LEGALITY
WHISTLEBLOWING
Segnalazione illeciti

Il software di riferimento per il **Whistleblowing**

Versione 4.2 del 16/03/2023

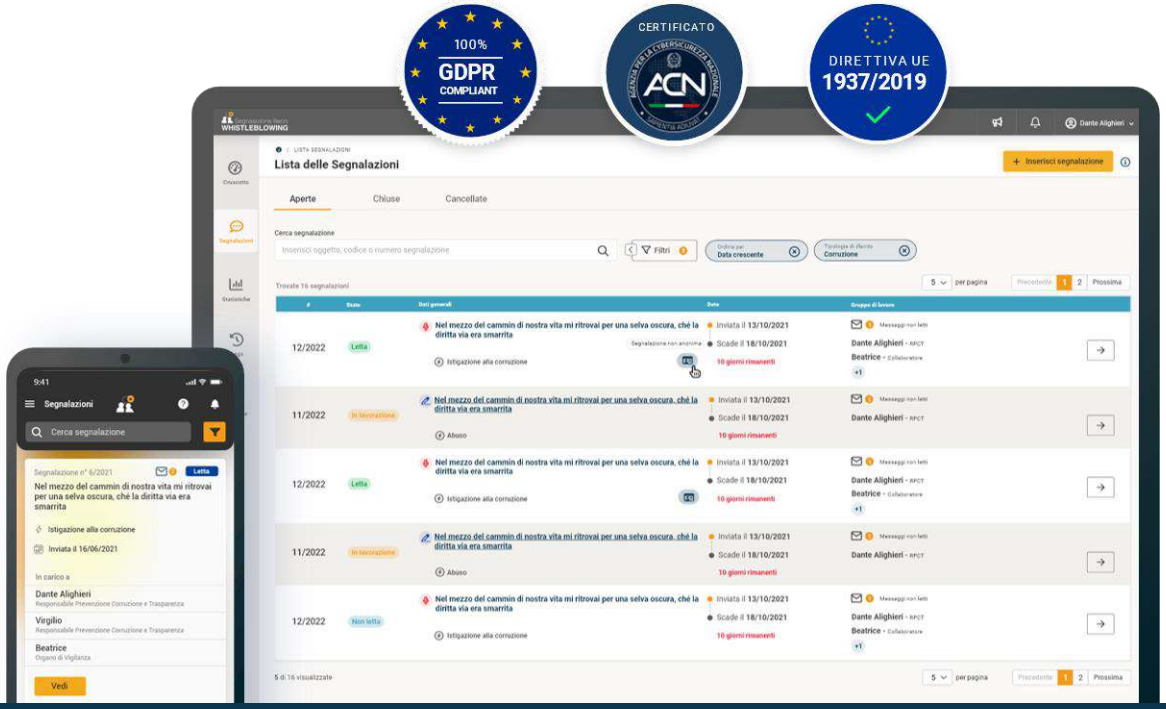
www.**segnalazioni**.net

Progettato e sviluppato da
DIGITALPA
We develop Innovation and Efficiency

LEGALITY WHISTLEBLOWING
Segnalazione illeciti

SOMMARIO

1. Introduzione 3
2. Tipologie di segnalazione 8
3. Ambiente di segnalazione 9
4. Area di Amministrazione 12
5. Fascicolo della segnalazione 13
6. Sicurezza e riservatezza lato Software 19
7. Servizi 23
8. Riferimenti normativi 26
9. Servizi Anticorruzione e Trasparenza 28



DigitalPA Srl
Via S. Tommaso d'Aquino, 18A – 09134 Cagliari
Altre sedi: Sulmona | Roma | Milano | Barcellona (Spagna)

Tel. +39 070 3495386
Email info@digitalpa.it | PEC digitalpa@pec.it

www.digitalpa.it

1. Introduzione

La piattaforma per la gestione del Whistleblowing, www.segnalazioni.net, è lo strumento informatico messo a disposizione dei *Segnalanti* e dei *Responsabili* del Whistleblowing, sia nel settore pubblico che in quello privato, finalizzato a gestire le segnalazioni di illeciti o di violazioni relative al Modello di Organizzazione e Gestione.

Segnalazione illeciti – Whistleblowing è conforme alla normativa vigente:

- *Linee guida in materia di Whistleblowing: Delibera ANAC n. 469 del 9 giugno 2021;*
- *Decreto Legislativo del 10 Marzo 2023 n. 24 "Attuazione della Direttiva (UE) 1937/2019 del 23 ottobre 2019 […], riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali."*
- *Legge n. 179 del 30 novembre 2017.*

1.1. Principali caratteristiche

- ✓ **Erogabile in configurazione** per Aziende Private, Società Partecipate ed Enti Pubblici;
- ✓ **Gestione dedicata** per i "Responsabili della Segnalazione" (RPCT, ODV) e i "Collaboratori" (Istruttori);
- ✓ **Assegnazione automatica** delle segnalazioni ai Responsabili in base alla tipologia (multicanale);
- ✓ **Possibilità di interazione con soggetti terzi** rispetto al segnalante, al Responsabile e all' Istruttore;
- ✓ **Possibilità di configurazione per Multitenant**;
- ✓ **Configurazione** del modulo di segnalazione;
- ✓ **Erogazione del servizio in S.a.a.S** *(Software as a Service);*
- ✓ **Multilingua**;
- ✓ **Possibilità di accesso tramite *smart card* e *SPID*;**
- ✓ **Autenticazione a due fattori** *(Strong Authentication)***;**
- ✓ **Accesso regolamentato a norma privacy GDPR 2018** *(complessità password e cambio password trimestrale);*
- ✓ **Netta separazione del processo di iscrizione dal processo di segnalazione,** per una corretta separazione dei dati a tutela dell'anonimato del segnalante;
- ✓ **Personalizzazione** dei contenuti, delle informative e delle policy di amministrazione;
- ✓ Possibilità di gestire segnalazioni riservate e/o completamente anonime (a discrezione del committente);
- ✓ **Accessibilità da qualsiasi dispositivo**;
- ✓ **Associabile all'App Legality Whistleblowing;**
- ✓ **Segnalazioni vocali** con distorsione della voce**;**
- ✓ **Complete statistiche** e **log di sistema ANONIMI** che tracciano tutte le operazioni effettuate sulla piattaforma;
- ✓ **Calendario degli eventi e scadenziario**;
- ✓ **Traduzione automatica delle segnalazioni;**
- ✓ **SLA *(Service Level Agreement)* di massimo livello** con garanzia di massima raggiungibilità del servizio, in linea con il Codice dell'Amministrazione Digitale.

Il sistema Segnalazione Illeciti - Whistleblowing è valido per **l'ottenimento delle certificazioni ISO**

ISO 37001
Gestione dell'Anticorruzione

ISO 37002
Gestione del Whistleblowing

ISO 37301
Gestione della Compliance

1.2. Ruoli degli utenti

Le figure coinvolte sono:

Segnalante (Whistleblower)

Dipendente, fornitore, in generale uno stakeholder, che intende segnalare un illecito.

Responsabile

Un dirigente o un'autorità competente (RPCT, ODV, Compliance, etc.) che riceve la segnalazione.

Collaboratore

Istruttore o soggetto nominato dal Responsabile che supporta l'attività del Responsabile stesso.

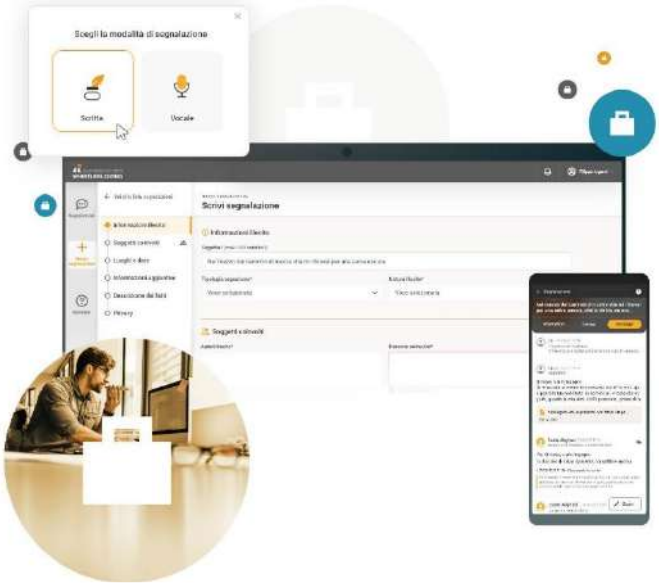
Soggetto Terzo

Soggetti differenti dagli utenti associati alla segnalazione, ma che possono collaborare nelle verifiche.

1.3. Ambiente di segnalazione

Il Segnalante o Whistleblower può:

- Accedere in maniera riservata e sicura al sistema in diverse modalità:
  - **Modalità Riservata**: registrandosi al sistema per l'invio di una segnalazione "nominativa e con gestione dell'identità riservata" (utente registrato);
  - **Modalità Anonima**: inviando una segnalazione senza registrazione e identificazione;
- **Inserire le proprie segnalazioni, scritte o vocali,** tramite una procedura intuitiva e di facile compilazione;
- Inviare la segnalazione tramite la **piattaforma web** oppure dall'**App mobile** Legality Whistlebowing;
- **Seguire la segnalazione** e visualizzare lo stato di lavorazione della segnalazione;

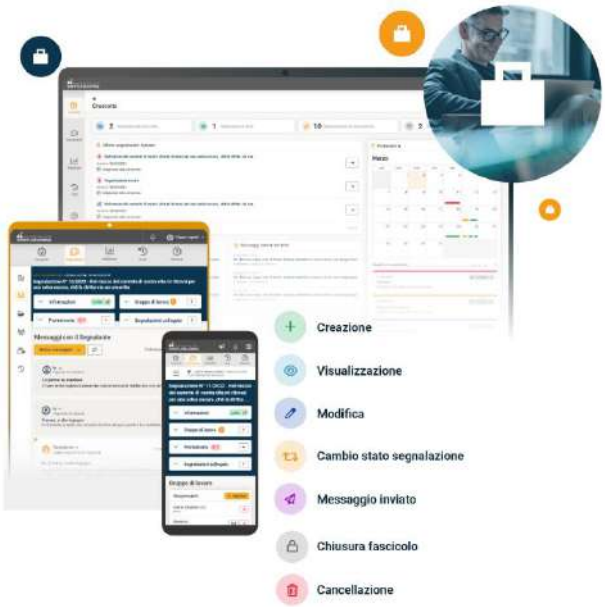


- **Scambiare messaggi** con il Responsabile e, se previsto, anche con i Collaboratori;
- **Ricevere via e-mail** avvisi di risposta alla propria segnalazione e ai messaggi.

1.4. Ambiente di amministrazione

L'ambiente di amministrazione consente al *Responsabile della segnalazione* di:

- **Ricevere via e-mail** un avviso di presenza di segnalazione nel sistema;
- **Gestire lo stato di lavorazione** della segnalazione;
- **Associare o trasferire la segnalazione** ad un altro Responsabile;
- **Condividere informazioni** con i Collaboratori (istruttori);
- **Scambiare messaggi** con il *Gruppo di lavoro*: Collaboratori/istruttori e altri Responsabili;
- **Scambiare messaggi** con il segnalante per eventuale richiesta di documentazione e integrazioni;
- **Redigere note interne** e condividere documenti con altri Responsabili e Collaboratori;
- **Inserire nel sistema segnalazioni** pervenute da altri canali (e-mail, busta chiusa, segnalazioni verbali, etc.);
- **Dialogare con un Soggetto Terzo** (accusato, persona informata sui fatti, testimoni, altri soggetti che possono contribuire alle verifiche o devono essere informati) tramite un'area messaggistica dedicata;



- **Creare report statistici;**
- **Ricevere e creare promemoria**, anche in maniera automatica.

1.5. **Architettura**

Il servizio viene erogato in **S.a.a.S.** (*Software as a Service*), garantendo la terzietà del sistema.

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.

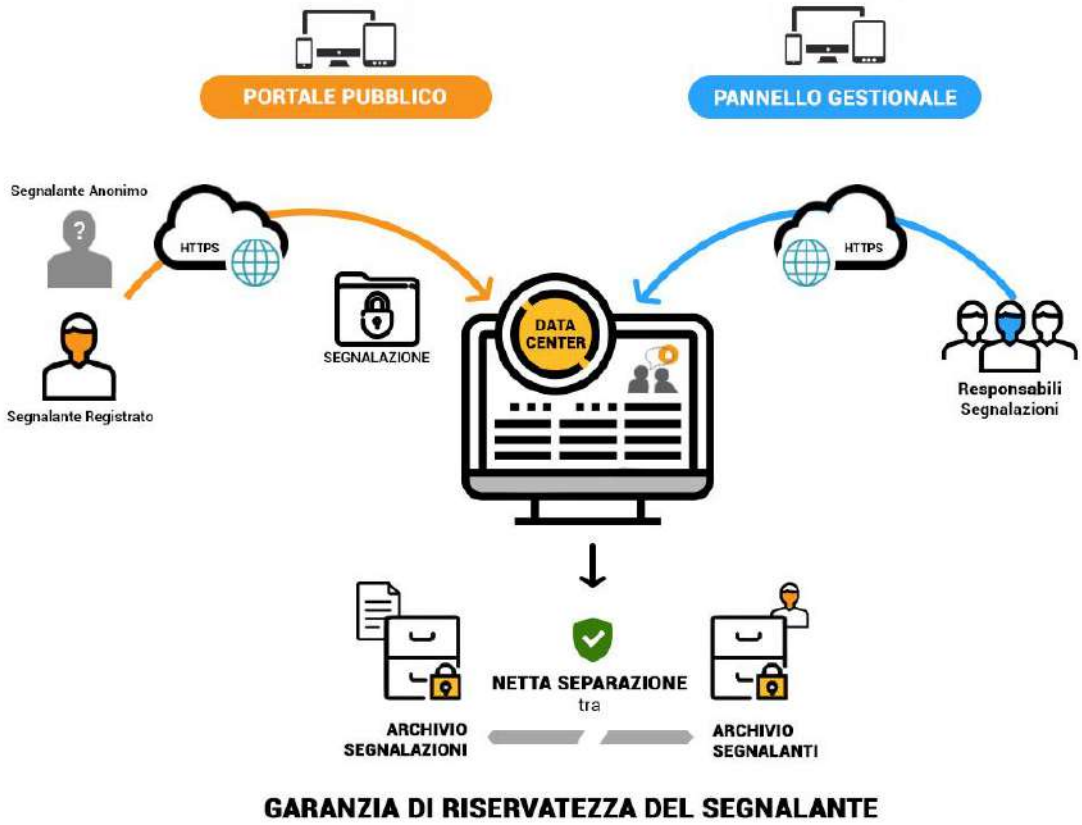
I dati inseriti nel sistema vengono **cifrati sia nella trasmissione**, tramite il protocollo HTTPS, **sia in memorizzazione,** tramite un avanzato sistema di cifratura.

Il sistema è installato su una infrastruttura di Server Dedicati **certificata *TIER IV***[1], che garantisce le migliori prestazioni in termini di sicurezza e di disponibilità dei dati.

Il processo di Registrazione è separato dalla segnalazione, il che consente la gestione delle segnalazioni riservate (nelle quali il segnalante è identificabile) in maniera anonima.

La piattaforma web *Segnalazione Illeciti - Whistleblowing* si suddivide in un ***Portale pubblico / Ambiente di Segnalazione*** **dedicato ai *segnalanti*** e un ***Pannello gestionale / Area di Amministrazione*** **dedicato al *Responsabile della segnalazione*** (o ai Responsabili e ad eventuali Collaboratori incaricati).

I segnalanti possono inviare la segnalazione anche attraverso **l'App Legality Whistleblowing**, collegata alla piattaforma web.



[1] **TIER IV**. È il livello più alto di garanzia che un datacenter può offrire, con una disponibilità del 99.99%, questa categoria di datacenter è completamente ridondata a livello di circuiti elettrici, di raffreddamento e di rete.

1.6. Configurazione

La piattaforma software può essere configurata in modo da consentire la gestione delle segnalazioni secondo il **proprio modello organizzativo** e secondo le proprie politiche di gestione. È possibile ad esempio:

- **Configurare più di un soggetto** Responsabile della segnalazione;
- **Configurare le tipologie** di segnalazione;
- **Associare automaticamente** ad ogni Responsabile le tipologie di segnalazione di propria competenza;
- **Configurare** la piattaforma in modo da consentire o meno segnalazioni di **utenti non registrati** (segnalazioni anonime);
- **Configurare il sistema di notifiche;**
- **Configurare le politiche di gestione delle password;**
- **Configurare le modalità di segnalazione** (con registrazione, senza registrazione, segnalazione vocale);
- Associare l'**App Legality Whistleblowing**;
- Configurare un sistema di ***data-retention.***

1.6.1. Configurazione Enti territoriali (Comuni, Province, Regioni, ecc.)

La configurazione per gli Enti Territoriali prevede tipicamente la presenza di **un solo Responsabile** (ad esempio il **Responsabile per la Prevenzione della Corruzione e della Trasparenza - RPCT**): in questo caso il sistema viene configurato con un singolo utente Responsabile che ha la completa gestione delle segnalazioni.

Oltre al Responsabile possono essere configurati degli **Utenti Collaboratori**, ovvero *gli istruttori che fanno parte della struttura di supporto del RPCT* e che possono intervenire solo all'interno di una segnalazione esplicitamente condivisa dal Responsabile.

In caso di necessità è possibile configurare più utenti Responsabili.

1.6.2. Configurazione Aziende (Società private, Enti di diritto pubblico, Società partecipate, ecc.)

La configurazione tipica per questa tipologia di organizzazioni prevede la coesistenza di **più soggetti preposti alla ricezione e gestione delle segnalazioni**: in questo caso il sistema può essere configurato in maniera tale da **assegnare automaticamente ad ogni Responsabile le tipologie di segnalazione di propria competenza**.

Gli organi competenti hanno la possibilità di trasferire o condividere le segnalazioni tra di loro e **assegnarle ai Collaboratori.**

1.6.3. Configurazione Multitenant o Gruppo

La configurazione **Multitenant** o **Gruppo** prevede la possibilità di raccogliere, in un'unica piattaforma, le segnalazioni provenienti da diverse Società facenti parte di un gruppo. L'inoltro ai Responsabili delle segnalazioni è automatizzato in base alla società e alla tipologia di segnalazione.

Nel form di segnalazione è presente un campo che consente al Whistleblower di indicare per quale Società vuole trasmettere la segnalazione.

Questo campo è collegato ai Responsabili e consente un'assegnazione precisa ai Responsabili di riferimento delle varie Società, sfruttando l'associazione "Società" e "Tipologia di illecito".

1.7. **Multilingua**

Il software **Legality Whistleblowing** è nativamente predisposto per il sistema **multilingua,** attivabile in molteplici lingue tra le più diffuse: italiano, inglese, francese, spagnolo, tedesco, portoghese, greco, rumeno, turco e altre su richiesta.

2. Tipologie di segnalazione

La piattaforma può essere configurata per consentire l'invio di segnalazioni "riservate" e segnalazioni "anonime".

2.1. **Segnalazioni Riservate**

Per segnalazioni riservate si intendono le segnalazioni di utenti identificabili. Le segnalazioni riservate prevedono la **registrazione preliminare** dell'utente e successivamente, una volta creato l'account, l'utente può inviare la segnalazione.

I dati del segnalante registrato sono separati dalla segnalazione, pertanto la segnalazione viene inviata al Responsabile in forma anonima.

Soltanto il Responsabile è in grado di associare la segnalazione all'utente che l'ha creata e quindi visualizzare l'identità del segnalante.

2.2. **Segnalazioni Anonime**

Le segnalazioni anonime sono segnalazioni che non consentono l'associazione della segnalazione al nominativo del segnalante, in quanto il dato del nominativo del segnalante non esiste.

In questo caso il segnalante non è obbligato a registrarsi al sistema e può inviare la segnalazione come utente non registrato.

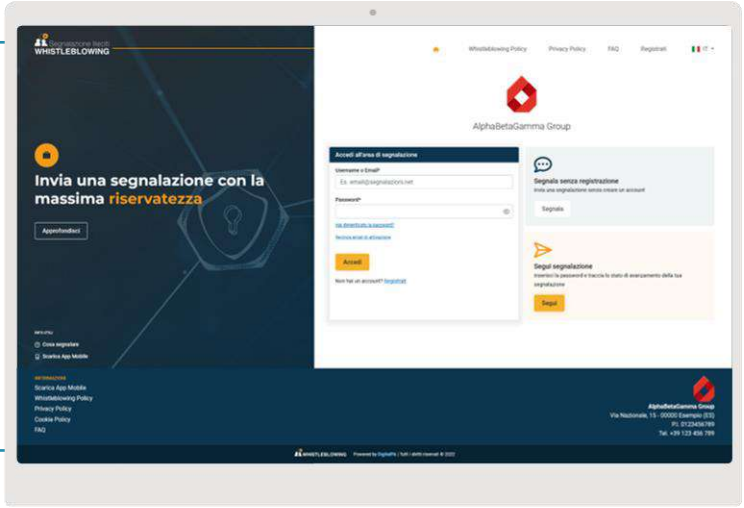
Homepage pubblica – Accesso area Segnalanti

A sinistra:

- *Card di accesso e registrazione*

A destra:

- *Card con bottone per la segnalazione anonima e il tracciamento dello stato di lavorazione*



3. Ambiente di segnalazione

L'accesso alla segnalazione è differente a seconda che la segnalazione sia stata inviata da un utente registrato (segnalazione riservata) oppure da un utente non registrato (segnalazione anonima).

- **Utente registrato:** accede alla segnalazione tramite lo username e la password scelte in fase di registrazione.
- **Utente non registrato:** accede alla segnalazione tramite i codici generati dal sistema nella fase di invio della segnalazione.

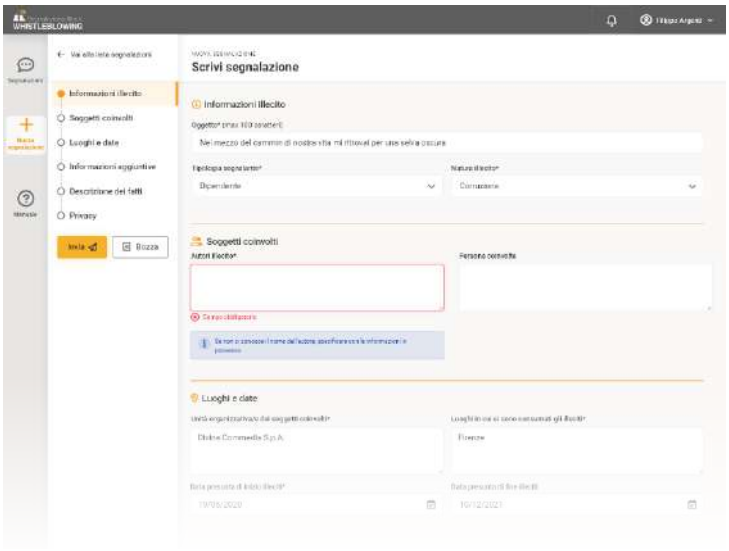
3.1. Form di segnalazione

A seconda della versione del software prescelta, sono disponibili **due modalità di segnalazione**: scritta e vocale.

Il form è personalizzabile: è possibile aggiungere nuovi campi, configurarne le etichette e la loro obbligatorietà.

3.1.1. Segnalazione Scritta

I campi di segnalazione scritta di default sono i seguenti:

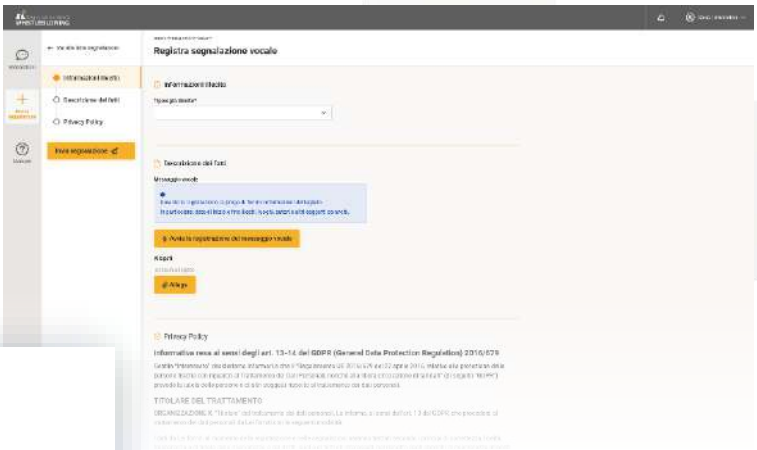


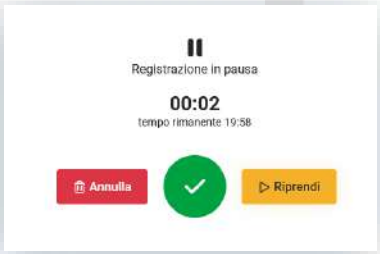
- **Informazioni illecito**
  - Oggetto *
  - Tipologia segnalante* (rapporto del segnalante con l'Organizzazione)
  - Natura Illecito* (elenco di valori preimpostati **configurabili** e selezionabili tramite menu a tendina)
- **Soggetti Coinvolti**
  - Autori illecito*
  - Persone informate
- **Luoghi e date**
  - Unità Organizzativa/e delle persone coinvolte*
  - Luogo in cui si è verificato il fatto*
  - Data (anche presunta) in cui si è verificato il fatto*
  - Data (anche presunta) di conclusione del fatto
- **Descrizione dei fatti***
- **Allegati** (con controllo dell'estensione degli allegati, al fine di limitare l'upload solo alle estensioni desiderate)

3.1.2. Segnalazione vocale

La segnalazione vocale consente al segnalante di compilare campi limitati e di fornire le informazioni tramite **messaggio vocale.**

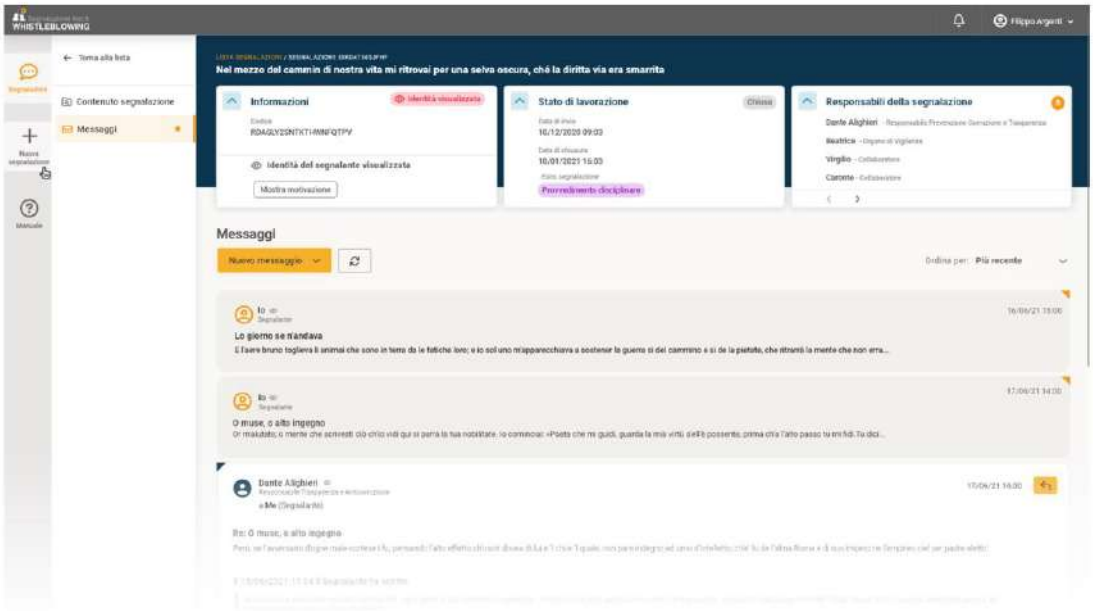
La voce del segnalante sarà irriconoscibile grazie ad un sistema integrato di distorsione vocale.





3.2. Monitoraggio e integrazione della segnalazione

Il segnalante può seguire lo stato di lavorazione della segnalazione, integrarla e rispondere ad eventuali richieste del Responsabile attraverso l'area messaggi integrata.



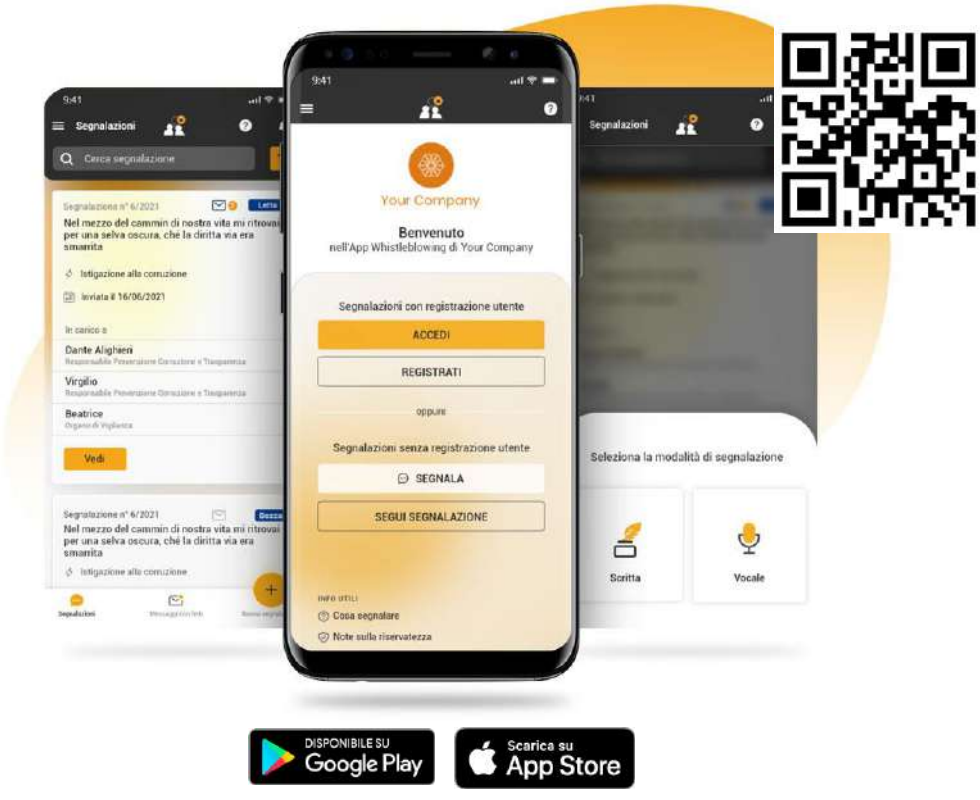
3.3. App Legality Whistleblowing

L'**App Legality Whistleblowing** consente a dipendenti, fornitori e collaboratori di inviare segnalazioni di irregolarità via **dispositivo mobile.**

L'applicazione è **compliant alle direttive nazionali e internazionali** (Direttiva UE 1937/2019 e Regolamento 679/2016 GDPR) e si configura come **canale alternativo al portale web**, per garantire la completa accessibilità all'ambiente di segnalazione e per offrire un sistema intuitivo che guidi il Whistleblower nel processo di segnalazione.

3.3.1. Principali caratteristiche dell'App

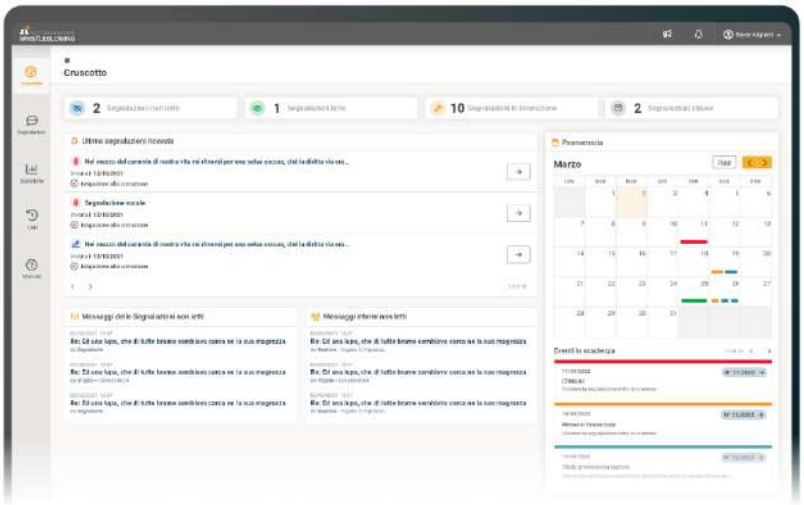
- ✓ **Accesso sicuro -** Autenticazione a due fattori e login con credenziali biometriche (impronta, faceID, etc);
- ✓ **Area esclusiva per singola Organizzazione -** Accessibile dai segnalanti tramite QR Code o codice alfanumerico univoco;
- ✓ **Modalità di segnalazione configurabili -** Segnalazioni scritte e vocali, possibilità di attivare le segnalazioni anonime o a seguito di registrazione;
- ✓ **Sicurezza avanzata -** Conformità normativa e protocolli di sicurezza avanzati (approfondisci al capitolo § 6. Sicurezza e riservatezza lato Software);
- ✓ **Multilingua -** Disponibile in molteplici lingue;
- ✓ **Notifiche configurabili -** Possibilità di attivare le *notifiche push* per aggiornamenti sullo stato di lavorazione della segnalazione;
- ✓ **User-friendly –** Workflow guidati per la trasmissione di segnalazioni e conformità ai requisiti di accessibilità degli strumenti informatici.



4. Area di Amministrazione

L'Area riservata al *Responsabile delle segnalazioni* consente la gestione rapida e funzionale di tutte le segnalazioni ricevute.

Il **Cruscotto** offre una panoramica delle ultime segnalazioni ricevute, degli ultimi messaggi ricevuti e delle attività programmate nel calendario promemoria.



4.1. Elenco segnalazioni

Le segnalazioni sono suddivise in tre elenchi:

Segnalazioni aperte

Segnalazioni appena ricevute e in lavorazione.

Segnalazioni chiuse

Segnalazioni gestite e/o archiviate.

Segnalazioni cancellate

È possibile cancellare una segnalazione se è stata chiusa da un periodo di tempo configurabile o se contrassegnata da uno stato particolare (es. Spam).

In ciascun elenco le segnalazioni sono suddivise in pagine sfogliabili grazie alla presenza di appositi comandi.

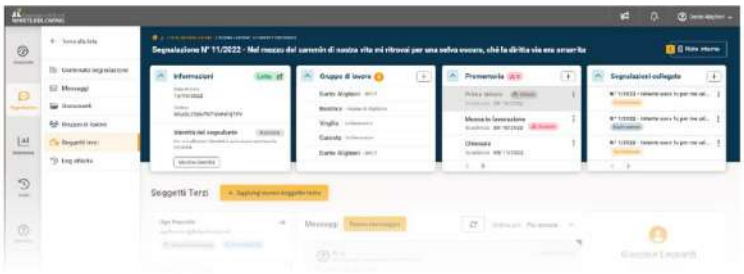
Il sistema consente, inoltre, di individuare le segnalazioni di proprio interesse attraverso i **filtri.**

4.2. Segnalazioni extra piattaforma

Nel caso in cui l'Organizzazione riceva una segnalazione da canali diversi rispetto al software, come nel tipico caso di una **segnalazione telefonica o via email**, il Responsabile può creare il fascicolo della segnalazione al fine di gestirla all'interno del software, preservando così il contenuto e l'identità del segnalante, e poter dare un riscontro oggettivo sulla sua gestione.

5. Fascicolo della segnalazione

Per ogni segnalazione viene creato un *fascicolo digitale* che contiene le informazioni inviate dal *Whistleblower* nella segnalazione iniziale e integrate attraverso l'area Messaggi, tutte le informazioni "interne" inserite dal Gruppo di Lavoro come le note, i documenti raccolti durante l'istruttoria e le comunicazioni del gruppo di lavoro (messaggi interni).



La navigazione del fascicolo può essere divisa concettualmente in due aree principali: le **comunicazioni con il segnalante** e le **informazioni sull'istruttoria.**

5.1. Comunicazioni con il segnalante

5.1.1. Contenuto segnalazione

Comprende tutte le informazioni trasmesse dal *Whistleblower* attraverso il form di segnalazione.

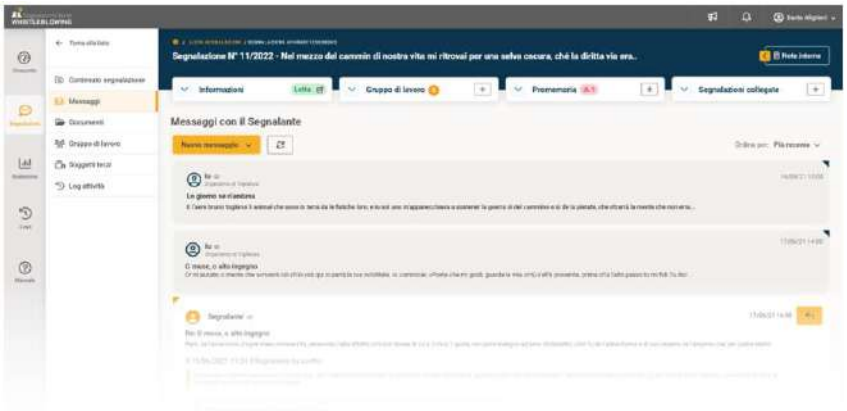
5.1.2. Messaggi

L'area *Messaggi* è una speciale bacheca nella quale confluiscono i messaggi scambiati tra il **Gruppo di Lavoro** e il **segnalante.**

Le informazioni sono visualizzabili esclusivamente in quest'area, mentre un sistema di notifiche avvisa gli utenti della presenza di nuovi messaggi in piattaforma.

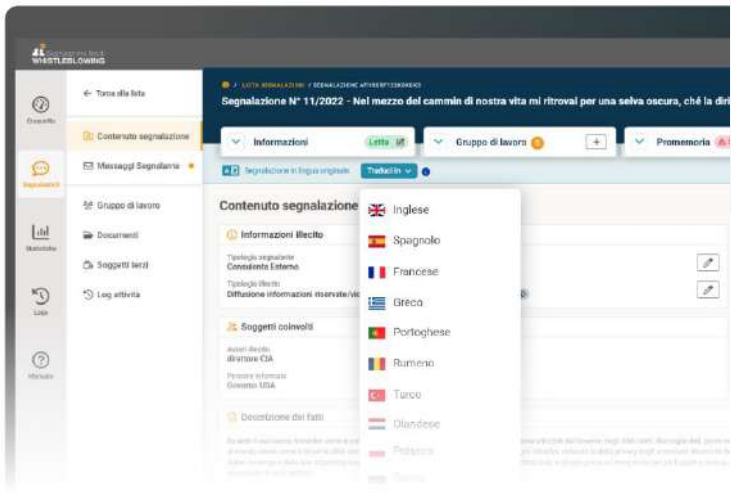
Se la **segnalazione vocale** è attiva, anche il Responsabile può inviare le comunicazioni tramite messaggio vocale.

I messaggi, come tutte le informazioni inserite in piattaforma, sono salvati in maniera cifrata.



TRADUZIONE AUTOMATICA DI SEGNALAZIONI E MESSAGGI

Legality Whistleblowing include un sistema avanzato di traduzione automatica del **Contenuto della segnalazione** e dei **Messaggi con il segnalante** per il **Responsabile,** e dei **Messaggi ricevuti** per il **Segnalante.**



Ciò consente di:

- **Abbattere le barriere linguistiche -** comprendere e ottenere informazioni complete sulla segnalazione ricevuta;
- **Tradurre in modo rapido e preciso** - risparmiando tempo e sforzi nel dover tradurre manualmente ogni singolo testo.

Il sistema si avvale di API di *DeepL*, sistema di traduzione multilingua di elevata qualità e di prestigio globale, è stato selezionato per l'adesione rigorosa alle leggi europee sulla **protezione dei dati** e all'**ISO 27001**, certificazione per la *Sicurezza delle Informazioni*. I testi tradotti non vengono salvati in archivi esterni e non sono utilizzati per addestrare modelli di traduzione.

5.1.3. Documenti

Nella sezione *Documenti* è possibile inserire la documentazione raccolta durante l'istruttoria.

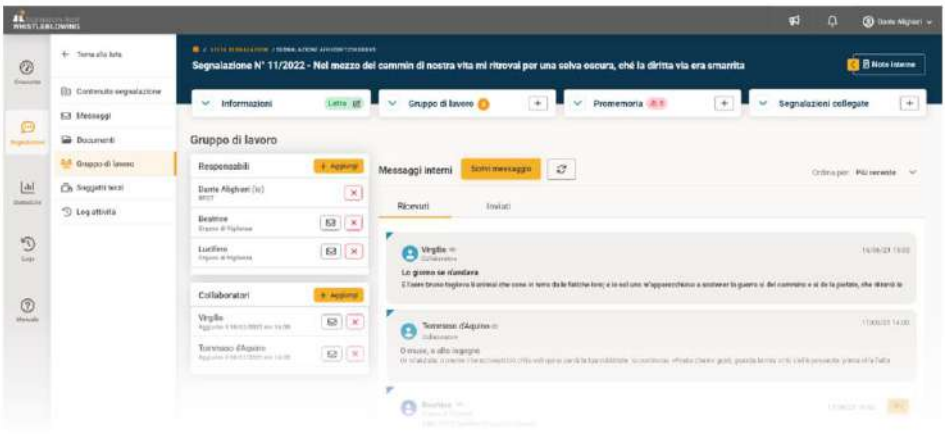
I documenti possono essere condivisi con gli altri **Responsabili**, con l'intero **Gruppo di Lavoro** (Responsabili + Collaboratori), oppure restare riservati ad esclusivo utilizzo di un utente.

5.1.4. Gruppo di Lavoro

La sezione Gruppo di Lavoro consente di gestire i Responsabili e i Collaboratori assegnati alla segnalazione.

Il sistema di *Messaggistica interna*, presente in questa sezione, permette lo scambio di comunicazioni tra i componenti del Gruppo di Lavoro.

Un **sistema di notifiche** avvisa gli utenti della presenza di nuovi messaggi in piattaforma.



5.1.5. Soggetti terzi

La sezione consente di creare un canale di comunicazione con un Soggetto Terzo (ad esempio un testimone, l'accusato o altre persone informate dei fatti) non registrato in piattaforma.

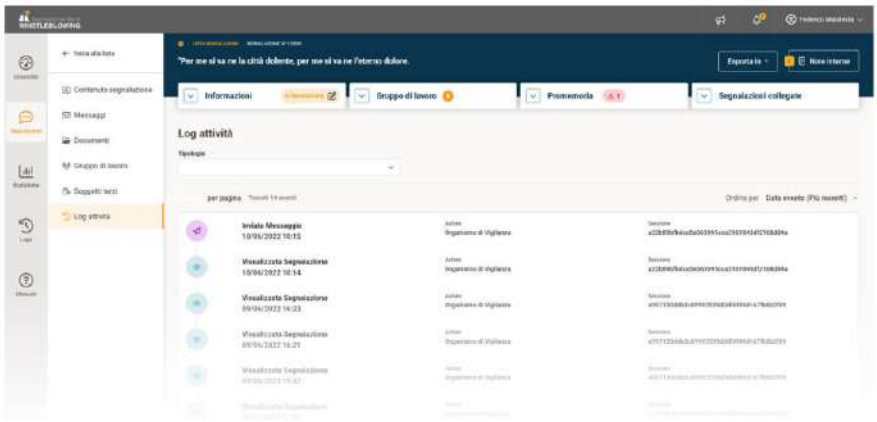
Il Soggetto Terzo accede ad un'area dedicata nella quale può inviare e ricevere messaggi e documenti dialogando esclusivamente con il Responsabile.

I messaggi scambiati in quest'area sono protetti con crittografia asimmetrica e sono decifrabili esclusivamente dal destinatario del messaggio tramite la specifica piattaforma software.

È possibile dialogare privatamente con un numero potenzialmente illimitato di Soggetti Terzi.

5.1.6. Log Attività

Tutte le operazioni effettuate sulle segnalazioni, da parte di tutti gli utenti, vengono registrate nei *Log di sistema* in maniera anonima e criptata per **garantire la massima riservatezza e anonimato.**



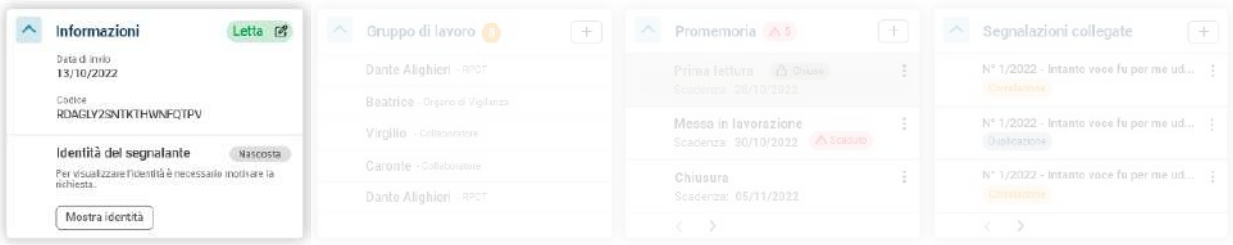
5.1.7. Note interne

Segnalazione Illeciti – Whistleblowing include un sistema di note interne, che i **Responsabili** possono utilizzare per aggiungere delle annotazioni alla segnalazione.

5.2. Dettagli della segnalazione

I dettagli generali della segnalazione sono inseriti in **card comprimibili presenti in alto nella pagina** e consultabili in tutte le sezioni del fascicolo.

5.2.1. Card Informazioni



La card Informazioni contiene lo stato di lavorazione, la data di ricezione, il codice alfanumerico identificativo della segnalazione e il bottone per lo sblocco della visibilità dell'identità del segnalante (in caso di utente registrato).

STATO DI LAVORAZIONE

Il Responsabile ha la facoltà di modificare lo stato in modo da organizzare in maniera efficiente le varie segnalazioni.

Gli *stati di lavorazione*, possono essere configurati e per default sono così definiti:

- Non letta (automatico);
- Letta (automatico);
- In lavorazione;
- Archiviata:
  - Rigettata (non si è ritenuto di dover prendere in considerazione la segnalazione);
  - Accettata;
  - Provvedimento disciplinare;
  - Inoltrata a soggetti terzi competenti;
  - Altro (…).

Le segnalazioni che hanno avuto un esito, vengono **archiviate** nell'elenco Segnalazioni Chiuse.

Lo ***Stato di Lavorazione*** è visibile anche al segnalante, 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.

IDENTITÀ DEL SEGNALANTE

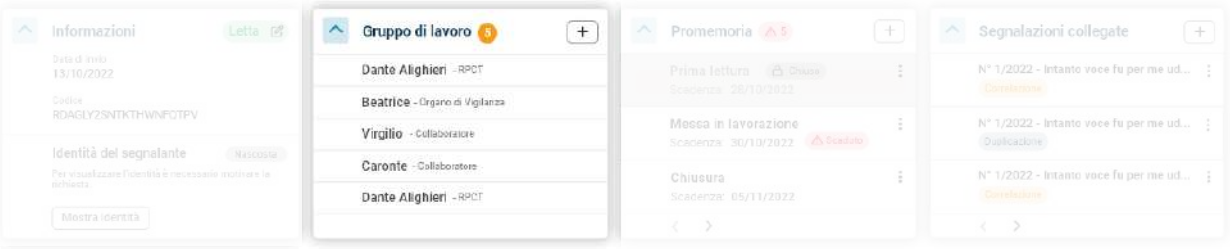
Qualora fossero attive le ***Segnalazioni Riservate*** (vedere § 2. Tipologie di Segnalazione), il Responsabile ha la possibilità di visualizzare l'Identità del segnalante a seguito della motivazione della richiesta.

Custode dell'identità

È possibile configurare il sistema in modo tale che l'identità sia richiesta ad un utente terzo, denominato ***Custode dell'identità,*** che può concedere ad un Responsabile la possibilità di accedere all'identità del segnalante.

Il Custode dell'Identità non ha accesso né alle segnalazioni, né alle identità.

5.2.2. Card gruppo di lavoro



La card Gruppo di Lavoro consente di consultare e associare Responsabili e Collaboratori alla segnalazione.

RESPONSABILI

È possibile la **condivisione o la riassegnazione della segnalazione** da parte di un Responsabile ad un altro, che potrà, quindi, gestire la segnalazione con le stesse facoltà.

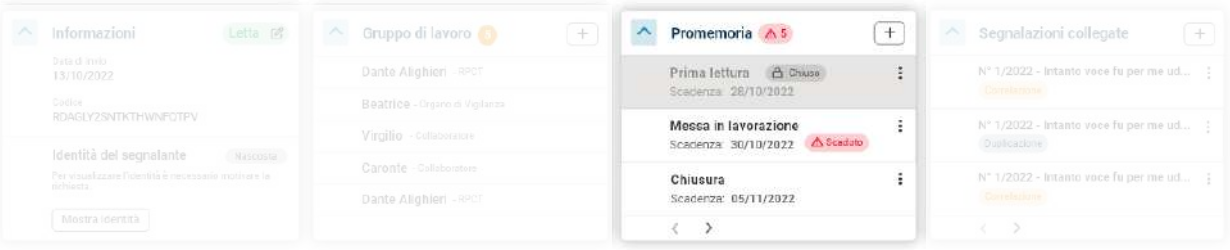
COLLABORATORI

Diversamente, il Collaboratore associato ad una segnalazione che entra a far parte del Gruppo di lavoro non ha accesso a tutte le sezioni del fascicolo.

Il collaboratore accede alle seguenti sezioni:

- Messaggi Interni;
- Documenti;
- Messaggi con il segnalante (opzionale).

5.2.3. Card Promemoria

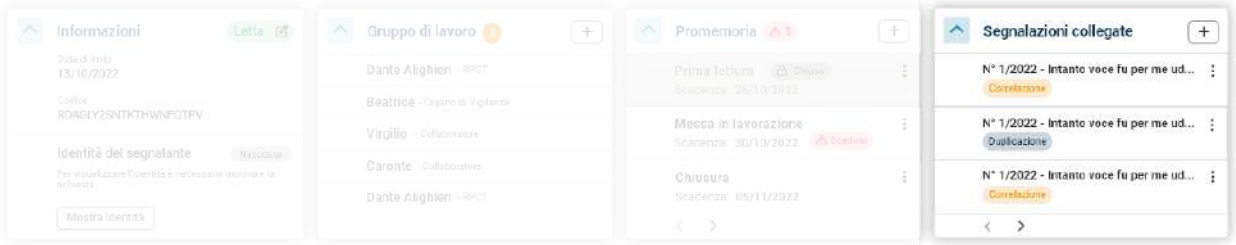


Attraverso la Card Promemoria è possibile configurare un sistema di *alert* basato su un calendario.

Ad esempio, è possibile impostare degli avvisi di **scadenza sulla lettura**, sulla **presa in carico**, la **chiusura** o altri avvisi personalizzati creati dal Responsabile.

Gli avvisi creati saranno visualizzati anche nel Calendario presente nel Cruscotto del Responsabile (vedere § 4. Area di Amministrazione).

5.2.4. Card segnalazioni collegate



La card Segnalazioni Collegate consente di creare delle relazioni tra diverse segnalazioni, in modo da tenere sotto controllo le segnalazioni analoghe e poter navigare agilmente tra i fascicoli.

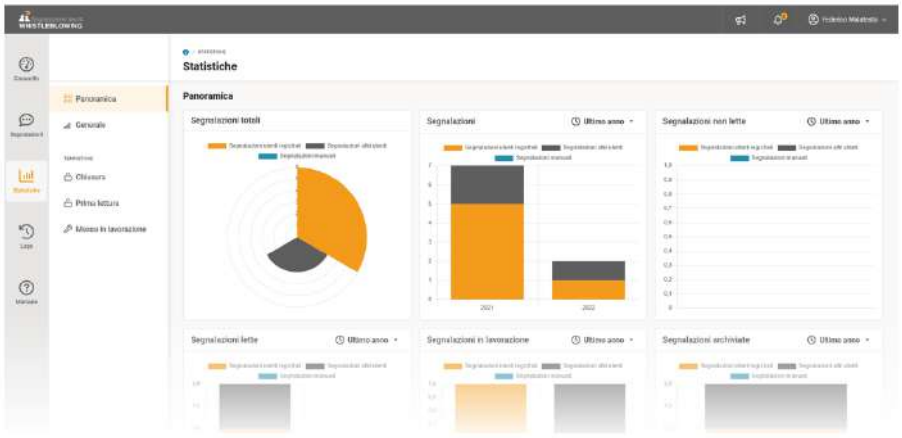
5.3. Statistiche

La piattaforma Segnalazione Illeciti - Whistleblowing è dotata di sofisticati strumenti di elaborazione dati in grado di restituire all'Organizzazione una visione sintetica delle attività di gestione del Whistleblowing.

I grafici presenti nell'area Statistiche consentono di visualizzare statistiche per stato di lavorazione, tipologia di segnalante (anonimo o registrato) e di inquadrarli all'interno di un periodo temporale.

Il sistema restituisce inoltre report riguardanti le **tempistiche di prima lettura, messa in lavorazione e chiusura delle segnalazioni.**

In qualsiasi momento l'utente può esportare i grafici in formato *xls.



6. Sicurezza e riservatezza lato Software

Sulla piattaforma **Segnalazione Illeciti - Whistleblowing** **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 segnalante, sono **protette da un sistema di cifratura.**

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 (segnalante) ed eventuali segnalazioni.

6.1. Caratteristiche tecniche del sistema di cifratura

6.1.1. Gestione password per autenticazione

Le 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 queste sono memorizzate in modalità cifrata, in combinazione con un *salt random*[2], nel database di sistema con algoritmo *Hash SHA512.*

Non è possibile, partendo dall'hash, ricalcolare la password originale.

6.1.2. Autenticazione a due fattori (*strong authentication*)

L'accesso al sistema deve essere confermato tramite inserimento di un codice inviato dal sistema all'indirizzo email dell'utente. L'opzione può essere disabilitata dall'utente stesso.

[2] *In crittografia, un sale (salt random) è una sequenza casuale di bit utilizzata assieme ad una password come input a una funzione unidirezionale, di solito una funzione hash, il cui output è conservato al posto della sola password, e può essere usato per autenticare gli utenti.*

Il sale è usato per salvaguardare le password salvate in memoria e viene generato casualmente ogni volta che viene generata una password.

LEGENDA

KpubS, KprivS	Coppia di chiavi pubblica e privata segnalante;
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.

6.1.3. 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 segnalante, **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 bit;
- una **chiave simmetrica** (KsimS) lunga 32 caratteri;
- una **chiave di cifratura** (Kmp) lunga 32 caratteri.

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.

6.2. Flusso cifratura e decifratura per il segnalante 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 segnalante 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 potranno decodificare i contenuti della segnalazione.

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

LEGENDA

KpubS, KprivS	Coppia di chiavi pubblica e privata segnalante;
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.

6.3. Flusso cifratura e decifratura per il segnalante 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 segnalante dopo l'invio della segnalazione.

Per la decifratura il sistema chiederà la Kmp al segnalante 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 segnalante inserisce dei contenuti per una segnalazione il sistema li cifra utilizzando la KsimS associata.

6.4. 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.

6.5. Cifratura dei log

L'accesso ai log è consentito esclusivamente al Responsabile delle Segnalazioni. 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.

6.6. 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 un'associazione tra la sessione e l'utente. Una volta scaduta la sessione, questa 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.

6.7. Sostituzione Responsabile e smarrimento password

Qualora il Responsabile debba essere sostituito (temporaneamente o definitivamente), è possibile farlo adottando la seguente procedura:

- Il Responsabile in carica consegna le credenziali per l'accesso alla piattaforma al nuovo Responsabile;
- Il nuovo Responsabile accede e modifica i dati anagrafici, l'indirizzo email e la password;
- A questo punto il nuovo Responsabile accede con le nuove credenziali formate dal nuovo indirizzo email e la nuova 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 Responsabile. I messaggi del precedente Responsabile saranno contrassegnati dal nome del vecchio Responsabile.

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

In caso di **smarrimento della password** di accesso del Responsabile o in caso di impossibilità di procedere in autonomia al passaggio di consegne è prevista la seguente procedura di emergenza.

Su richiesta del "nuovo" Responsabile, l'utente Super User (DigitalPA) modifica l'indirizzo email del "vecchio" Responsabile al fine di consentire il reset password al "nuovo" Responsabile.

7. Servizi

L'attenzione alle esigenze della Pubblica Amministrazione e delle Aziende è, da sempre, il focus per DigitalPA.

Per questo motivo offriamo ai nostri Clienti l'eccellenza attraverso un team costituito da **consulenti, legali** ed **esperti** dalle elevate competenze tecniche ed analitiche che lavorano a stretto contatto con un gruppo di **sviluppatori senior** costantemente aggiornati sulle dinamiche del cambiamento tecnologico.

Da quest'unione, scaturiscono **soluzioni software dall'interfaccia semplice ed intuitiva** che celano un'anima complessa e altamente tecnologica.

Vogliamo mettere a vostra completa disposizione la nostra professionalità, offrendo, oltre ad una selezione di software di alto livello, anche una gamma di **servizi completi** ad alto contenuto di specializzazione.

Riteniamo fondamentale offrire ai nostri Clienti un valore aggiunto ai servizi, quali:

- Consulenza;
- Installazione;
- Assistenza;
- Manutenzione.

Un unico obiettivo: agevolare il lavoro delle risorse umane, massimizzarne l'efficacia, guidarle nel processo di transizione al digitale e consentire al Cliente di essere immediatamente adempiente alle più recenti disposizioni normative.

7.1. Installazione e configurazione

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

7.1.1. 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 e-mail.

Una volta ricevuta la lista degli utenti e dei relativi indirizzi di posta elettronica, DigitalPA provvederà alla creazione delle utenze in stato "**non attivo**".

Alla consegna del software, in accordo con le indicazioni del Cliente, si provvederà ad attivare le utenze: il sistema invierà contestualmente le e-mail 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 dell'utente amministratore creare le utenze e scegliere se inviare, contestualmente alla creazione, l'e-mail 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 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.

7.2. **Formazione sul software**

La formazione è la base imprescindibile per un utilizzo appropriato e approfondito degli applicativi.

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'Organizzazione 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.

All'interno del software sono presenti, inoltre, una serie di strumenti formativi di supporto:

- Manuali operativi per Segnalanti e Responsabili (disponibili su richiesta in varie lingue);
- Videoguide per i Responsabili.

7.3. 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 e-mail** (canale prioritario): per la richiesta di chiarimenti o spiegazioni del programma e segnalazioni di malfunzionamenti;
- **Assistenza telefonica,** per la richiesta di chiarimenti e segnalazioni di malfunzionamenti, tutti i giorni lavorativi dal lunedì al giovedì, dalle ore 9.30 alle ore 17,30, il venerdì dalle ore 9,30 alle ore 15,00.

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

7.3.1. 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.

7.4. SLA *(Service Level Agreement)* garantiti

Le statistiche degli ultimi 3 anni riportano un uptime del 99,9%.

Adeguamenti del software alla vigente normativa (Manutenzione normativa)

Vengono immediatamente pianificati alla pubblicazione di una nuova disposizione normativa e hanno azione prioritaria.

Manutenzione programmata del Software

Vengono pianificati rilasci di aggiornamenti con cadenza mensile o, ove necessario, con maggiore frequenza, per nuove implementazioni e 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

L'intervento è pressoché immediato sia per problemi bloccanti che non bloccanti.

2h lavorative	Risoluzione problemi bloccanti	4gg lavorativi	Risoluzione problemi non bloccanti	5gg lavorativi	Risoluzione problemi minori	30gg lavorativi	Allineamento normativo

8. Riferimenti normativi

8.1. Legge 179/2017 sul Whistleblowing

"Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato" in vigore dal il 29/12/2017 a tutela del dipendente pubblico e privato e che prevede che sia predisposto "*almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante.*"

8.2. D.lgs. 10 Marzo 2023, n. 24 - recante le norme di attuazione della Direttiva (UE) 2019/1937 del 23 ottobre 2019

Disciplina la protezione delle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato

Il Decreto impone a tutte le aziende private con una media nell'ultimo anno di ***almeno 50 dipendenti*** *a tempo determinato o indeterminato, o che, anche se non abbiano raggiunto detta media, abbiano adottato un MOG ai sensi della Legge 231, l'istituzione di canali interni sicuri per la segnalazione degli illeciti.*

Sono obbligati ad adottare un canale di gestione del Whistleblowing ***tutte le Amministrazioni pubbliche*** *di cui all'art. 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, le autorità amministrative indipendenti di garanzia, vigilanza o regolazione, gli enti pubblici economici, gli organismi di diritto pubblico di cui all'articolo 3, lettera d), del decreto legislativo 18 aprile 2016, n. 50, i concessionari di pubblico servizio, le società a controllo pubblico e le società in house, così come definite, rispettivamente, dall'art. 2, comma 1, lettere m) e o), del decreto legislativo 19 agosto 2016, n. 175, anche se quotate.*

8.3. Linee guida ANAC e PNA

8.3.1. Regolamento ANAC del 12 luglio 2023

Regolamento per la gestione delle segnalazioni esterne e per l'esercizio del potere sanzionatorio ANAC – Delibera n. 301 – 12.07.2023

Il regolamento, emanato il 12 luglio 2023 dall'Autorità Nazionale Anticorruzione, si pone l'obiettivo di:

- disciplinare la gestione delle segnalazioni esterne effettuate dal whistleblower ;
- accertamento di ritorsioni adottate nei confronti del whistleblower e degli altri soggetti coinvolti – facilitatori, colleghi di lavoro, persone nel medesimo contesto lavorativo e così via – nei settori pubblico e privato;
- accertamento della violazione dell'obbligo di riservatezza;
- accertamento dell'assenza di canali di segnalazione e di adeguate procedure per effettuare e gestire le segnalazioni di illeciti;
- accertamento del mancato svolgimento dell'attività di verifica e analisi delle segnalazioni di illeciti;
- accertamento della fattispecie sanzionatoria nei confronti del whistleblower "quando è accertata, anche con sentenza di primo grado, la sua responsabilità

- civile per diffamazione o calunnia nei casi di dolo o colpa grave" (art. 21, comma 1, lett. c) del D.Lgs. 24/2023).

Il Regolamento conferisce ad ANAC il potere sanzionatorio d'ufficio o, a seconda dei casi, su comunicazione o esposto.

8.3.2. Delibera n. 469 del 9 giugno 2021

L'ANAC, con la *Delibera n. 469 del 9 giugno 2021* ha emesso le "*Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis, del d.lgs. 165/2001 (c.d. whistleblowing)*" con la chiara indicazione che le segnalazioni, al fine di tutelare il segnalante, debbano essere trattate con sistemi informatizzati e crittografici.

8.3.3. Piano Nazionale Anticorruzione 2019

Delibera ANAC n. 1064 del 13 novembre 2019:

> *"Il RPCT, oltre a ricevere e prendere in carico le segnalazioni, pone in essere gli atti necessari ad una prima attività di verifica e di analisi delle segnalazioni ricevute da ritenersi obbligatoria in base al co. 6 dell'Art. 54-bis. si rammenta infatti che la richiamata disposizione prevede che ANAC irroghi sanzioni pecuniarie da 10.000 a 50.000 euro qualora venga accertato il mancato svolgimento da parte del Responsabile di attività di verifica e analisi delle segnalazioni ricevute."*

8.4. Ulteriori indicazioni normative

8.4.1. Art. 1, comma 51, della Legge n. 190/2012

"Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione" introduce nel D.lgs. n. 165/2001 "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche", una nuova disposizione, l'Articolo 54-bis, intitolato *"Tutela del dipendente pubblico che segnala illeciti"*. La norma, introduce di fatto per la prima volta, **la regolamentazione del whistleblowing nell'ambito della Pubblica Amministrazione**. Prevista la tutela per il lavoratore pubblico che segnali un illecito o violazione ai soggetti preposti, proteggendolo contro le eventuali ritorsioni da parte di colleghi o superiori.

8.4.2. Articolo 6, comma 2-bis del D.lgs. n. 231/2001

Introdotto dall'Art. 2 della Legge n. 179 del 2017, prevede l'utilizzo di "*almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante."*

8.4.3. Regolamento ANAC

Il regolamento per la gestione delle segnalazioni e per **l'esercizio del potere sanzionatorio** in materia di tutela degli autori di segnalazioni di illeciti o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro di cui *all'art. 54 bis Decreto legislativo n. 165/2001* - pubblicato nella Gazzetta Ufficiale - *Serie Generale n. 205 del 18 agosto 2020.*

9. Servizi Anticorruzione e Trasparenza

La Legge 190/2012 Art.1 e l'ANAC impongono **obblighi di formazione** mirata in materia di Anticorruzione e Trasparenza ai **Responsabili della Prevenzione della Corruzione e della Trasparenza** (RPCT), ai referenti, ai componenti degli organismi di controllo, ai dirigenti e funzionari addetti alle aree di rischio.

Tale formazione deve avere carattere specifico, al fine di formare tali soggetti in relazione alle specificità che caratterizzano il loro lavoro, ovvero alle diverse casistiche di esposizione ai rischi di corruzione e, di conseguenza, alle specifiche misure di prevenzione da porre in atto.

DigitalPA eroga programmi di formazione mirati che consentono agli RPCT di conoscere e assolvere agli obblighi normativi di loro competenza.

9.1. Programma del corso Anticorruzione e Trasparenza

9.1.1. Modulo Anticorruzione

- **Legge 6 novembre 2012, n. 190 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione"**

  Risvolti pratici e aspetti operativi, analisi delle principali autorità e delle figure chiave atte alla prevenzione della Corruzione e i documenti da redigere e aggiornare.
- **Piano Nazionale Anticorruzione**

  Ambito locale, Estensione degli obblighi e metodologie per la gestione del rischio e redazione del Piano Triennale di Prevenzione della Corruzione e della Trasparenza (PTPCT).
- **L. 179/2017 per la tutela dei segnalanti**

  Estensioni, mezzi e sanzioni.
- **Linee guida ANAC**

9.1.2. Modulo Trasparenza

- **Trasparenza e Piano Triennale, obbligo di pubblicità, diritto di Accesso e Adempimenti**

  ai sensi del D.Lgs. 33/2013.
- **Linee guida ANAC**

  Analisi delle circolari in materia di trasparenza amministrativa: Attuazione degli obblighi di pubblicità, trasparenza e diffusione di informazioni contenute nel D.lgs. 33/2013 come modificato dal d.lgs. 97/2016.
- **Rispetto dell'Accessibilità nella Trasparenza Amministrativa**

  ai sensi della L. 4/2004, Circolare AgID n. 61/2013, D.lgs. n. 106/2018.

Il corso include:

- Slide e altro materiale formativo;
- Attestato del completamento del corso di formazione per la rendicontazione.

Metodologie didattiche:

- **e-Learning**: Ogni partecipante dovrà dotarsi semplicemente di una connessione internet e di un pc o dispositivo mobile;
- **Lezioni frontali:** presso le sedi DigitalPA di Cagliari e Sulmona;
- **Corsi in house:** presso la sede del Cliente o altra location predisposta.