



Segnalazione Illeciti P.A.  
**WHISTLEBLOWING**

**ALLEGATO TECNICO SEGNALAZIONI.NET**

Data di aggiornamento	Revisione
04/01/2018	3.0

## Sommario

---

<b>1</b>	<b>Introduzione</b>	<b>3</b>
1.1	Architettura	3
1.2	Flusso	4
1.3	Documentazione	4
<b>2</b>	<b>Tipologie di segnalatori e registrazione</b>	<b>5</b>
<b>3</b>	<b>Area Segnalatore - La segnalazione</b>	<b>6</b>
3.1	Nuova segnalazione utente non registrato	6
3.2	Accesso all'area riservata	9
3.3	Nuova Segnalazione utente registrato	10
3.4	Gestione della Segnalazione	11
<b>4</b>	<b>Area Responsabile/OdV - Gestione delle Segnalazioni</b>	<b>12</b>
4.1	Elenco segnalazioni	13
4.2	FASCICOLO DELLA SEGNALAZIONE	14
4.3	Dettaglio segnalazione	14
4.4	Messaggi	16
4.5	Note interne	17
4.6	Collaboratori	17
4.7	Messaggistica interna	17
<b>5</b>	<b>Segnalazioni cartacee o da altri canali</b>	<b>18</b>
<b>6</b>	<b>Multilingua</b>	<b>19</b>
<b>7</b>	<b>Statistiche</b>	<b>19</b>
<b>8</b>	<b>Logs</b>	<b>20</b>
<b>9</b>	<b>Sicurezza e riservatezza lato Software</b>	<b>21</b>
9.1	Caratteristiche tecniche del sistema di cifratura:	21
9.2	Flusso cifratura e decifratura per il segnalatore registrato	21
9.3	Flusso cifratura e decifratura per il segnalatore anonimo	22
9.4	Flusso cifratura e decifratura per il Responsabile e i Collaboratori	22
9.5	Cifratura dei log	22
9.6	Gestione della password in fase di sessione	22
9.7	Sostituzione Responsabile e smarrimento password	23
	<b>Servizi</b>	<b>24</b>
9.8	Installazione e configurazione (cronoprogramma)	24
9.9	Formazione delle risorse	25
9.10	Manutenzione e Assistenza	25
9.11	SLA (Service Level Agreement) garantiti	26

## 1 Introduzione

---

Il Whistleblowing è lo strumento messo a disposizione dei dipendenti (*Segnalatori*) e del Responsabile della Prevenzione della Corruzione (qui denominato per semplicità anche *Responsabile* o "RPCT") e/o dell'*Organismo di Vigilanza* ("OdV") di Enti o Aziende, finalizzato a gestire le segnalazioni di illeciti nell'ambito lavorativo.

In linea con il dettato normativo, **Segnalazioni.net** consente di regolamentare le procedure atte ad incentivare e proteggere le segnalazioni degli illeciti, permettendo agli operatori dell'Ente o dell'Azienda di inviare segnalazioni con la garanzia di estrema riservatezza.

Il segnalante o whistleblower può:

- Accedere in maniera riservata e sicura al sistema;
- Inserire le proprie segnalazioni tramite una procedura intuitiva e di facile compilazione;
- Comunicare con il Responsabile anticorruzione in maniera del tutto riservata, come da dettato normativo;
- Integrare le segnalazioni effettuate;
- Ricevere via Email un avviso di risposta alla propria segnalazione.

L'ambiente di amministrazione consente al Responsabile della Prevenzione della Corruzione (RPCT) o all'Organismo di Vigilanza (ODV) di:

- Ricevere via Email un avviso di presenza di segnalazione nel sistema;
- Accedere ad un'area riservata e prendere visione delle segnalazioni ricevute;
- Interagire con il segnalante e richiedere ulteriori informazioni o documenti, sempre preservandone l'identità;
- Monitorare e gestire la procedura in tutte le sue fasi, con la modifica dello stato della segnalazione (Nuova, Letta, In lavorazione, Archiviata, etc.);
- Interagire con i dirigenti responsabili;
- Possibilità di configurare il sistema in modo da avere più soggetti (RPCT e OdV, ad esempio) in grado di ricevere e gestire la segnalazione.

### 1.1 Architettura

---

Il servizio viene generalmente erogato in SaaS (Software as a Service), garantendo la terzietà del sistema, o in particolari strutture complesse, installato in un server del committente. Sono garantiti continui aggiornamenti di sicurezza del software ed efficienza dell'Help Desk dedicato. È quindi un software accessibile tramite la rete internet esclusivamente attraverso il protocollo HTTPS ed è ottimizzato per la visualizzazione su qualsiasi recente browser e qualsiasi dispositivo. Attraverso il protocollo HTTPS i dispositivi client si collegano ai server dedicati in maniera sicura. I dati relativi alla segnalazione vengono gestiti separatamente dalle utenze; tale separazione, in linea con le disposizioni normative assicura la totale riservatezza.

Il sistema è composto da un Front End dedicato ai Segnalatori, dal quale è possibile creare una segnalazione e intraprendere uno scambio di messaggi con il Responsabile, e da un Back End dedicato al Responsabile (ed eventualmente ad altri organismi preposti alla gestione delle segnalazioni, come ad esempio un Organo di Vigilanza o collaboratori incaricati). Attraverso il sistema vengono gestiti i fascicoli delle segnalazioni ed è possibile scambiare messaggi e documenti riservati con i segnalatori; è inoltre presente un canale dedicato alle comunicazioni tra tutti i soggetti preposti alla gestione delle segnalazioni (RPCT, Organismo di Vigilanza, collaboratori).

La piattaforma software può essere configurata in modo da gestire più soggetti responsabili (RPCT e OdV ad esempio) in grado di ricevere e gestire la segnalazione. In questo caso il Segnalatore ha la facoltà di scegliere a chi inoltrare la segnalazione, e gli stessi responsabili possono condividere le informazioni desiderate.



Figura 1 - Architettura

## 1.2 Flusso

Il Segnalatore, accedendo alla propria pagina personale, ha la possibilità di creare la segnalazione, inviarla al RPCT/OdV o ad entrambi, inserendo i dati ed eventuali allegati, in un secondo momento dopo la presa in carico da parte del *Responsabile* o dall'*OdV*, ha la possibilità di rispondere ad eventuali messaggi e seguire l'iter della propria segnalazione.

Il sistema provvede alla cifratura e alla memorizzazione della segnalazione separandola dall'identità del segnalatore e ad inviare una Email di notifica di nuova segnalazione al RPCT/OdV ed eventualmente su una di avvenuto invio al segnalatore stesso; tale Email non contiene nessun elemento della segnalazione, ma un codice hash che assicura l'originalità della segnalazione. L'invio delle Email è può essere disabilitato a discrezione del Committente.

La segnalazione viene presa in carico dal RPCT/OdV, che nella sua area riservata ha una serie di funzionalità per la gestione del **fascicolo della segnalazione**, tra le quali:

- inserimento degli stati di lavorazione
- invio e ricezione di messaggi con il segnalatore
- possibilità di assegnare la segnalazione ad un collaboratore
- possibilità di condividere o riassegnare la segnalazione ad un altro soggetto come ad esempio l'OdV/RPCT
- possibilità di inviare e ricevere messaggi con un collaboratore nell'ambito della segnalazione

Ad ogni risposta/messaggio il sistema invia un promemoria via Email ad entrambi gli utenti (RPCT/OdV e segnalatore e se coinvolto il collaboratore). Se richiesto è possibile disabilitare l'invio delle Email.

## 1.3 Documentazione

All'interno del software è presente un manuale operativo. L'interfaccia è estremamente intuitiva grazie all'utilizzo di elementi grafici di facile interpretazione e di diffuso utilizzo. La procedura inoltre è stata studiata per avere un flusso logico ed estremamente intuitivo.

## 2 Tipologie di segnalatori e registrazione

Il sistema prevede la gestione di due tipologie di segnalatori:

1. Utenti non registrati, che possono inviare e visualizzare una segnalazione anche senza utilizzare un account.
2. Utenti registrati, che accedono ad un account per l'invio e la visualizzazione della segnalazione.

Inoltre il sistema consente due modalità di registrazione dei segnalatori, attuabili anche congiuntamente:

1. il segnalatore si registra al sistema in maniera indipendente
2. il segnalatore viene registrato da un amministratore di sistema

Nel primo caso il segnalatore segue una breve procedura di registrazione nella quale deve allegare un documento di identità e compilare e firmare una autocertificazione.

The screenshot shows a registration form titled "REGISTRAZIONE UTENTE". It includes the following fields and sections:

- Username \* (with a "Genera" button)
- Email \*
- Password \*
- Verifica \*
- Nome \*
- Cognome \*
- Autocertificazione identità \* (with a link to "Modello autocertificazione" and a file upload field "Nessun file Allegato" and "Allega" button)
- Carta d'identità (with a file upload field "Nessun file Allegato" and "Allega" button)
- A blue "Registra" button at the bottom right.

Figura 2 – Registrazione utente

Una volta inviata la richiesta, il sistema invia una email all'indirizzo indicato con un link per l'attivazione del profilo.

La seconda modalità invece prevede che l'amministratore della piattaforma inserisca gli utenti da un apposito pannello di gestione. In fase di startup del sistema, tale operazione viene effettuata dalla DigitalPA. Successivamente l'amministratore del sistema può inserire autonomamente nuove utenze o disabilitare quelle non più necessarie. Tale attività può essere affidata con un servizio aggiuntivo alla DigitalPA.

È possibile usufruire di entrambe le opzioni o disabilitarne una.

## 3 Area Segnalatore - La segnalazione

Per poter effettuare la segnalazione è necessario accedere alla home page:



Figura 3 – Home Page

È possibile configurare il software in modo da consentire le segnalazioni solo ad utenti registrati, solo ad utenti non registrati, oppure attivare entrambe le possibilità.

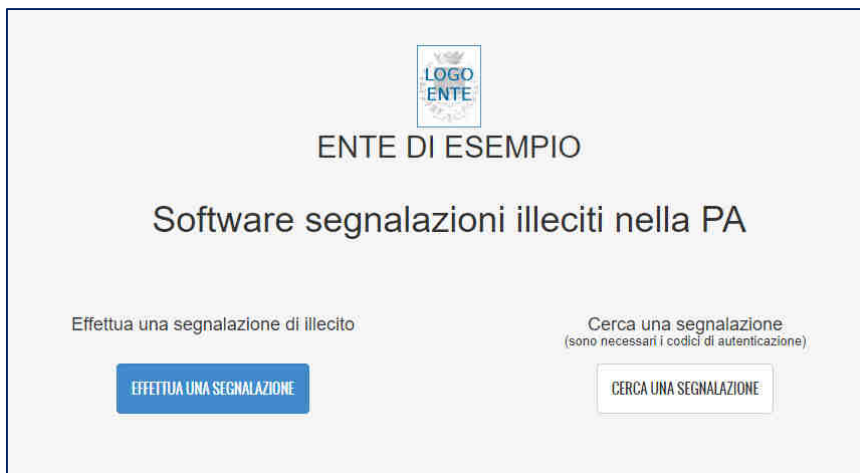
Cliccando su “Accedi”, si apre la schermata di login descritta in seguito, dove l’utente segnalatore, attraverso le proprie credenziali, può accedere all’area riservata per creare la segnalazione o seguirne l’iter. Cliccando su “Registrati”, il segnalatore può invece crearsi un account tramite il quale inviare e gestire una o più segnalazioni.

Cliccando sul pulsante “segnalazioni altri soggetti”, il segnalatore può inviare una segnalazione senza dover accedere ad un profilo registrato.

Nel pannello di gestione del responsabile queste due tipologie vengono contraddistinte graficamente con icone differenti.

### 3.1 Nuova segnalazione utente non registrato

Il segnalatore “non registrato” può inviare una segnalazione senza necessità di registrarsi; durante la compilazione vengono richiesti, in due campi opzionali, il nome e cognome del segnalatore. Tale dato sarà accessibile al Responsabile solo tramite la procedura di visualizzazione dell’identità del segnalante, descritta in seguito. Prima dell’invio della segnalazione è previsto un reCaptcha tramite il quale l’utente deve attestare di “non essere un robot”.



### SEGNALAZIONE

**Responsabile \***

RPCT (Responsabile Prevenzione Corruzione e Trasparenza)

OdV (Organismo di Vigilanza)

RPCT e OdV

**Oggetto \***

**Natura illecito \***

**Autori illecito \***

**Persone Coinvolte**


**Unità Organizzativa (Servizio, Area, Reparto, etc.) \***

**Luoghi in cui si sono consumati gli illeciti \***

**Data presunta Inizio Illeciti**

**Data Fine Illeciti**

**Messaggio \***

 **Allega**

risultati allegato


**Informazioni facoltative**

**Nome**

**Cognome**

Non sono un ente? [Autorizza il sistema a rivelare la tua identità?](#)

\* Si ricorda che l'unico soggetto autorizzato alla visualizzazione dell'identità del segnalante (ovvero l'opportunità di pubblicazione) è esclusivamente il Responsabile per la Prevenzione della Corruzione, autorizzando a rivelare la propria identità, questo potrà essere riferito solo in caso di assoluta necessità e al fine di indagini esclusivamente ad eventuali altro responsabile (o superiore gerarchico); il sistema sarà comunque tenuto a garantire la massima riservatezza ai sensi dell'art. 54 bis del D.Lgs. n. 155 del 30 marzo 2001

Non sono un ente?


Salva e Invia

Figura 4 – Segnalazione utente non registrato

Una volta inviata la segnalazione il sistema rilascia dei codici univoci (token), che devono essere salvati e conservati dal segnalatore per poter accedere alla segnalazione, seguirne l'iter e accedere alla messaggistica del sistema.

✔ Segnalazione inserita correttamente

Si prega di memorizzare scrupolosamente il codice segnalazione e la password associata. Le credenziali saranno indispensabili per accedere successivamente. Attenzione: In caso di smarrimento non sarà più possibile accedere alla Segnalazione.

Codice segnalazione:	XGOUNPZ5D8WEZATZPMUTK
Password:	6KRGORYO3TGNWWWIV2WGS

Figura 5 – Token Segnalazione utente non registrato

### RECUPERA SEGNALAZIONE

⚠
Recupera Segnalazione

Codice Segnalazione:

Password \*

Figura 6 – Ricerca segnalazione tramite token



### 3.2 Accesso all'area riservata

---

Attraverso la pagina di Login (comune sia all'utente Segnalatore registrato che all'utente Responsabile) si esegue l'accesso alla piattaforma per la gestione delle segnalazioni.

Ciascun utente effettua l'accesso attraverso l'inserimento delle proprie credenziali:

- ✓ Username: l'indirizzo Email utilizzato per la registrazione
- ✓ Password: la password associata allo username

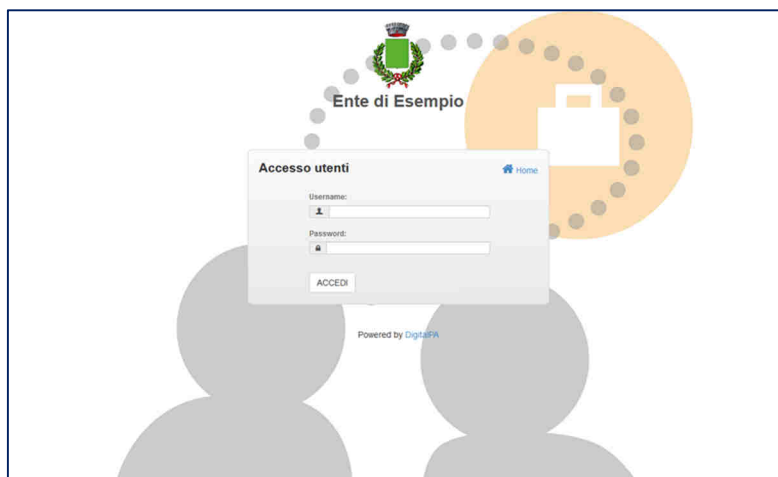


Figura 7 – Log-in

Per questioni di sicurezza il sistema richiede la sostituzione della password temporanea fornita per il primo accesso. La password deve avere le seguenti caratteristiche:

- ✓ Lunghezza minima 8 caratteri
- ✓ Contenere almeno un carattere numerico
- ✓ Contenere almeno un carattere MAIUSCOLO
- ✓ Contenere almeno un carattere speciale

La password ha una durata di 90 giorni. Alla sostituzione, la nuova password non può essere uguale ad una delle ultime 5 precedentemente utilizzate.

### 3.3 Nuova Segnalazione utente registrato

L'inserimento di una segnalazione per un utente registrato prevede la compilazione di una serie di campi con la possibilità di inserire uno o più allegati, come nel caso dell'utente anonimo. In questo caso, non è necessario inserire il proprio nominativo, in quanto il sistema consente di risalire all'identità del segnalatore registrato tramite la procedura descritta in seguito.

Crucetta Elenco Segnalazioni Nuova Segnalazione

#### NUOVA SEGNALAZIONE

Responsabile \*  RPCT (Responsabile Prevenzione Corruzione e Trasparenza)  OdV (Organismo di Vigilanza)  RPCT e OdV   
nessun allegato

Oggetto \*

Natura illecito \*

Autori illecito \*

Persone Coinvolte

Unità Organizzativa (Servizio, Area, Reparto, etc.) \*

Luoghi in cui si sono consumati gli illeciti \*

Data presunta Inizio illeciti \*

Data Fine Illeciti \*

Messaggio \*

no Autorizzo a rivelare la mia identità \*

\* Si ricorda che l'unico soggetto autorizzato alla visualizzazione dell'identità del segnalante (previa opportuna motivazione) è esclusivamente il Responsabile per la Prevenzione della Corruzione, autorizzando a rivelare la propria identità, questa potrà essere rifiutata (solo in caso di assoluta necessità e ai fini di indagine) esclusivamente ad eventuale altro responsabile (o superiore gerarchico). Il quale sarà comunque tenuto a garantire la massima riservatezza ai sensi dell'Art. 54-bis del D.Lgs. n. 165 del 30 marzo 2001

Figura 8 – Inserimento Nuova Segnalazione

Una volta composto il messaggio, si può salvare una bozza e riprendere la compilazione successivamente, oppure salvarla ed inviarla al Responsabile.

### 3.4 Gestione della Segnalazione

Il segnalatore, dalla propria area riservata, può seguire lo stato di lavorazione di ogni segnalazione inviata. L'accesso a tale area, per un utente registrato, avviene tramite l'inserimento delle credenziali per l'accesso, dalla pagina di login. Per un utente non registrato, l'accesso alla segnalazione avviene tramite l'inserimento del token (come descritto in precedenza).

The screenshot shows the 'CRUSCOTTO' dashboard of the 'Segnalazione Illeciti P.A. WHISTLEBLOWING' system. The top navigation bar includes 'Cruscotto', 'Elenco Segnalazioni', and 'Nuova Segnalazione'. The main content area is divided into two sections:

- Ultime segnalazioni inserite:** A list of three recent reports:
  - Oggetto: ST segnalazione 030118, Data: 03/01/2018 14:06, with a 'Vedi' button and a link to 'Istigazione Alla Corruzione'.
  - Oggetto: Segnalazione di Abuso, Data: 27/12/2017 14:23, with a 'Vedi' button and a link to 'Abuso'.
  - Oggetto: Assenze Ingiustificate, Data: 06/12/2017 10:32, with a 'Vedi' button and a link to 'Assente/Ingiustificato'.
- Messaggi:** A section for messages, showing one message:
  - Oggetto: Ulteriori chiarimenti, Inviato il: 04/01/2018 11:41:24 da: Giuseppe Spalletti, with a 'Leggi' button.

Figura 9 – Cruscotto

Il Segnalatore può gestire le proprie segnalazioni, seguendone lo stato di lavorazione e le risposte del Responsabile attraverso un intuitivo pannello di controllo o *Cruscotto*. È possibile accedere alla segnalazione e visualizzare tutto il fascicolo oppure accedere agli ultimi messaggi ricevuti.

The screenshot shows the 'SEGNALAZIONE' detail page. The top navigation bar includes 'Dettaglio segnalazione' and 'Messaggi'. The main content area is divided into two sections:

- Summary:** A table showing key information:
  - Inviato il: 03/01/2018 14:06
  - Stato della segnalazione: Inviata
  - Stato di lavorazione: In lavorazione
  - In carico a: Giuseppe Spalletti (rpct)
- Details:** A table showing specific details:
  - Oggetto: ST segnalazione 030118
  - Natura illecito: Istigazione Alla Corruzione
  - Autori illecito: Franco Rossi
  - Persone Coinvolte: Aldo Bianchi
  - Data presunta Inizio Illeciti: 10/10/2017
  - Data Fine Illeciti:
- Allegati:** A section for attachments, showing 'nessun allegato salvato'.

Figura 10 – Visualizzazione Segnalazione

Oggetto:	Segnalazione Assenteismo
Data invio:	07/04/2016 10:45:13
Stato della segnalazione:	Inviata
Natura Illecito:	Assenteismo
Autori Illecito:	Domenica Manca
Persone Coinvolte:	Domenica Manca
Data Inizio Illeciti:	01/04/2016
Data Fine Illeciti:	08/04/2016
Luoghi in cui si sono consumati gli illeciti:	Sede Assessorato LL.PP.
Servizio:	Settore Finanziario
Stato di lavorazione:	In lavorazione
Autorizzo a rivelare la mia identità:	SI

**Messaggio**

Oggetto: Richiesta

Ricevuto il: 12/04/2016 15:19:04

Contenuto

A questo punto indagherò con il Responsabile del settore del Sig. Neri, il Dott. Rossi. Grazie per la segnalazione.

[Rispondi](#)

Allegati

nessun allegato salvato

Figura 11 – Visualizzazione Messaggio

## 4 Area Responsabile/OdV - Gestione delle Segnalazioni

L'Area riservata al *Responsabile* consente la gestione rapida e funzionale di tutte le Segnalazioni ricevute. Una volta effettuato l'accesso, il *Responsabile* visualizza il *Cruscotto*, in cui sono presenti:

- ✓ Un menu superiore che rimanda alle diverse sezioni del gestionale
- ✓ Box con i collegamenti veloci a
  1. ultime segnalazioni ricevute
  2. ultimi messaggi ricevuti dai segnalatori
  3. ultimi messaggi ricevuti da eventuali collaboratori o altri soggetti responsabili

The screenshot shows the 'WHISTLEBLOWING' dashboard with a navigation menu at the top: Cruscotto, Segnalazioni Aperte, Segnalazioni Chiuse, Statistiche, and Logs. The main content area is divided into three sections:

- Ultime segnalazioni ricevute:** A list of reports with details like 'ST segnalazione 030118', 'OGGETTO', and 'Data'. Each entry has a 'Vedi segnalazione' button. A red '1' is placed next to the second entry.
- Ultimi messaggi pervenuti non letti:** A list of messages with details like 'Oggetto: Conferme', 'Inviato il:', and 'da: Segnalatore'. Each entry has a 'Leggi messaggio' button. A red '2' is placed next to the second entry.
- Ultimi messaggi interni non letti:** A list of internal messages with details like 'Oggetto: importanti novità sulla segnalazione n. 2', 'Inviato il:', and 'da: Stefano Orrù'. Each entry has a 'Leggi messaggio' button. A red '3' is placed next to the second entry.

Figura 12 - Cruscotto

Cliccando su un messaggio o su una segnalazione, viene aperto il relativo *Fascicolo*, che consente di consultarne i dettagli.

## 4.1 Elenco segnalazioni

Le segnalazioni sono gestite tramite due elenchi:

- Segnalazioni Aperte, nel quale sono presenti le segnalazioni non lette o in lavorazione.
- Segnalazioni Chiuse, nel quale sono presenti le segnalazioni archiviate.

Nella pagina *Segnalazioni aperte* è presente una lista ordinata delle segnalazioni ricevute e in corso di lavorazione. Le segnalazioni sono suddivise in pagine sfogliabili grazie alla presenza degli appositi comandi. Un sistema di icone permette di distinguere le segnalazioni di utenti registrati da quelle provenienti da segnalatori non registrati.

Il sistema consente di individuare le segnalazioni di proprio interesse tramite i filtri presenti nella parte superiore della pagina. I filtri sono i seguenti:

- ✓ Numero di segnalazioni presenti per ogni pagina.
- ✓ Natura dell'illecito.
- ✓ Intervallo di ricezione e ordinamento per data.
- ✓ Stato della lavorazione della segnalazione

### SEGNALAZIONI APERTE

[Nuova segnalazione cartacea](#)

10 per pagina   Ordina per Data decrescenti   Natura Illecito - Tutte   Stato di lavorazione - Tutte   Data inizio   Data fine   Pagina 1 di 1

stato di lavorazione	codice interno / oggetto	messaggi interni
In lavorazione	11 / Segnalazione Registrato <b>Furto</b> Inviato il: 20/10/2017 16:05 In carico a: Felice Antonio (rpct) Alessandro Bianchi (odv)	Ricevuti: 2 Non letti: 0
In lavorazione	9 / ANONIMA: RPCT -> ODV <b>Assenza</b> Inviato il: 19/10/2017 16:38 In carico a: Alessandro Bianchi (odv)	Ricevuti: 0 Non letti: 0
Letta	7 / ANONIMA: RPCT + ODV <b>Istigazione Alla Corruzione</b> Inviato il: 19/10/2017 11:25 In carico a: Felice Antonio (rpct) Alessandro Bianchi (odv)	Ricevuti: 6 Non letti: 1
In lavorazione	6 / ANONIMA: ODV + COLL <b>Mobbing</b> Inviato il: 19/10/2017 10:08 In carico a: Alessandro Bianchi (odv)	Ricevuti: 1 Non letti: 1
In lavorazione	3 / spionaggio <b>Abuso</b> Inviato il: 18/10/2017 10:26 In carico a: Felice Antonio (rpct) Alessandro Bianchi (odv)	Ricevuti: 3 Non letti: 1
In lavorazione	2 / ST Corruzione 1 <b>Corruzione</b> Inviato il: 18/10/2017 10:03 In carico a: Felice Antonio (rpct) Alessandro Bianchi (odv)	Ricevuti: 1 Non letti: 0

### SEGNALAZIONI CHIUSE

Risultati per pagina: 20   Trovate 2 Segnalazioni   Ordina per: Data di Chiusura [dalle più recenti]   Filtro   reset

stato di lavorazione	codice interno / oggetto	messaggi interni
Accettata (la segnalazione avrà un seguito successivo)	13 / REGISTRATO -> ODV <b>Mobbing</b> Inviato il: 20/10/2017 17:20:42   Chiuso il: 23/10/2017 09:47:57   In carico a: Alessandro Bianchi (odv) Felice Antonio (rpct)	
Rigettata (non si è ritenuto di dover prendere in considerazione la segnalazione)	8 / ANONIMA: ODV + RPCT <b>Assenteismo</b> Inviato il: 19/10/2017 12:06:22   Chiuso il: 23/10/2017 09:28:17   In carico a: Felice Antonio (rpct) Alessandro Bianchi (odv)	

Codice Interno

Natura Illecito

Modalità di Invio

Stato del procedimento

Data di Invio

Data di Chiusura

Figura 13 – Elenco Segnalazioni

## 4.2 FASCICOLO DELLA SEGNALAZIONE

Il Fascicolo della segnalazione è accessibile dal Cruscotto e dall'Elenco delle Segnalazioni, ed è composto da varie schede: Dettaglio segnalazione, Messaggi, Note interne, Messaggistica interna, Collaboratori.

### 4.3 Dettaglio segnalazione

Nella scheda Dettaglio Segnalazione sono presenti le informazioni inserite dal Segnalatore.

SEGNALAZIONE	
<div style="display: flex; justify-content: space-between;"> <span>Q Dettaglio segnalazione</span> <span>Messaggi</span> <span>Note interne</span> <span>Messaggistica Interna</span> <span>Collaboratori</span> <span>Log Attività</span> </div>	
<div style="display: flex; justify-content: space-between;"> <span>Stato di lavorazione</span> <span>Modifica Natura Illecito</span> <span>Riassegna/Condividi</span> <span>Stampa</span> </div>	
Inviato il:	20/10/2017 16:05
Stato della segnalazione:	Inviata
Stato di lavorazione:	In lavorazione
In carico a:	Felice Antonio (rpct) Alessandro Bianchi (odv)
Oggetto:	Segnalazione illecito
Natura illecito:	Furto ▲
Autori illecito:	Piero delle vigne
Persone Coinvolte:	
Data presunta inizio illeciti:	10/10/2017
Data Fine Illeciti:	24/10/2017
Luoghi in cui si sono consumati gli illeciti:	ufficio
Unità Organizzativa (Servizio, Area, Reparto, etc.):	ufficio
Messaggio:	<p>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean commodo ligula eget dolor. Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus.</p>
Allegati:	<p>allegato generico.pdf dimensione 92.7 KB</p>
Autorizzo a rivelare la mia identità:	No
Identità segnalatore:	<p>L'identità del segnalante viene mostrata cliccando sul pulsante "Mostra Identità" dopo aver motivato la richiesta.</p> <p style="text-align: center;"><span>Mostra Identità</span></p>

Figura 14 – Fascicolo della Segnalazione

#### 4.3.1 Stato di lavorazione

L'iter della segnalazione viene gestito dal Responsabile attraverso l'utilizzo degli stati di lavorazione. Lo **Stato di Lavorazione** è visibile nell'area dedicata al segnalatore che può così seguire lo stato di avanzamento della propria segnalazione. Lo stato passa da *Non Letta* a *Letta* in maniera automatica quando si accede per la prima volta al Fascicolo; il Responsabile ha la facoltà di modificare lo stato in modo da organizzare in maniera efficiente le varie segnalazioni. Gli "stati di lavorazione" sono così definiti:

- Non Letta
- Letta
- In Lavorazione
- Archiviata
  - Rigettata (non si è ritenuto di dover prendere in considerazione la segnalazione)

- Accettata (la segnalazione avrà un seguito)
- Provvedimento disciplinare
- Inoltrata a soggetti terzi competenti

#### 4.3.2 Mostra identità

In questa scheda è presente il pulsante “Mostra Identità”. Il Responsabile ha la possibilità di visualizzare l’identità del segnalante nel caso in cui lo ritenga necessario ai fini dell’indagine, ad esempio qualora la segnalazione sfoci in un procedimento giudiziario ed il nominativo gli sia richiesto dalla magistratura inquirente o giudicante ai fini di indagine. La visualizzazione dell’identità deve essere giustificata inserendo una motivazione. Il sistema provvede a memorizzare l’operazione sui log di sistema e ad informare il Segnalatore che il Responsabile ha deciso di visualizzare la sua identità, mostrandogli la motivazione inserita.

Il diagramma illustra il processo di visualizzazione dell'identità del segnalante in tre fasi:

- Fase 1:** Una schermata con il titolo "Identità segnalatore:" e un messaggio informativo: "L'identità del segnalante viene mostrata cliccando sul pulsante 'Mostra Identità' dopo aver motivato la richiesta." Sotto il messaggio c'è un pulsante "Mostra Identità".
- Fase 2:** Una schermata con il titolo "Inserire Motivazione \*". Al centro c'è un campo di testo vuoto. Sotto il campo ci sono due pulsanti: "Annulla" e "Salva Motivazione e Mostra Identità".
- Fase 3:** Una schermata con il titolo "Identità segnalatore:". Sotto il titolo, a sinistra, c'è il campo "Nominativo: Utente Segnalatore". A destra c'è un checkbox "Mostra Identità" che è stato selezionato.

Figura 15 – Mostra Identità

#### 4.3.3 Modica natura illecito

È possibile modificare la natura dell’illecito, qualora questa sia stata classificata in maniera errata dal segnalatore; il sistema tiene memoria della modifica.

#### 4.3.4 Riassegnazione

È possibile la condivisione o la riassegnazione della segnalazione da parte del RPCT ad un eventuale soggetto (ad esempio un OdV) che potrà gestire la segnalazione con le stesse facoltà.

Lo screenshot mostra l'interfaccia del sistema di segnalazione. A sinistra, la scheda "SEGNALAZIONE" mostra i dettagli di una segnalazione:

- Inviato il: 20/12/2017 14:53
- Stato della segnalazione: Inviata
- Stato di lavorazione: Letta
- In carico a: Stefano Omù (rpct)
- Oggetto: Segnalazione assenteismo
- Natura illecito: Assenteismo
- Autori illecito: Stefano Omù

A destra, la finestra "Condivisione - Cambio Assegnazione" è aperta. In alto, ci sono tre radio button per selezionare il destinatario della segnalazione:

- RPCT (Responsabile Prevenzione Corruzione e Trasparenza)
- OdV (Organismo di Vigilanza)
- RPCT e OdV

Sotto le radio button, c'è un campo di testo per il "Messaggio di riassegnazione:" con un editor di testo standard.

Figura 16 – Condivisione-Riassegnazione

## 4.4 Messaggi

L'area **Messaggi** è dedicata alla corrispondenza tra il Segnalatore e il Responsabile (ed eventuali collaboratori). Sfruttando il sistema di cifratura della piattaforma è possibile inviare e ricevere i messaggi in maniera sicura e protetta.

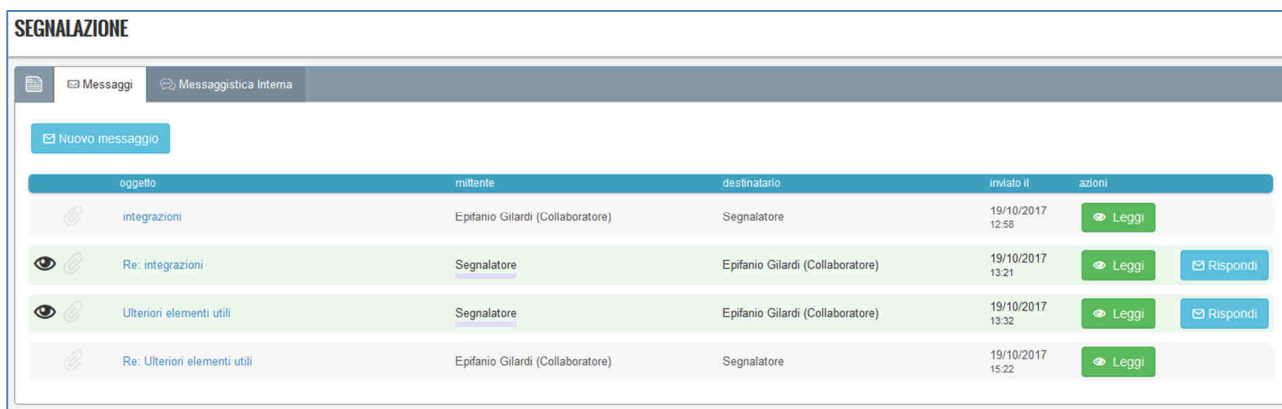


Figura 17 – Area Messaggi

Le icone e i colori rendono facilmente distinguibili i messaggi inviati e i messaggi ricevuti.

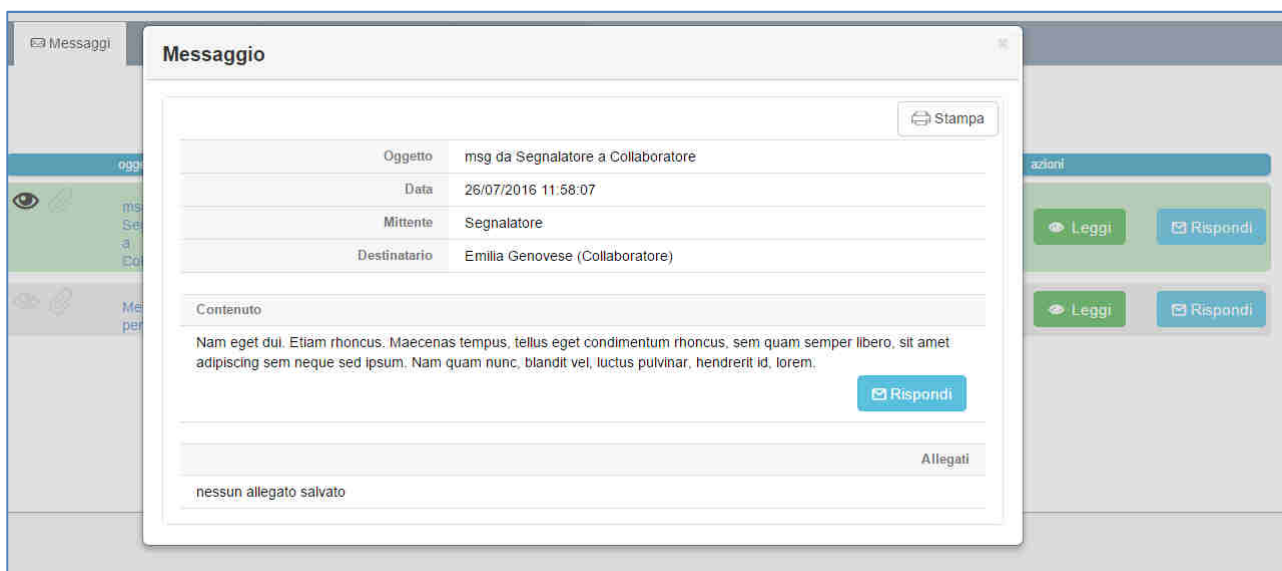


Figura 18 – Messaggio

Il Responsabile può scrivere all'utente Segnalatore cliccando sul tasto *Rispondi*, ad esempio per richiedere ulteriore documentazione o maggiori informazioni.

Il Segnalatore potrà a sua volta rispondere tramite la propria area riservata.

Se presenti degli allegati, questi possono essere immediatamente scaricati sulla propria postazione di lavoro.



## 4.5 Note interne

Nella scheda *Note interne* si ha la possibilità di aggiungere delle annotazioni alla segnalazione, anche al fine di rendicontare le attività intraprese. Le annotazioni sono visibili al solo Responsabile.

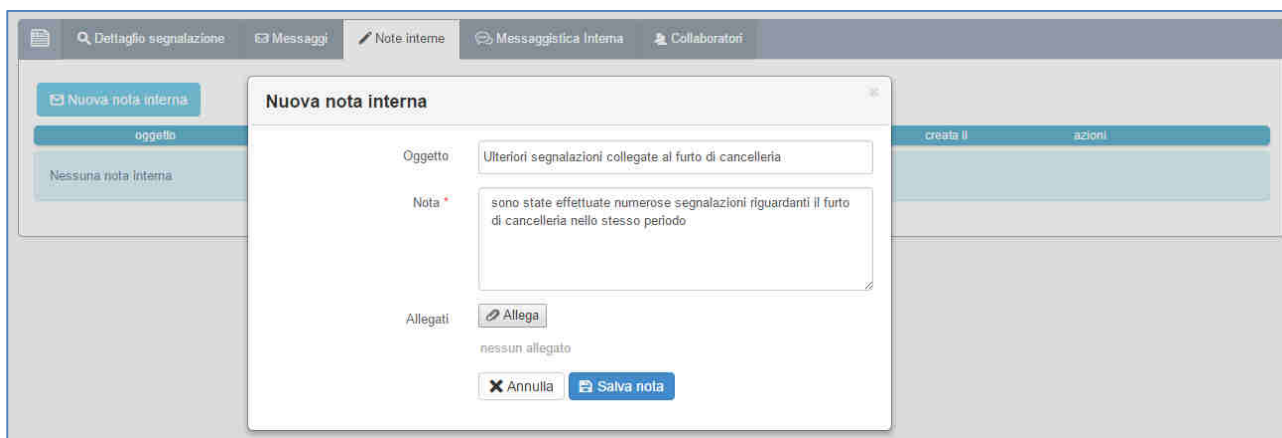


Figura 19 – Note interne

## 4.6 Collaboratori

Il Responsabile/OdV può assegnare una segnalazione ad un Collaboratore. Il Collaboratore, sulle segnalazioni assegnategli, può scambiare dei messaggi con il segnalatore, messaggi che saranno sempre visibili anche al Responsabile, nell'area Messaggi. La stessa segnalazione può essere assegnata a più di un collaboratore.

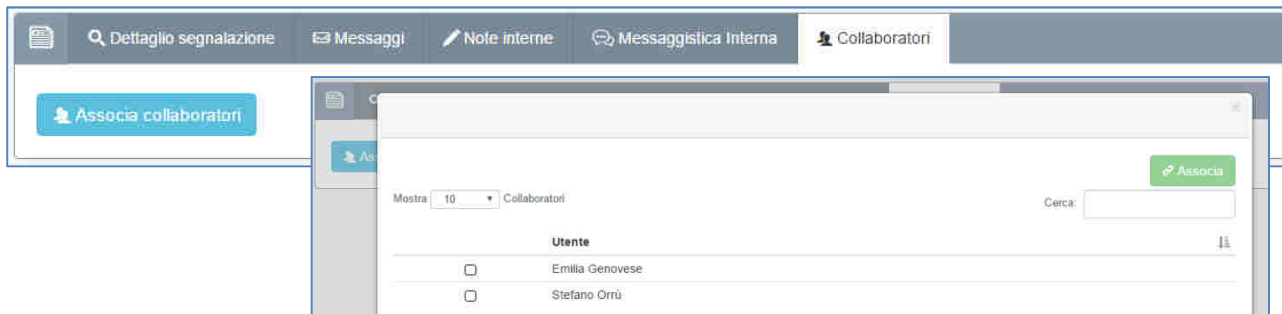


Figura 20 – Assegnazione al collaboratore

Ciascun collaboratore può avere accesso solo ai messaggi inviati alla propria attenzione; un collaboratore non può visualizzare i messaggi destinati ad un altro collaboratore. Solo il Responsabile ha il pieno accesso a tutti i messaggi.

Dopo aver effettuato l'associazione, nella scheda viene riportato il nome del Collaboratore e la data di assegnazione; in qualsiasi momento è possibile rimuovere l'associazione. Tutte le operazioni vengono registrate sui log.

## 4.7 Messaggistica interna

Attraverso la messaggistica interna il Responsabile può dialogare privatamente con un altro responsabile e con i propri collaboratori. Questi messaggi non vengono inviati al segnalatore: il Responsabile può così intraprendere uno scambio di messaggi interni con i propri collaboratori sfruttando la sicurezza offerta dalla piattaforma.

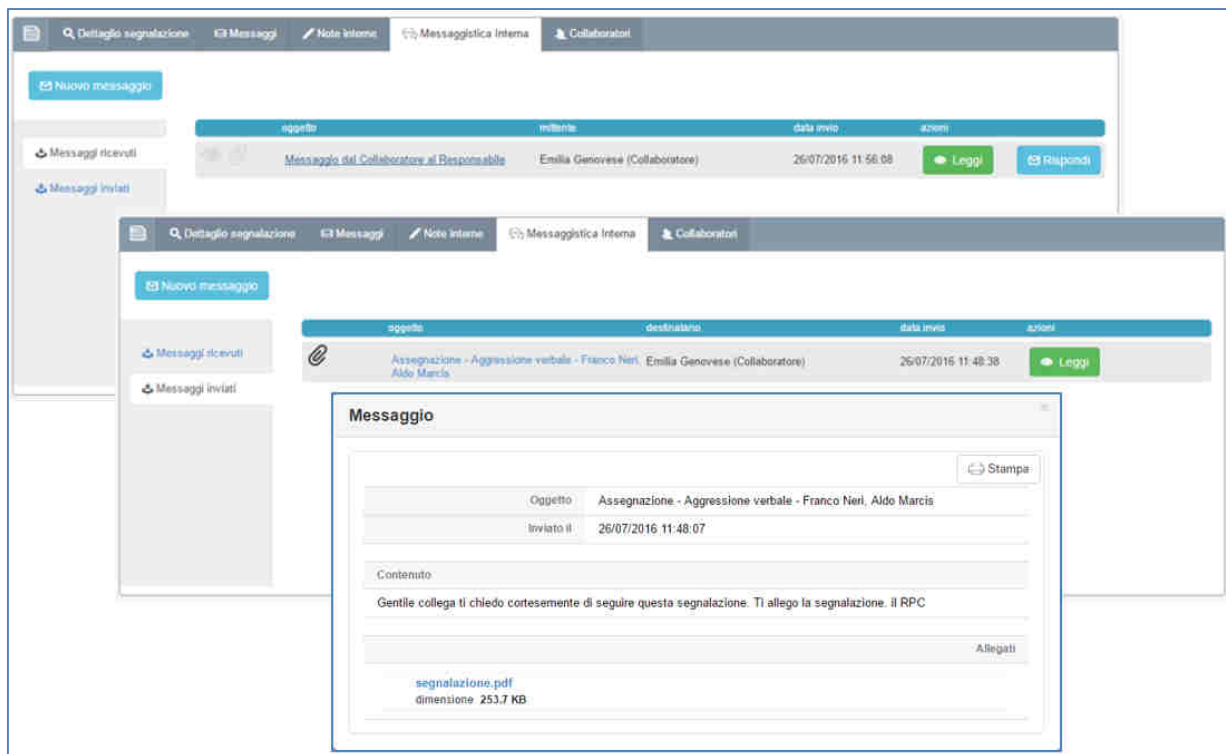


Figura 21 – Messaggistica interna

## 5 Segnalazioni cartacee o da altri canali

Il RPCT e/o l'ODV possono aprire/creare autonomamente un fascicolo in completa autonomia nel caso in cui si riceva una segnalazione da canali diversi rispetto al software, come nel tipico caso di una segnalazione verbale o scritta. Il sistema consente l'immissione di dati e documenti tali da rendere il fascicolo facilmente implementabile e consultabile.

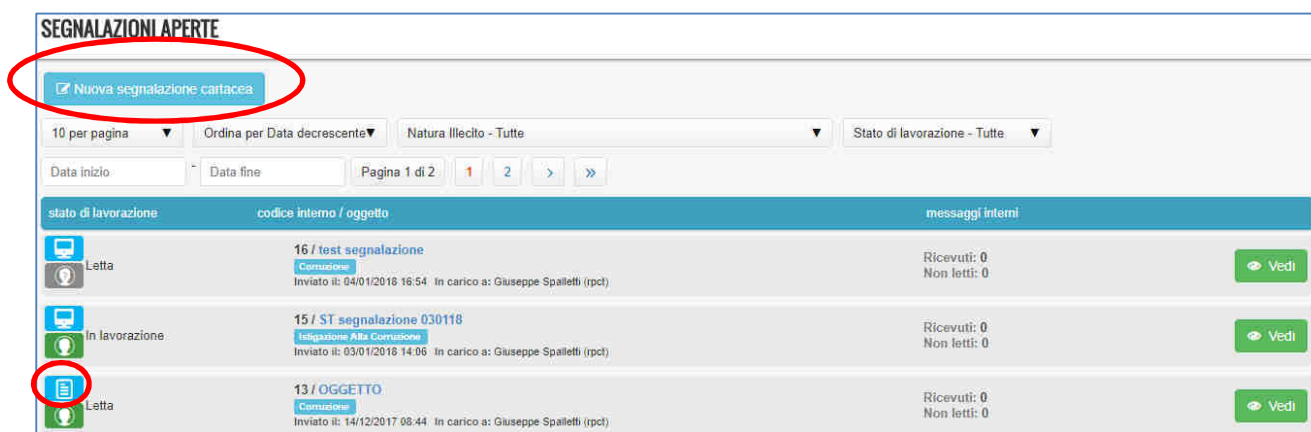


Figura 22 – Messaggistica interna

Una volta inserita, la segnalazione cartacea viene identificata da un'icona che la distingue rispetto alle altre segnalazioni, e può essere gestita con le stesse modalità delle segnalazioni pervenute attraverso il sistema.

## 6 Multilingua

Il software SEGNALAZIONI.NET, è nativamente predisposto per il multilingua, attivabile su richiesta in italiano e inglese. Ulteriori lingue possono essere attivate su richiesta.

## 7 Statistiche

Nella pagina *Statistiche* sono presenti vari grafici con le statistiche delle segnalazioni in base agli stati. Sfogliando i tab è possibile visualizzare tali statistiche per anno, mese e giorno. Inoltre è possibile produrre dei report grafici riguardanti le tempistiche di chiusura delle segnalazioni.

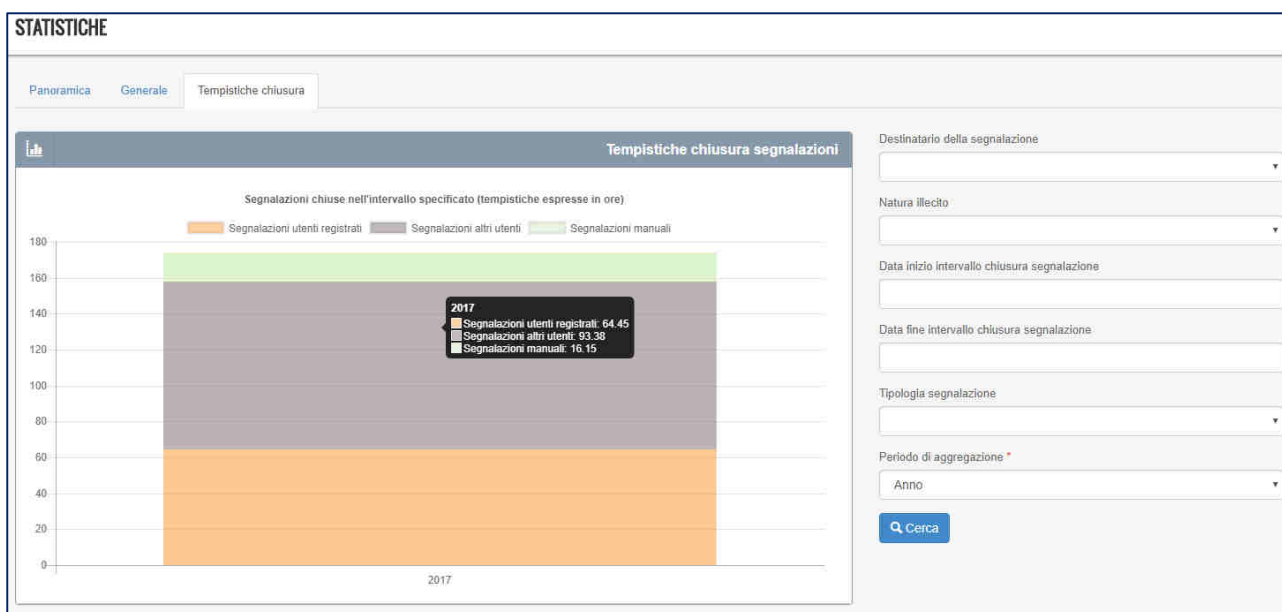
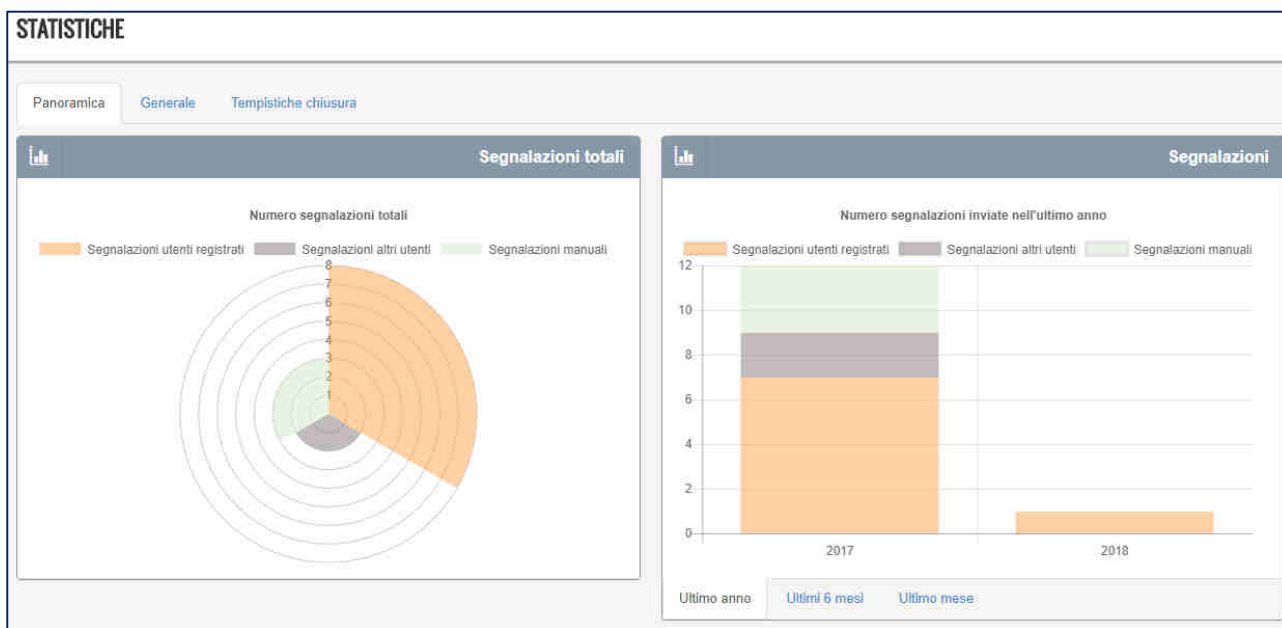


Figura 23 - Statistiche

## 8 Logs

Tutte le operazioni effettuate sulle segnalazioni, sia da parte dei Segnalatori sia da parte dei Responsabili, vengono registrate sui log di sistema in maniera anonima e criptata per garantire la massima riservatezza e anonimato.

ELENCO LOGS EVENTI			
Risultati per pagina <input type="text" value="20"/>		Trovati 652 Logs	
		Ordina per <input type="text" value="Data evento (Più recenti)"/>	
data azione	azione	autore	dettagli
20/11/2017 17:00	Segnalazione n° 11 Visualizzata Segnalazione	RPCT	Sessione: 3fc1aec990dfb153d3d8a5d9aae0e1dc7a7004d
20/11/2017 16:58	Segnalazione n° 12 Visualizzata Segnalazione	RPCT	Sessione: 3fc1aec990dfb153d3d8a5d9aae0e1dc7a7004d
20/11/2017 16:55	Segnalazione n° 13 Visualizzata Segnalazione	Segnalatore	Sessione: b04414e2783b2c2ffb412c035ed496934f7768a
25/10/2017 13:28	Modifica utente	--	Sessione: c86e54bb578782a8cb13dcfeb42602f9efc0594f IP: ██████████
25/10/2017 09:08	Segnalazione n° 11 Visualizzata Segnalazione	OdV	Sessione: 60a4456a0ce76bee78286b927b0a2cbf8b03dfdb
24/10/2017 17:43	Segnalazione n° 11 Visualizzata Segnalazione	OdV	Sessione: 179686c4ef31b99fd0f264806d7ff626a7761a29
24/10/2017 17:27	Segnalazione n° 11 Visualizzata Segnalazione	OdV	Sessione: 179686c4ef31b99fd0f264806d7ff626a7761a29
24/10/2017 17:21	Segnalazione n° 15 Modificato Stato Segnalazione	RPCT	Sessione: 0ba49a4581395cbe3d7071208b7e12523f822030 stato precedente : Letta stato corrente : Archiviata

**Filtro**

Tipologia

Nessuna selezione

Figura 24 - Logs

L'elenco dei Log è filtrabile per la tipologia di operazione eseguita: visualizzazione di una segnalazione, creazione nuova segnalazione, etc.

## 9 Sicurezza e riservatezza lato Software

---

Sulla piattaforma Whistleblowing, SEGNALAZIONI.NET, tutte le informazioni che possono rivelare i contenuti di una segnalazione e l'identità del suo autore, o che possono dare indicazioni sull'attività di un Segnalatore, sono protette e cifrate a più livelli.

Le segnalazioni (comprese le bozze), gli allegati (anche quelli temporanei), i log di attività e le sessioni sono cifrate; inoltre non esiste alcuna correlazione diretta tra utente della piattaforma (Segnalatore) ed eventuali segnalazioni.

La decifrazione dei contenuti riservati è consentita solo attraverso i dati a conoscenza del Responsabile e del Segnalatore; i log sono decifrabili solo dal Responsabile.

### 9.1 Caratteristiche tecniche del sistema di cifratura:

---

#### 9.1.1 Gestione password per autenticazione

La password non sono memorizzate in chiaro nel database, in maniera da impedirne un eventuale, seppure improbabile furto o visualizzazione. Nemmeno gli amministratori di sistema possono risalire alla password in quanto le password utente sono memorizzate in modalità cifrata, in combinazione con un salt random, nel database di sistema, con algoritmo hash sha512.

Non è possibile, partendo dall'hash, ricalcolare la password originale. L'algoritmo di cifratura è configurabile in funzione della necessità.

#### 9.1.2 Cifratura dei contenuti

Tutte le informazioni che possono rivelare i contenuti di una segnalazione e l'identità del suo autore o che, al limite, possono dare indicazioni sull'attività di un Segnalatore, sono protette e cifrate a più livelli.

Per ogni segnalazione vengono create una coppia di chiavi, pubblica (KpubS) e privata (KprivS), di tipo RSA con un keysize di 4096 Byte, una chiave simmetrica (KsimS) lunga 32 Byte e una chiave di cifratura (Kmp) lunga 32 Byte.

Inoltre, per il Responsabile e per ogni Collaboratore vengono generate una coppia di chiavi, pubblica (KpubR) e privata (KprivR). Quest'ultima è cifrata con l'algoritmo di cifratura simmetrica AES-256-CBC, utilizzando come chiave di cifratura la password dell'utente a cui è associata.

### 9.2 Flusso cifratura e decifratura per il segnalatore registrato

---

Quando viene creata una segnalazione, come descritto in precedenza, vengono create la coppia di chiavi KpubS e KprivS, la chiave simmetrica KsimS e la chiave di cifratura Kmp.

- I contenuti della segnalazione vengono cifrati con la KsimS tramite l'algoritmo AES-256-CBC.
- La KsimS viene cifrata con la chiave KpubS.
- La KprivS viene cifrata con la Kmp tramite l'algoritmo AES-256-CBC.
- La Kmp viene associata alla segnalazione e al segnalatore e cifrata con la sua password tramite l'algoritmo AES-256-CBC.

Per la decifratura il sistema recupera in sessione la password opportunamente cifrata (come descritto in seguito) inserita all'atto del login. La password viene utilizzata per decifrare la Kmp che a sua volta decifrerà la KprivS che consentirà di decifrare la KsimS con la quale si potrà decodificare i contenuti della segnalazione.

Quando il segnalatore inserisce dei contenuti per una segnalazione il sistema li cifra utilizzando la KsimS associata.

### 9.3 Flusso cifratura e decifratura per il segnalatore anonimo

---

Quando viene creata una segnalazione, come descritto in precedenza, vengono create la coppia di chiavi\* KpubS e KprivS, la chiave simmetrica KsimS e la chiave di cifratura Kmp.

- I contenuti della segnalazione vengono cifrati con la KsimS tramite l'algoritmo AES-256-CBC.
- La KsimS viene cifrata con la chiave KpubS.
- La KprivS viene cifrata con la Kmp tramite l'algoritmo AES-256-CBC.
- La Kmp viene comunicata al segnalatore dopo l'invio della segnalazione.

Per la decifratura il sistema chiederà la Kmp al segnalatore e la utilizzerà per decifrare la KprivS che consentirà di decifrare la KsimS con la quale si potrà decodificare i contenuti della segnalazione.

Quando il segnalatore inserisce dei contenuti per una segnalazione il sistema li cifra utilizzando la KsimS associata.

### 9.4 Flusso cifratura e decifratura per il Responsabile e i Collaboratori

---

Quando viene inserita una segnalazione, la KsimS generata viene cifrata anche per il Responsabile e i Collaboratori con la loro KpubR.

Per la decifratura il sistema recupera la KpriR decifrandola con la password inserita all'atto del login e utilizzandola poi per decifrare la KsimS e accedere ai contenuti.

Quando il Responsabile e i Collaboratori inseriscono dei contenuti per una segnalazione il sistema li cifra utilizzando la KsimS associata.

### 9.5 Cifratura dei log

---

L'accesso ai log è consentito esclusivamente al Responsabile Anticorruzione. Per ogni voce di log memorizzata viene generata una chiave simmetrica KsimL. La KsimL viene cifrata sia con la KpubR che con la chiave pubblica degli Amministratori del sistema KpubA.

La decifratura avviene utilizzando le rispettive chiavi private decodificate attraverso la password usata all'atto del login.

### 9.6 Gestione della password in fase di sessione

---

Le password non vengono trascritte in chiaro ma il software provvede a criptare la parte di sessione relativa alla password durante l'utilizzo della piattaforma da parte degli utenti. Per aumentare ulteriormente il livello di protezione di questo dato, la sessione viene quindi cifrata con l'algoritmo AES-256-CBC utilizzando una chiave di cifratura generata dal client dell'utente. Ulteriore misura di sicurezza è l'assenza sul server di una associazione tra la sessione e l'utente. Una volta scaduta la sessione viene eliminata dal sistema.

La porzione di software che consente la criptazione tramite algoritmo della password in sessione è compilata e non accessibile ai system administrator. Il software è stato inoltre secretato nelle specifiche funzioni di criptazione e decriptazione in sessione. Gli sviluppatori non hanno accesso ai sistemi in produzione.

#### \*Legenda:

**KpubS, KprivS:** Coppia di chiavi pubblica e privata Segnalatore

**KsimS:** Chiave simmetrica con la quale viene cifrata la Segnalazione

**Kmp:** Chiave di cifratura della KprivS

**KpubR, KpriR:** Coppia di chiavi pubblica e privata Responsabile

**KsimL:** Chiave simmetrica con la quale vengono cifrati i Log

**KprivA, KpubA:** Coppia di chiavi pubblica e privata Amministratore

## 9.7 Sostituzione Responsabile e smarrimento password

---

Qualora il Responsabile per la Prevenzione alla Corruzione e Trasparenza debba essere sostituito (temporaneamente o definitivamente) è possibile farlo adottando la seguente procedura:

1. L'RPCT in carica consegna la propria password per l'accesso alla piattaforma al nuovo RPCT che potrà al primo accesso variare la propria anagrafica e la propria email di corrispondenza.
2. A questo punto il nuovo RPCT accede con le credenziali formate dal nuovo indirizzo email e la Password fornitagli dal precedente RPCT. Al primo accesso sarà obbligato a modificare la password.

Dopo tali modifiche, gli utenti avranno evidenza del cambiamento, in quanto tutte le nuove comunicazioni inviate o ricevute al/dal nuovo Responsabile riporteranno il nome del nuovo RPCT. I messaggi del precedente RPCT saranno contrassegnati dal nome del vecchio Responsabile.

Nel caso di sostituzione temporanea, quando il Responsabile temporaneo deve essere sostituito dal RPCT originario, si deve ripetere la procedura con ruoli invertiti.

In caso di **smarrimento della password** di accesso del responsabile o in caso di mancata consegna per qualsivoglia motivo, sono previste procedure di emergenza e di accesso.

1. Account di backup/recupero. È possibile creare un account di "backup" le cui credenziali dovranno essere custodite con estrema cura e attenzione.
2. Reset password tramite Utente Super User.
3. È possibile registrare una smart card associata al Responsabile, che consente di effettuare l'accesso senza l'utilizzo delle credenziali.

Nel secondo caso è possibile utilizzare una procedura tramite la quale un utente con particolari permessi (Super User), le cui credenziali devono essere custodite scrupolosamente ed utilizzate solo per questo scopo, può modificare l'indirizzo email del responsabile, attraverso il quale il responsabile può effettuare il recupero della password. Il ruolo di utente Super User può essere demandato anche alla DigitalPA.

La fornitura di un Software è fondamentale che venga accompagnata dall'offerta di servizi, quali:

- ✓ Consulenza
- ✓ Installazione
- ✓ Assistenza
- ✓ Manutenzione

Per far questo ci avvaliamo della professionalità di nostri tecnici specializzati negli applicativi gestionali.

Le figure che sono a disposizione dei clienti pre e post acquisto sono:

- ✓ Responsabili commerciali, con mansioni di coordinamento generale e consulenziale
- ✓ Operatori commerciali
- ✓ Studio di consulenza legale specialistica
- ✓ Tecnici sistemisti per l'assistenza diretta telefonica, via Email e remota
- ✓ Tecnici sviluppatori senior, per assistenza specialistica
- ✓ Tecnici sviluppatori junior, per assistenza e formazione
- ✓ Tecnici sistemisti senior
- ✓ Numerosi partner qualificati capillari nel territorio

## 9.8 Installazione e configurazione (cronoprogramma)

L'installazione del software avverrà a cura dei nostri tecnici sistemisti; successivamente, i tecnici software provvederanno alla configurazione e personalizzazione della piattaforma a voi dedicata.

Il coinvolgimento dell'amministrazione sarà minimo e consisterà esclusivamente nel fornire i dati necessari alla configurazione del gestionale (dati PEC, utenti utilizzatori, permessi, ecc.).

### 9.8.1 Fasi di start-up

La fase di start-up prevede la creazione delle utenze di gestione e la configurazione generale del software con i relativi test di funzionamento.

Tenendo ben presente che il whistleblower può iscriversi in autonomia o inviare una segnalazione senza obbligo di registrazione, può essere ulteriormente implementata su richiesta una prima pianta organica dei dipendenti. Qualora il cliente voglia attivare questa procedura, dovrà fornire un file con la lista degli utenti e relativa mail. Una volta ricevuta la lista degli utenti e dei relativi indirizzi Email, DigitalPA provvederà alla creazione delle utenze in stato "non attivo"; alla consegna del software, concordemente con le indicazioni dell'Ente, si provvederà ad attivare le utenze, il sistema invierà contestualmente le Email di notifica agli utenti, contenenti le credenziali temporanee per il primo accesso.

Successivamente, sarà possibile inserire nuovi utenti attraverso il pannello di amministrazione. È facoltà per l'utente amministratore creare le utenze e scegliere se inviare, contestualmente alla creazione, l'Email contenente le credenziali, oppure inviare tali credenziali in un secondo momento.

- Installazione del software: media 7 gg dal ricevimento dell'ordine.
- Configurazione: entro 48 ore dal ricevimento dei file di configurazione compilati.

Nell'eventualità sia richiesta l'installazione presso il ced della stazione appaltante, o siano richieste particolari personalizzazioni (grafiche o funzionali), i tempi di implementazione dovranno essere valutati caso per caso.

La consegna e l'attivazione con la visibilità al Pubblico sarà sempre concordata con l'Amministrazione, nel rispetto dei tempi di consegna previsti.



## 9.9 Formazione delle risorse

---

Al fine di garantire un rapido apprendimento nell'uso del software da parte degli operatori, si propongono specifici corsi di formazione sugli applicativi oggetto del presente documento.

È inoltre possibile richiedere la presenza di un nostro tecnico specializzato presso la sede dell'amministrazione per l'erogazione di una o più giornate di formazione.

Il personale dell'Ente sarà adeguatamente formato sul corretto utilizzo delle funzionalità e delle procedure da seguire per la gestione del software in funzione dei ruoli ricoperti.

In particolare gli utenti saranno messi in condizione di:

- ✓ Acquisire le informazioni necessarie per la comprensione del funzionamento del sistema;
- ✓ Acquisire la consapevolezza delle varie funzionalità operative e procedure informatiche;
- ✓ Migliorare il proprio servizio in termini di efficienza operativa, efficacia e qualità attraverso un utilizzo ottimale delle nuove risorse informatiche.

Le attività di addestramento consistono nell'illustrazione di tutte le funzionalità del software.

Sono previsti specifici percorsi formativi per le diverse figure professionali che saranno coinvolte nell'utilizzo e nella gestione del Sistema Informativo.

Il corso potrà anche essere rivolto a personale informatico dell'Ente al fine di poter rendere autonomo il processo di formazione di nuove figure dell'ente stesso e fornire supporto tecnico. Agli specialisti informatici è richiesta la partecipazione a tutti i corsi di addestramento.

## 9.10 Manutenzione e Assistenza

---

Il servizio di **manutenzione** prevede, nell'ambito della versione acquistata:

- ✓ L'aggiornamento del software e della relativa documentazione in relazione a **nuove funzionalità** introdotte.
- ✓ L'aggiornamento del software e della relativa documentazione in relazione a **nuove implementazioni e migliorie**.
- ✓ L'adeguamento dei gestionali e della relativa documentazione in relazione ad **adeguamenti legislativi**.

Operativamente gli aggiornamenti saranno disponibili nell'immediato e implementati dal nostro staff tecnico. L'installazione degli stessi non è in alcun modo demandata al Cliente al quale non si richiedono conoscenze di tipo tecnico.

L'**Assistenza agli utenti istituzionali**, sempre **compresa nell'offerta base**, prevede:

- ✓ Supporto Email (canale prioritario): per la richiesta di chiarimenti o spiegazioni del programma e segnalazioni di malfunzionamenti;
- ✓ Teleassistenza (urgenze): il servizio permette ad un tecnico specializzato di connettersi al computer del cliente per comprendere visivamente e con un rapporto diretto le difficoltà segnalate.

È inoltre possibile richiedere:

- ✓ Assistenza telefonica, per la richiesta di chiarimenti e segnalazioni di malfunzionamenti, tutti i giorni lavorativi dal lunedì al venerdì, dalle ore 9.00 alle ore 18.00.

Il contratto di manutenzione e assistenza decorre dalla data di consegna del programma. Avrà durata variabile, dipendente dall'offerta economica sottoscritta.

### 9.11 SLA (Service Level Agreement) garantiti

---

- Adeguamenti del Software alla vigente normativa: vengono immediatamente pianificati alla pubblicazione di una nuova disposizione normativa e hanno azione prioritaria.
- Disponibilità del Software: le statistiche degli ultimi 3 anni riportano un uptime del 100%.
- Manutenzione programmata del Software: vengono pianificati rilasci di aggiornamenti con cadenza mensile o, ove necessario, con maggiore frequenza, per nuove implementazioni, miglioramenti tecnologici. Tali rilasci vengono ampiamente testati su piattaforme di test da addetti specializzati. Ogni nuova versione è preceduta da una comunicazione che elenca le novità in rilascio.
- Interventi su guasto occorso al Software sia per problemi bloccanti che non bloccanti, l'intervento è pressoché immediato.
- Disaster recovery: i nostri sistemi di clustering rendono remota l'evenienza di un disaster recovery; nel caso di intervento, come da BCP interno, l'intervento prevede il tentativo di risoluzione sul server in produzione. In caso di intervento che dovesse protrarsi oltre le 4 ore, sono a disposizione numerosi server su cui reinstallare in massimo un'ora la piattaforma con gli ultimi set di dati disponibili.

Risoluzione problemi bloccanti	2 ore lavorative
Risoluzione problemi non bloccanti	4 giorni lavorativi
Risoluzione problemi minori	5 giorni lavorativi
Allineamento normativo	30 giorni lavorativi