



	ISTRUZIONI OPERATIVE		IO01/Protocollo 7
	GESTIONE DELLE SEGNALAZIONI WHISTLEBLOWING		Rev. Dicembre 2023
			Pag. 1 di 14

Indice

1. SCOPO.....	2
2. RESPONSABILITÀ	2
3. FLUSSO DEI DATI.....	2
4. MODALITÀ OPERATIVE	3
5. CARATTERISTICHE DEL SOFTWARE	13
6. DOCUMENTAZIONE DI RIFERIMENTO	14

Rev	Data	Descrizione	Redatto		Approvato	
0	Dicembre 2023	Prima Emissione	RSI		DSGTL	

	ISTRUZIONI OPERATIVE	IO01/Protocollo 7
	GESTIONE DELLE SEGNALAZIONI WHISTLEBLOWING	Rev. Dicembre 2023
		Pag. 2 di 14

1. SCOPO E GENERALITA'

La presente IO è redatta allo scopo di descrivere le caratteristiche generali e le funzionalità della piattaforma SignalEthic per l'invio e la gestione delle segnalazioni Whistleblowing ex art. 4 e 5 d.lgs. 24 del 2023 ed è parte integrante del protocollo 07 del Modello di Organizzazione Gestione e Controllo d.lgs. 231/01 adottato da FSR.

Il processo di gestione delle segnalazioni, comunemente chiamato Whistleblowing, ha lo scopo di promuovere e facilitare la segnalazione da parte di dipendenti e collaboratori, di illeciti presunti e/o perpetrati, commessi all'interno della struttura.

Il processo di inserimento e gestione della segnalazione è stato progettato per permettere di tutelare la riservatezza del soggetto segnalante consentendo, al contempo, l'indagine e l'approfondimento della segnalazione stessa.

2. DESTINATARI E RESPONSABILITÀ

- **Utente segnalante:** è il soggetto intenzionato ad effettuare la segnalazione; a tal fine segue le istruzioni riportate in questa IO.
- **Gestore delle segnalazioni:** è il soggetto incaricato da parte del titolare (FSR) di acquisire e gestire le segnalazioni; ai fini dell'utilizzo del sistema, segue le indicazioni riportate in questa IO.
- **Responsabile Sistemi Informativi:** configura e assegna l'utenza al gestore e verifica il funzionamento dell'applicazione interagendo con la Software House per le incombenze del caso.
- **Direttore Servizi Generali Tecnici e Logistici:** supervisiona il sistema nel suo complesso, verificandone, anche con il contributo dei consulenti e del DPO, le caratteristiche di appropriatezza e la funzionalità.

3. FLUSSO DEI DATI

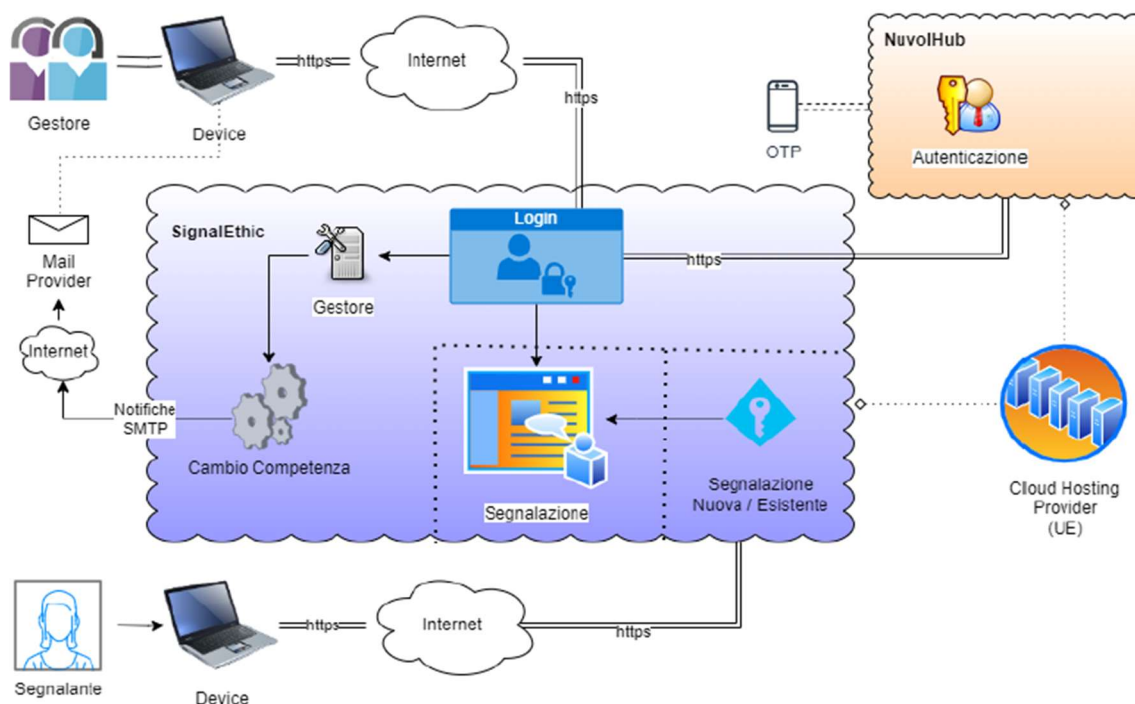
Il whistleblower può inoltrare una segnalazione in modo del tutto anonimo, se desidera, non è infatti richiesta alcuna registrazione. La segnalazione e l'eventuale esito possono essere consultati dal whistleblower esclusivamente accedendo al sistema mediante il codice numerico e password generati all'atto della conclusione dell'inserimento della segnalazione. Questo codice identifica tutta la documentazione connessa alla segnalazione in modo univoco e sicuro.

Il Gestore della segnalazione riceve un alert via mail in merito alla segnalazione ricevuta e mediante il sistema dà riscontro alla segnalazione.

Nel momento in cui il Gestore della segnalazione dà riscontro alla segnalazione di illecito, il suo autore riceverà in tempo reale un alert mediante email (se inserita) e potrà consultare il riscontro mediante il codice numerico generato durante la creazione.

	ISTRUZIONI OPERATIVE		IO01/Protocollo 7
	GESTIONE DELLE SEGNALAZIONI WHISTLEBLOWING		Rev. Dicembre 2023
			Pag. 3 di 14

Diagramma dell'architettura e del flusso dei dati



4. MODALITÀ OPERATIVE

4.1 COLLEGAMENTO ALLA PIATTAFORMA

Si accede alla piattaforma SignalEthic tramite browser Internet, collegandosi all'indirizzo <https://fondazione-sanitaericerca.signalethic.it> il cui link è disponibile anche nella pagina dedicata del sito aziendale. In ogni caso, come ulteriore misura di sicurezza del segnalante, l'accesso è possibile tramite qualsiasi dispositivo, personale e non.

4.2 INSERIMENTO DELLA SEGNALAZIONE

	ISTRUZIONI OPERATIVE		IO01/Protocollo 7
	GESTIONE DELLE SEGNALAZIONI WHISTLEBLOWING		Rev. Dicembre 2023
			Pag. 4 di 14

Dall'home page della piattaforma, cliccare su “Inserisci segnalazione” per accedere al Form on line per la compilazione e l'invio della segnalazione




Inserisci Segnalazione

IMPORTANTE: Questa pagina non fa parte del sito o dell'intranet di FONDAZIONE SANITÀ E RICERCA. Questa pagina si trova in un server protetto di Signalethic ospitato da Sanmarco Informatica S.P.A su infrastruttura AWS.

Non utilizzare questa pagina per reclami, comunicazioni, suggerimenti o ringraziamenti sui servizi sanitari e socio assistenziali di Fondazione Sanità e Ricerca. Consulta la pagina dedicata alle **segnalazioni** se hai necessità di inviare una segnalazione di tale fattispecie.

Clicca su “Inserisci segnalazione”, per inserire segnalazioni di fatti e circostanze consistenti che riguardano atti e/o fatti, omissioni, anche solo potenzialmente, contrari alla legge o alle normative interne della Fondazione e in particolare che ledono l'interesse pubblico e l'integrità della Fondazione stessa.

 **Inserisci Segnalazione**

Accedi a segnalazione **Riscatta credenziali**

Inserisci il numero segnalazione e la password ottenute in fase di inserimento segnalazione, al fine di integrarla o di verificarne gli aggiornamenti.

Numero Segnalazione

Password Segnalazione

Visualizza

Accedi come utente interno

Inserisci le credenziali personali per accedere come utente interno.

4.2.1 Resta Informato - opzionale

Nella sezione “Resta Informato”, nel caso in cui si vogliano ricevere aggiornamenti in tempo reale sullo stato della propria segnalazione, è possibile inserire il proprio personale indirizzo mail; sempre per maggior tutela del segnalante, è sconsigliato indicare la mail aziendale.

Resta informato - opzionale

Se vuoi ricevere aggiornamenti in tempo reale sullo stato della tua segnalazione, puoi inserire il tuo indirizzo mail.

All'atto dell'invio della segnalazione, verrà inviata una prima mail all'indirizzo inserito, al fine di verificarne l'autenticità. Tale indirizzo sarà utilizzato solo al fine di mantenere una comunicazione attiva e non sarà visibile da nessuno.

Tale scelta è completamente facoltativa poiché, in ogni caso, potrai rimanere aggiornato accedendo alla piattaforma attraverso il codice univoco e la password che ti verranno rilasciati dopo l'inserimento della segnalazione.

Se vuoi visualizzare l'informativa completa sul trattamento dei tuoi dati personali, clicca [qui](#).

Attenzione: Al fine di proteggere la tua privacy, ti consigliamo di inserire un indirizzo mail personale e non quello aziendale.

Indirizzo email

Ripeti l'indirizzo email

Lingua comunicazioni via email

Italiano

All'atto dell'invio della segnalazione, verrà inviata una prima mail all'indirizzo inserito, al fine di verificarne l'autenticità.

Tale indirizzo sarà utilizzato solo al fine di mantenere una comunicazione attiva e non sarà visibile da nessuno.

	ISTRUZIONI OPERATIVE	IO01/Protocollo 7
	GESTIONE DELLE SEGNALAZIONI WHISTLEBLOWING	Rev. Dicembre 2023
		Pag. 5 di 14

In qualsiasi momento il segnalante può modificare la e-mail inserita o annullare l'adesione a questa funzione.

4.2.2 La Tua Identità - *opzionale*

L'inserimento della segnalazione può essere fatto in maniera completamente ANONIMA, tuttavia, se si decide di non fare una segnalazione anonima, in questa sezione è possibile inserire nome, cognome e il tipo di rapporto che si ha con l'azienda a cui si sta inviando la segnalazione.

Se si decide di rivelare la propria identità, le informazioni saranno visibili solo al gestore della segnalazione per darvi seguito. In ogni caso, la propria identità non sarà rivelata a persone diverse dal gestore della segnalazione salvo un espresso consenso e nei casi previsti dalla normativa.

La tua identità - opzionale

L'immissione di una segnalazione può essere fatta in maniera **ANONIMA**.
Tuttavia, potrà successivamente esserti chiesto di identificarti, previo specifica motivazione da parte del gestore.
Se vuoi identificarti adesso - e quindi non fare una segnalazione anonima - inserisci il tuo nome e cognome e il tipo di rapporto che hai con l'ente a cui si sta rivolgendo la segnalazione.
Se decidi di rivelare la tua identità, tali informazioni saranno condivise con il gestore della tua segnalazione per darvi seguito.
In ogni caso, la tua identità non sarà rivelata a persone diverse dal gestore della segnalazione salvo un tuo espresso consenso e nei casi previsti dalla normativa.
Se vuoi visualizzare l'informativa completa sul trattamento dei tuoi dati personali, clicca [qui](#).

Il tuo nome e cognome

Tipo rapporto

- Dipendente
- Ex Dipendente
- Fornitore
- Altro

4.2.3 Altre Persone Coinvolte - *opzionale*

In questa sezione è possibile inserire i nomi di eventuali altre persone coinvolte (soggetto segnalato, altri soggetti a conoscenza, etc.).

Altre persone coinvolte - opzionale

Usa questa sezione se vuoi includere l'identità di una o più persone coinvolte nella segnalazione.

Attenzione: Le informazioni di seguito riguardano altre persone coinvolte nella segnalazione. Trattandosi di dati sensibili e personali, è tua responsabilità assicurarti che siano pertinenti e necessari. Tali informazioni saranno visibili solo al gestore della segnalazione, al fine di poter procedere con la pratica stessa.
Le informazioni inserite saranno protette e trattate come da informativa privacy (disponibile [qui](#)).

Nome e cognome

Nome e cognome

	ISTRUZIONI OPERATIVE	IO01/Protocollo 7
	GESTIONE DELLE SEGNALAZIONI WHISTLEBLOWING	Rev. Dicembre 2023
		Pag. 6 di 14

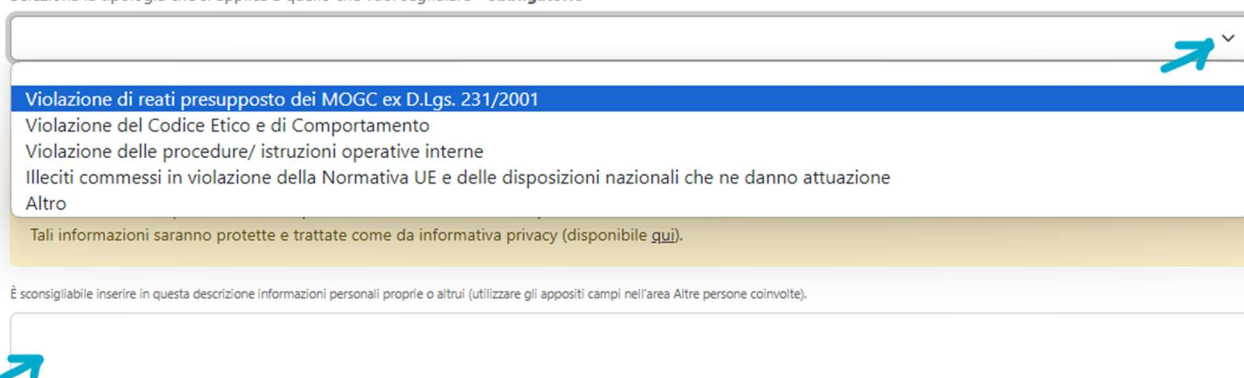
4.2.4 Oggetto della Segnalazione - *obbligatorio*

In questa sezione si deve selezionare la tipologia di segnalazione tra quelle presenti nel menu a tendina; questa scelta è obbligatoria e indirizzerà la segnalazione verso il gestore designato dall'Azienda.

Dopo avere selezionato la tipologia si deve obbligatoriamente inserire la descrizione del fatto che si sta segnalando.

Oggetto della segnalazione

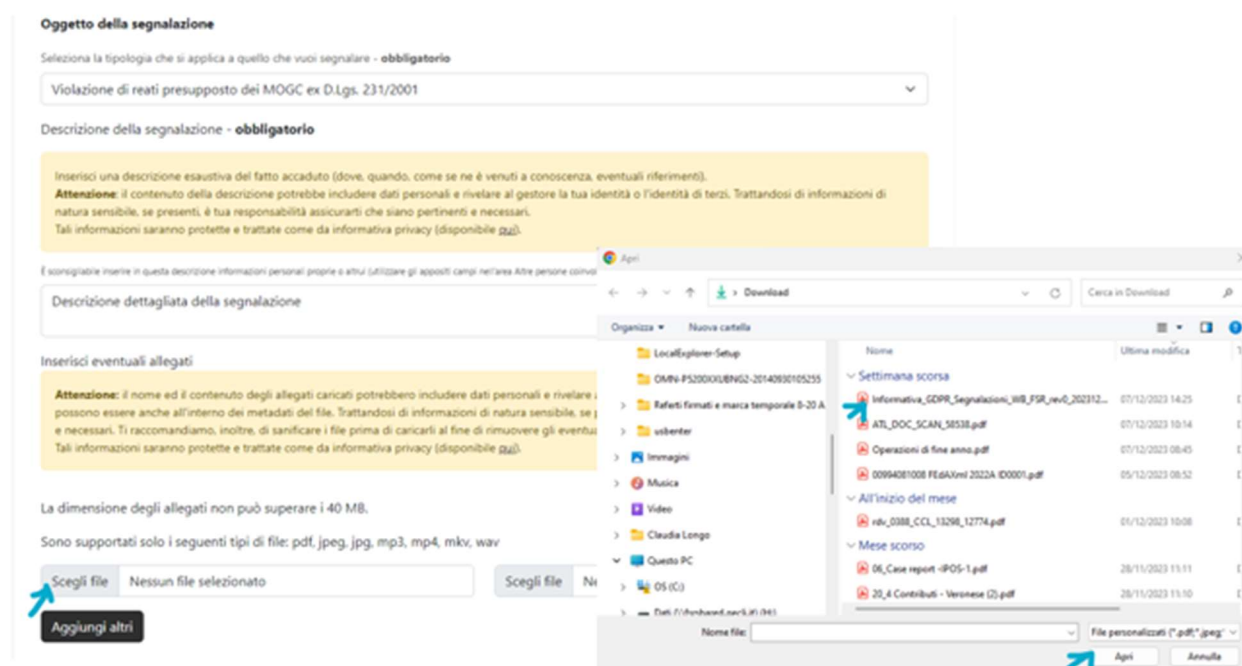
Seleziona la tipologia che si applica a quello che vuoi segnalare - **obbligatorio**



È sconsigliabile inserire in questa descrizione informazioni personali proprie o altrui (utilizzare gli appositi campi nell'area Altre persone coinvolte).

N.B. Si raccomanda di non inserire informazioni sensibili/personali non necessarie alla segnalazione, e di utilizzare gli appositi campi descritti sopra per esplicitare nomi e cognomi delle persone coinvolte.

Da questa sezione è inoltre possibile inserire eventuali allegati (pdf, jpeg, jpg, mp3, mp4, mkv, wav), la cui dimensione non può superare i 40 MB.



	ISTRUZIONI OPERATIVE	IO01/Protocollo 7
	GESTIONE DELLE SEGNALAZIONI WHISTLEBLOWING	Rev. Dicembre 2023
		Pag. 7 di 14

N.B. Il nome ed il contenuto degli allegati caricati potrebbero includere dati personali e rivelare al gestore la propria identità o l'identità di terzi. Tali informazioni possono essere anche all'interno dei metadati del file. Trattandosi di informazioni di natura sensibile, se presenti, è responsabilità del segnalante assicurarsi che siano pertinenti e necessari.

4.2.5 Invio della Segnalazione

Per poter procedere con l'invio della segnalazione, infine, è necessario leggere e confermare il disclaimer sulla generazione del codice segnalazione e relativa password.

Una volta confermata la presa visione del disclaimer, tramite apposito flag, cliccare su “Invia segnalazione” per procedere con l'invio.

Attenzione: All'invio della segnalazione verranno generati un codice segnalazione e la relativa password. Salva e mantieni queste informazioni poiché ti serviranno in seguito per poter accedere alla segnalazione inserita, verificarne lo stato o per eventuali integrazioni.

☒ Confermo di aver capito che ho bisogno di copiare il codice e la password della segnalazione se vorrò accedervi dopo che è stata inserita.

[Invia segnalazione](#)

4.2.6 Codice Segnalazione e relativa Password

A questo punto il sistema genera e rende disponibili a video due codici:

- Il numero della segnalazione appena inserita, generato dal sistema.
- La password di accesso alla segnalazione appena inserita.

Tramite l'apposita funzione “Copia negli appunti” è possibile copiare i due codici generati e incollarli su un file di testo per eventuali accessi futuri.

IMPORTANTE: Salva i seguenti dati per poter accedere successivamente alla tua segnalazione.

Numero Segnalazione
306706aa-5bf9-47fe-aeb5-9267bc058eca

Password segnalazione
C60qA-yHBjU-tPuk6

[Copia negli appunti](#) [Torna alla Home](#)

22AFE-0084(22AFE-008 * IT10762980588_X0080_ * Numero Segnalazione * +

File Modifica Visualizza

Numero Segnalazione: 306706aa-5bf9-47fe-aeb5-9267bc058eca
Password segnalazione: C60qA-yHBjU-tPuk6

4.2.7 Monitoraggio delle Segnalazioni Inserite

Dall'home page della piattaforma, nella sezione “Accedi a segnalazione”, inserire il numero della segnalazione che si intende monitorare e la relativa password di accesso, quindi cliccare su “Visualizza” per accedere al Form on line con i dati precedentemente inseriti.

Inserisci Segnalazione

IMPORTANTE: Questa pagina non fa parte del sito o dell'intranet di FONDAZIONE SANITÀ E RICERCA.

Questa pagina si trova in un server protetto di Signalethic ospitato da Sanmarco Informatica S.P.A su infrastruttura AWS.

Non utilizzare questa pagina per reclami, comunicazioni, suggerimenti o ringraziamenti sui servizi sanitari e socio assistenziali di Fondazione Sanità e Ricerca. Consulta la pagina dedicata alle **segnalazioni** se hai necessità di inviare una segnalazione di tale fattispecie.

Clicca su "Inserisci segnalazione", per inserire segnalazioni di fatti e circostanze consistenti che riguardano atti e/o fatti, omissioni, anche solo potenzialmente, contrari alla legge o alle normative interne della Fondazione e in particolare che ledono l'interesse pubblico e l'integrità della Fondazione stessa.

Inserisci Segnalazione

Accedi a segnalazione

Riscatta credenziali

Inserisci il numero segnalazione e la password ottenute in fase di inserimento segnalazione, al fine di integrarla o di verificarne gli aggiornamenti.

Numero Segnalazione

Password Segnalazione

Visualizza

Accedi come utente interno

Inserisci le credenziali personali per accedere come utente interno.

Username

mail@mail.com

Password

Password dimenticata

Accedi

4.4 DASHBOARD GESTORE

Eseguito il login, il gestore accede alla Dashboard dove può visualizzare l'elenco di tutte le segnalazioni presenti a sistema (nuove, in gestione e chiuse).

Per ciascuna segnalazione in elenco sono presenti i seguenti dati:

- numero della segnalazione;
- data di inserimento;
- tipologia;
- ultima attività;
- stato;
- azioni.

Tramite apposito filtro applicabile ai dati sopra elencati, è possibile eseguire ricerche trasversali tra le diverse segnalazioni.

NUOVE

5

IN GESTIONE

12

CHIUSE

Visualizza

Aggiungi segnalazione per conto del segnalatore

Cerca

Numero segnalazione	Data inserimento	Tipologia	Ultima attività	Stato	Apri
e3817e7d-3c65-4fbc-9409-cb1ce9138805	2023-09-27 11:14	Altro	2023-09-27 11:14	gestione 1	Apri
26f9b8b0-ee12-458b-927b-c66fa7ceebfa	2023-09-27 17:58	Altro	2023-09-27 18:03	In corso	Apri
d0a51b79-b49d-41ae-8f93-2a8a268492b7	2023-10-05 12:37	Illeciti penali o altre violazioni della legge	2023-10-05 12:37	In corso	Apri
5688163d-ebb6-4519-80f2-c26942137ab8	2023-09-28 15:49	Illeciti penali o altre violazioni della legge	2023-09-28 15:50	In corso	Apri
019f1674-4bc9-4689-9252-7846252879af	2023-10-05 12:08	Illeciti penali o altre violazioni della legge	2023-10-05 12:10	Richiesta	Apri
566b5dd8-0601-453d-9c34-6c16ce9327720	2023-10-05 12:43	Altro	2023-10-05 12:43	In corso	Apri
08b547ed-4457-486c-85ba-2eddb0b118726	2023-10-02 09:41	Divulgazione non autorizzata di informazioni riservate	2023-10-02 09:41	In corso	Apri
24aec377-8e4d-421a-87d7-7b2e65006609	2023-10-12 17:10	Illeciti penali o altre violazioni della legge	2023-10-12 17:10	In corso	Apri

Informativa privacy


Termini e condizioni

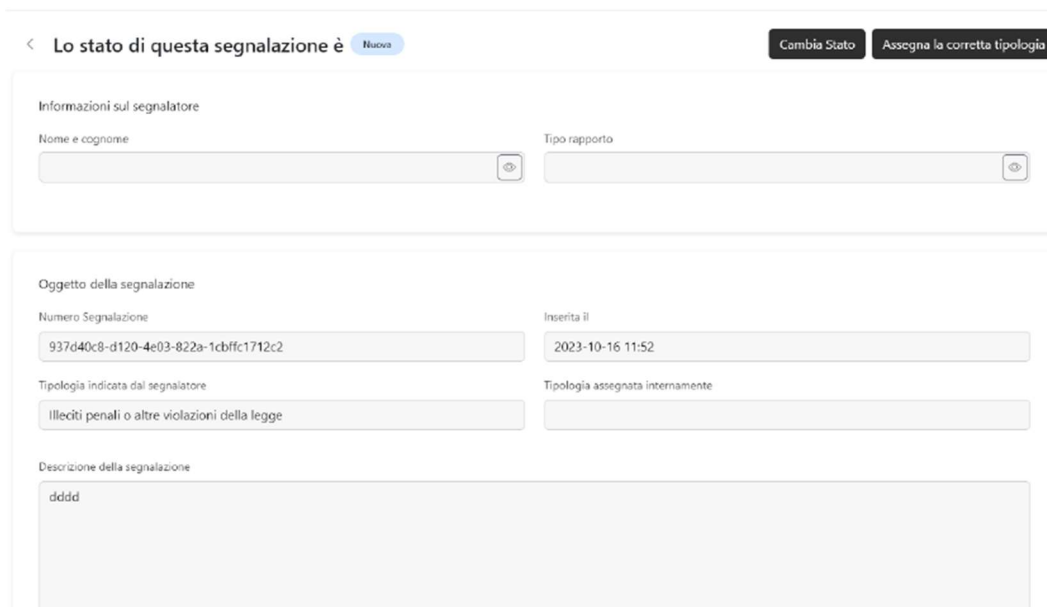
© 2023 Sanmarco Informatica. All rights reserved

Manuale segnalazioni

	ISTRUZIONI OPERATIVE		IO01/Protocollo 7
	GESTIONE DELLE SEGNALAZIONI WHISTLEBLOWING		Rev. Dicembre 2023
			Pag. 10 di 14

4.5 GESTIONE DELLA SEGNALAZIONE

Cliccando sul pulsante  si accede a tutti contenuti della singola segnalazione: informazioni obbligatorie (tipologia di segnalazione e descrizione della segnalazione), informazioni facoltative (dati del segnalante, tipo rapporto, altre persone coinvolte e allegati), numero della segnalazione e tipologia assegnata dal gestore.



Il gestore può effettuare le attività di seguito descritte.

4.5.1 Aggiornare lo stato

La segnalazione può assumere 3 diversi stati:

- nuova – non ancora presa in carico
- in gestione – presa in carico dal gestore
- chiusa – chiusa dal gestore



Il gestore modifica lo stato della segnalazione in base all'avanzamento della stessa. Il flusso di “cambio stato” segue la logica di risoluzione della segnalazione, perciò da “Nuova” passa a “In gestione” e successivamente allo stato “Chiusa”.

Il gestore ha la possibilità di definire ed applicare tempi di conservazione per tipologia di segnalazione oppure per singola segnalazione al fine di soddisfare i requisiti della limitazione della conservazione dei dati. Il periodo di conservazione configurato di default è di 5 anni.

	ISTRUZIONI OPERATIVE	IO01/Protocollo 7
	GESTIONE DELLE SEGNALAZIONI WHISTLEBLOWING	Rev. Dicembre 2023
		Pag. 11 di 14

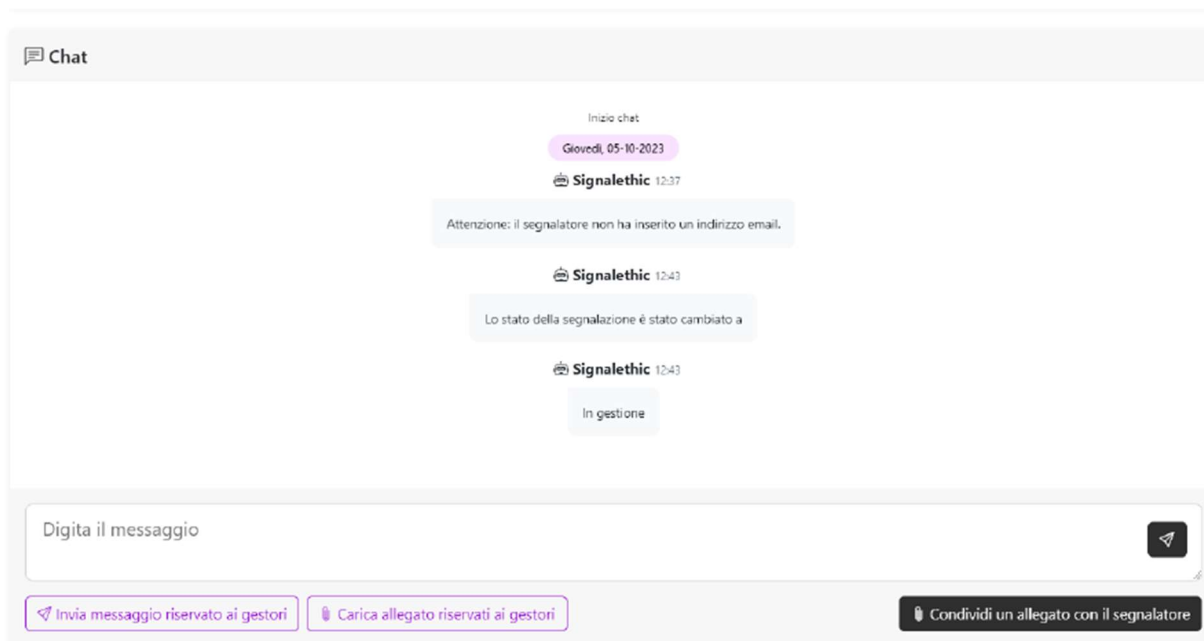
4.5.2 Assegnare la corretta tipologia

Il gestore può, se necessario, modificare la tipologia inserita dal segnalante. Questa riassegnazione interna, non visibile al segnalante, è utile per semplificare la gestione della segnalazione stessa.



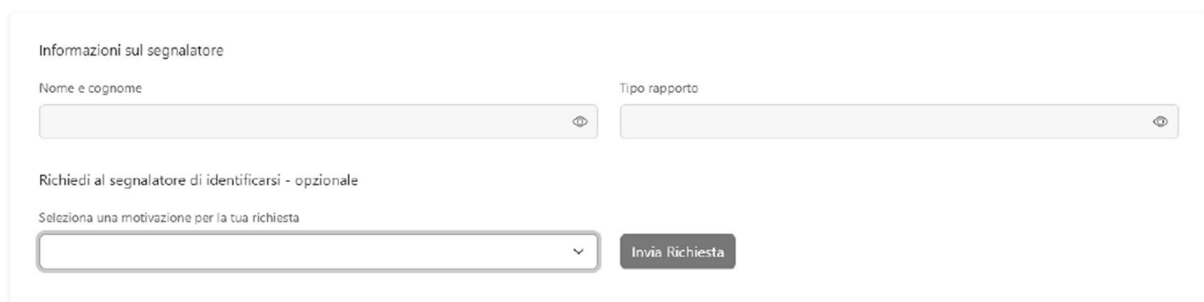
4.5.3 Attivare la Chat

Il gestore può scambiare dei messaggi con il segnalatore mediante l'utilizzo della chat, attivabile solo se lo stato della segnalazione è diverso da "Nuova" e "Chiusa".



4.5.4 Richiedere al segnalatore di identificarsi

Il gestore, nei casi eventualmente previsti dalla normativa di riferimento, può richiedere al segnalatore di identificarsi e dunque indicare nome, cognome e tipo rapporto.

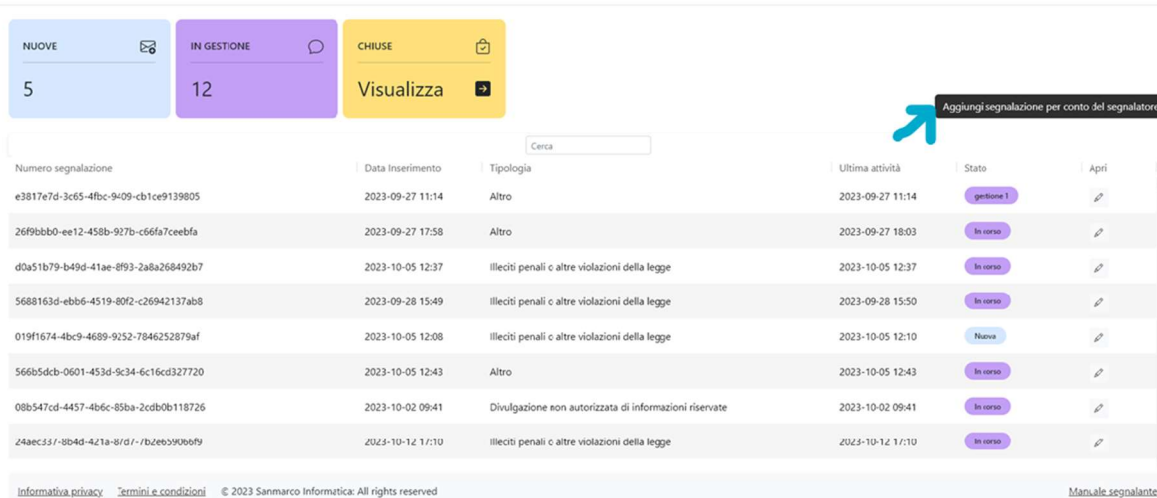


4.5.5 Chiudere una segnalazione

In fase di chiusura di una segnalazione viene richiesto di indicare un periodo di mantenimento del dato all'interno del sistema, dopo tale periodo la segnalazione verrà eliminata.

4.5.6 Inserimento della segnalazione per conto del segnalante

Il gestore può inserire la segnalazione per conto del segnalante, nei casi in cui questa sia stata effettuata tramite richiesta di un incontro in presenza con il gestore o tramite chiamata verso il gestore. L'inserimento avviene attraverso la funzione *“Aggiungi segnalazione”*.



NUOVE	IN GESTIONE	CHIUSE
5	12	Visualizza

Numero segnalazione	Data inserimento	Tipologia	Ultima attività	Stato	Apri
e3817e7d-3c65-4fbc-9409-cb1ce9139805	2023-09-27 11:14	Altro	2023-09-27 11:14	gestione 1	
26f9bb6b-ee12-458b-927b-c66fa7ceebfa	2023-09-27 17:58	Altro	2023-09-27 18:03	In corso	
d0a51b79-b49d-41ae-8f93-2a8a268492b7	2023-10-05 12:37	Illeciti penali e altre violazioni della legge	2023-10-05 12:37	In corso	
5688163d-ebb6-4519-80f2-c26942137ab8	2023-09-28 15:49	Illeciti penali e altre violazioni della legge	2023-09-28 15:50	In corso	
019f1674-4bc9-4689-9252-7846252879af	2023-10-05 12:08	Illeciti penali e altre violazioni della legge	2023-10-05 12:10	Nuova	
566b5dcb-0601-453d-9c34-6c16cd327720	2023-10-05 12:43	Altro	2023-10-05 12:43	In corso	
08b547cd-4457-4b6c-85ba-2cddb0b118726	2023-10-02 09:41	Divulgazione non autorizzata di informazioni riservate	2023-10-02 09:41	In corso	
24aec33f-bd4d-421a-81d1-fb2eb0906bf9	2023-10-12 17:10	Illeciti penali e altre violazioni della legge	2023-10-12 17:10	In corso	

[Informativa privacy](#)
[Termini e condizioni](#)
 © 2023 Sanmarco Informatica. All rights reserved
 [Manuale segnalante](#)

Il gestore deve indicare il canale di arrivo della segnalazione (chiamata telefonica o incontro in presenza) e inserire i dati indicati dal segnalante.

La schermata di inserimento segnalazione è identica a quella che il segnalante avrebbe utilizzato collegandosi al link dell'azienda.

Inserimento segnalazione per conto del segnalatore



Canale di arrivo

Seleziona un'opzione

Chiamata telefonica

Incontro in presenza

Al termine dell'inserimento il sistema rilascia un Token (codice a 16 cifre) che deve essere comunicato al segnalante per poter riscattare le credenziali della segnalazione.

Segnalazione inserita



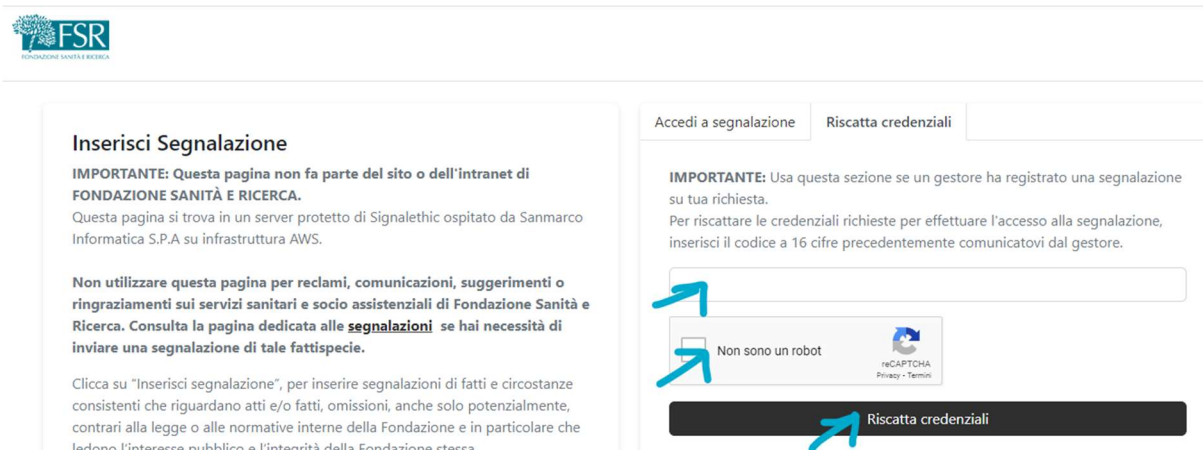
Nota bene: Comunica il seguente codice di 16 cifre al segnalante. Questo codice potrà essere utilizzato nella sezione **Riscatta credenziali** della Home page.

[16-digit token]

[Copia negli appunti](#)
[Torna alla Home](#)

	ISTRUZIONI OPERATIVE	IO01/Protocollo 7
	GESTIONE DELLE SEGNALAZIONI WHISTLEBLOWING	Rev. Dicembre 2023
		Pag. 13 di 14

Il segnalante (o il gestore, se espressamente richiesto dal segnalante) può riscattare le credenziali della segnalazione nell'apposita sezione;



Inserisci Segnalazione

IMPORTANTE: Questa pagina non fa parte del sito o dell'intranet di FONDAZIONE SANITÀ E RICERCA. Questa pagina si trova in un server protetto di Signalethic ospitato da Sanmarco Informatica S.P.A su infrastruttura AWS.

Non utilizzare questa pagina per reclami, comunicazioni, suggerimenti o ringraziamenti sui servizi sanitari e socio assistenziali di Fondazione Sanità e Ricerca. Consulta la pagina dedicata alle **segnalazioni** se hai necessità di inviare una segnalazione di tale fattispecie.

Clicca su "Inserisci segnalazione", per inserire segnalazioni di fatti e circostanze consistenti che riguardano atti e/o fatti, omissioni, anche solo potenzialmente, contrari alla legge o alle normative interne della Fondazione e in particolare che ledono l'interesse pubblico e l'integrità della Fondazione stessa.

Accedi a segnalazione Riscatta credenziali

IMPORTANTE: Usa questa sezione se un gestore ha registrato una segnalazione su tua richiesta. Per riscattare le credenziali richieste per effettuare l'accesso alla segnalazione, inserisci il codice a 16 cifre precedentemente comunicatoti dal gestore.

Non sono un robot

reCAPTCHA Privacy - Termini

Riscatta credenziali

Inserendo il Token e cliccando su “Riscatta credenziali” verranno fornite le credenziali della segnalazione.

5. CARATTERISTICHE DEL SOFTWARE

Signalethic di Sanmarco Informatica è una soluzione Cloud Based per la gestione delle segnalazioni Whistleblowing; il portale è accessibile tramite browser da qualsiasi device collegato ad internet e non richiede l'installazione di un client sul device del segnalante.

La parte applicativa della soluzione e il Backend database sono ospitati su servizi Cloud forniti da Amazon Web Services EMEA SARL (AWS).

I dati e l'applicativo sono conservati in due data center nella stessa Region EU-West-1 per finalità di data replica al fine di assicurare la resilienza e continuità del servizio.

I whistleblower accedono ai loro rapporti utilizzando codice segnalazione e relativa password che sono rispettivamente sequenze di 36 e 17 cifre generate casualmente dal Backend quando la segnalazione viene creata per la prima volta.

Per finalità di sicurezza, le comunicazioni inviate al segnalante via mail per informarlo che la propria segnalazione è stata aggiornata, includono solo il riferimento a SignalEthic e le ultime cifre del numero di segnalazione (per permettere al segnalante di identificare la specifica segnalazione). Non includono, quindi, nell'oggetto o nel corpo della mail il nome del segnalante, il nome dell'azienda o altre informazioni che potrebbero permetterne l'identificazione.

La registrazione e l'autenticazione degli utenti gestori della segnalazione avviene tramite la soluzione NuvolHub di Sanmarco Informatica, anche questa Cloud Based. L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali. Il sistema prevede l'utilizzo di password complesse con numero di caratteri da 8 a 16 e su base alfanumerica con requisito di utilizzo di numeri, lettere maiuscole, minuscole e caratteri speciali. Per impostazione predefinita, il sistema obbliga gli utenti a cambiare la propria password ogni 60 giorni. Le password non vengono mai archiviate in testo normale, ma il sistema mantiene solo un hash a riposo.

	ISTRUZIONI OPERATIVE	IO01/Protocollo 7
	GESTIONE DELLE SEGNALAZIONI WHISTLEBLOWING	Rev. Dicembre 2023
		Pag. 14 di 14

La piattaforma archivia le password degli utenti gestori tramite funzione di hash con un sale casuale, unico per ogni cifratura.

I dati delle segnalazioni, le password e gli allegati sono protetti tramite crittografia dei dati At Rest a livello di database ed In Transit.

SignalEthic registra le attività effettuate dagli utenti e dal sistema tramite un sistema di audit log sicuro e privacy preserving, al fine di assicurare la massima riservatezza richiesta dai processi di whistleblowing. I log delle attività del segnalante non includono informazioni identificative quali indirizzi IP e User Agent.

I sistemi sono soggetti a backup remoto giornaliero (tra le 22.00 e le 6.00 UTC) con policy di Data Retention di 7 giorni necessari per finalità di Business Continuity e Disaster Recovery.

6. DOCUMENTAZIONE DI RIFERIMENTO

- D.lgs. 24 del 2023
- SignalEthic - Brochure Tecnica.pdf
- Protocollo 07 del MOGC d.lgs. 231/01