

Per gli utenti di Reparto (con profilo utente di tipologia *Subunit User*), la visibilità sulle segnalazioni è limitata a quelle relative al proprio Reparto di appartenenza (come definito alla creazione del profilo utente).

Sono previste le seguenti funzionalità:

1. Visualizzazione dati sintetici segnalazione
2. Esportazione report segnalazione

1.Visualizzazione dati sintetici segnalazione

RUOLI: RESPONSABILE DI GESTIONE, SUPPORTO DI GESTIONE, GESTORE PRIVACY, SUPERVISORE

Permette di visualizzare un riepilogo dei dati contenuti in ogni segnalazione di evento avverso ricevuta.

2.Esportazione report segnalazione

RUOLI: RESPONSABILE DI GESTIONE, SUPPORTO DI GESTIONE, GESTORE PRIVACY, SUPERVISORE

Permette di esportare i dati di riepilogo di una segnalazione di evento avverso come file pdf.

Gestione Segnalazioni

RUOLI: RESPONSABILE DI GESTIONE, SUPPORTO DI GESTIONE, GESTORE PRIVACY, SUPERVISORE

Sezione dedicata alla gestione del processo di valutazione, correzione e chiusura delle segnalazioni di evento avverso su cui ha visibilità un utente.

Per gli utenti di Reparto (con profilo utente di tipologia *Subunit User*), la visibilità sulle segnalazioni è limitata a quelle relative al proprio Reparto di appartenenza (come definito alla creazione del profilo utente).

Sono previste le seguenti funzionalità:

1. Visualizzazione elenco segnalazioni
2. Visualizzazione dati segnalazione
3. Pseudonimizzazione segnalazione
4. Classificazione segnalazione
5. Visualizzazione Classificazione segnalazione

6. Valutazione evento avverso
7. Visualizzazione Valutazione evento avverso
8. Gestione Azioni correttive evento avverso
9. Visualizzazione Azioni correttive evento avverso
10. Chiusura segnalazione

1.Visualizzazione elenco segnalazioni

RUOLI: RESPONSABILE DI GESTIONE, SUPPORTO DI GESTIONE, GESTORE PRIVACY, SUPERVISORE

Permette di visualizzare l'elenco di tutte le segnalazioni di evento avverso inviate dagli operatori dell'Organizzazione e ricevute nel sistema, con i dati sintetici delle stesse.

2.Visualizzazione dati segnalazione

RUOLI: RESPONSABILE DI GESTIONE, SUPPORTO DI GESTIONE, GESTORE PRIVACY, SUPERVISORE

Permette di visualizzare tutti i dati contenuti in una segnalazione più i dati riepilogativi di gestione della stessa, con una cronologia basilare relativa alle varie fasi di lavorazione. Eventuali campi che potrebbero contenere dati sensibili sono nascosti (agli utenti non profilati con il Ruolo Gestore Privacy) fino al completamento del processo di pseudonimizzazione.

3.Pseudonimizzazione segnalazione

RUOLI: GESTORE PRIVACY

Permette di pseudonimizzare i dati contenuti nelle segnalazioni inviate dagli operatori, sostituendo dove fosse necessario eventuali dati sensibili (a cui non devono avere accesso gli utenti di sistema non autorizzati al trattamento dati, quindi non profilati con il ruolo Gestore Privacy) con altre parole chiave in modo da permettere una corretta gestione della stessa a tutti gli utenti.

4.Classificazione segnalazione

RUOLI: RESPONSABILE DI GESTIONE, SUPPORTO DI GESTIONE

Permette di effettuare il processo di Classificazione di una segnalazione specificando determinati parametri tra cui la catalogazione come tipologia di evento e la sua definizione, con una indicazione visiva di quali sono gli eventi sentinella. Permette inoltre di associare la segnalazione ad un raggruppamento (auto-inseribile) per successive gestioni massive ed assegnare un titolo per una ricerca veloce.

5.Visualizzazione Classificazione segnalazione

RUOLI: SUPERVISORE

Permette di visualizzare i dati sintetici del processo di Classificazione già completato per una segnalazione, con un resoconto della cronologia delle operazioni effettuate.

6.Valutazione evento avverso

RUOLI: RESPONSABILE DI GESTIONE, SUPPORTO DI GESTIONE(*)

Permette di effettuare la valutazione dell'evento calcolando gli indici relativi di Probabilità (IPC) e Priorità del Rischio (IPR) utilizzando matrici 5x5, partendo dall'inserimento di dati stimati dall'utente in termini di Rilevabilità, Probabilità e Gravità dell'evento. È possibile inoltre individuare un Indice di Impatto Organizzativo (IIO) per mantenere un riferimento del peso che comporta, a livello di organizzazione, la gestione di un determinato evento.

(*) limitato all'inserimento di sole proposte di Valutazione, sottoposte ad accettazione degli utenti Ruolo RESPONSABILE DI GESTIONE.

7.Visualizzazione Valutazione evento avverso

RUOLI: SUPERVISORE

Permette di visualizzare i dati sintetici del processo di Valutazione già completato per una segnalazione, con un resoconto della cronologia delle operazioni effettuate.

8.Gestione Azioni correttive evento avverso

RUOLI: RESPONSABILE DI GESTIONE, SUPPORTO DI GESTIONE(*)

Permette di definire delle Azioni da svolgere a correzione/prevenzione dell'evento identificato da una segnalazione, specificando un elenco di attività da svolgere (con calendarizzazione) e l'utente responsabile del procedimento, più l'insieme dei relativi utenti interessati al suddetto. Sono inoltre possibili meccaniche di aggiornamento e/o sostituzione totale di eventuali Azioni già definite ed in corso d'opera.

(*) limitato all'inserimento di sole proposte di Azioni, sottoposte ad accettazione degli utenti Ruolo RESPONSABILE DI GESTIONE.

9.Visualizzazione Azioni correttive evento avverso

RUOLI: RESPONSABILE DI GESTIONE, SUPPORTO DI GESTIONE

Permette di visualizzare i dati sintetici delle Azioni associate ad una segnalazione, che siano già completate oppure no.

10.Chiusura segnalazione

RUOLI: RESPONSABILE DI GESTIONE, SUPPORTO DI GESTIONE(*)

Permette di avviare il procedimento di Chiusura della gestione di una segnalazione, per quelle che non prevedono Azioni assegnate o che siano completate totalmente. Come ultimo step è consentito il ritorno in lavorazione o la chiusura definitiva.

(*) limitato all'inserimento di sole proposte di Chiusura, sottoposte ad accettazione degli utenti Ruolo RESPONSABILE DI GESTIONE.

Azioni Correttive/Preventive

RUOLI: RESPONSABILE DI GESTIONE, SUPPORTO DI GESTIONE, SUPERVISORE

Sezione dedicata alla gestione e monitoraggio delle azioni correttive/preventive e delle relative attività di miglioramento che le contraddistinguono in riferimento alle rispettive segnalazioni su cui ha visibilità un utente.

È possibile visualizzare l'elenco completo delle azioni inserite in tre formati grafici differenti:

- TABELLARE, in cui i dati delle azioni sono visualizzate in forma tabellare con rappresentazioni numeriche
- PLANNING, in cui le azioni sono formattate come un diagramma di Gantt
- CALENDARIO, in cui le azioni sono formattate su una visione a calendario

Sono previste le seguenti funzionalità:

1. Gestione Azioni non completate
2. Visualizzazione Azioni non completate
3. Gestione Attività di miglioramento
4. Visualizzazione Azioni completate

1.Gestione Azioni non completate

RUOLI: RESPONSABILE DI GESTIONE, SUPPORTO DI GESTIONE(*)

Permette di definire delle Azioni da svolgere a correzione/prevenzione di un evento inserito nel sistema, specificando un elenco di attività da svolgere (con calendarizzazione) e l'utente responsabile del procedimento, più l'insieme dei relativi utenti interessati al suddetto. Sono inoltre possibili meccaniche di aggiornamento e/o sostituzione totale di eventuali Azioni già definite ed in corso d'opera, qual ora sia rilevata la necessità di variare/rettificare quanto precedentemente previsto.

(*) limitato all'inserimento di sole proposte di nuove Azioni, sottoposte ad accettazione degli utenti Ruolo RESPONSABILE DI GESTIONE.

2.Visualizzazione Azioni non completate

RUOLI: SUPERVISORE

Permette la sola visione dei dettagli delle Azioni non completate

3.Gestione Attività di miglioramento

RUOLI: RESPONSABILE DI GESTIONE

Permette di chiudere le Attività di miglioramento per ciascuna Azione, rendicontando l'esito con la possibilità di caricamento di evidenze documentali.

4.Visualizzazione Azioni completate

RUOLI: RESPONSABILE DI GESTIONE, SUPPORTO DI GESTIONE, SUPERVISORE

Permette di visualizzare l'elenco completo delle Azioni inserite e già completate nel sistema, consultandone tutti i dettagli.

Relazione Consuntiva Rischio Clinico

RUOLI: RESPONSABILE DI GESTIONE, SUPPORTO DI GESTIONE

Sezione dedicata alla generazione di un documento di tipo Relazione Consuntiva Rischio Clinico per un determinato presidio su cui ha visibilità un utente, riportante i dati correntemente memorizzati nel sistema, in un intervallo di tempo selezionabile, l'analisi degli stessi e la rendicontazione e la programmazione delle attività specifiche del processo. Il documento viene generato sulla base di un template (layout grafico, struttura, paragrafi) già integrato nel sistema.

Prima di creazione e download del documento, l'utente ha la possibilità di modificare manualmente alcuni testi e dati numerici riportati.

Relazione Consuntiva ICA

RUOLI: RESPONSABILE DI GESTIONE, SUPPORTO DI GESTIONE

Sezione dedicata alla generazione di un documento di tipo Relazione Consuntiva ICA per un determinato presidio su cui ha visibilità un utente, riportante i dati correntemente memorizzati nel sistema relativamente alle Infezioni Correlate all'Assistenza (ICA), in un intervallo di tempo selezionabile, l'analisi delle stesse e la rendicontazione e la programmazione delle attività specifiche del processo. Il documento viene generato sulla base di un template (layout grafico, struttura, paragrafi) già integrato nel sistema.

Prima di creazione e download del documento, l'utente ha la possibilità di modificare manualmente alcuni testi e dati numerici riportati.

Relazione Consuntiva Eventi

RUOLI: RESPONSABILE DI GESTIONE, SUPPORTO DI GESTIONE

Sezione dedicata alla generazione di un documento di tipo Relazione Consuntiva Eventi Avversi (in accordo con la Legge Gelli) per un determinato presidio su cui ha visibilità un utente, riportante i dati correntemente memorizzati nel sistema relativamente a tutti gli eventi avversi, in un intervallo di tempo selezionabile, l'analisi degli stessi. Il documento viene generato sulla base di un template (layout grafico, struttura, paragrafi) già integrato nel sistema.

Prima di creazione e download del documento, l'utente ha la possibilità di modificare manualmente alcuni testi e dati numerici riportati.

Notifiche

RUOLI: RESPONSABILE DI GESTIONE, SUPPORTO DI GESTIONE, GESTORE PRIVACY

Di seguito sono indicate le notifiche generate dal modulo, con i *Ruoli* degli utenti destinatari e relativi parametri di funzionamento:

TITOLO	TRIGGER DI ATTIVAZIONE	DISTANZA DA TRIGGER	RUOLI UTENTI DESTINATARI	ITERATIVA (*)	COPIA EMAIL
Segnalazione con possibile evento sentinella non letta	Ricezione segnalazione contenente parole chiavi Sentinella	0 giorni (tempo reale)	PRI (con visibilità su segnalazione)	✗	✓
Segnalazione non letta	Ricezione segnalazione non contenente parole chiavi Sentinella	1 giorni	PRI (con visibilità su segnalazione)	✗	✓
Avviso Segnalazione con possibile evento sentinella non letta	Ricezione segnalazione contenente parole chiavi Sentinella	7 giorni	PRI (con visibilità su segnalazione)	✓	✓
Avviso Segnalazione non letta	Ricezione segnalazione non contenente parole chiavi Sentinella	7 giorni	PRI (con visibilità su segnalazione)	✓	✓
Avviso Segnalazione con possibile evento sentinella non pseudonimizzata	Lettura segnalazione contenente parole chiavi Sentinella	7 giorni	PRI (con visibilità su segnalazione)	✓	✓

Avviso Segnalazione non pseudonimizzata	Lettura segnalazione non contenente parole chiavi Sentinella	14 giorni	PRI (con visibilità su segnalazione)	✓	✓
Avviso Segnalazione con possibile evento sentinella non classificata	Pseudonimizzazione segnalazione contenente parole chiavi Sentinella	7 giorni	RDG, SDG (con visibilità su segnalazione)	✓	✓
Avviso Segnalazione non classificata	Pseudonimizzazione segnalazione non contenente parole chiavi Sentinella	14 giorni	RDG, SDG (con visibilità su segnalazione)	✓	✓
Avviso Segnalazione di evento sentinella non valutata	Prima classificazione segnalazione contenente parole chiavi Sentinella	3 giorni	RDG, SDG (con visibilità su segnalazione)	✓	✓
Avviso Segnalazione non valutata	Prima classificazione segnalazione non contenente parole chiavi Sentinella	14 giorni	RDG, SDG (con visibilità su segnalazione)	✓	✓
Proposta valutazione Segnalazione	Inserimento proposta di valutazione segnalazione da SGR	0 giorni (tempo reale)	RDG (con visibilità su segnalazione)	✗	✓
Proposta gestione Segnalazione	Inserimento proposta di azione correttiva da SGR	0 giorni (tempo reale)	RDG (con visibilità su segnalazione)	✗	✓
Richiesta chiusura Segnalazione	Click su pulsante Avvia chiusura in Gestione Segnalazioni->Chiusura	14 giorni	RDG (con visibilità su segnalazione)	✓	✓
Attività di Azione Correttiva in avvicinamento	Data di inizio attività in azione correttiva	-3 giorni	RDG, SDG (solo utenti selezionati come Responsabile Azione, Responsabile Attività, Interessati all'Azione)	✓	✓
Attività di Piano di Miglioramento in avvicinamento	Data di inizio attività in piano di miglioramento	-3 giorni	RDG, SDG (solo utenti selezionati come Responsabile Piano, Responsabile Attività, Interessati al Piano)	✓	✓

NOTA(*): *Una notifica "iterativa" si ripete nel tempo ad intervalli regolari, stabiliti dal valore DISTANZA DA TRIGGER, finché la condizione TRIGGER DI ATTIVAZIONE resta soddisfatta.*

WebApp di Segnalazione Evento Avverso

RUOLI: NON DIPENDENTE DA RUOLI

WebApp specifica dedicata all'invio di una segnalazione di possibile evento avverso nel sistema, a cui soltanto gli operatori in possesso di un Codice Operatore inserito nel sistema ed abilitato (da un utente ruolo *Responsabile di Gestione*) possono accedere.

I dati che è possibile specificare nella segnalazione sono almeno i seguenti:

- Presidio di riferimento
- Reparto di riferimento
- Nominativo segnalatore
- Qualifica segnalatore
- Data/ora di accadimento evento
- Luogo di accadimento
- Tipologia di prestazione

- Descrizione dell'accadimento
- Testimonianze sull'accadimento
- Checklist Fattori contribuenti all'evento (multi-selezione)
- Checklist Fattori riducenti l'esito dell'evento (multi-selezione)
- Suggerimenti per la prevenzione dell'evento.

Le segnalazioni possono essere inviate anche in forma anonima nel pieno rispetto della normativa GDPR.

Risorse cloud riservate

Quantità di risorse garantite

La licenza acquistata per il **modulo GRC** garantisce all'Organizzazione licenziata una predeterminata quantità di risorse cloud riservate in base alla quantità di presidi considerati nella licenza, con possibilità di espansione previa acquisto di pacchetti appositi.

Nella tabella successiva sono riepilogate le tipologie di risorse e le quantità garantite dal **modulo GRC**:

RISORSA	QUANTITÀ PER PRESIDIO (*)
SPAZIO DISCO	5 GB
ACCESSI UTENTE	N. 4

NOTA(*): *Il totale garantito per ciascuna risorsa è il risultante della formula RISORSA_MODULO_GRC = QUANTITÀ PER PRESIDIO x N_PRESIDI_LICENZIATI.*

Esempio: Licenza multipresidio n.5 presidi, n.2 moduli (modulo GRC + altro modulo)

- *SPAZIO_DISCO_MODULO_GRC = 5 GB x n.5 presidi = 25 GB*
- *ACCESSI_UTENTE_MODULO_GRC = n. 4 accessi utente * n.5 presidi = N. 20 ACCESSI UTENTE*

Modalità di condivisione risorse garantite

Le risorse garantite dalla licenza acquistata per il **modulo GRC** sono soggette a predeterminati vincoli che ne abilitano/disabilitano la condivisione tra i presidi all'interno del modulo e tra i moduli della stessa.

Nella tabella successiva sono riepilogate le modalità di condivisione delle suddette risorse:

RISORSA	CONDIVISIONE PRESIDI (*)	CONDIVISIONE MODULI (**)
SPAZIO DISCO	✗	✗
ACCESSI UTENTE	✓	✓

NOTA(*): *Una condivisione non abilitata significa che l'utilizzo della risorsa è vincolato per ciascun presidio e la quantità singola è calcolata secondo la formula RISORSA_SINGOLO_PRESIDIO = RISORSA_MODULO_GRC /*

N_PRESIDI_LICENZIATI; una condivisione abilitata significa che l'utilizzo della risorsa è condiviso tra tutti i presidi licenziati per il modulo e la quantità è equivalente a RISORSA_MODULO_GRC.

***NOTA(**):** Una condivisione abilitata significa che l'utilizzo della risorsa è condiviso con gli altri moduli, e la quantità si somma alle quantità garantite dagli altri moduli secondo la formula RISORSA_MODULI = RISORSA_MODULO_GRC + RISORSA ALTRI MODULI.*

Esempio: Licenza multipresidio n.5 presidi, n.2 moduli (modulo GRC + altro modulo)

- *SPAZIO_DISCO_SINGOLO_PRESIDIO = 25 GB / n.5 presidi = 5 GB*
- *ACCESSI_UTENTE_MODULI = N. 20 ACCESSI UTENTE (da modulo GRC) + N. 20 ACCESSI UTENTE (ipotizzati da altro modulo) = 40 ACCESSI UTENTE*

Aggiornamenti

Il **modulo GRC** viene aggiornato esclusivamente secondo le necessità e le tempistiche individuate da HIT. Le specifiche riportate nel presente documento sono soggette a variazione senza alcun preavviso.

MATRICI DI RIEPILOGO FUNZIONALITÀ

Matrice Licenze-Funzionalità del Sistema

FUNZIONALITÀ DIPENDENTI DA TIPO LICENZA	LICENZA STANDARD	LICENZA MANAGER
ANAGRAFICA AZIENDE/PRESIDI	✗	✓
ANAGRAFICA REPARTI IN PRESIDI	✗	✓
ANAGRAFICA UTENTI	✗	✓
ANAGRAFICA ACCESSI UTENTE AL SISTEMA	✗	✓
CREAZIONE ACCESSI UTENTE AL SISTEMA – IN AUTONOMIA (SYSTEM ADMINISTRATOR)	✗	✓
CREAZIONE ACCESSI UTENTE AL SISTEMA – SU RICHIESTA	✓	✗
CREAZIONE ACCESSI UTENTE AL SISTEMA PER PRESIDIO	✓	✓
CREAZIONE ACCESSI UTENTE AL SISTEMA PER REPARTO (*)	✗	✓
INTEGRAZIONE FUNZIONALE CON DATI DA ALTRI MODULI (*)	✓	✓
PERSONALIZZAZIONE PARAMETRI NOTIFICHE (*)	✗	✓
PERSONALIZZAZIONE MAPPATURA TIPOLOGICA DOCUMENTI INCREMENTALE (*)	✗	✓
PERSONALIZZAZIONE GRAFICA BANNER DASHBOARD	✗	✓
NUMERO DI PRESIDI LICENZIABILI	**1-7**	**≥ 5**

(*) la funzionalità potrebbe non essere disponibile per tutti i Moduli

Matrice Ruoli-Funzionalità del Modulo

FUNZIONALITÀ DIPENDENTI DA RUOLO UTENTE – MODULO GRC	RDG	SDG	PRI	SUP
CONFIGURAZIONE PARAMETRI MODULO	✓	✗	✗	✗
VISUALIZZAZIONE RIEPILOGO UTENTI CON ACCESSO MODULO	✓	✗	✗	✗
VISUALIZZAZIONE RESOCONTO SEGNALAZIONI	✓	✓	✓	✓
VISUALIZZAZIONE ELENCO SEGNALAZIONI	✓	✓	✓	✓
PSEUDONIMIZZAZIONE DATI SEGNALAZIONE	✗	✗	✓	✗
CLASSIFICAZIONE SEGNALAZIONE	✓	✓	✗	✗
VALUTAZIONE EVENTO AVVERSO	✓	✗	✗	✗
VALUTAZIONE EVENTO AVVERSO - PROPOSTA	✗	✓	✗	✗
GESTIONE AZIONI CORRETTIVE SINGOLO EVENTO AVVERSO	✓	✗	✗	✗
GESTIONE AZIONI CORRETTIVE SINGOLO EVENTO AVVERSO - PROPOSTA	✗	✓	✗	✗

CHIUSURA SEGNALAZIONE	✓	✗	✗	✗
CHIUSURA SEGNALAZIONE - PROPOSTA	✗	✓	✗	✗
GESTIONE AZIONI CORRETTIVE GENERALE	✓	✓	✗	✗
GENERAZIONE RELAZIONE CONSUNTIVA RISCHIO CLINICO	✓	✓	✗	✗
GENERAZIONE RELAZIONE CONSUNTIVA ICA	✓	✓	✗	✗
GENERAZIONE RELAZIONE CONSUNTIVA EVENTI	✓	✓	✗	✗
NOTIFICHE	✓	✓	✓	✗
INVIO SEGNALAZIONE POSSIBILE EVENTO AVVERSO	**SOLO TRAMITE CODICE OPERATORE**			