Cerved AML

Manuale Operativo

Procedura Whistleblowing

TIPO DI DOCUMENTO	MANUALE UTENTE
Redazione	Silvia Maimone – AML Senior Analyst
Verifica	Silvia Maimone – AML Senior Analyst

N° REV.	DATA REV.	NOTE
2	09/11/2023	

Documento riservato ad uso interno di Cerved AML

L'utilizzatore ha l'obbligo di verificare validità e aggiornamento di eventuali copie cartacee di questo documento

INDICE

1.1 Storia del documento 6

1.2 Nomenclatura 6

1.3 Premessa 8
1.3.1 Contesto 8
1.3.2 Destinatari 9
1.3.3 Canali di segnalazione 9
1.3.4 Gestione della segnalazione 9
1.3.5 Trattamento dei dati 10

1.4 Evoluzione normativa 10

1.5 Oggetto della procedura 12
1.5.1 Processo 12
1.5.2 Attori coinvolti 13
1.5.3 Piattaforma 14
1.5.3.1 Homepage 14
1.5.4 Interfaccia Whistleblower 15
1.5.4.1 Inserimento nuova Segnalazione 15
1.5.4.1 Generazione Key code 19
1.5.4.1 Modulo di inserimento generalità 20
1.5.4.1 Dashboard del whistleblower 21
1.5.4.2 Servizio di messaggistica 22
1.5.5 Componente Back Office per il Whistleblowing team 23
1.5.5.1 Gestione dell'autenticazione 23
1.5.5.2 Dashboard super operatore 26
1.5.5.3 Dettaglio delle segnalazioni da assegnare 27
1.5.5.4 Dettaglio delle segnalazioni assegnate 29
1.5.5.1 Dettaglio delle segnalazioni chiuse 31
1.5.5.2 Inserimento di segnalazioni pervenute da altri canali 32
1.5.5.3 Gestione Fascicolo 32
1.5.5.4 Statistiche 34
1.5.5.5 Scadenzario 35
1.5.5.6 Dashboard operatore 36
1.5.5.7 Dettaglio delle segnalazioni da lavorare 37
1.5.5.8 Dettaglio delle segnalazioni in lavorazione 40
1.5.5.9 Dashboard gestore identità 42
1.5.5.10 Dashboard ADMIN 44

1.6 Caratteristiche tecniche del SISTEMA 48
1.6.1 Crittografia 48
1.6.2 Anonimizzazione 48
1.6.3 Partizionamento 48
1.6.4 Controllo degli accessi logici 48

1.6.5 Tracciabilità 48
1.6.6 Archiviazione 48
1.6.7 Vulnerabilità 48
1.6.8 Lotta contro il malware 48
1.6.9 Sicurezza dei siti web 49
1.6.10 Backup 49
1.6.11 Contratto con il responsabile del trattamento 49
1.6.12 Prevenzione delle fonti di rischio 49
1.6.13 Protezione contro fonti di rischio non umane 49

INDICE DELLE FIGURE

FIGURA 1 – HOMEPAGE WHISTLEBLOWER 14
FIGURA 2 – PULSANTI FUNZIONE 15
FIGURA 3 – INSERIMENTO SEGNALAZIONE – RACCOMANDAZIONI PER IL SEGNALANTE 16
FIGURA 4 – INSERIMENTO SEGNALAZIONE – SELEZIONE TIPOLOGIA 16
FIGURA 5 – MODULO SEGNALAZIONE – STRUTTURA ORGANIZZATIVA 17
FIGURA 6 – MODULO SEGNALAZIONE – DATI SEGNALAZIONE 18
FIGURA 7 – MODULO SEGNALAZIONE – SOGGETTI SEGNALATI 18
FIGURA 8 – MODULO SEGNALAZIONE – ALTRI SOGGETTI COINVOLTI 18
FIGURA 9 – MODULO SEGNALAZIONE – ALLEGATI 19
FIGURA 10 – MODULO SEGNALAZIONE – CONFERMA DELL'INVIO 19
FIGURA 11 – CREAZIONE KEYCODE 20
FIGURA 12 – DISCLAIMER TRATTAMENTO DATI PRIVACY 21
FIGURA 13 – MODULO IDENTITÀ DEL SEGNALANTE 21
FIGURA 14 – DASHBOARD DEL SEGNALANTE 22
FIGURA 15 – SERVIZIO DI MESSAGGISTICA 23
FIGURA 16 – ACCESSO ALL'AREA RISERVATA AGLI UTENTI 23
FIGURA 17 – ACCESSO ALL'AREA RISERVATA 24
FIGURA 18 – MENU FUNZIONI DISPONIBILI 24
FIGURA 19 – ACCESSO ALL'AREA RISERVATA 25

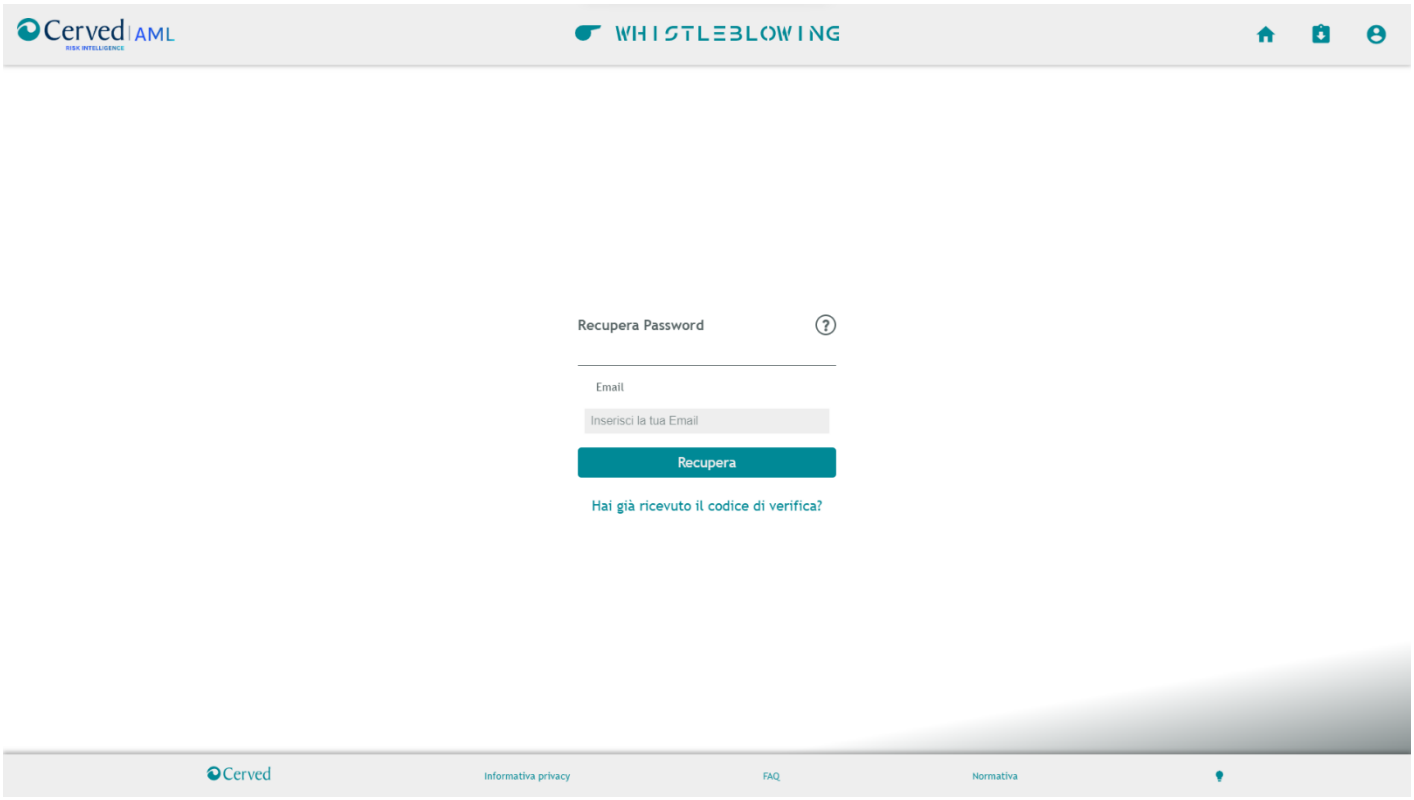

FIGURA 20 – RICHIESTA CODICE DI VERIFICA 25
FIGURA 21 – MODIFICA PASSWORD 26
FIGURA 22 – DASHBOARD DEL SUPER OPERATORE 27
FIGURA 23 – LISTA SEGNALAZIONI DA ASSEGNARE 28
FIGURA 24 – SELEZIONE AMBITO E FUNZIONE PER L'ASSEGNAZIONE 28
FIGURA 25 – SELEZIONE OPERATORE 29
FIGURA 26 – RICHIESTA ACCESSO ALLE GENERALITÀ DEL SEGNALANTE 29
FIGURA 27 – LISTA SEGNALAZIONI ASSEGNATE 30
FIGURA 28 – LISTA SEGNALAZIONI CHIUSE 31
FIGURA 29 – INSERIMENTO DI SEGNALAZIONI PERVENUTE DA CANALI TRADIZIONALI 32
FIGURA 30 – GESTIONE FASCICOLO 33
FIGURA 31 – DETTAGLIO DELLA PRATICA NEL FASCICOLO 33
FIGURA 32 – DETTAGLIO DEL FASCICOLO 34
FIGURA 33 – STATISTICHE 35
FIGURA 34 – SCADENZARIO 36
FIGURA 35 – DASHBOARD OPERATORE 37
FIGURA 36 – LISTA SEGNALAZIONI DA LAVORARE 38
FIGURA 37 – PASSAGGIO DI STATO 38
FIGURA 38 – INSERIMENTO DI NOTA E ALLEGATO AL PASSAGGIO DI STATO 39
FIGURA 39 – RIEPILOGO 40
FIGURA 40 – LISTA SEGNALAZIONI IN LAVORAZIONE 40
FIGURA 41 – PASSAGGIO DI STATO 41
FIGURA 42 – DEFINIZIONE DELLA PRATICA 41
FIGURA 43 – RICHIESTA INTEGRAZIONE 42
FIGURA 44 – DASHBOARD GESTORE IDENTITÀ 43
FIGURA 45 – LISTA AUTORIZZAZIONE RICHIESTE 44
FIGURA 46 – GESTIONE UTENTI 45
FIGURA 47 – CREAZIONE NUOVO UTENTE 46
FIGURA 48 – GESTIONE CLASSIFICAZIONE 46
FIGURA 49 – CONFIGURAZIONE SCADENZE 47
FIGURA 50 – IMPOSTAZIONE LINGUE 47

INDICE DELLE TABELLE

TABELLA 1 – NOMENCLATURA 7
. TABELLA 2 – NORMATIVA 11

1. Storia del documento

Definitivo

2. Nomenclatura

Glossario delle definizioni e acronimi utilizzati o riferimento al glossario del progetto.

Termine	Descrizione
Codice Etico	Un Codice di condotta o Codice etico è un insieme di linee guida etiche e responsabilità di un'organizzazione. Il servizio di whistleblowing è il mezzo più efficace per salvaguardare il rispetto delle linee guida etiche contenute nel codice.
Conflitto d'interesse	Il conflitto di interessi è una situazione che crea un conflitto tra gli interessi personali e gli interessi del datore di lavoro. Un conflitto di interessi esiste quando è dubbio che le tue motivazioni siano nel migliore interesse del tuo datore di lavoro.
Conformità	Conformità significa conformarsi a regole, politiche, standard o leggi. È una conferma che l'autore di un'azione soddisfa i requisiti delle pratiche o della legislazione accettate.
Corruzione	La corruzione è l'abuso del potere affidato a scopo di lucro. Comprende l'azione di fare o ricevere un regalo o una cortesia aziendale al fine di influenzare una decisione. Vedi conflitto di interessi.
Crittografia	La crittografia è la trasformazione dei dati in un codice, in modo che sia illeggibile a tutti, ad eccezione del destinatario. La crittografia è il modo più efficace per ottenere la sicurezza dei dati. La pseudonimizzazione è una misura per ridurre al minimo l'esposizione dei dati. Vedi pseudonimizzazione.
Dati personali	I dati personali sono informazioni che possono identificare un individuo, direttamente (ad esempio nome o numero di identificazione) o indirettamente (ad esempio descrizione della persona).
Etica professionale	L'etica aziendale è una forma di etica applicata che esamina i principi etici e i problemi morali o etici che sorgono in un ambiente aziendale. L'etica di un'azienda o di un'organizzazione è descritta nel suo Codice di condotta.
Informazioni di sicurezza	La sicurezza delle informazioni è la pratica di prevenire l'uso non autorizzato delle informazioni. Può essere utilizzato indipendentemente dal fatto che i dati siano elettronici o fisici.
Privacy dei dati	La privacy dei dati esiste ovunque vengano raccolte, archiviate, utilizzate e infine distrutte o cancellate informazioni di identificazione personale o altre informazioni sensibili, in forma digitale o in altro modo. Quando un'organizzazione utilizza i dati che le sono stati affidati da un informatore, i dati devono essere trattati secondo lo scopo concordato e i requisiti legali.

Protezione degli informatori	La protezione degli informatori è essenziale per un'efficace segnalazione delle irregolarità e per la trasparenza sul luogo di lavoro. Un informatore che segnala comportamenti o reati non etici gravi dovrebbe essere tutelato dalle linee guida dell'organizzazione in materia di whistleblowing e, in un numero crescente di paesi, anche dalla legge.
Responsabile della Prevenzione della Corruzione e della Trasparenza dell'Amministrazione	Il Responsabile per la prevenzione della corruzione e della trasparenza svolge attività di controllo sull'adempimento degli obblighi normativi.
Segnalazione anonima	La segnalazione anonima è il processo di invio di informazioni su un incidente a una destinazione desiderata, senza rivelare le tue informazioni personali.
Sicurezza dei dati	La sicurezza dei dati è la protezione dei dati da accessi non autorizzati. I dati sensibili e l'identità dell'informatore dovrebbero essere protetti sia da minacce esterne che interne. (Vedi crittografia)
Sistema di whistleblowing	Un sistema di whistleblowing è una soluzione per le denunce, che include un canale di comunicazione per gli informatori e uno strumento di gestione dei casi.
Strumento di gestione dei casi	Lo strumento di gestione dei casi consente una gestione sicura e corretta dei casi degli informatori da parte di soggetti incaricati.
Tangente	Una tangente è un atto di offerta o ricezione di oggetti di valore a/da persone in cambio di una decisione favorevole.
Whistleblower (WB)	Chi conosce di un illecito o di un'irregolarità sul luogo di lavoro, durante lo svolgimento delle proprie mansioni, e decide di segnalarlo a una persona o a un'autorità che possa agire efficacemente al riguardo. Pur rischiando atti di ritorsione a causa della segnalazione, egli svolge un ruolo di interesse pubblico, dando conoscenza di problemi o pericoli all'ente di appartenenza o alla comunità.
Whistleblower Communication	Il canale di comunicazione dell'informatore è un canale bidirezionale attraverso il quale un informatore invia un messaggio, in modo anonimo o meno, o riceve informazioni di follow-up o una domanda. La comunicazione è possibile via web e per telefono.
Whistleblowing	È un termine di origine anglosassone che definisce l'azione di segnalare irregolarità o illeciti da parte di dipendenti di enti, amministrazioni o aziende private. È l'attività di regolamentazione delle procedure volte a incentivare e proteggere tali segnalazioni.
Whistleblowing team	Il whistleblowing team che riceve i messaggi dell'informatore e decide come affrontarli, in conformità con le linee guida per il whistleblowing.
Wrongdoing	L'oggetto della segnalazione che può essere - un comportamento scorretto già in essere; - un comportamento censurabile che secondo la percezione del WHISTLEBLOWING potrebbe determinarsi in futuro.

Tabella 1 – Nomenclatura

Premessa

L'articolo 54bis del Decreto legislativo 30 marzo 2001, n.165, introdotto dalla Legge Anticorruzione n.190/2012 e poi modificato dalla Legge n.179/2017, introduce le "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", il cosiddetto whistleblowing.
In particolare, il comma 5 dispone che, in base alle nuove linee guida di ANAC, le procedure per il whistleblowing debbano avere caratteristiche precise. In particolare "prevedono l'utilizzo di modalità anche informatiche e promuovono il ricorso a strumenti di crittografia per garantire la riservatezza dell'identità del segnalante e per il contenuto delle segnalazioni e della relativa documentazione".
Gli enti devono prevedere la gestione del caricamento da una piattaforma informatica che corrisponda agli obblighi normativi e alle garanzie di sicurezza per le segnalazioni.
La segnalazione è fatta attraverso la compilazione di un questionario e può essere inviata in forma anonima. Se anonima, sarà presa in carico solo se adeguatamente circostanziata.
La segnalazione viene ricevuta dall'operatore del whistleblowing team e da lui gestita mantenendo il dovere di confidenzialità assoluta.
Il whistleblower è il dipendente che segnala illeciti di interesse generale e non di interesse individuale, di cui sia venuto a conoscenza in ragione del rapporto di lavoro.
Nel momento dell'invio della segnalazione, il segnalante riceve un codice numerico che deve utilizzare per poter accedere nuovamente alla segnalazione, verificare la presa in carico e dialogare rispondendo a richieste di chiarimenti o approfondimenti.
La tutela dell'anonimato è garantita in ogni circostanza.
Il decreto legislativo numero 24 del 10 marzo 2023, ha definitivamente attuato la Direttiva europea 2019/1937 riguardante la protezione delle persone che segnalano violazioni.
Il decreto disciplina, sulla base delle disposizioni della direttiva europea, la protezione dei whistleblowers che segnalano violazioni di disposizioni normative che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui siano venuti a conoscenza in un contesto lavorativo pubblico o privato.

Contesto

Gli obiettivi della Direttiva Europea sul Whistleblowing sono:

- Rilevare e prevenire comportamenti scorretti e violazioni di leggi e regolamenti e dare concreta attuazione ai principi di trasparenza e legalità
- Migliorare l'applicazione della legge implementando canali di segnalazione efficaci, affidabili e sicuri per proteggere i segnalanti da eventuali ritorsioni;
- Proteggere i whistleblower aiutandoli a denunciare atti illeciti o irregolarità in modo sicuro, garantendo la possibilità di segnalare in modo anonimo.
    - Separare i dati identificativi del segnalante dal contenuto della segnalazione, prevedendo l'adozione di codici sostitutivi dei dati identificativi, in modo che la segnalazione possa essere processata in modalità anonima e rendere possibile la successiva ricostruzione dell'identità del segnalante nei soli casi consentiti, garantendo l'efficacia del processo di segnalazione degli illeciti all'interno dell'ente attraverso una procedura informatica, che tuteli la riservatezza del segnalante e gli permetta di seguirne gli sviluppi delle indagini.
    - Gestire le segnalazioni attraverso un iter procedurale definito con termini certi per l'avvio e la conclusione dell'istruttoria, garantendo la gestione della segnalazione da parte dell'utente ricevente selezionato facente parte del Whistleblowing team.
    - Mantenere riservato il contenuto delle segnalazioni durante l'intera fase di gestione della segnalazione.
    - Adottare strumenti di crittografia per i contenuti delle segnalazioni e dell'eventuale documentazione allegata;

- Adottare adeguate modalità di conservazione dei dati e della documentazione
- Fornire strumenti di elaborazione statistica sui dati relativi alle segnalazioni

Per violazioni si intendono comportamenti, atti o omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato e che consistono in:

- Illeciti amministrativi;
- illeciti rilevati ai sensi del decreto legislativo 231/01;
- Illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione Europea o nazionali;
- attivo omissioni che ledono gli interessi finanziari dell'unione di cui all'articolo 325 del trattato sul funzionamento dell'Unione Europea;
- atti o omissioni riguardanti il mercato interno virgola di cui all'articolo 26, paragrafo 2, del trattato sul funzionamento dell'Unione Europea;
- atti o comportamenti che vanificano l'oggetto o le finalità delle disposizioni di cui agli atti dell'Unione Europea nei settori indicati nei numeri 3, 4 e 5.

Le disposizioni del decreto non si applicano:

- alle contestazioni rivendicazioni o richieste legate ad un interesse di carattere personale della persona segnalante che attengono esclusivamente ai propri rapporti individuali di lavoro;
- alle segnalazioni di violazioni laddove già disciplinate in via obbligatoria dagli atti dell'Unione Europea o nazionali;
- alle segnalazioni di violazioni in materia di sicurezza nazionale.

Destinatari

I destinatari della normativa sono individuati dall'art. 3 del decreto legislativo Decreto legislativo 10/03/2023, n. 24.

Sono destinatari i soggetti privati che:

- hanno impiegato nell'ultimo anno la media di almeno 50 lavoratori subordinati con contratti di lavoro a tempo indeterminato o determinato;
- che si occupino di alcuni specifici settori (servizi, prodotti e mercati finanziari e prevenzione del riciclaggio o del finanziamento del terrorismo, sicurezza dei trasporti e tutela dell'ambiente come in applicazione degli atti dell'Unione Europea di cui alle parti I B e II dell'allegato), anche se nell'ultimo anno non hanno raggiunto la media di lavoratori subordinati di cui al numero 1;
- sono diversi dai soggetti di cui al numero 2, rientrano nell'ambito di applicazione del decreto legislativo 231/01 e adottano modelli di organizzazione e gestione ivi previsti, anche se nell'ultimo anno non hanno raggiunto la media di lavoratori subordinati di cui al numero 1;
- i soggetti pubblici quali: amministrazione pubbliche, enti pubblici economici, società in House, organismi di diritto pubblico, concessionari di pubblico servizio.

Canali di segnalazione

L'art. 6 del Decreto legislativo 10/03/2023, n. 24 prevede l'attuazione di una serie di misure di sicurezza per le comunicazioni interne:

A. obbligo della presenza di canali interni per effettuare la segnalazione;
B. gestione del canale interno da parte personale formato;
C. previsione di tempistiche precise di gestione (avviso di ricevimento della segnalazione entro 7 giorni; riscontro alla segnalazione entro tre mesi);
D. previsione di sistemi alternativi per le segnalazioni (forma scritta, forma orale e denuncia *de visu*).

Gestione della segnalazione

La gestione del canale di segnalazione deve essere affidata a personale specificamente formato, che può essere:

- interno all'ufficio,
- soggetti esterni autonomi dedicati.

Trattamento dei dati

L'Azienda, ai sensi del regolamento generale sulla protezione dei dati – GDPR 2016/679, gestisce il trattamento dei dati personali relativi al ricevimento e alla gestione delle segnalazioni in qualità di titolare del trattamento dati. Fornisce le informazioni necessarie sulla Regolamento per la gestione di segnalazioni di violazione di normative nazionali dell'Unione Europea (WHISTLEBLOWING) tutela privacy e gestione dati al segnalante e alle persone coinvolte ai sensi degli artt. 13-14 GDPR, pubblicando sul sito la relativa informazione privacy è mediante comunicazione automatizzata al momento dell'effettuazione della segnalazione. L'Azienda gestisce solo i dati che risultano utili e finalizzati al trattamento della segnalazione. Il software applica misure idonee a proteggere i dati personali dei segnalanti sulla base dello svolgimento di dell'indagine e provvede alla cancellazione dei dati non utili alla segnalazione nel rispetto dei principi di finalità e minimizzazione del trattamento nel termine di 5 anni.

Evoluzione normativa

L'istituto del whistleblowing è stato recentemente oggetto di riforma per effetto del D.Lgs. n. 24 del 10 marzo 2023, il quale 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.

La novella legislativa recepisce, a livello interno, la Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019.

L'istituto è volto, da un lato, a garantire il diritto di manifestazione della libertà di espressione e d'informazione, mentre dall'altro si pone quale strumento di prevenzione e contrasto della corruzione, promuovendo l'emersione di illeciti commessi non solo all'interno della Pubblica Amministrazione, ma anche degli enti di diritto privato.

Decreto legislativo 10/03/2023, n. 24	Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, 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. Pubblicato nella Gazz. Uff. 15 marzo 2023, n. 63.
Legge 179/2017 "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"	Introduce il whistleblowing quale istituto giuridico volto a disciplinare la condotta di quelle persone che segnalano irregolarità o addirittura illeciti penali all'interno del proprio ambito lavorativo, garantendo la tutela dei lavoratori segnalanti, con l'obbligo per le società private e pubbliche amministrazioni di attivare al proprio interno canali di segnalazione delle violazioni, di cui uno almeno con modalità informatiche. Dispone che i Modelli di organizzazione, gestione e controllo prevedano uno o più canali che consentano ai soggetti Destinatari del Modello stesso di effettuare segnalazioni, a tutela dell'integrità dell'ente.
Direttiva 23/10/2019, n. 2019/1937/UE DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO	Direttiva riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione. Introduce l'obbligatorietà per le aziende con più di 50 dipendenti, le istituzioni del settore pubblico, le autorità e i Comuni con più di 10.000 abitanti sono obbligati a predisporre adeguati canali di segnalazione interni di dotarsi di canali sicuri di segnalazione (anche dal punto di vista informatico) e completano ancora indicazioni relative alla protezione adeguata dei segnalanti da eventuali ritorsioni.

Articolo 52 bis del Testo Unico Bancario (T.U.B.)	Disciplina il quadro dei sistemi interni di segnalazione delle violazioni facendo rimando alle disposizioni attuative dell'Autorità di Vigilanza. La Circolare 285 del 17 Dicembre 2013 emanata da Banca d'Italia, al Titolo IV, Capitolo 3, Sezione VIII, definisce gli aspetti di natura procedurale e organizzativa dei sistemi interni di segnalazione delle violazioni che le banche devono adottare.
Decreto Legislativo n. 90/2017, in attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo (IV Direttiva Antiriciclaggio). Introduce nel Decreto Legislativo n. 231/2007 all'art. 48 l'istituzione dei "Sistemi interni di segnalazione delle violazioni".	il whistleblowing è espressamente disciplinato anche nell'ambito della normativa di contrasto al riciclaggio e al finanziamento del terrorismo. Con il recepimento della quarta direttiva europea (Dir. UE 2015 slash 849), ad opera del D.Lgs. 90/2017, il legislatore nazionale ha infatti introdotto nel D.Lgs. 231/2007 il capo VII ("segnalazione di violazioni") e, al suo interno, l'articolo 48 (segnalazione di violazioni), che impone ai soggetti destinatari della normativa antiriciclaggio di adottare procedure per consentire la segnalazione, da parte di dipendenti di soggetti assimilati, di violazioni "potenziali o effettive" delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo.
Decreto legislativo n. 129/2017, in attuazione della direttiva 2014/65/UE	Introduce nel D.lgs. n. 58/1998 una disciplina unitaria dei sistemi di segnalazione delle violazioni nel settore del mercato finanziario. La nuova disciplina è contenuta negli articoli 4- undecies e 4- duodecies concernenti, rispettivamente sistemi di segnalazioni interni ed esterni.
Decreto legislativo n. 68/2018, in attuazione della direttiva (UE) 2016/97, relativa alla distribuzione assicurativa	introduce nel Codice delle Assicurazioni Private (D.lgs. 209/2005) l'articolo 10 quater relativo all'adozione di Sistemi interni di segnalazione delle violazioni nelle Imprese di assicurazione o di riassicurazione e per gli intermediari assicurativi e riassicurativi.
l. n. 190/2012 (Legge anticorruzione)	Introduce la prima forma di tutela espressa della figura del Whistleblowing, seppur circoscritta al settore del pubblico impiego.
Linee Guida ANAC - Determinazione n. 6 del 28.04.15	introducono l'obiettivo di offrire alle amministrazioni pubbliche una disciplina applicativa rispetto alle disposizioni della l. n. 190/2012 attraverso un modello procedurale per il trattamento delle segnalazioni.

. Tabella 2 – Normativa

1. Oggetto della procedura

Il presente documento descrive le caratteristiche le funzionalità della procedura per la gestione delle segnalazioni whistleblowing (WB).

Il Sistema di gestione delle segnalazioni delle violazioni rappresenta lo strumento per l'individuazione di atti o fatti che possano costituire violazioni.

Il sistema di gestione delle segnalazioni Whistleblowing ha lo scopo di promuovere e facilitare la segnalazione di illeciti commessi all'interno della struttura stessa da parte di dipendenti e collaboratori di un'organizzazione.

La piattaforma gestisce il sistema interno di segnalazione da parte dei dipendenti di eventuali irregolarità o violazioni della normativa applicabile e delle procedure interne.

Sono presenti due tipologie di segnalazione parallele:

- Segnalazioni ambito Antiriciclaggio per violazioni, potenziali o effettive, delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo
- Segnalazioni di altre tipologie di reati o irregolarità di cui il segnalante sia venuto a conoscenza nell'ambito delle proprie attività lavorative

Tali segnalazioni, anonime o dichiarate, sono indirizzate al responsabile interno preposto alla gestione delle segnalazioni in ambito whistleblowing competente per ambito tramite lo specifico canale di segnalazione, anonimo e indipendente, proporzionato alla natura e alle dimensioni del soggetto obbligato.

Il sistema provvede a:

- Gestire la raccolta, la conservazione e la gestione dei dati e degli elementi relativi alle segnalazioni;
- Fornire la situazione riassuntiva delle segnalazioni presenti in archivio in tempo reale;
- Digitalizzare la gestione di tutte le segnalazioni, nonché di tutta la documentazione relativa;
- Istruire la lavorazione delle segnalazioni;
- Gestire le notifiche di integrazione
- Aggiornare puntualmente i dati.

Il sistema si interfaccia con gli utenti esterni e con gli operatori abilitati all'istruttoria delle segnalazioni, profilati a sistema.

L'utilizzo del sistema garantisce:

- Un'efficace tutela del whistleblower
  - impossibilità di accesso alla segnalazione al di fuori dell'Whistleblowing team
  - nessuna discriminazione del segnalante
- la riservatezza delle informazioni contenute nella segnalazione
- la maggiore completezza delle informazioni per la trattazione della segnalazione
- l'efficienza nella gestione delle segnalazioni e facilitazione del compito degli istruttori

1.1.1 Processo

La funzionalità consente a chiunque (dipendenti e collaboratori, fornitori e qualsiasi altro soggetto che abbia avuto rapporti d'affari con la Società) di segnalare attraverso un percorso guidato on-line.

Il processo di Segnalazione si articola nei seguenti step:

1. Invio della Segnalazione (Segnalante)
2. Notifica automatica di ricezione in piattaforma per il super operatore (da hawk.user.mbx@cerved.com)
3. Presa in carico (Whistleblowing team) e notifica del passaggio della segnalazione al segnalante sulla dashboard (entro 7gg)
4. Istruttoria e eventuale contatto con il segnalante attraverso la piattaforma per richiesta integrazioni

5. Definizione entro tre mesi dalla ricezione

Il primo step può essere avviato solo dal Segnalante tramite la creazione di una Segnalazione, i successivi – che afferiscono alla gestione della stessa – sono in carico alle funzioni interne

Il sistema consente attraverso la pagina predisposta:

a) Creazione della segnalazione: il whistleblower può creare una nuova segnalazione, riportando tutte le parti necessarie;
b) Invio della segnalazione al Whistleblowing team per gestire le fasi successive.
c) Lavorazione della segnalazione
d) Richiesta di informazioni aggiuntive attraverso lo scambio di messaggistica
e) Consultazione dello status della pratica: La funzionalità consente agli attori di consultare in ogni momento dalla propria interfaccia lo status della pratica.

Il sistema garantisce una fruizione in modalità anonima, senza tracciatura di dati tecnici relativi alla rete e/o al dispositivo utilizzato.

1.1.2 Attori coinvolti

La tipologia degli utenti coinvolti:

- **Whistleblower** - Il segnalante di atti o fatti che possono costituire una violazione delle norme di cui ha avuto notizia durante lo svolgimento del proprio lavoro. È il dipendente o un soggetto che collabora anche esternamente con l'ente che segnala un illecito all'interno dell'organizzazione.
  Ha la visibilità delle proprie segnalazioni nelle diverse fasi previste, dalla compilazione fino al provvedimento finale.
- **Superoperatore Whistleblowing team** - è l'utente che presidia il processo dedicato, riceve le segnalazioni e gestisce l'attribuzione, accede alla consultazione dei dati. Il Super operatore riceve le notifiche mail sulle segnalazioni di whistleblowing inserite a sistema e le assegna a ciascun operatore chiamato a gestire l'istruttoria delle singole segnalazioni.
  Il super operatore è responsabile per:
  - la ricezione,
  - l'assegnazione
  - il monitoraggio dello stato delle segnalazioni.
  - prioritariamente la formulazione la richiesta di autorizzazione ai dati al Gestore dell'Identità.
- **Operatore Whistleblowing team -** è l'utente che esamina le segnalazioni e istruisce il relativo procedimento; l'operatore WHISTLEBLOWING team ha visibilità sulle pratiche a lui assegnate dal super operatore, può gestire fino alla definizione di un iter per le pratiche prese in carico con una nota scritta in cui riporta le eventuali attività di accertamento svolte, le decisioni adottate per dare comunicazione al segnalante, può determinare la chiusura.
  L'operatore è responsabile per:
  - Presa in carico
  - Trattamento
  - Archiviazione.
- **Gestore identità Whistleblowing team**, responsabile per l'autorizzazione all'accesso dei dati identificativi dei segnalanti. La funzione, definita da LLGG n. 469/2021, disciplina la figura del custode dell'identità quale ulteriore garanzia per la tutela della riservatezza del segnalante, può essere attribuita ad un soggetto interno o esterno purché possieda i requisiti di terzietà e imparzialità che la legge prevede. La figura è una supplementare tutela per la riservatezza del whistleblower, essendo esplicitato dalla normativa il divieto di divulgare i dati del segnalante senza il suo consenso espresso, salvo eccezioni particolari. Il Gestore dell'Identità deve essere autorizzato e debitamente istruito in merito al trattamento dei dati personali. Non essendo una figura "obbligatoria" il ruolo può essere ricoperto anche dal super operatore o dall'operatore già abilitato. Laddove il ruolo di Gestore dell'identità corrisponda con il Super operatore, sarà quest'ultimo il soggetto competente a

sbloccare i dati identificativi del segnalante. In tale ipotesi, il sistema traccia l'accesso all'identità da parte del Super Operatore mantenendo comunque traccia delle ragioni che hanno reso necessario conoscere l'identità del segnalante.

- **ADMIN,** operatore abilitato alla creazione e manutenzione delle utenze e delle classi, configurazione delle lingue, impostazione dei termini.

1.1.3 Piattaforma

1.1.3.1 Homepage

Il Segnalante accede al servizio di segnalazione attraverso browser, richiamando l'URL di accesso all'Homepage della procedura.
Il Segnalante accedendo alla piattaforma può inserire una nuova segnalazione di illecito o consultare le segnalazioni già inserite, digitando il keycode corrispondente alla segnalazione, al fine di verificare lo stato di avanzamento e dialogare con il whistleblowing team tramite l'apposita funzionalità di messaggistica.

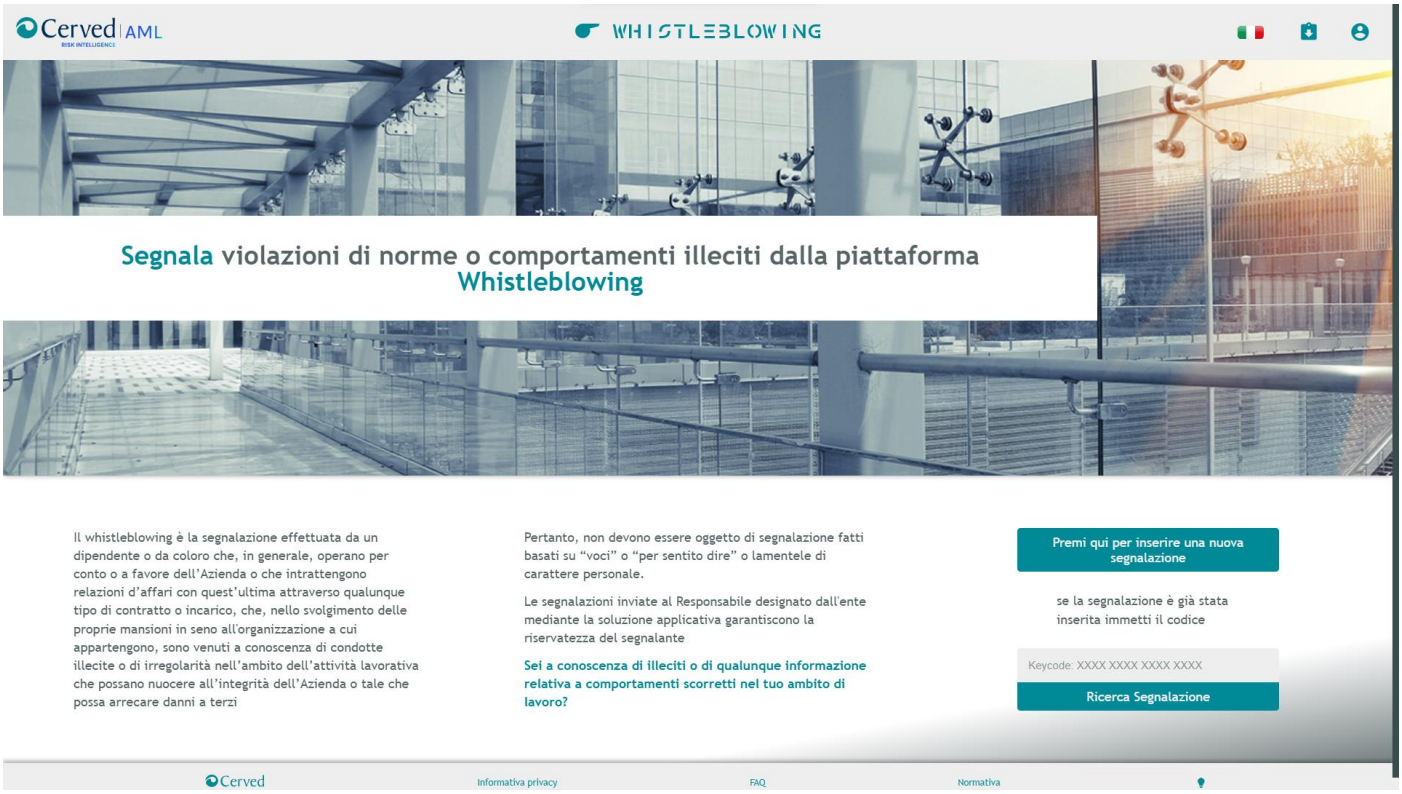

Figura 1 – Homepage whistleblower

Dalla homepage del whistleblower è possibile:

- Inserire Nuova richiesta - effettuare una segnalazione
- Recuperare una richiesta presentata - richiamando con la chiave identificativa (keycode) una precedente segnalazione inserita.

Inoltre, il sistema prevede nella barra superiore i pulsanti per

- l'accesso all'area riservata per gli operatori addetti
- la possibilità di selezione lingua, cliccando sulla bandiera e selezionando l'opzione desiderata.
- l'accesso rapido all'inserimento e alla ricerca della segnalazione

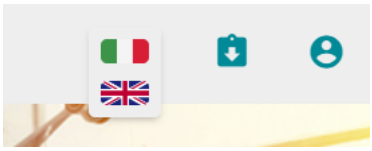

Figura 2 – Pulsanti funzione

Nella barra inferiore i pulsanti per accedere a:

- la descrizione del trattamento dei dati
- l'accesso alle FAQ
- la consultazione della normativa tematica
- la funzione per rendere la visualizzazione in B/N

1.1.4 Interfaccia Whistleblower

L'accesso per il segnalante è la URL accessibile anche al WHISTLEBLOWING Team.

Il ricevimento delle segnalazioni avviene in forma scritta mediante la Piattaforma informatizzata, dove sarà possibile sia aprire una nuova segnalazione, che verificarne lo stato, o avere più informazione in merito alle segnalazioni.

Per inserire una segnalazione il segnalante accede alla funzionalità dall'homepage della piattaforma.

Per recuperare una segnalazione effettuata in precedenza inserisce il keycode, restituito dalla piattaforma al momento dell'inserimento, all'interno del campo di testo.

Si illustrano di seguito le principali funzionalità della procedura eseguibili dal segnalante.

1.1.4.1 Inserimento nuova Segnalazione

La segnalazione è una rivelazione spontanea da parte di un soggetto, detto "segnalante" o "whistleblower") di un illecito o di un'irregolarità commessa all'interno dell'ente, del quale lo stesso sia stato testimone nell'esercizio delle proprie funzioni.

Il whistleblower, selezionando la funzionalità Inserisci Nuova segnalazione, può procedere alla compilazione dei dati descrittivi dell'illecito.

Il Segnalante si collega al sistema senza inserire credenziali.

L'utente può navigare in modo completamente anonimo.

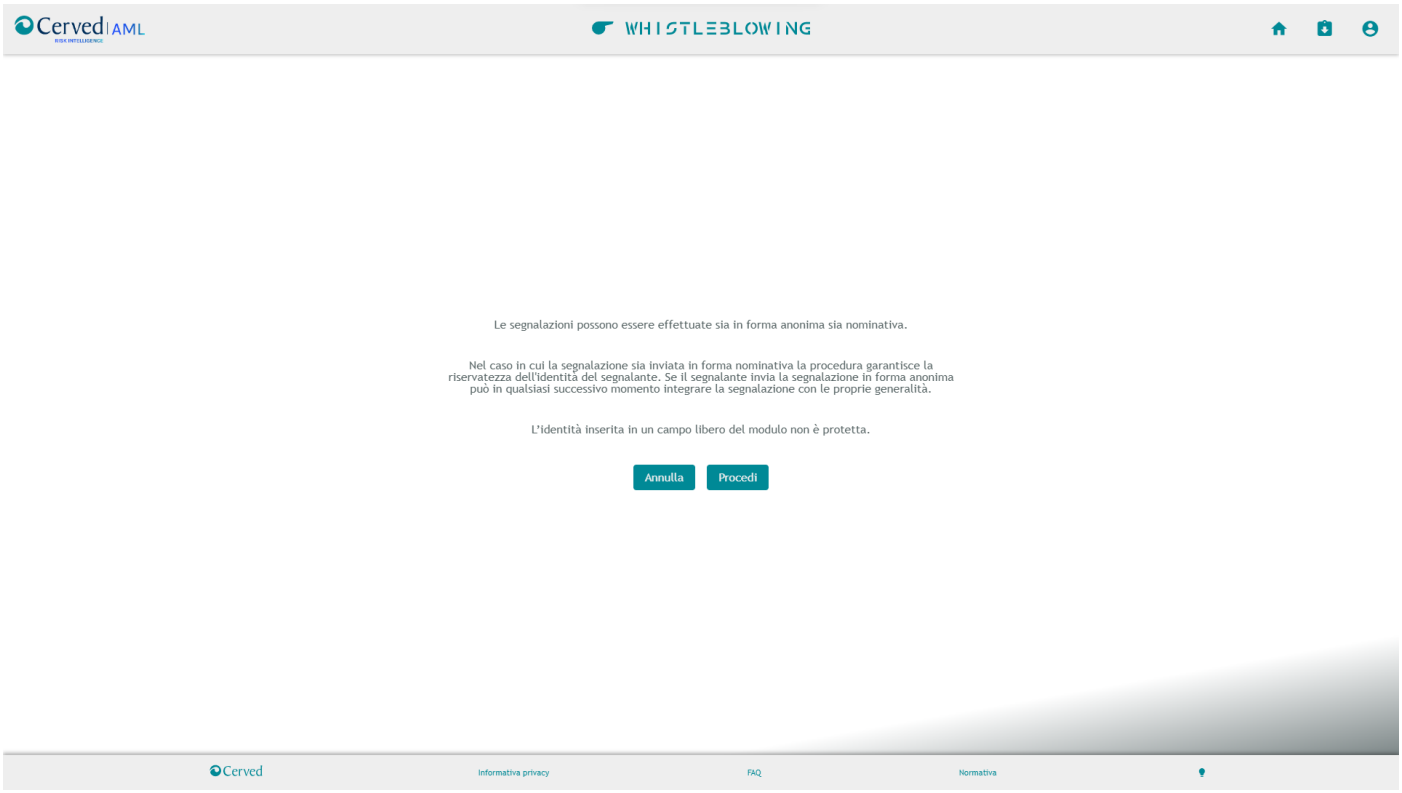

Figura 3 – Inserimento segnalazione – Raccomandazioni per il segnalante

La funzionalità consente di inserire la segnalazione attraverso la compilazione di un apposito modulo on line.
La funzionalità consente di acquisire i dati della Segnalazione presentata dal Whistleblower in base alla tipologia prescelta tra quelle riportate in selezione.

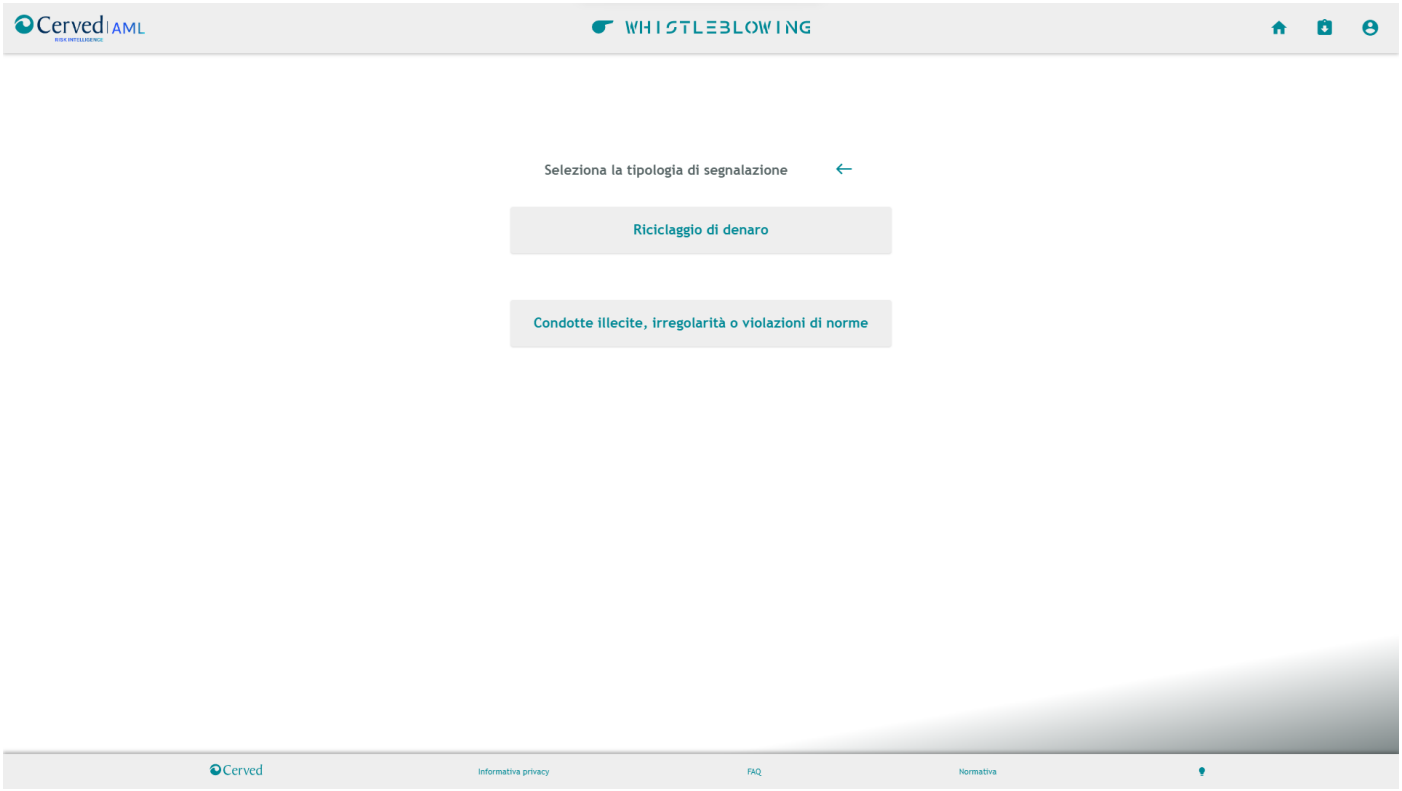

Figura 4 – Inserimento segnalazione – Selezione tipologia

Scegliendo di inviare una nuova segnalazione, l'utente visualizza la form in cui indicare le informazioni sulla segnalazione.
La form guida l'utente nel procedere con l'inserimento dei dati di base per contestualizzare la segnalazione e l'invio.
Il sistema facilita il compito del segnalatore attraverso un questionario, la cui compilazione avviene mediante una serie di sezioni, che costituiscono un percorso guidato in cui l'utente è indirizzato all'inserimento dei dati utili e necessari.
Le informazioni da compilare sono necessarie affinchè la segnalazione sia il più possibile circostanziata, al fine di consentire all'operatore del whistleblowing team la verifica dell'ammissibilità della stessa e procedere ai dovuti e appropriati accertamenti a riscontro della fondatezza dei fatti oggetto di segnalazione.
La segnalazione pertanto deve contenere i seguenti elementi:
- Oggetto della segnalazione
- esposizione chiara e precisa dei fatti, nonché del luogo e dell'arco temporale in cui si sono verificati;
- indicazione o allegazione di documenti che possano fornire ulteriore prova dei fatti segnalati (La funzionalità consente all'utente di caricare a sistema gli allegati relativi);
- indicazione di ulteriori soggetti che possano riferire sui fatti
- qualsiasi tipo di informazione utile al riscontro circa la sussistenza dei fatti oggetto di segnalazione.
- facoltativamente le generalità del segnalante

Le sezioni e il relativo contenuto sono configurabili in base alla versione del SW acquistato.
Le sezioni proposte sono:

1. Struttura organizzativa

In cui descrivere il contesto del segnalante.

Dipendente: le persone aventi la qualità di lavoratore;

Collaboratore/lavoratore di impresa fornitrice: le persone aventi la qualità di lavoratore autonomo; qualsiasi persona che lavora sotto la supervisione e la direzione di appaltatori, subappaltatori e fornitori (…) comprese le persone segnalanti il cui rapporto di lavoro non è ancora iniziato nei casi in cui le informazioni riguardanti una violazione sono state acquisite durante il processo di selezione o altre fasi delle trattative precontrattuali;

Cliente/terzo: gli azionisti e i membri dell'organo di amministrazione, direzione o vigilanza di un'impresa, compresi i membri senza incarichi esecutivi, i volontari e i tirocinanti retribuiti e non retribuiti.

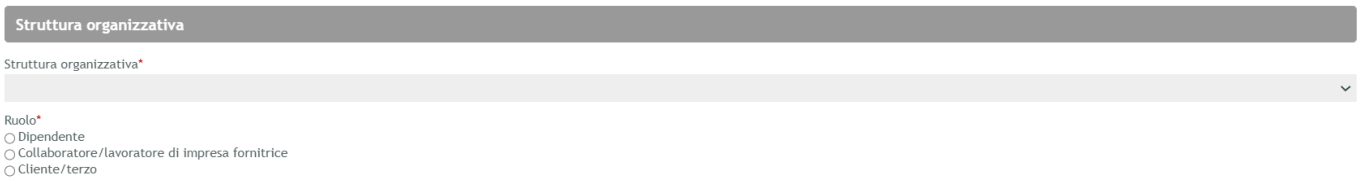

Figura 5 – Modulo segnalazione – Struttura organizzativa

2. Segnalazione

Dove specificare l'oggetto, la descrizione e il contesto della segnalazione. Non esiste una lista precisa di azioni pregiudizievoli che possano costituire oggetto del whistleblowing, ma le segnalazioni devono riguardare condotte illecite di cui il soggetto ne sia venuto a conoscenza in ragione del rapporto di lavoro, come comportamenti, rischi, reati, consumati o tentati, a danno dell'interesse pubblico o privato.

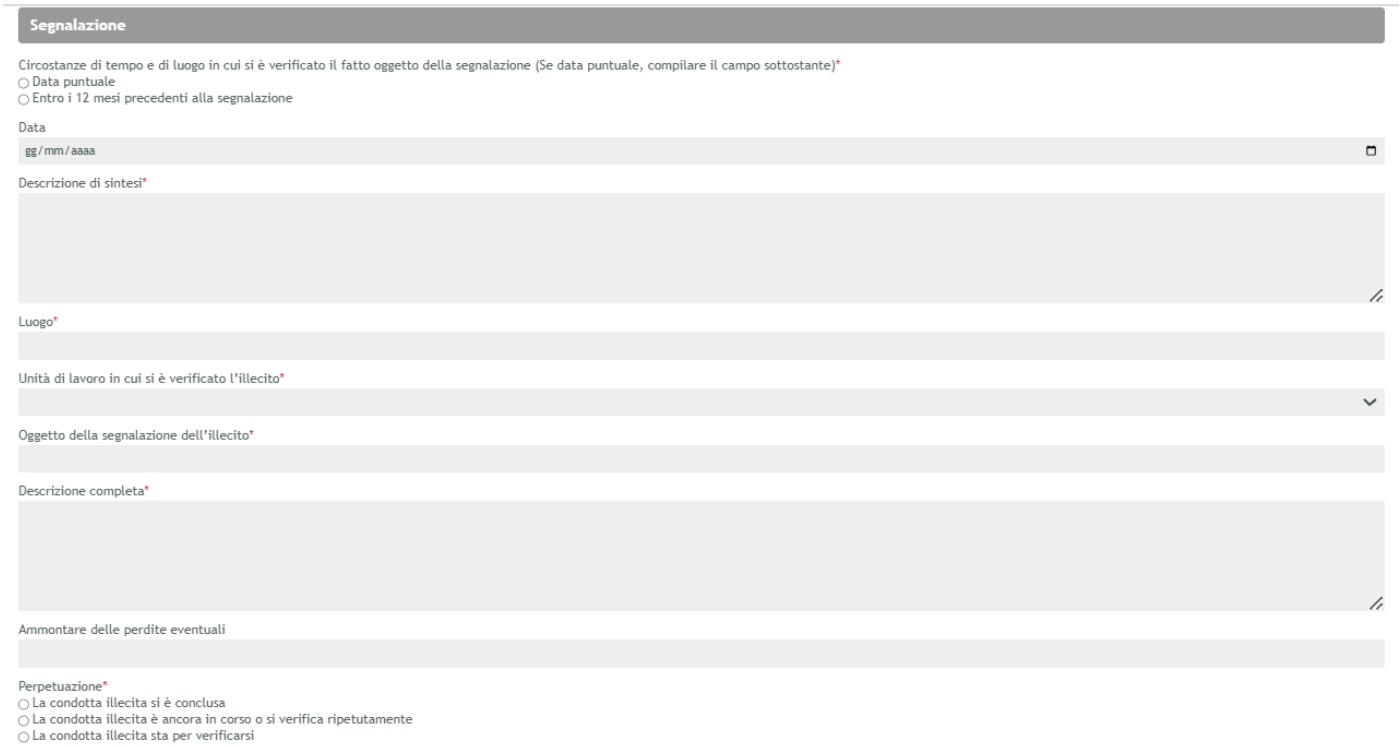

Figura 6 – Modulo segnalazione – Dati segnalazione

3. Soggetti segnalati

La sezione consente di inserire uno o più soggetti autori dell'illecito oggetto della segnalazione.

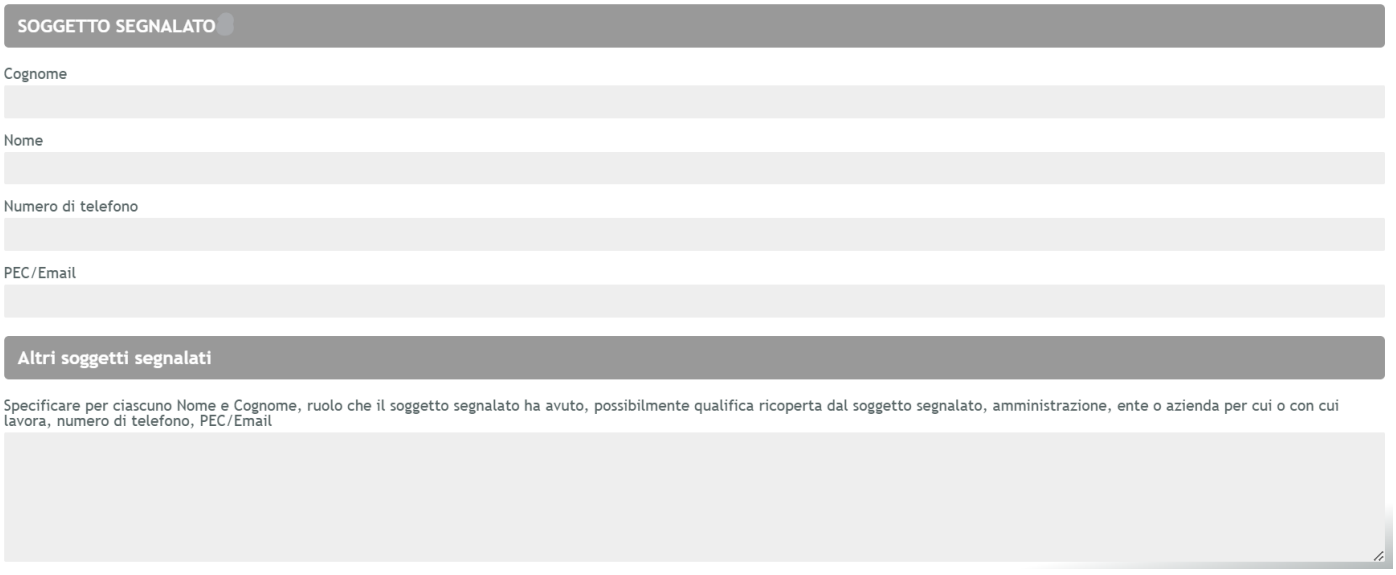

Figura 7 – Modulo segnalazione – Soggetti segnalati

4. Altri soggetti coinvolti

Figura 8 – Modulo segnalazione – Altri soggetti coinvolti

5. Allegati

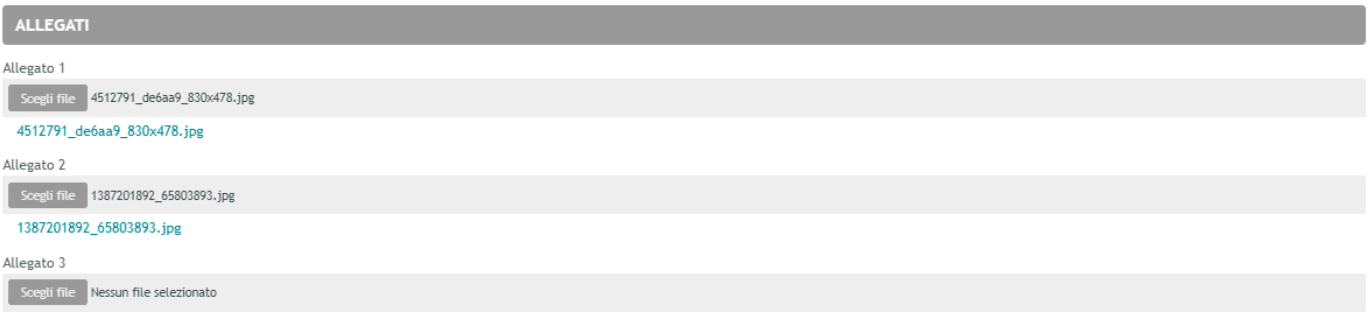

Figura 9 – Modulo segnalazione – Allegati

Alcuni campi sono richiesti obbligatoriamente per minimizzare la genericità della Segnalazione e aiutare il WHISTLEBLOWING team a comprendere i fatti oggetto della Segnalazione. I campi obbligatori sono indicati e il software indica l'eventuale mancata compilazione (in rosso).
L'identità inserita in un campo libero del modulo di segnalazione non è protetta.

La trasmissione avviene mediante il pulsante "invia segnalazione". Il sistema richiede la conferma per l'invio dei dati inseriti, in quanto non è successivamente possibile modificare i dati o annullare la segnalazione.

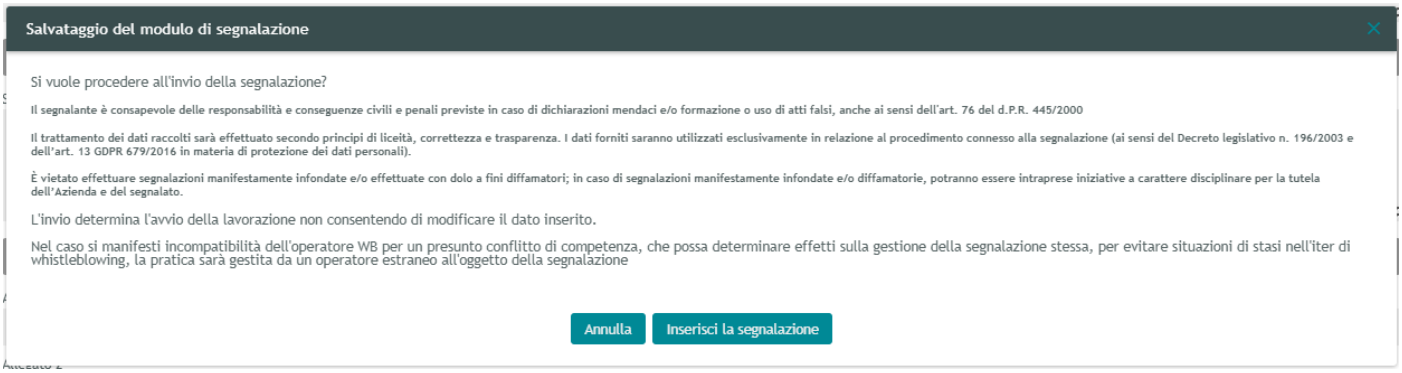

Figura 10 – Modulo segnalazione – Conferma dell'invio

Le segnalazioni inviate non possono essere modificate o eliminate.
L'avvenuta trasmissione della segnalazione è notificata automaticamente al super operatore del WHISTLEBLOWING TEAM competente per l'attribuzione della lavorazione. Il sistema invia automaticamente una notifica via mail al super operatore per comunicare la ricezione di una nuova segnalazione (da hawk.user.mbx@cerved.com).
Il testo della mail di notifica non riporta nessuna informazione sul contenuto della segnalazione e sul whistleblower.

1.1.4.2 Generazione keycode

Dopo l'invio dei dati, viene generato dal sistema un identificativo della segnalazione inserita e un codice per poter consultare la propria pratica in modo anonimo.
Il sistema genera automaticamente il codice identificativo univoco interno a fronte dell'invio della segnalazione da procedura.
Il codice alfanumerico da 16 caratteri deve essere annotato e conservato dal Segnalante, in quanto non sarà possibile recuperarlo in caso di smarrimento.

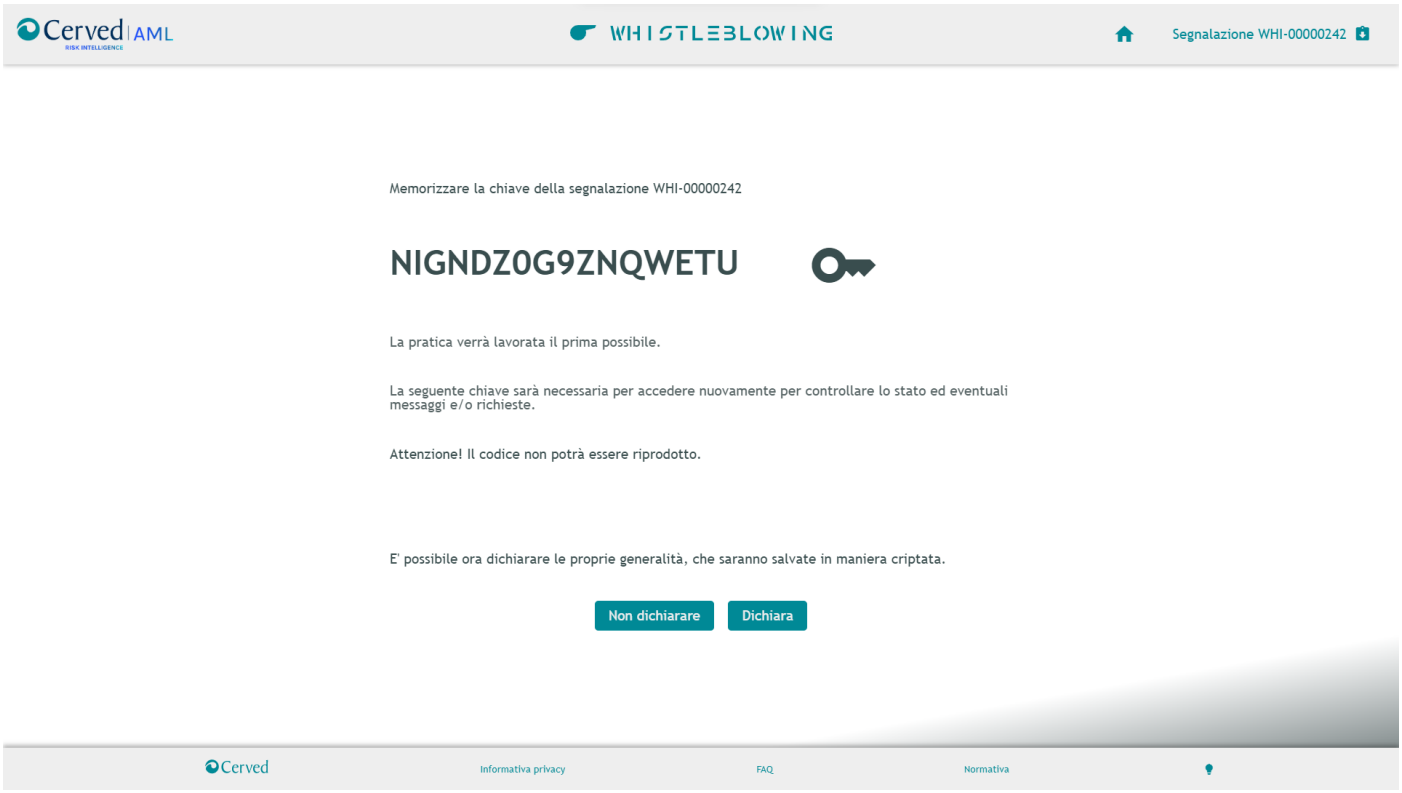

Figura 11 – Creazione keycode

1.1.4.3 Modulo di inserimento generalità

Le segnalazioni, a esclusione di quelle relative al riciclaggio di denaro, possono essere effettuate sia in forma anonima sia nominativa.
Il segnalante può scegliere se compilare la form sulle generalità.
La segnalazione di un illecito può essere in forma confidenziale o anonima.
Nel caso in cui la segnalazione sia inviata in forma nominativa la procedura garantisce la riservatezza dell'identità del segnalante.
L'applicativo propone il testo relativo al trattamento dei dati al segnalante, l'accettazione è determinante per procedere all'inserimento.

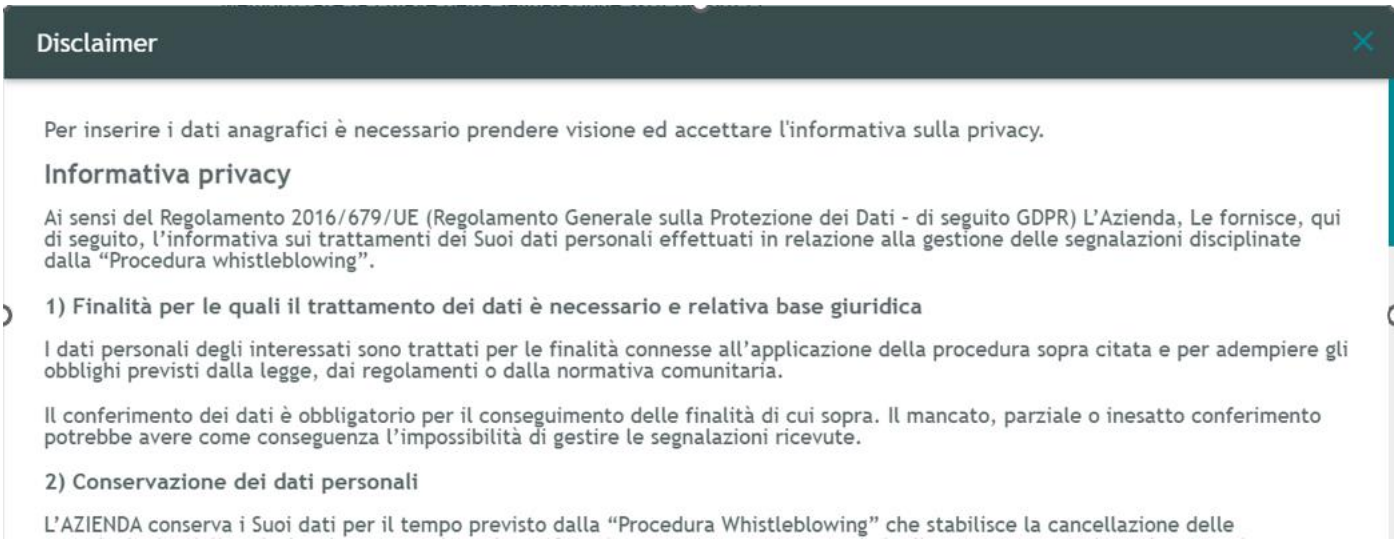

Figura 12 – Disclaimer trattamento dati privacy

Il consenso dell'utente alla raccolta di tali informazioni va manifestato on line attraverso l'apposizione di un flag sull'apposita check-box posta in calce all'informativa.

Se il segnalante invia la segnalazione in forma anonima può in qualsiasi successivo momento integrare la segnalazione con le proprie generalità.

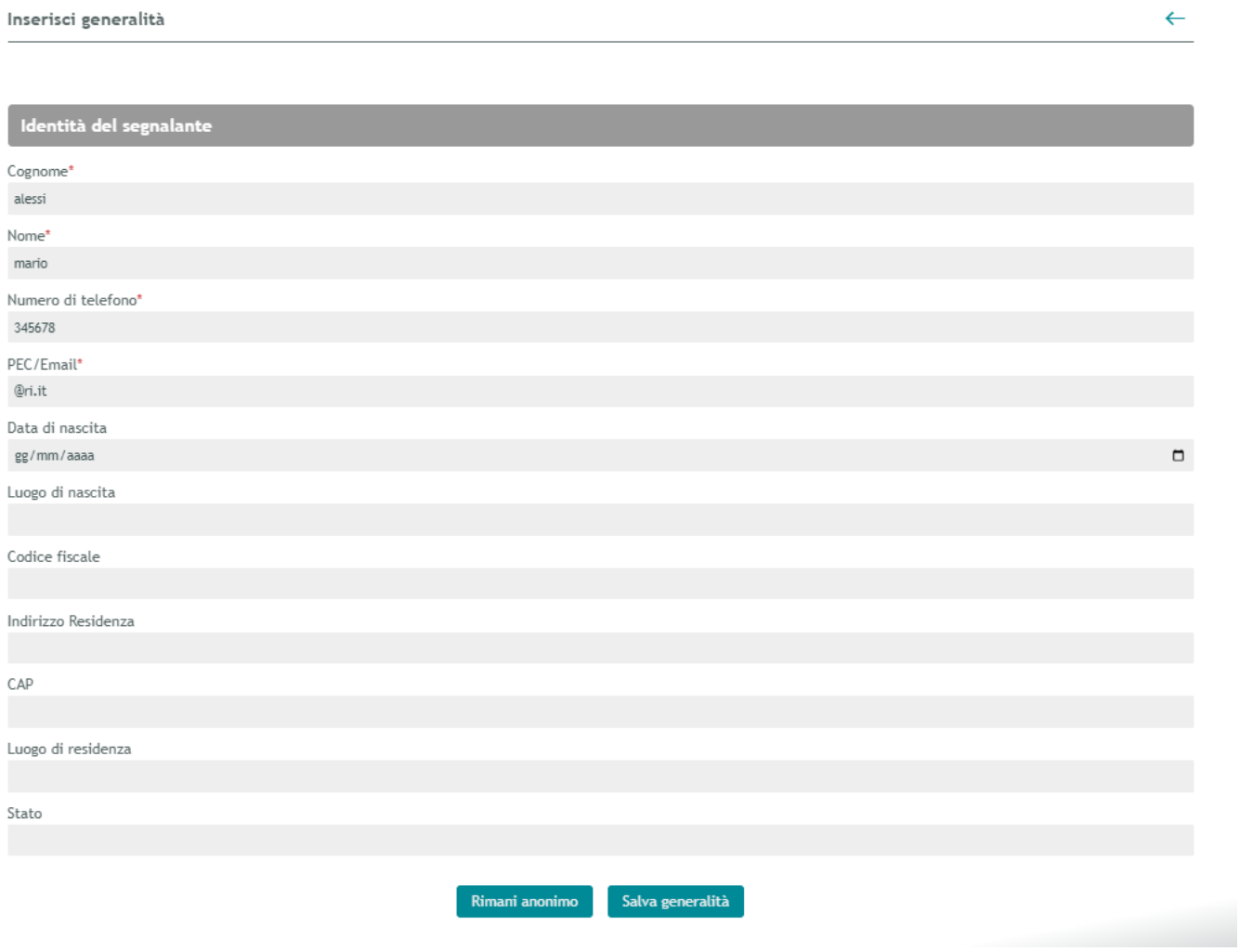

Figura 13 – Modulo identità del segnalante

I campi obbligatori sono indicati e il software indica l'eventuale mancata compilazione (in rosso).

Per le segnalazioni aventi ad oggetto tematiche antiriciclaggio non è previsto di inserire i dati di identità, in quanto questo tipo di segnalazione va effettuata sempre in modalità anonima.

1.1.4.4 Dashboard del whistleblower

La pagina è l'interfaccia a disposizione del segnalante ogni volta che rientrerà con il keycode per la consultazione della segnalazione.

La dashboard riporta per la segnalazione interrogata:

- lo stato di lavorazione della segnalazione;
- le informazioni rilasciate nel modulo della segnalazione;
- le generalità, se dichiarate.

- L'area di messaggistica con il whistleblowing team per rispondere a richieste di integrazione o inviare eventuali integrazioni. Questa funzionalità consentirà anche in seguito di ricevere eventuali comunicazioni da parte dell'Operatore, visualizzando l'intero thread.

Il segnalante può accedere alla procedura in qualsiasi momento successivo all'invio per consultare lo stato di lavorazione della segnalazione.

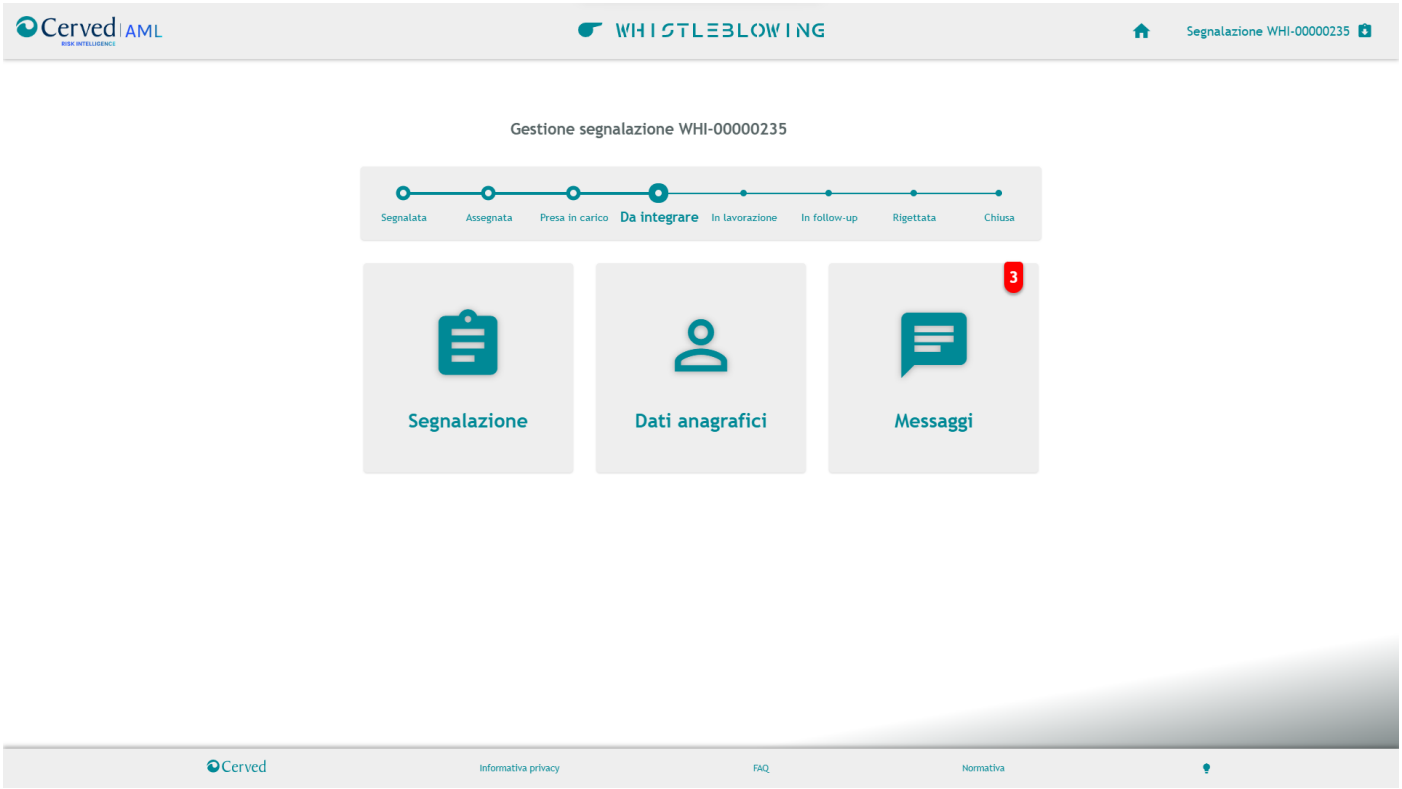

Figura 14 – Dashboard del segnalante

La funzionalità consente l'accesso al modulo di segnalazione solo tramite il keycode.

La funzionalità consente la visualizzazione del modulo e dello stato di avanzamento della segnalazione:

- segnalata (inviata ma non ancora letta dal whistleblowing team)
- Presa in carico (letta e in fase di valutazione)
- In lavorazione (segnalazione accolta per avvio indagine)
- In follow-up
- Chiusa (indagine conclusa con adozione del provvedimento amministrativo ovvero con inoltro all'autorità competente esterna all'ente)
- Rigettata (segnalazione non accolta per mancanza di elementi essenziali)

È possibile riportare la richiesta in compilazione nel caso in cui il whistleblower si renda conto di dover apportare modifiche dopo la generazione keycode, solo fino a quando la stessa viene presa in carico.

1.1.4.5 Servizio di messaggistica

Il sistema consente una comunicazione bidirezionale anche dopo l'inserimento della segnalazione.

La funzionalità consente all'operatore di dialogare con il Whistleblower attraverso una chat asincrona.

Sull'widget è presente un badge numerico indicante il totale dei messaggi non ancora letti.

Il sistema registra e mantiene il thread delle conversazioni tra i due soggetti registrando la data e l'orario di ogni singolo messaggio inserito.

La funzionalità consente di inserire la risposta alle richieste di chiarimenti da parte dell'operatore incaricato della segnalazione e inviare file in allegato al Whistleblowing TEAM attraverso pulsante preposto.

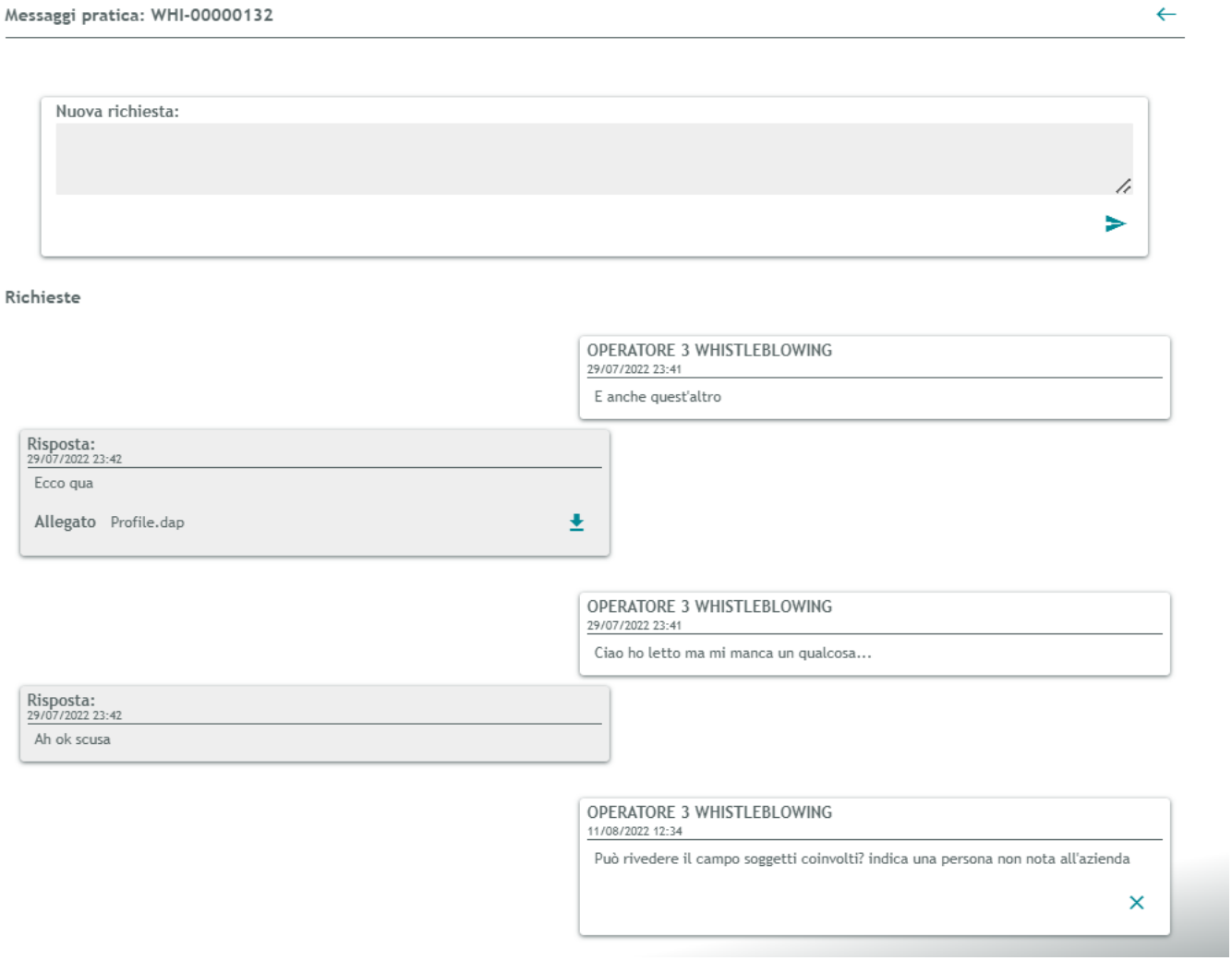

Figura 15 – Servizio di messaggistica

1.1.5 Componente Back Office per il Whistleblowing team

L'accesso per gli operatori è la URL accessibile anche per il segnalante.

Si illustrano di seguito le principali funzionalità della procedura eseguibili dall'operatore WHISTLEBLOWING Team.

1.1.5.1 Gestione dell'autenticazione

L'utente può effettuare l'accesso mediante l'inserimento delle credenziali nella pagina di log-in, accessibile dall'homepage.

L'operatore può accedere all'area riservata dal pulsante "Accesso" riportato nell'barra superiore.

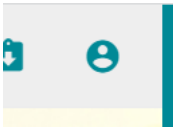

Figura 16 – Accesso all'area riservata agli utenti

Il sistema consente l'accesso all'area riservata inserendo le credenziali Username e password.

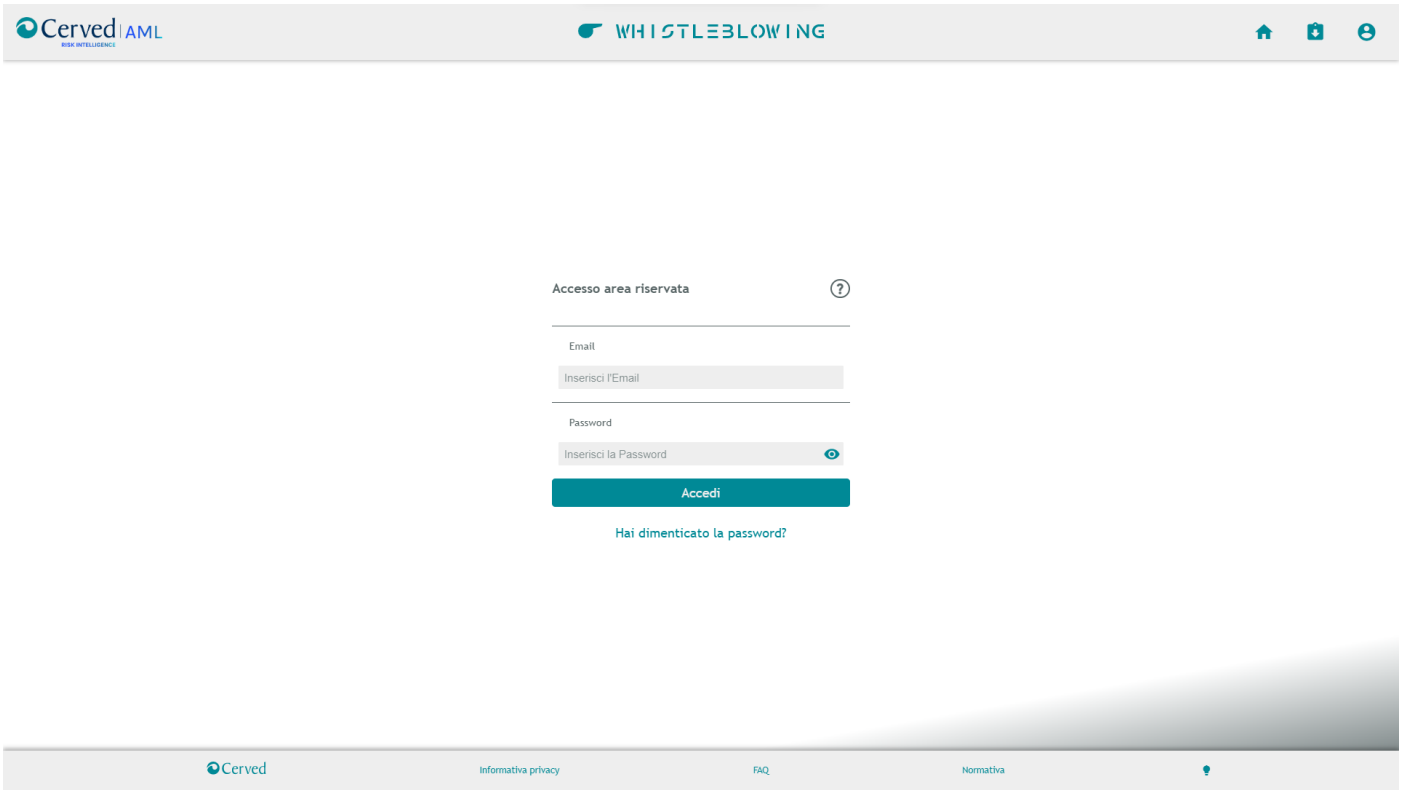

Figura 17 – Accesso all'area riservata

La funzionalità consente all'operatore del WHISTLEBLOWING team, in qualità di soggetto autorizzato al trattamento dei dati delle segnalazioni, di accedere alla procedura secondo la propria abilitazione.
Accreditandosi l'operatore accede alla dashboard prevista per ruolo con i contenuti di operatività relativi alle segnalazioni assegnate.
Dove autorizzato a più ruoli, l'operatore può scegliere dal menu accessibile nella barra superiore il tipo di operatività desiderata.

Figura 18 – Menu funzioni disponibili

1.1.5.2 Cambio password

Per poter accedere alla funzionalità di cambio password è necessario cliccare il pulsante "Hai dimenticato la password?" sulla pagina di login.

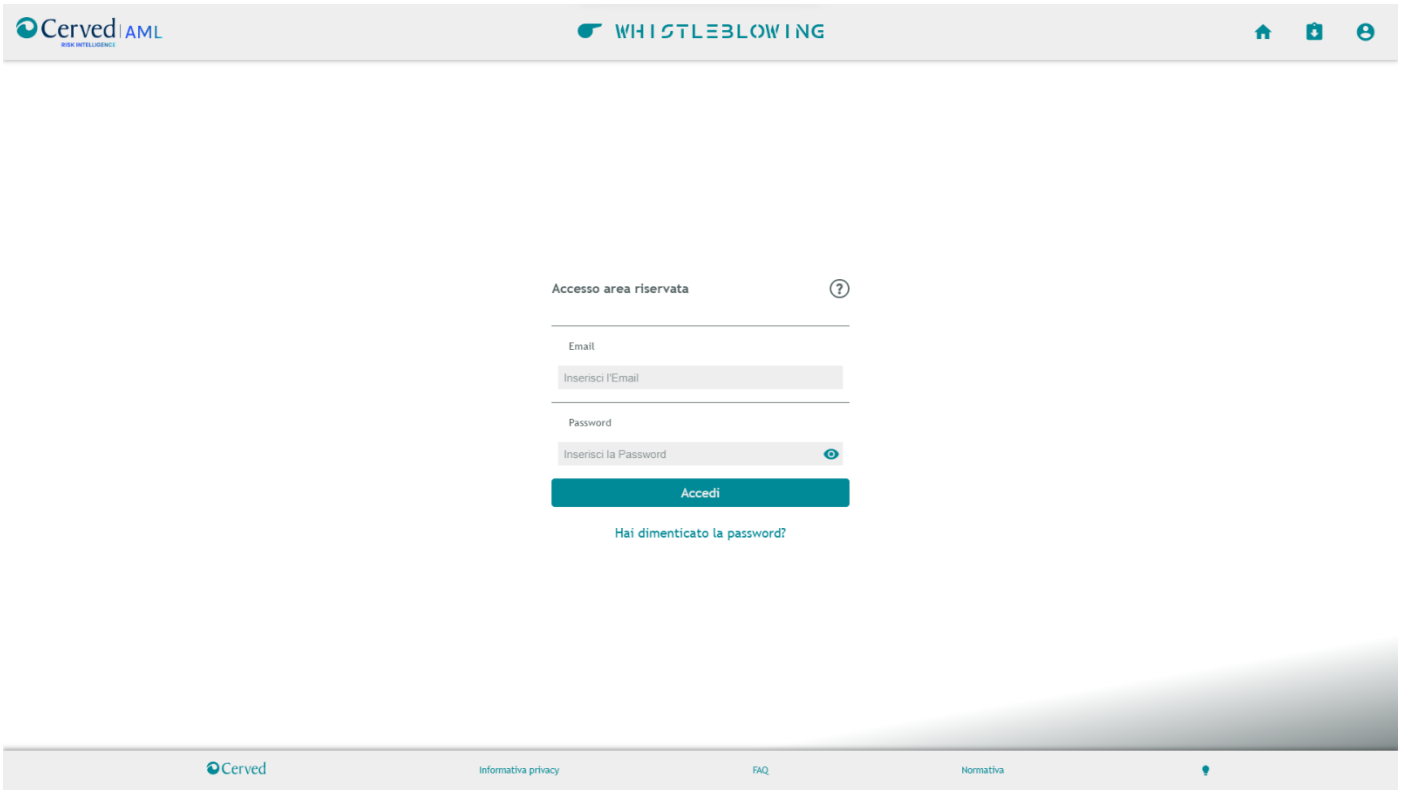

Figura 19 – Accesso all'area riservata

Il sistema presenterà una pagina in cui è possibile procedere con la richiesta del codice di verifica inserendo la propria mail.

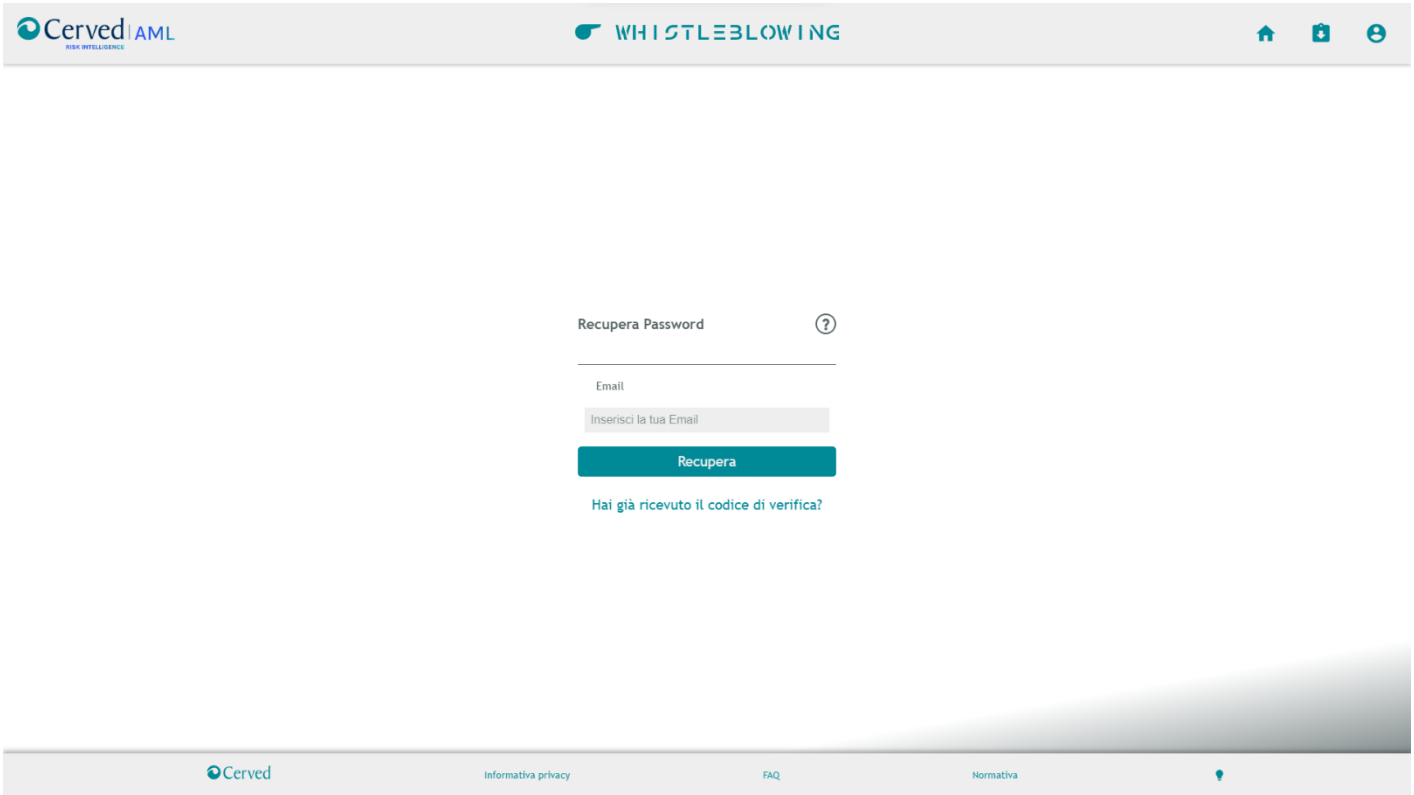

Figura 20 – richiesta codice di verifica

Procedendo, Il sistema presenterà una pagina in cui è possibile procedere con la modifica della password inserendo il codice ricevuto via mail.
Per poter procedere sarà necessario confermare due volte la nuova password.
La password scelta deve essere scelta seguendo i seguenti criteri:

- Deve contenere almeno una lettera maiuscola, un carattere speciale e un numero.
- Deve essere maggiore di 8 caratteri.
- Deve essere diversa dalla username

Per confermare l'operazione sarà necessario selezionare il pulsante "Cambia password".

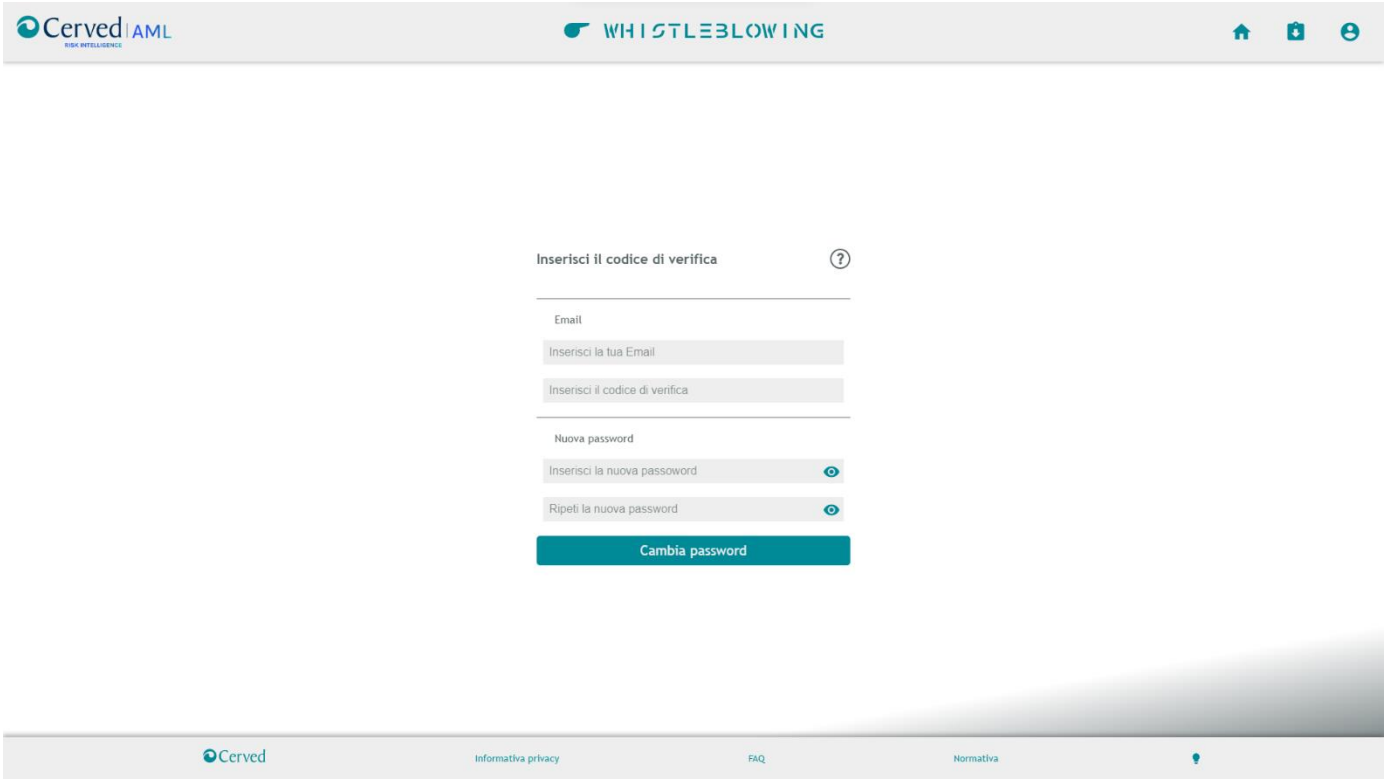

Figura 21 – Modifica password

1.1.5.3 Dashboard super operatore

La homepage del super operatore è denominata "dashboard". In questa pagina l'utente può visualizzare i widget disponibili in base al ruolo.
La funzionalità consente al super operatore di gestire l'iter di assegnazione delle segnalazioni prevenute al WHISTLEBLOWING team, ovvero di controllare in tempo reale tutti i casi che sono a sistema, le scadenze e le statistiche.
La dashboard è il punto centralizzato per la raccolta e lo smistamento agli operatori WHISTLEBLOWING competenti, la schermata prevede di accedere alle relative pagine di dettaglio con il riepilogo dei dati relativi alle Segnalazioni totali e alle segnalazioni assegnate all'operatore e il monitoraggio dei tempi di risposta.

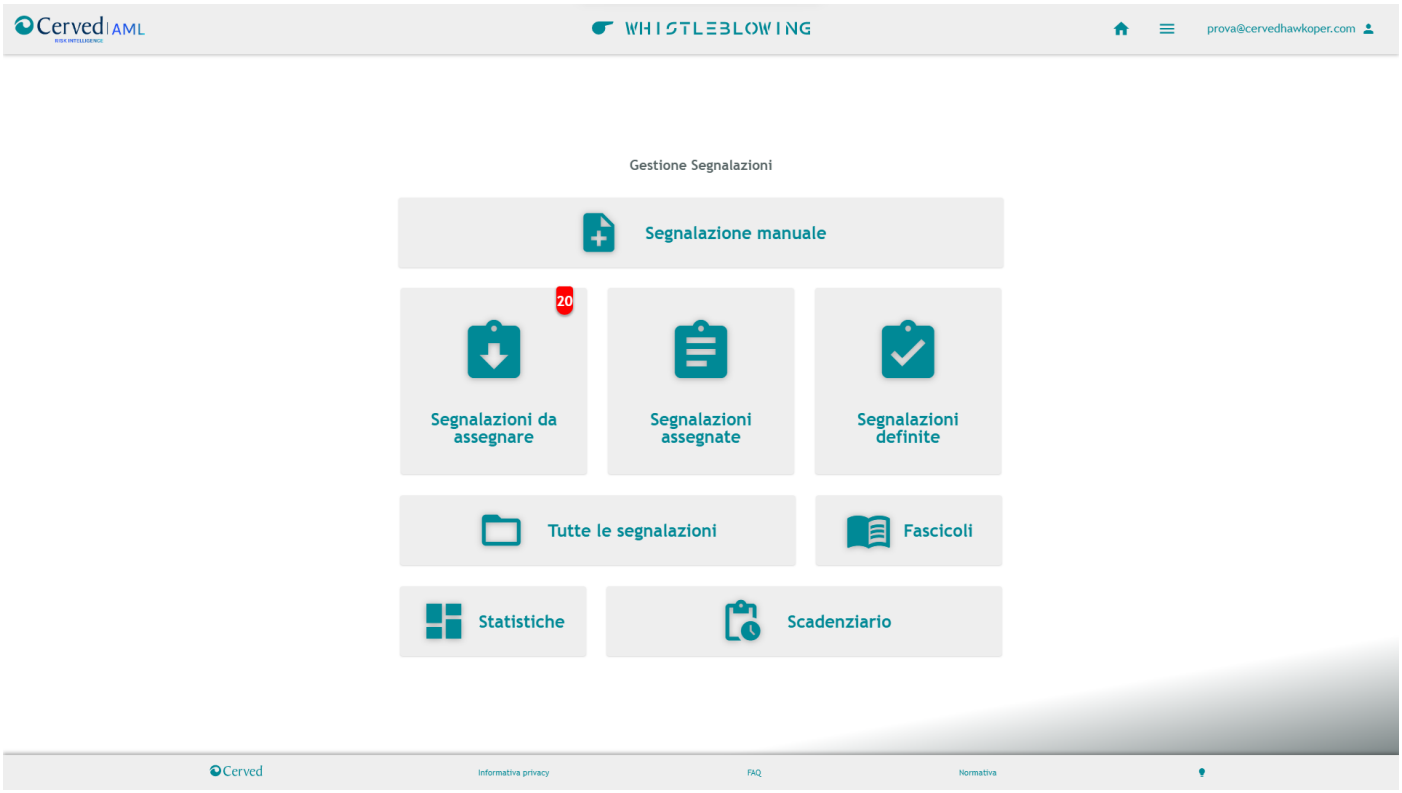

Figura 22 – Dashboard del super operatore

La funzionalità consente la visualizzazione delle segnalazioni:

- Da assegnare, ovvero pervenute di recente e da assegnare per la lavorazione. Il sistema porta in evidenza in rosso sulla dashboard la numerica delle “Nuove segnalazioni” non assegnate con la data di inserimento.
- Assegnate (inviata ma non ancora prese in carico dall’operatore dell’whistleblowing team o già in lavorazione)
- Chiuse
- Tutte

Oltre ad accedere alle funzionalità:

- Segnalazione manuale, per inserire una segnalazione proveniente da un canale esterno
- Fascicoli, per creare un fascicolo
- Statistiche
- Scadenzario

Accedendo al dettaglio il sistema riporta in forma tabellare il relativo elenco.

1.1.5.4 Dettaglio delle segnalazioni da assegnare

Accedendo al dettaglio “Lista segnalazioni da assegnare” il sistema riporta in forma tabellare il relativo elenco per visualizzare lo stato di avanzamento della segnalazione.

La griglia prevede una funzione di filtro per agevolare la ricerca.

Dalla lista delle segnalazioni riportata è possibile visualizzare il contenuto della segnalazione e accedere alle relative funzionalità di gestione.

I dati riportabili sono ordinabili per campo e la visualizzazione per vista può essere gestita in base alla selezione della quantità di risultati da mostrare.

La pagina può essere stampata dal pulsante riportato in altro a destra.

Dalla freccia in altro è possibile trovare indietro, per tornare alla Dashboard.

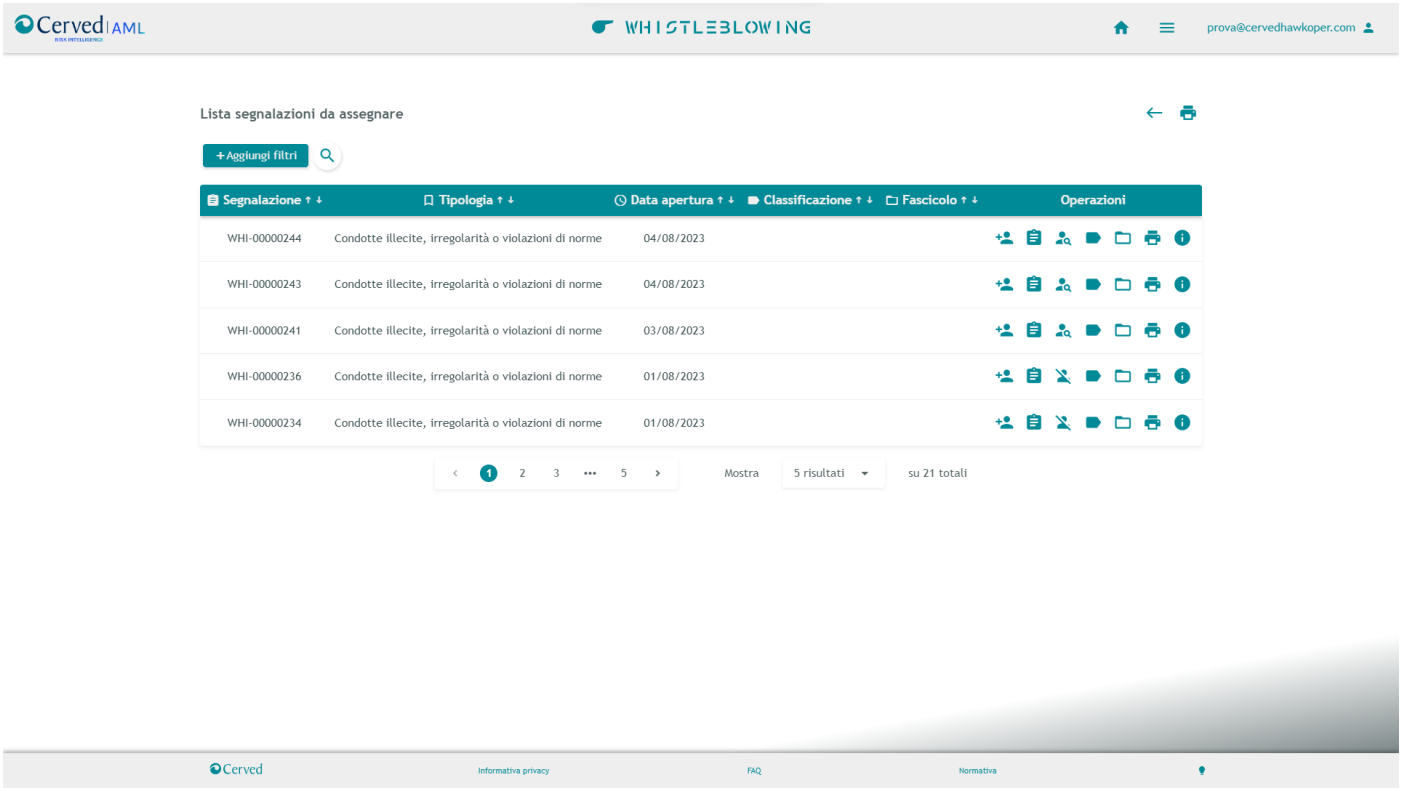

Figura 23 – Lista segnalazioni da assegnare

Il sistema visualizza le principali informazioni associate alle segnalazioni in griglia:

- ID Segnalazione
- Tipologia segnalazione
- Data apertura
- Classificazione attribuita
- Fascicolo attribuito
- Pulsanti Operazione
    - Assegna segnalazione - Il sistema permette un facile instradamento delle segnalazioni agli operatori del WHISTLEBLOWING team, l'azione apre la finestra di secondo livello su cui selezionare l'operatore a cui assegnare tra quanti abilitati a sistema per ambito e funzione selezionata.

Figura 24 – Selezione ambito e funzione per l'assegnazione

In base all'indicazione inserita il sistema ritorna gli operatori compatibili.

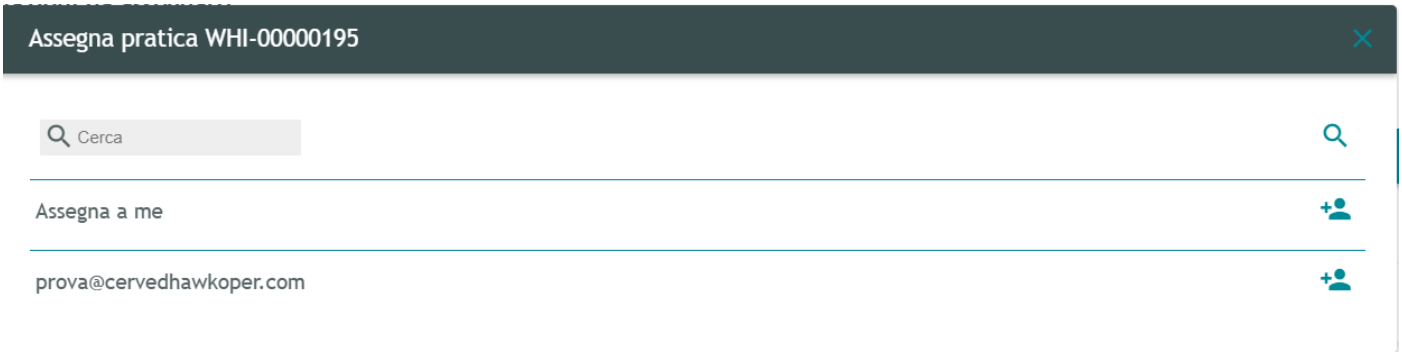

Figura 25 – Selezione operatore

- Consultazione dei dati inseriti al momento dell'inserimento della segnalazione
- Consultazione dati anagrafici. Se disponibili, ma ancora non abilitati, la piattaforma consente di richiedere l'accesso, motivato da nota, all'operatore che gestisce l'identità delle generalità del segnalante, se inserite.

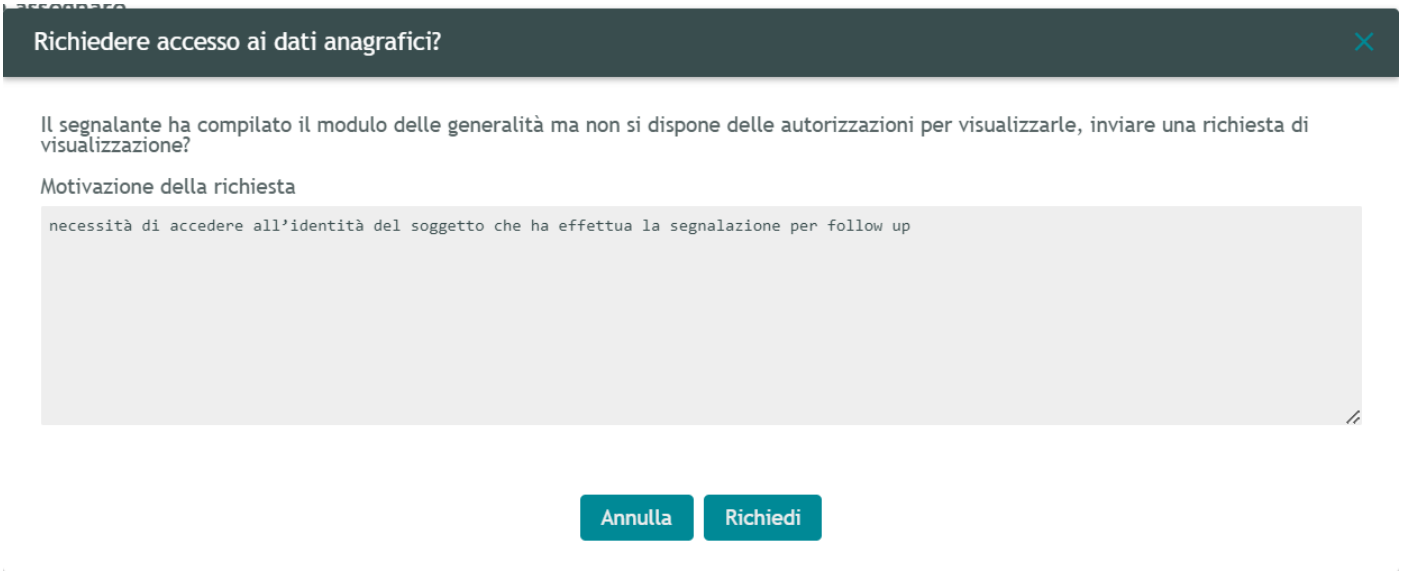

Figura 26 – Richiesta accesso alle generalità del segnalante

- Classificazione - In relazione al contenuto delle segnalazioni il super operatore può assegnare una tipologia, tra quante disponibili in base alla configurazione predisposta.
- Inserimento in fascicolo, selezionandone uno già esistete a cui associare la segnalazione in lavorazione per gestire in modo aggregato segnalazioni che riguardano lo stesso illecito.
- Stampa segnalazione, la funzionalità consente all'operatore abilitato di esportare i dati della segnalazione selezionata in un PDF (download)
- Riepilogo, riporta la cronologia della segnalazione grazie al tracciamento automatico delle operazioni svolte.

1.1.5.5 Dettaglio delle segnalazioni assegnate

Accedendo al dettaglio "Lista segnalazioni assegnate" il sistema riporta in forma tabellare il relativo elenco.

La griglia prevede una funzione di filtro per agevolare la ricerca.

Dalla lista delle segnalazioni riportata è possibile visualizzare il contenuto della segnalazione e accedere alle relative funzionalità di gestione.

I dati riportabili sono ordinabili per campo e la visualizzazione per vista può essere gestita in base alla selezione della quantità di risultati da mostrare.

La pagina può essere stampata dal pulsante riportato in altro a destra.

Dalla freccia in altro è possibile trovare indietro, per tornare alla Dashboard.

.

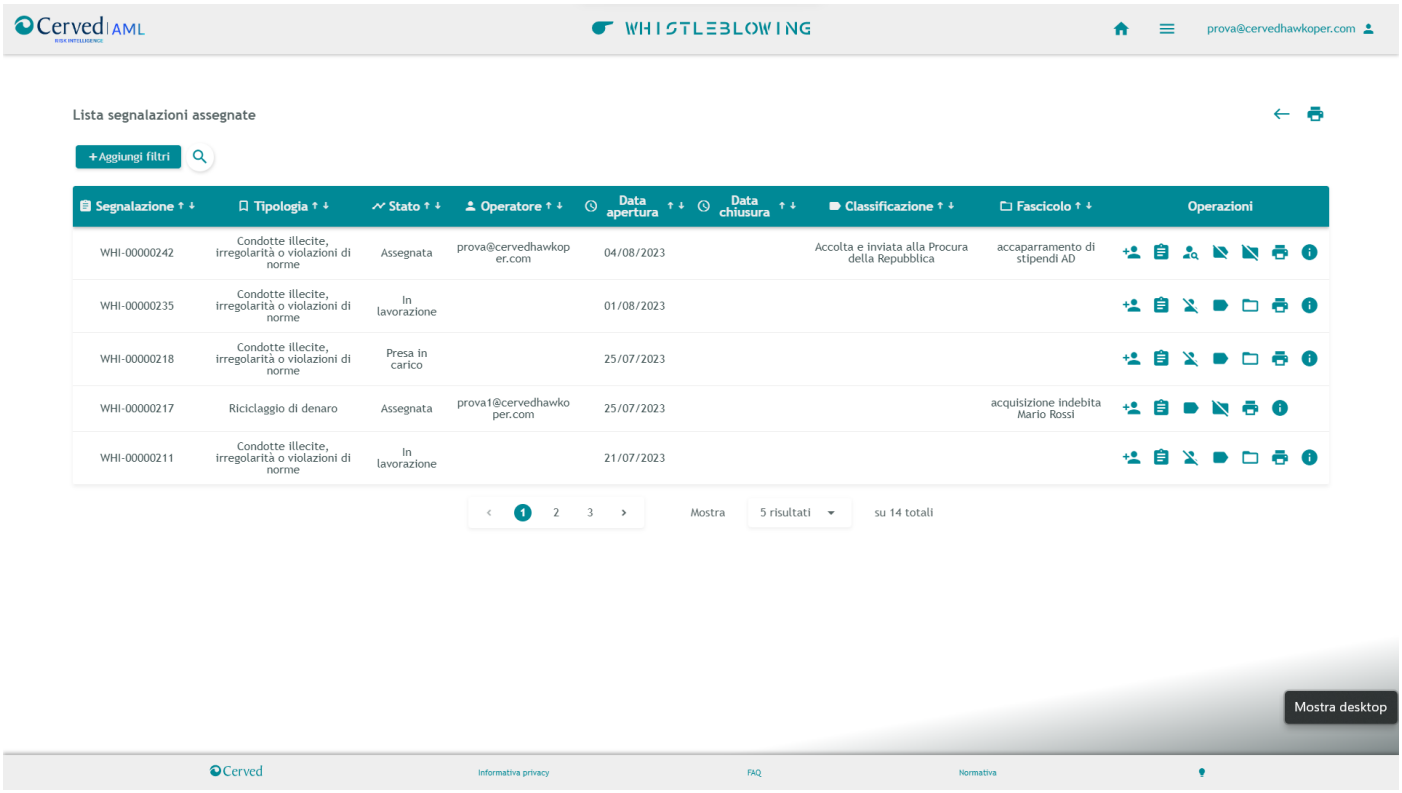

Figura 27 – Lista segnalazioni assegnate

Il sistema visualizza le principali informazioni associate alle segnalazioni in griglia:

- ID Segnalazione
- Tipologia
- Stato
- Operatore
- Data apertura
- Data chiusura
- Classificazione
- Fascicolo
- Pulsanti Operazione
    - Assegna segnalazione (da utilizzare in caso di riassegnazione)
    - Consultazione segnalazione
    - Consultazione dati anagrafici. Se disponibili, ma ancora non abilitati, la piattaforma consente di richiedere l'accesso, motivato da nota, all'operatore che gestisce l'identità delle generalità del segnalante, se inserite.
    - Classificazione
    - Inserimento in fascicolo Inserimento in fascicolo, selezionandone uno già esistete a cui associare la segnalazione in lavorazione per gestire in modo aggregato segnalazioni che riguardano lo stesso illecito.
    - Stampa segnalazione, la funzionalità consente all'operatore abilitato di esportare i dati della segnalazione selezionata in un PDF (download)
    - Riepilogo, riporta la cronologia della segnalazione grazie al tracciamento automatico delle operazioni svolte.

1.1.5.6 Dettaglio delle segnalazioni chiuse

Accedendo al dettaglio “Lista segnalazioni chiuse” il sistema riporta in forma tabellare il relativo elenco.

La griglia prevede una funzione di filtro per agevolare la ricerca.

Dalla lista delle segnalazioni riportata è possibile visualizzare il contenuto della segnalazione e accedere alle relative funzionalità di gestione.

I dati riportabili sono ordinabili per campo e la visualizzazione per vista può essere gestita in base alla selezione della quantità di risultati da mostrare.

La pagina può essere stampata dal pulsante riportato in altro a destra.

Dalla freccia in altro è possibile trovare indietro, per tornare alla Dashboard.

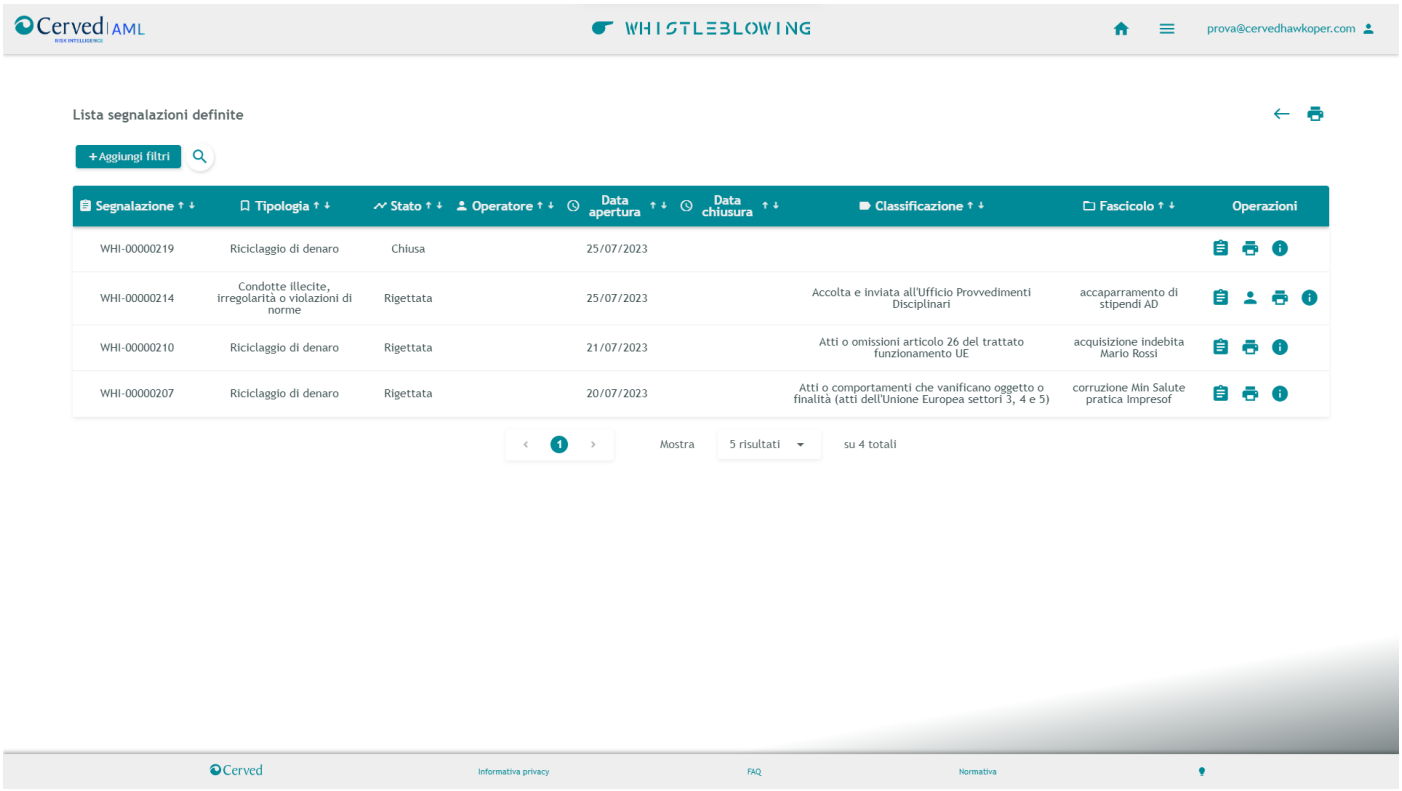

Figura 28 – Lista segnalazioni chiuse

Il sistema visualizza le principali informazioni associate alle segnalazioni in griglia:

- ID Segnalazione
- Tipologia
- Stato
- Operatore
- Data apertura
- Data chiusura
- Classificazione
- Fascicolo
- Pulsanti Operazione
    - Consultazione segnalazione
    - Consultazione dati anagrafici. Se disponibili, ma ancora non abilitati, la piattaforma consente di richiedere l’accesso, motivato da nota, all’operatore che gestisce l’identità delle generalità del segnalante, se inserite.

- Stampa segnalazione, la funzionalità consente all'operatore abilitato di esportare i dati della segnalazione selezionata in un PDF (download)
- Riepilogo, riporta la cronologia della segnalazione grazie al tracciamento automatico delle operazioni svolte.

1.1.5.7 Inserimento di segnalazioni pervenute da altri canali

La funzionalità “segnalazione manuale” consente all’operatore di inserire a sistema le segnalazioni esterne pervenute da canali alternativi alla piattaforma.

Resta tuttavia consigliato di procedere mediante comunicazione informatica, in quanto la piattaforma dispone di un protocollo di crittografia che garantisce una maggior sicurezza durante il processo di segnalazione.

Il super operatore deve specificare il canale di provenienza con il quale stata presentata la segnalazione, quindi peocedere all’inserimento in modo analogo al segnalante.

L’operatore può selezionare tra i canali di provenienza ammessi.

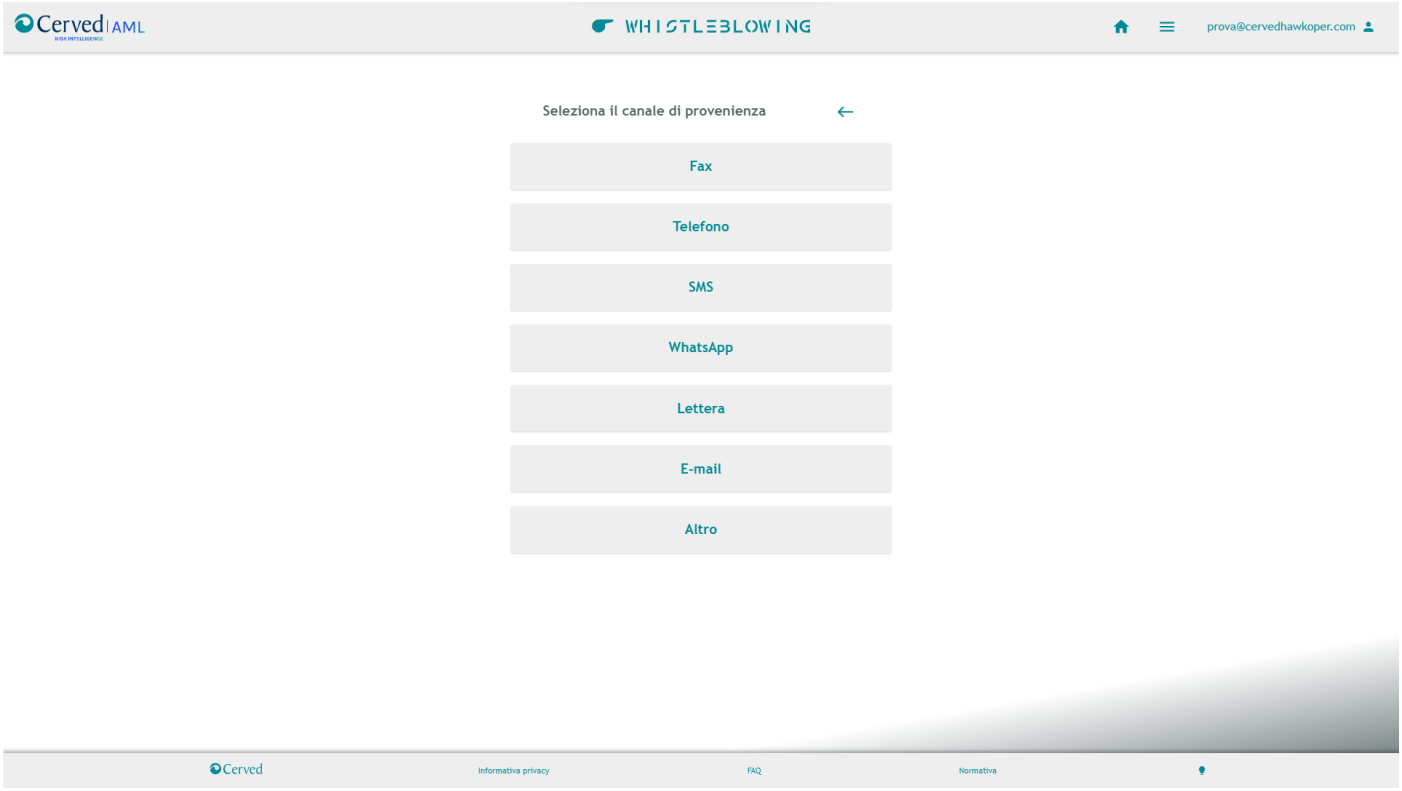

Figura 29 – Inserimento di segnalazioni pervenute da canali tradizionali

L’inserimento da parte dell’operatore prevede lo stesso questionario del whistleblower e, a fronte dell’acquisizione, il sistema genera il Keycode da comunicare al segnalante, qualora abbia comunicato i riferimenti di contatto o la propria e-mail.

La possibilità di inserire tutte le segnalazioni garantisce la generazione della completa reportistica.

1.1.5.8 Gestione Fascicolo

Attraverso questa funzione, l’operatore crea o aggiorna un fascicolo, a cui potrà associare una segnalazione raggruppando in base ad un criterio comune (segnalazione duplicata, medesimo illecito).

La funzionalità consente all’operatore di aggregare più segnalazioni, perché associate a uno stesso illecito.

Il sistema consente di inserire per ogni fascicolo un nome.

La griglia riporta il numero di segnalazioni incluse nell’aggregato.

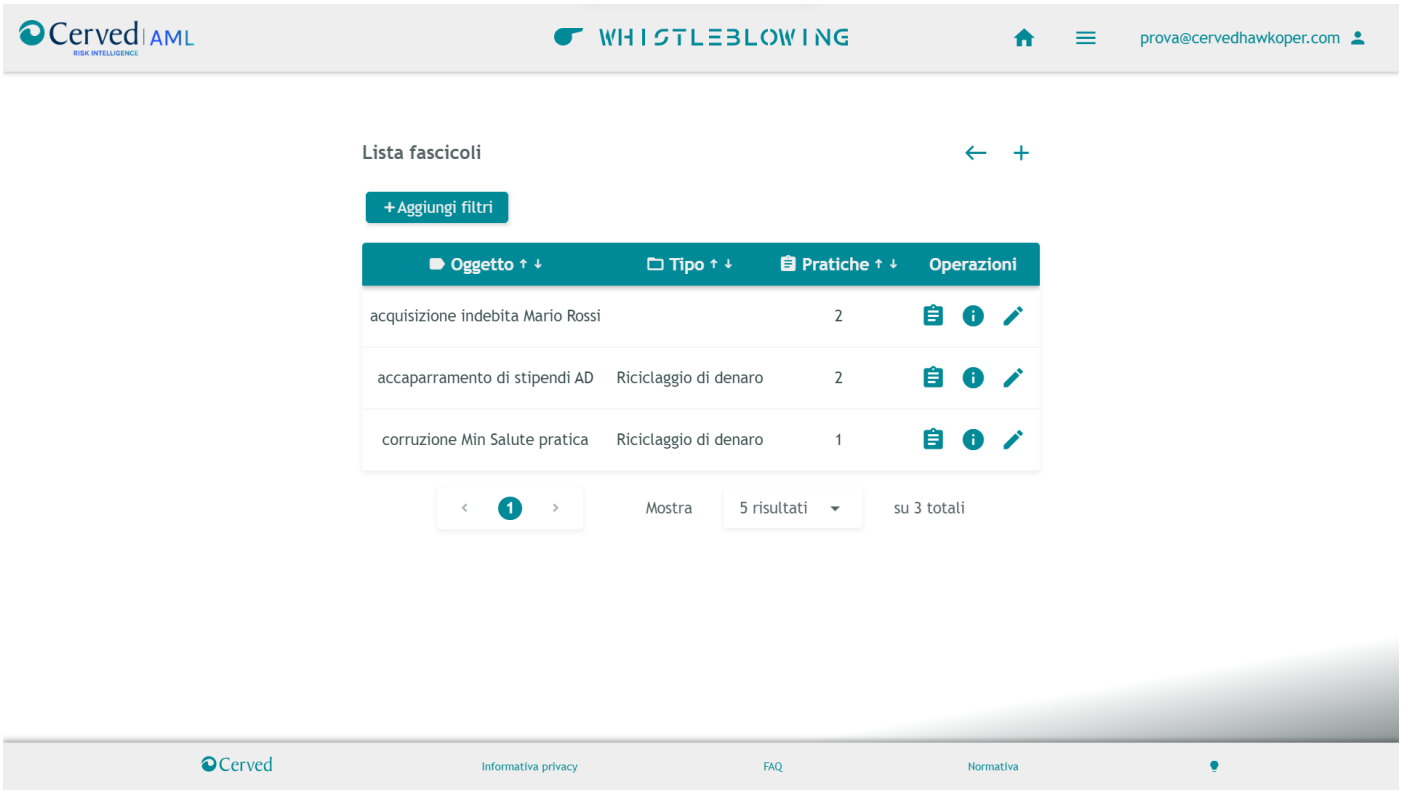

Figura 30 – Gestione fascicolo

L'operatore può provvedere a consultare i fascicoli esistenti, la funzionalità consente all'operatore di consultare la schermata fascicolo da cui consultare i fascicoli esistenti e le segnalazioni associate al relativo all'iter

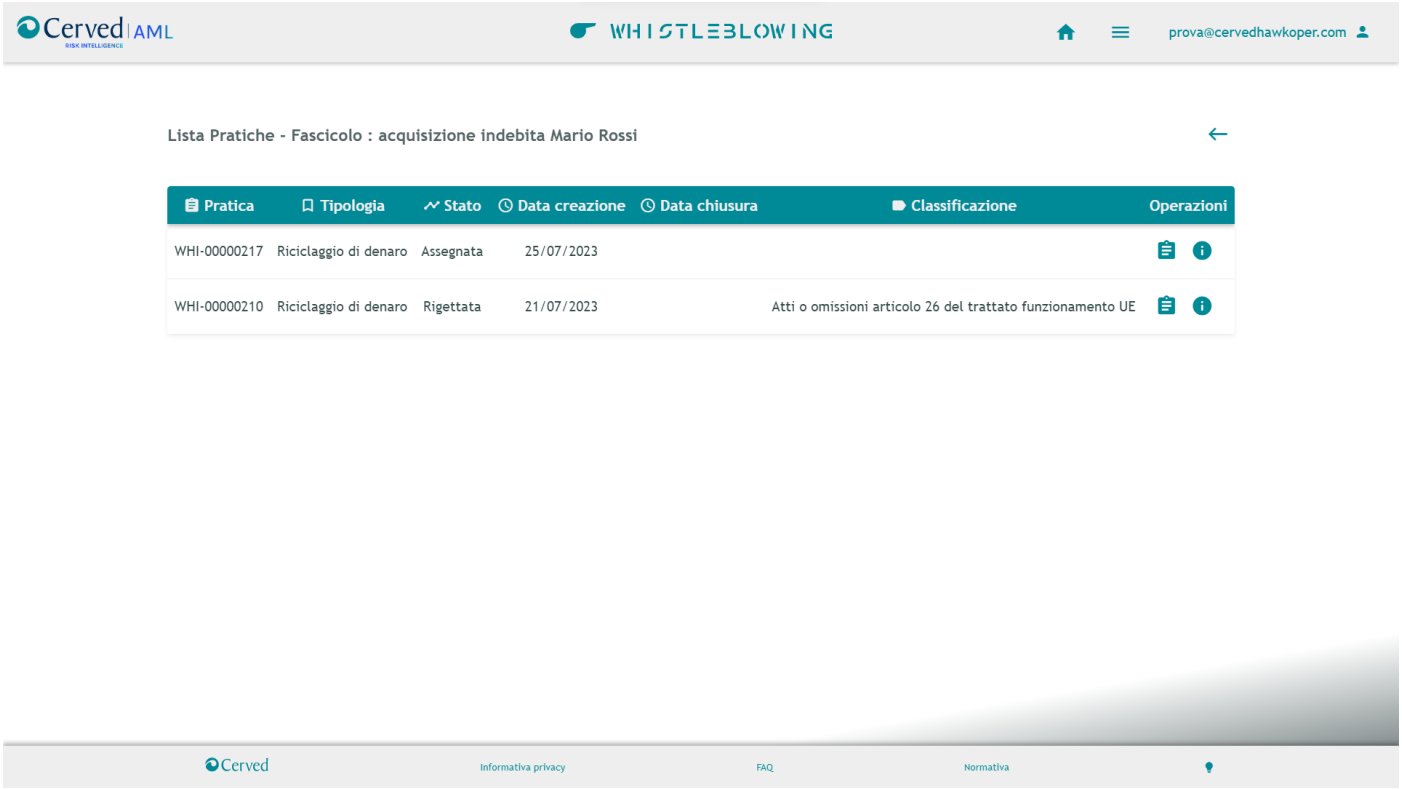

Figura 31 – Dettaglio della pratica nel fascicolo

L’operatore può provvedere a consultare le caratteristiche del fascicolo

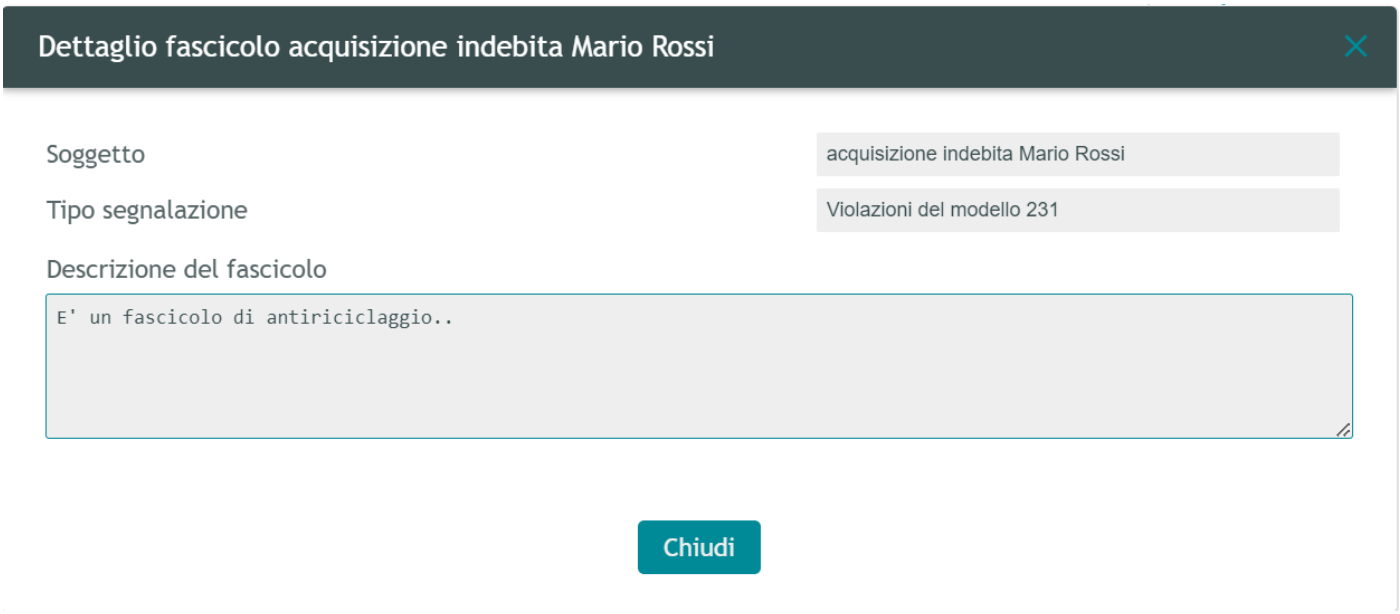

Figura 32 – Dettaglio del fascicolo

L’operatore può provvedere a modificare i fascicoli esistenti o crearne uno nuovo dal pulsante + in altro a destra.

1.1.5.9 Statistiche

La funzionalità consente la visualizzazione delle statistiche sui dati relativi alle segnalazioni:

- per tipologia di illecito
- per canale di provenienza
- per stato di lavorazione

La funzionalità consente all'operatore abilitato di monitorare periodicamente gli andamenti e le casistiche più frequenti di segnalazione, restituendo le numeriche e consentendone la stampa.

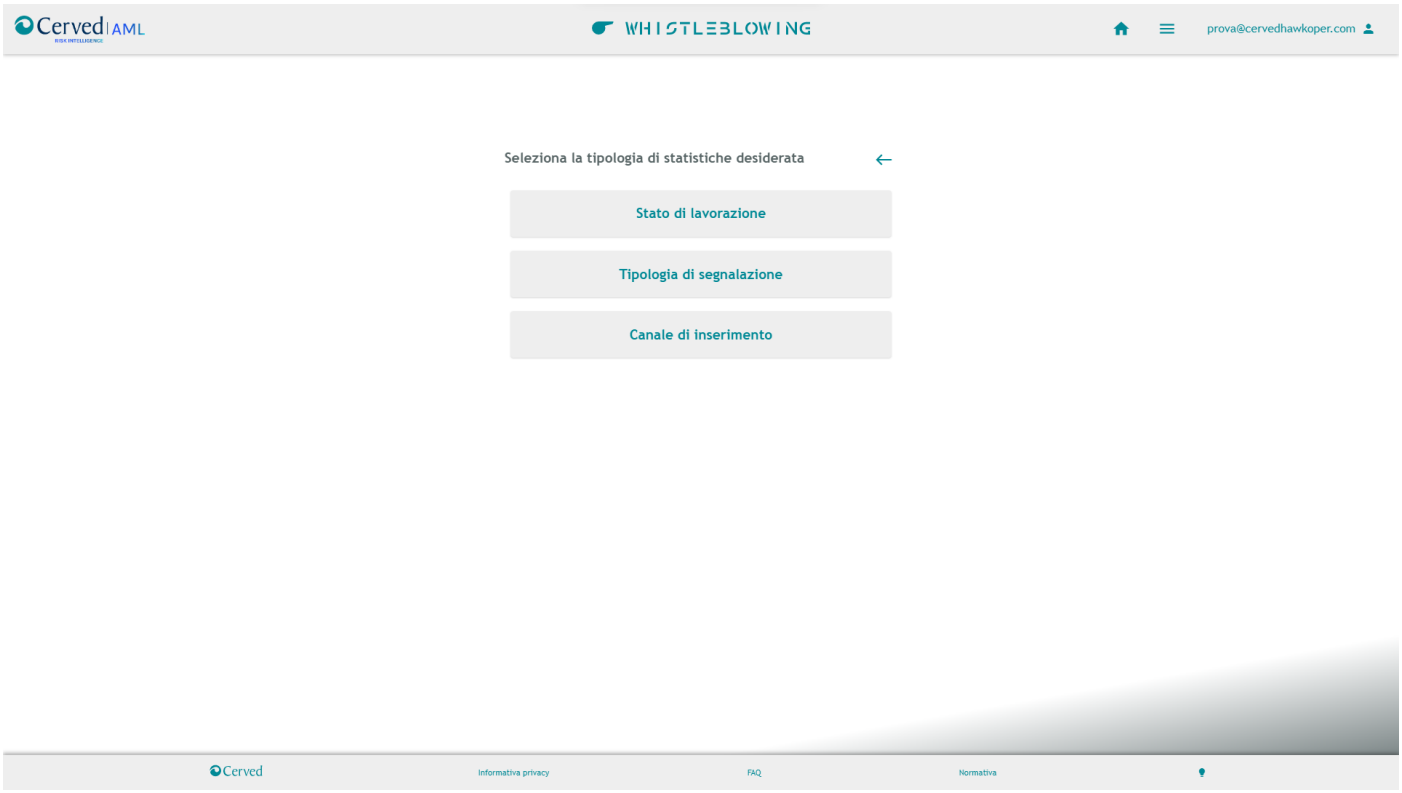

Figura 33 – Statistiche

1.1.5.10 Scadenzario

Il sistema evidenzia sulla dashboard:

- La necessaria assegnazione della nuova segnalazione
- Evidenzia come criticità
  - la mancata assegnazione per le pratiche ricevute e non assegnate da più di 7 giorni.
  - il termine per la presa in carico
  - il termine per la definizione dell'istruttoria.

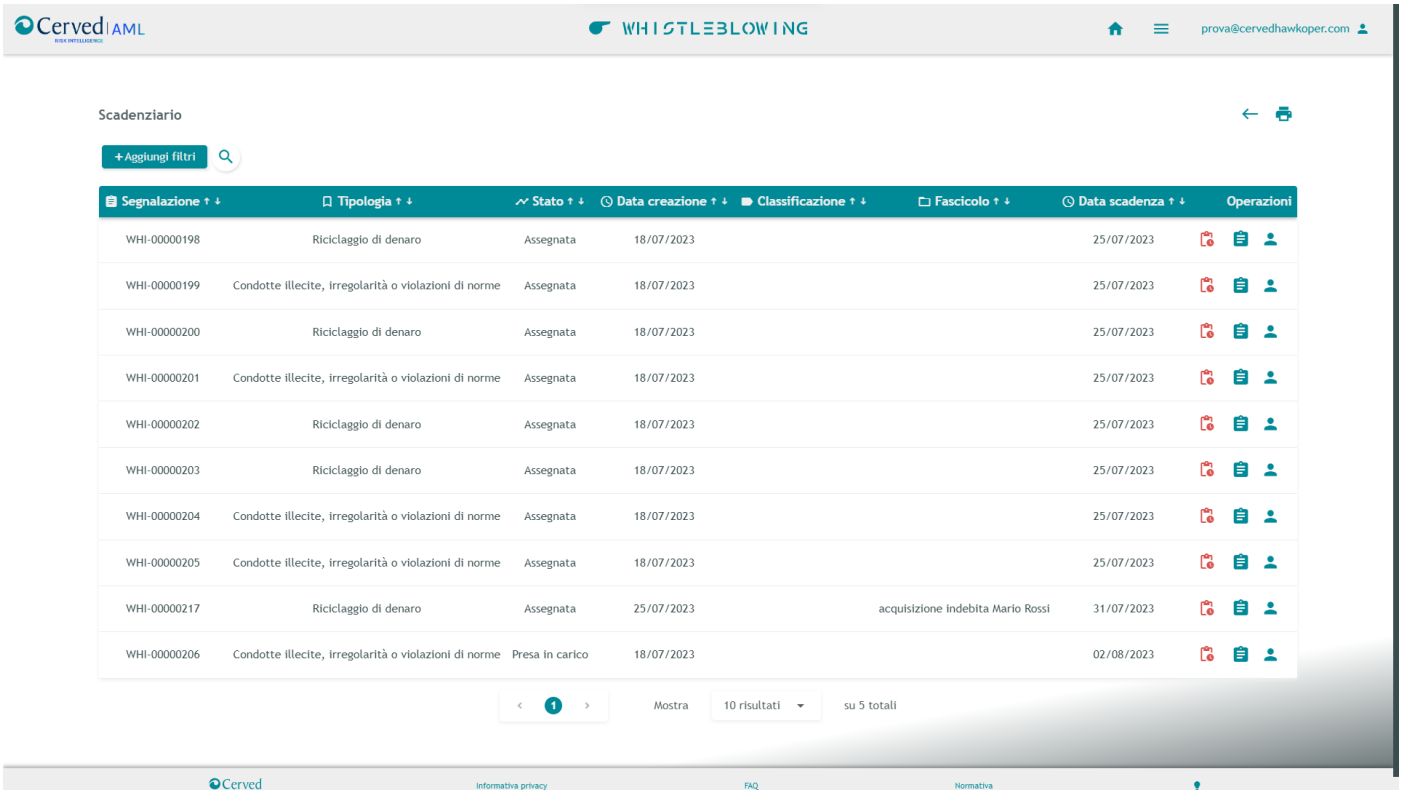

Figura 34 – Scadenzario

1.1.5.11 Dashboard operatore

Una volta autenticato nel sistema, il sistema reindirizza l'operatore sulla propria dashboard, dalla quale può visualizzare la homepage dell'operatore è denominata "dashboard". In questa pagina l'utente può visualizzare i widget relativi ai moduli attivi a cui ha accesso. La funzionalità consente all'operatore di gestire l'iter delle segnalazioni a lui assegnate.

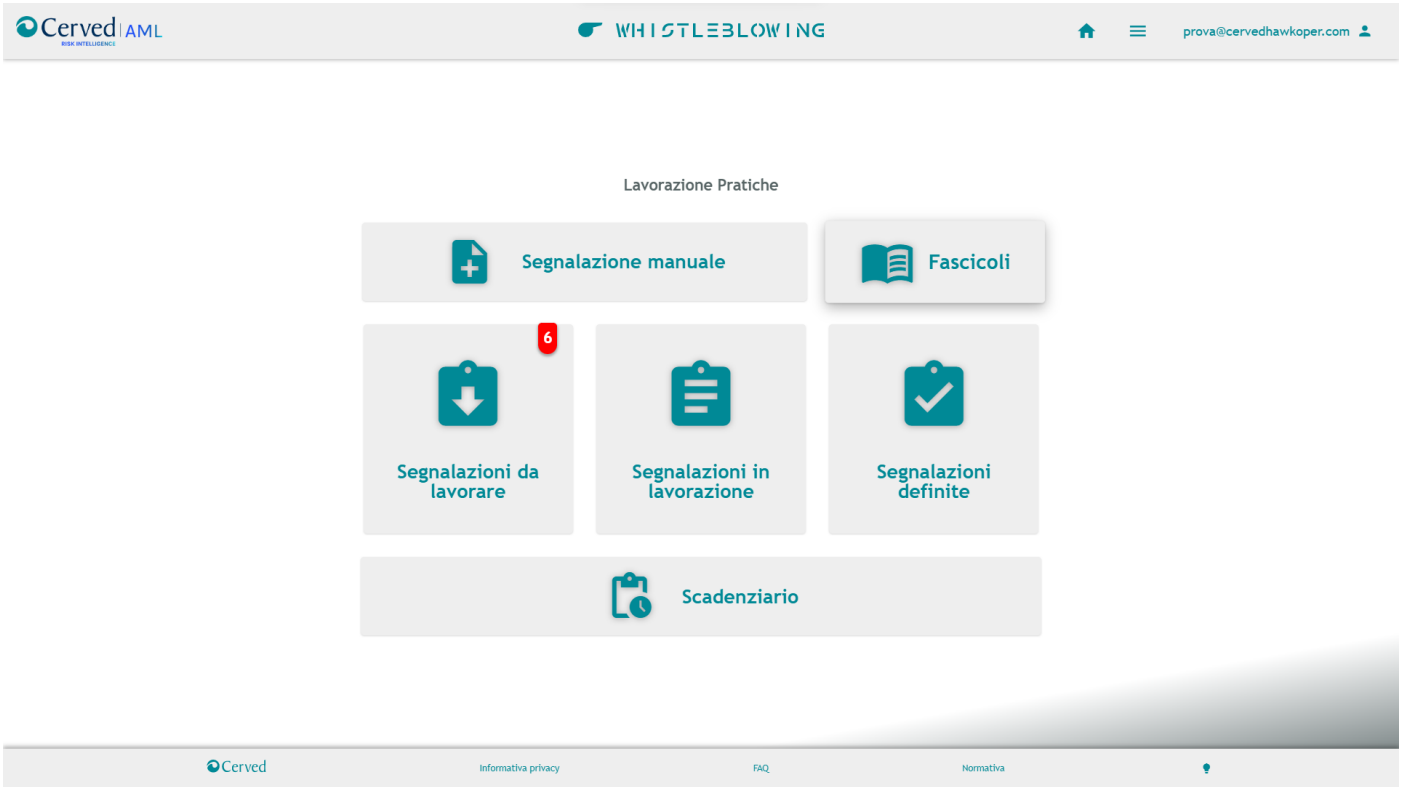

Figura 35 – Dashboard operatore

La dashboard consente di accedere alle relative pagine di dettaglio con il riepilogo dei dati relativi alle segnalazioni assegnate all'operatore.

- la lista delle segnalazioni a lui assegnate
    - la lista delle segnalazioni prese in carico con la data di inserimento e la data di acquisizione.
    - In lavorazione (indagine in corso)
- la lista delle segnalazioni chiuse.

Oltre ad accedere alle funzionalità:

- Segnalazione manuale, per inserire una segnalazione proveniente da un canale esterno
- Fascicoli, per creare un fascicolo
- Scadenzario

1.1.5.12 Dettaglio delle segnalazioni da lavorare

Una volta ricevuta la segnalazione e assegnata all'operatore, quest'ultimo deve provvedere ad adottare le azioni ritenute da lui più consone, per garantire la massima riservatezza e istruire l'accertamento.

Accedendo al dettaglio "Lista segnalazioni da lavorare" il sistema riporta in forma tabellare l'elenco delle pratiche da prendere in carico.

Il sistema crea una coda di lavoro contente le nuove segnalazioni inserite nel sistema.

La griglia prevede una funzione di filtro per agevolare la ricerca.

Dalla lista delle segnalazioni riportata è possibile visualizzare il contenuto della segnalazione e accedere alle relative funzionalità di gestione.

I dati riportabili sono ordinabili per campo e la visualizzazione per vista può essere gestita in base alla selezione della quantità di risultati da mostrare.

La pagina può essere stampata dal pulsante riportato in altro a destra.

Dalla freccia in altro è possibile trovare indietro, per tornare alla Dashboard.

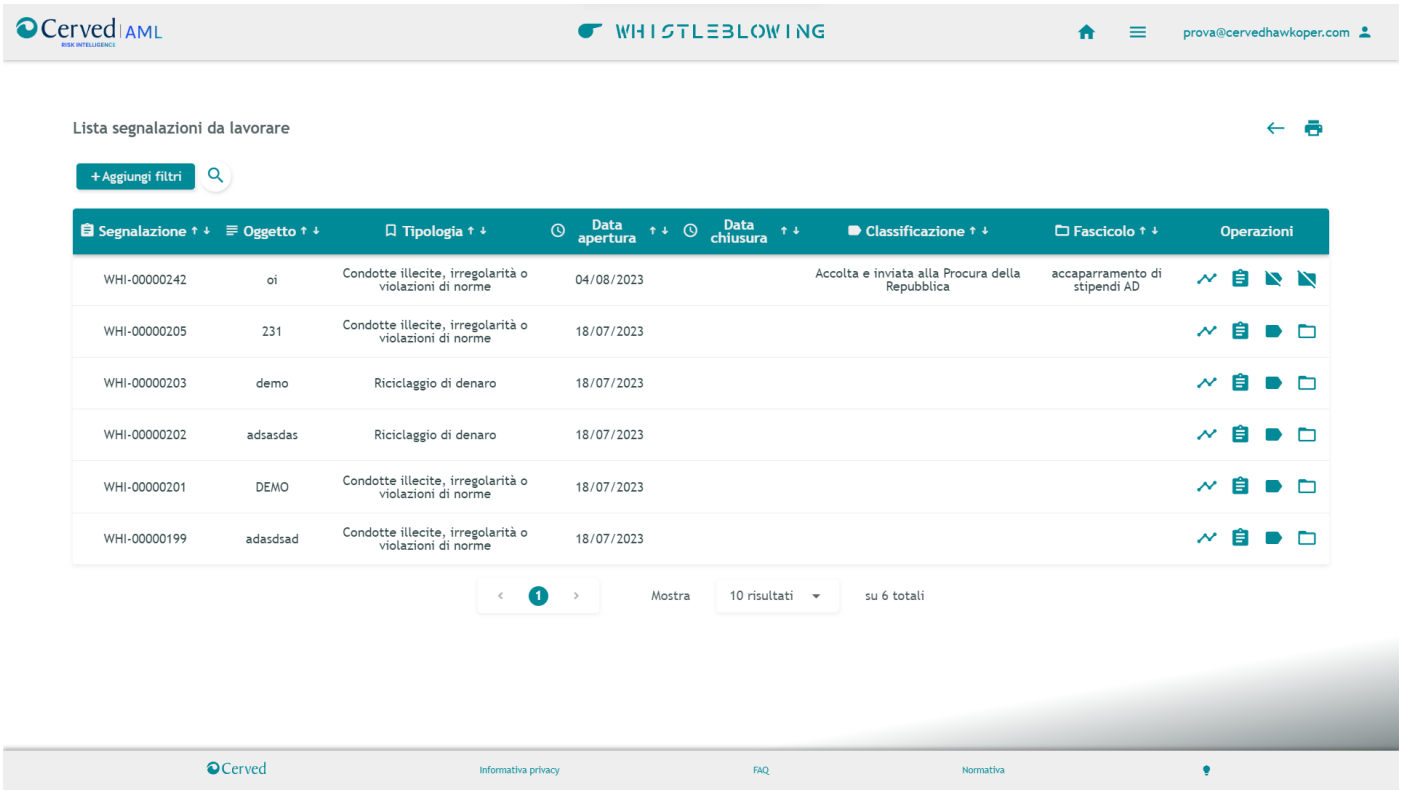

Figura 36 – Lista segnalazioni da lavorare

Il sistema visualizza le principali informazioni associate alle segnalazioni in griglia:

- ID Segnalazione
- Tipologia
- Data apertura
- Classificazione
- Fascicolo
- Pulsanti Operazione
    - Passaggio di stato – Presa in carico – L'operatore, ricevuta l'assegnazione della segnalazione, procede ad una prima verifica e analisi del contenuto, in modo da verificare la sussistenza dei presupposti e dei requisiti oggettivi e soggettivi prescritti dalla normativa vigente. Il sistema permette di modificare lo stato della segnalazione con il passaggio di stato, l'azione apre la finestra di secondo livello su cui effettuare la presa in carico e per l'operatore inserire una nota o un allegato, motivando le ragioni. L'operatore deve fornire riscontro alla segnalazione entro sette (7) giorni dalla presentazione della segnalazione.

Il sistema permette di inserire una nota nella segnalazione, motivando le ragioni;

Figura 37 – Passaggio di stato

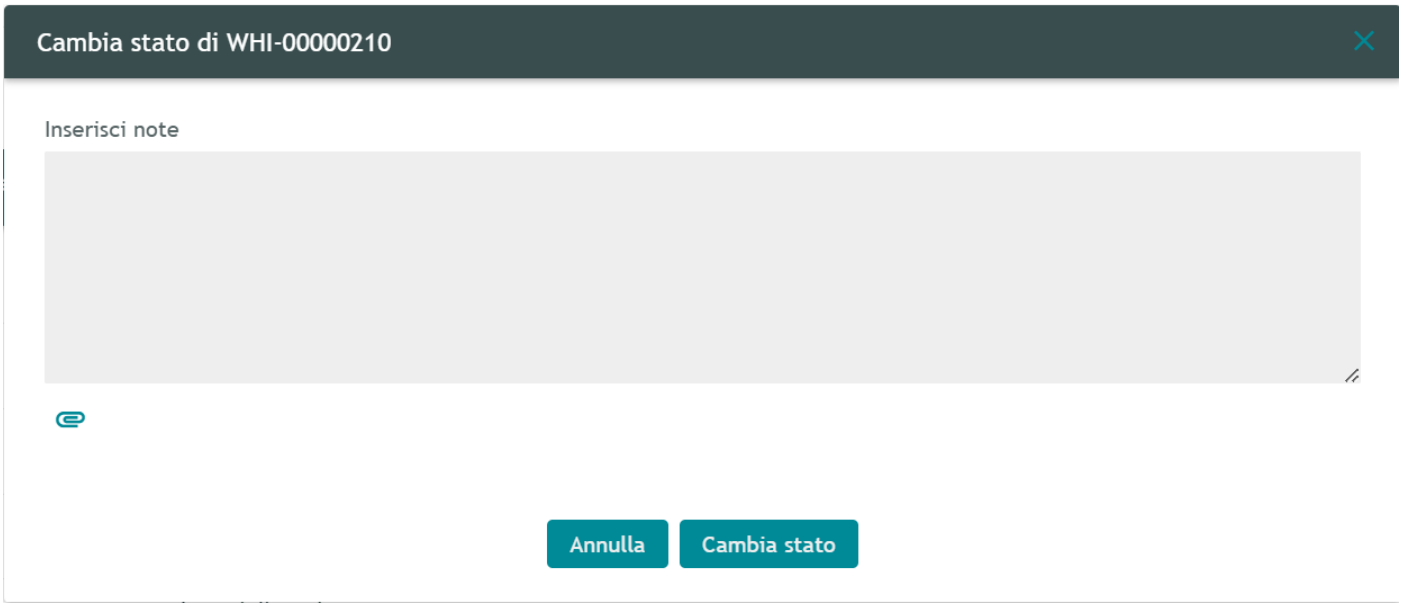

Figura 38 – Inserimento di nota e allegato al passaggio di stato

- Consultazione dei dati inseriti al momento dell'inserimento della segnalazione
- Consultazione dati anagrafici. Se disponibili, ma ancora non abilitati, la piattaforma consente di richiedere l'accesso, motivato da nota, all'operatore che gestisce l'identità delle generalità del segnalante, se inserite.
- Classificazione - In relazione al contenuto delle segnalazioni il super operatore può assegnare una tipologia, tra quante disponibili in base alla configurazione predisposta.
- Inserimento in fascicolo, selezionandone uno già esistete a cui associare la segnalazione in lavorazione per gestire in modo aggregato segnalazioni che riguardano lo stesso illecito.
- Riepilogo, riporta la cronologia della segnalazione grazie al tracciamento automatico delle operazioni svolte.

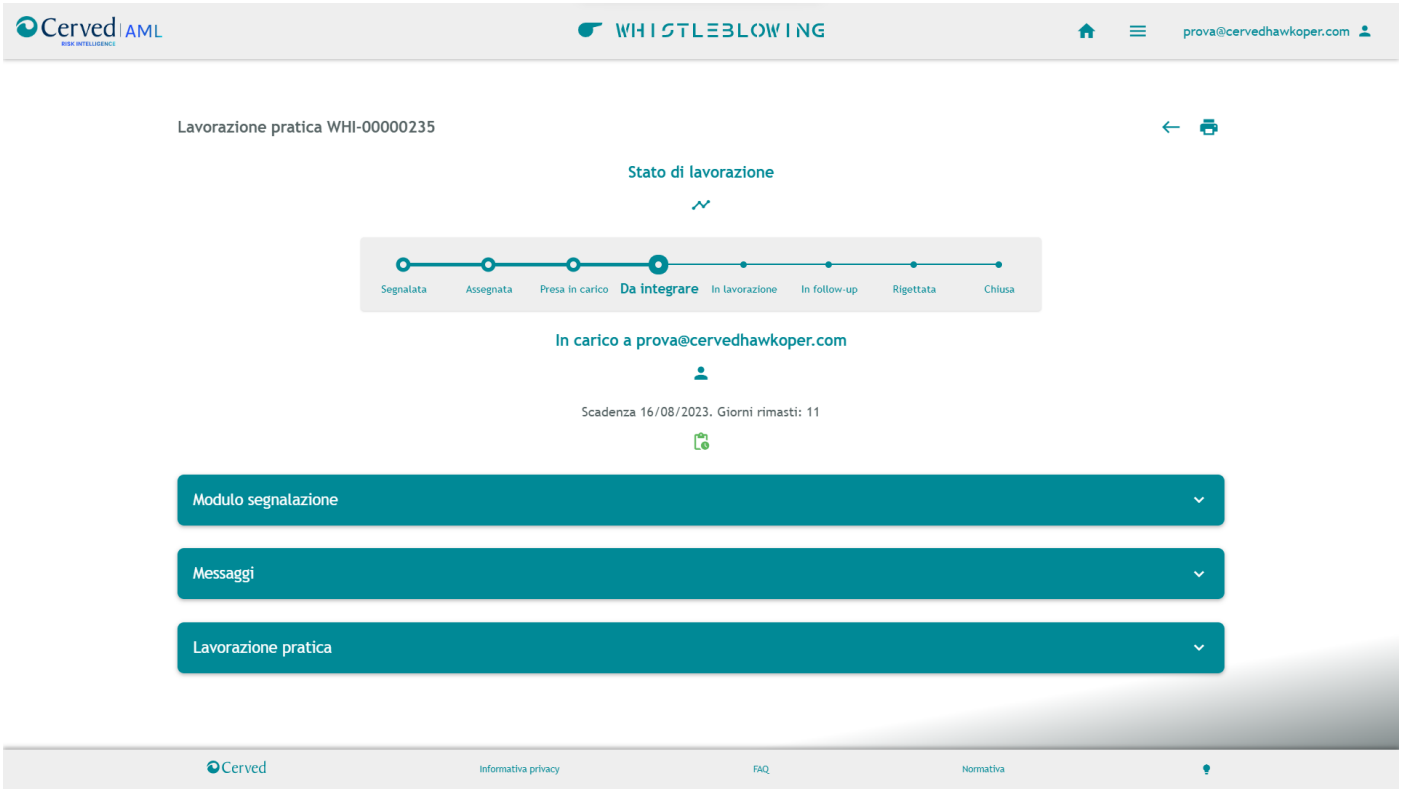

Figura 39 – Riepilogo

1.1.5.13 Dettaglio delle segnalazioni in lavorazione

Accedendo al dettaglio “Lista segnalazioni in lavorazione” il sistema riporta in forma tabellare l’elenco delle pratiche per cui è in corso l’istruttoria.

Il sistema crea una coda di lavoro contente le pratiche prese in carico.

La griglia prevede una funzione di filtro per agevolare la ricerca.

Dalla lista delle segnalazioni riportata è possibile visualizzare il contenuto della segnalazione e accedere alle relative funzionalità di gestione.

I dati riportabili sono ordinabili per campo e la visualizzazione per vista può essere gestita in base alla selezione della quantità di risultati da mostrare.

La pagina può essere stampata dal pulsante riportato in altro a destra.

Dalla freccia in altro è possibile trovare indietro, per tornare alla Dashboard.

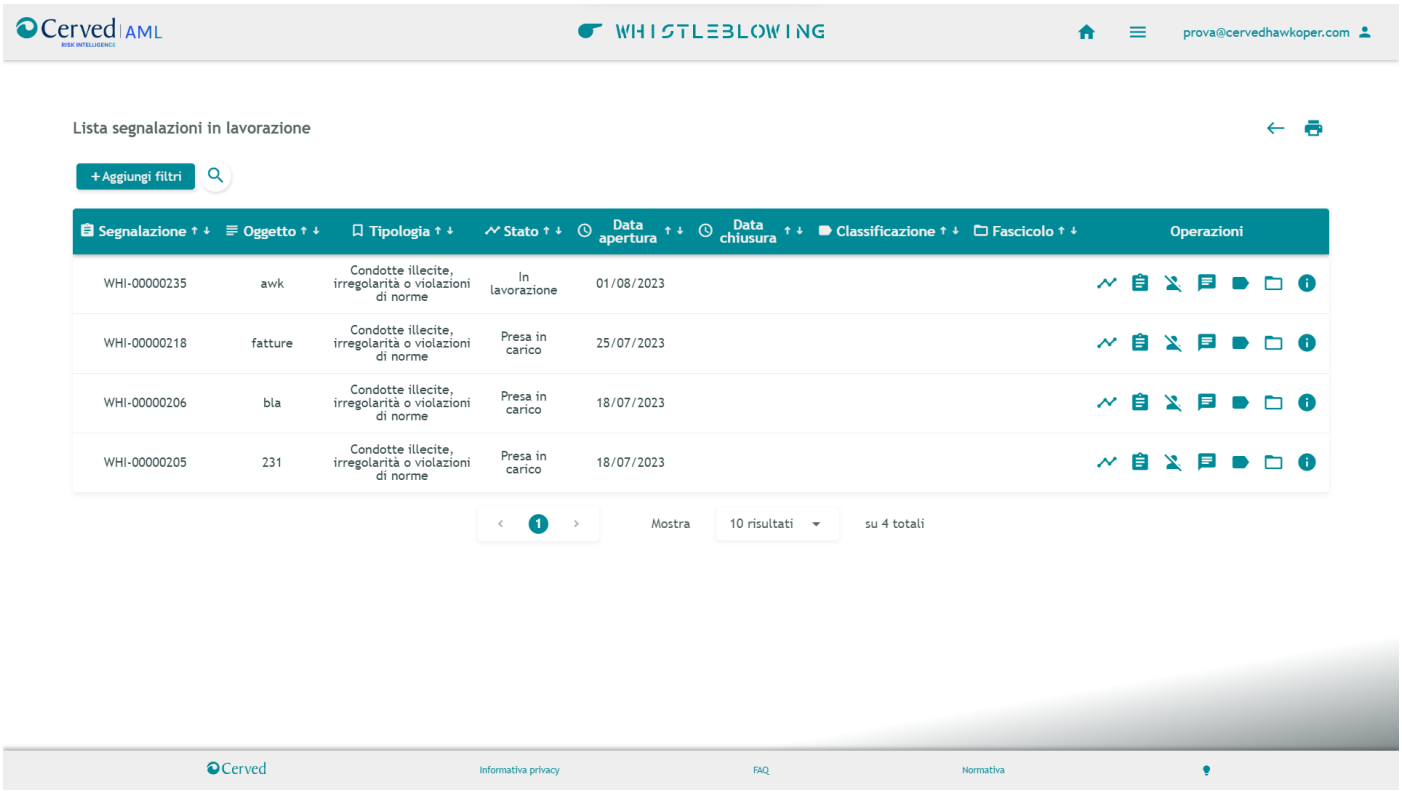

Figura 40 – Lista segnalazioni in lavorazione

Il sistema visualizza le principali informazioni associate alle segnalazioni in griglia:

- ID Segnalazione
- Oggetto
- Tipologia
- Stato lavorazione
- Data apertura
- Classificazione
- Fascicolo
- Pulsanti Operazione

- Passaggio di stato - istruttoria, l'operatore può avviare un dialogo con il whistleblower (richiesta integrazione), chiedendo chiarimenti, documenti o informazioni ulteriori. L'operatore può inoltre richiedere una collaborazione a delle strutture competenti nel proseguo dell'attività (follow up), sempre nel rispetto della tutela della riservatezza. L'operatore deve fornire riscontro alla segnalazione entro tre mesi (90 giorni) dalla data dell'avviso di ricevimento. Il sistema permette di modificare lo stato della segnalazione con il passaggio di stato sulla relativa pagina di gestione, a seconda della fase di avanzamento della pratica. L'azione apre la finestra di secondo livello su cui effettuare l'avanzamento della lavorazione e inserire una nota o un allegato, motivando le ragioni, fino alla definizione.

Il sistema permette di inserire una nota nella segnalazione e procedere eventualmente alla definizione

Figura 41 – Passaggio di stato

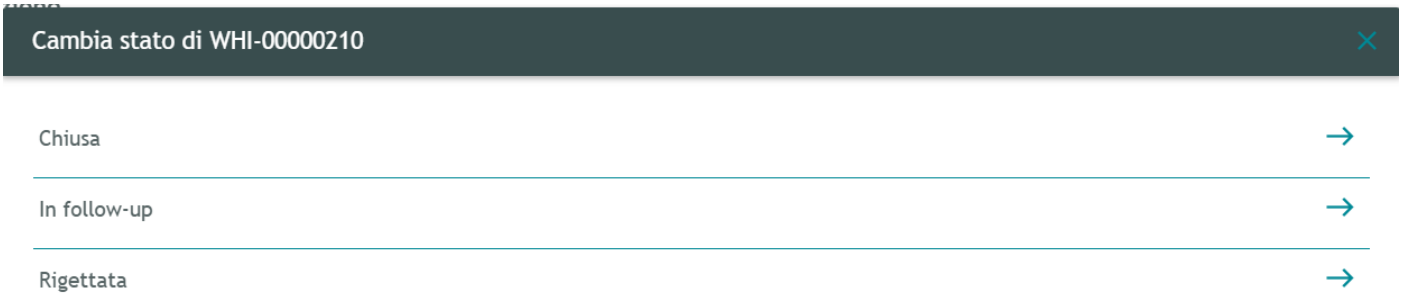

Figura 42 – Definizione della pratica

- Nel caso di rigetto della segnalazione è opportuno completare la nota esplicitando che non sussistono i presupposti per procedere, esplicitandone il motivo.

- Consultazione dei dati inseriti al momento dell'inserimento della segnalazione
- Consultazione dati anagrafici. Se disponibili, ma ancora non abilitati, la piattaforma consente di richiedere l'accesso, motivato da nota, all'operatore che gestisce l'identità delle generalità del segnalante, se inserite.
- Richiesta integrazione, consente di avviare una interlocuzione tra l'utente e il whistleblower attraverso la sezione "Messaggio" da utilizzare qualora la segnalazione non sia adeguatamente circostanziata. La funzionalità consente all'utente di chiedere al segnalante elementi integrativi attraverso la stessa procedura per garantire la riservatezza delle comunicazioni.

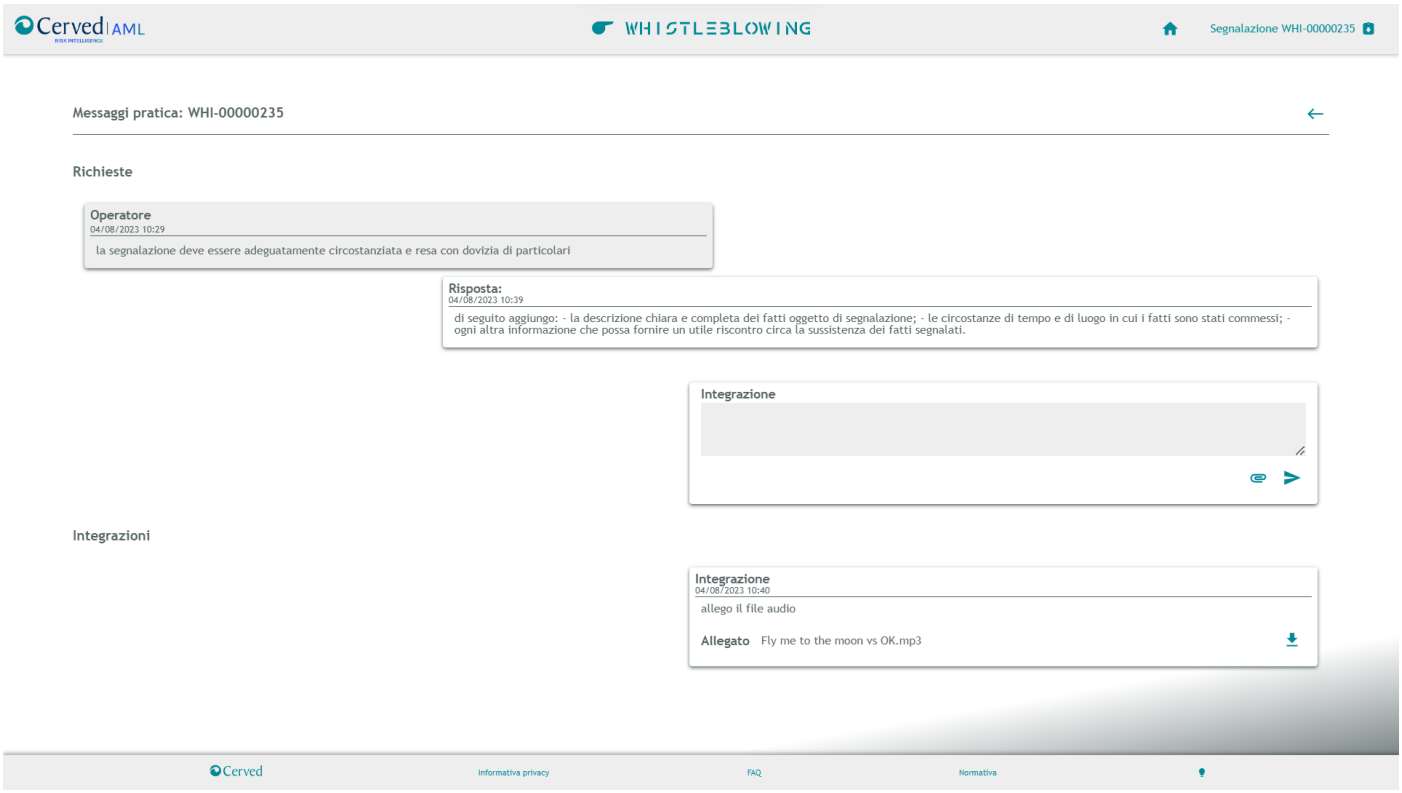

Figura 43 – Richiesta integrazione

- Classificazione - In relazione al contenuto delle segnalazioni il super operatore può assegnare una tipologia, tra quante disponibili in base alla configurazione predisposta.
- Inserimento in fascicolo, selezionandone uno già esistete a cui associare la segnalazione in lavorazione per gestire in modo aggregato segnalazioni che riguardano lo stesso illecito.
- Riepilogo, riporta la cronologia della segnalazione grazie al tracciamento automatico delle operazioni svolte.

1.1.5.14 Dashboard gestore identità

Il Gestore dell'identità può consentire o meno l'accesso all'identità del segnalante. L'identità del whistleblower non può essere rivelata a persona diversa da quelle autorizzate.

L'accesso può avvenire solo esclusivamente dietro espresso consenso del gestore, che prende in carico le richieste di autorizzazioni pervenute e, consultando la nota allegata, autorizza o meno l'accesso alle generalità del segnalante.

La funzionalità consente all'operatore Gestore dell'identità di autorizzare dalla procedura l'accesso all'identità del Segnalante.

Il gestore atterra su una dashboard che prevede 3 widget:

- autorizzazione richieste
- autorizzazioni concesse
- autorizzazioni negate

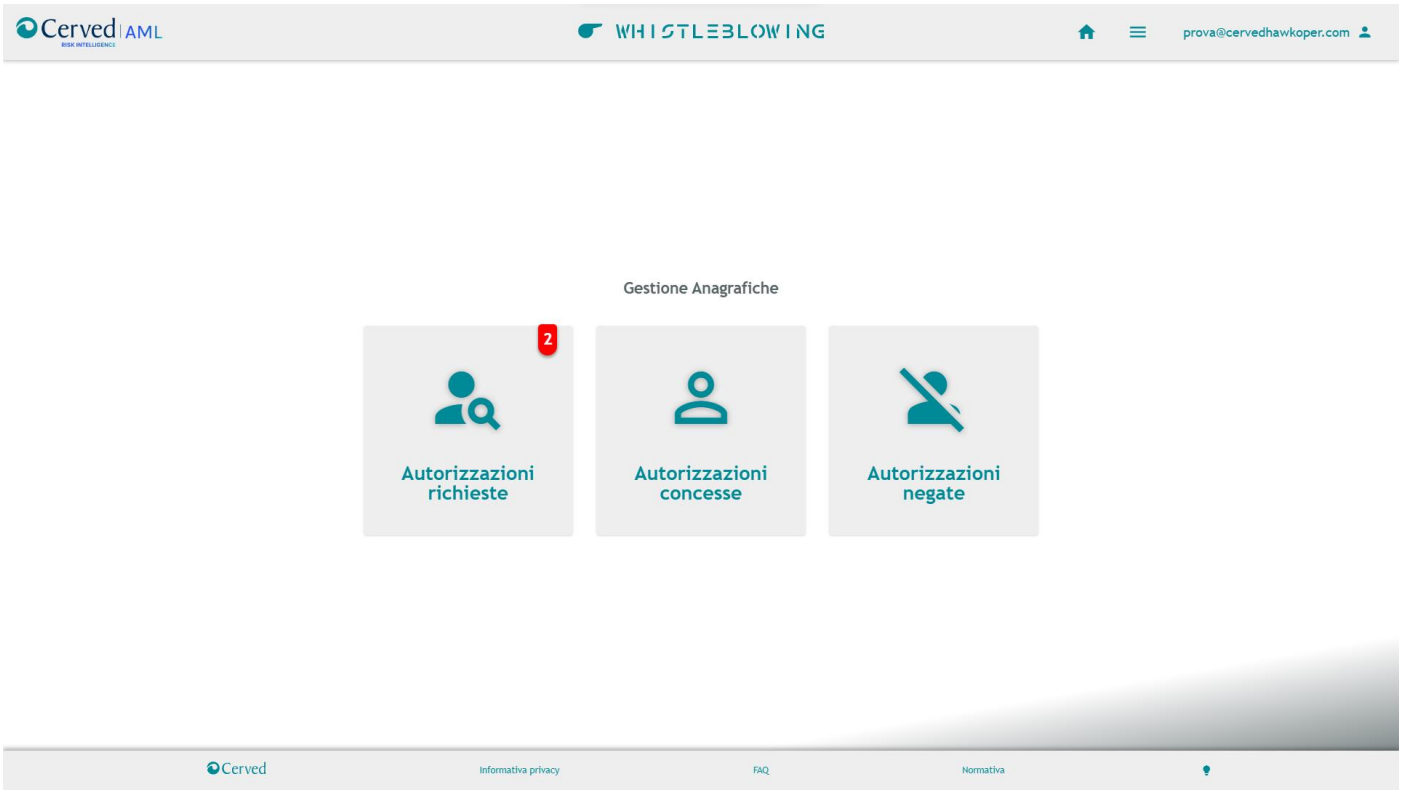

Figura 44 – Dashboard gestore identità

La funzionalità di richiesta di accesso è attiva in funzione dello stato della pratica, è possibile richiedere l'identità del segnalante solo da quando la segnalazione è in stato di lavorazione.

L'accesso ai dati del segnalante è condizionato della motivazione addotta, accessibile nel menu "Autorizzazioni richieste".

Le motivazioni possono essere varie:

- necessità di fornire i dati identificativi del whistleblower all'Autorità giudiziaria cui è stata trasmessa la segnalazione;
- coinvolgimento di più uffici interni e, quindi, per evitare di mettere a rischio il segnalante è necessario conoscerne l'identità;
- dubbi in merito al dipendente segnalato dichiarato dal segnalante.

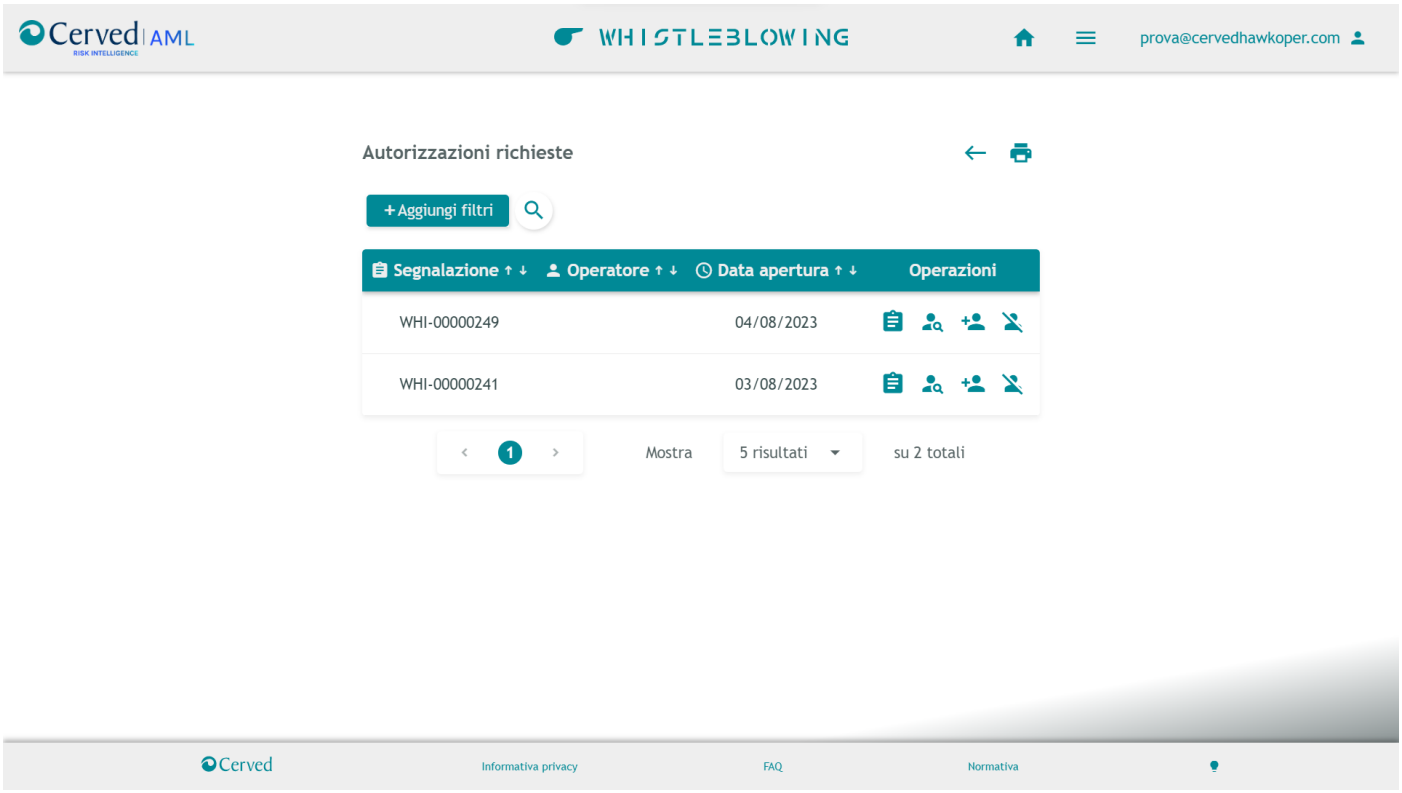

Figura 45 – Lista autorizzazione richieste

Se il Gestore dell'identità autorizza l'accesso alle informazioni anagrafiche, l'operatore può accedere alle informazioni del segnalante che saranno visibili sul dettaglio della segnalazione. I soggetti coinvolti nella gestione della segnalazione sono tenuti a tutelarne la riservatezza.

1.1.5.15 Dashboard ADMIN

La funzionalità consente all'utente amministratore di operare per abilitazione su:

- Gestione utenti, da cui il sistema consente all'Amministratore la gestione degli utenti abilitati alla procedura, con relativa assegnazione dei ruoli e delle relative funzioni.
  La funzionalità consente all'amministratore di accedere all'elenco degli utenti accreditati.
  Il sistema consente all'Amministratore:
  - di aggiornare un utente già presente;
  - di modificare le abilitazioni assegnate;
  - di eliminare un utente già presente;
  - di inserire un nuovo utente.

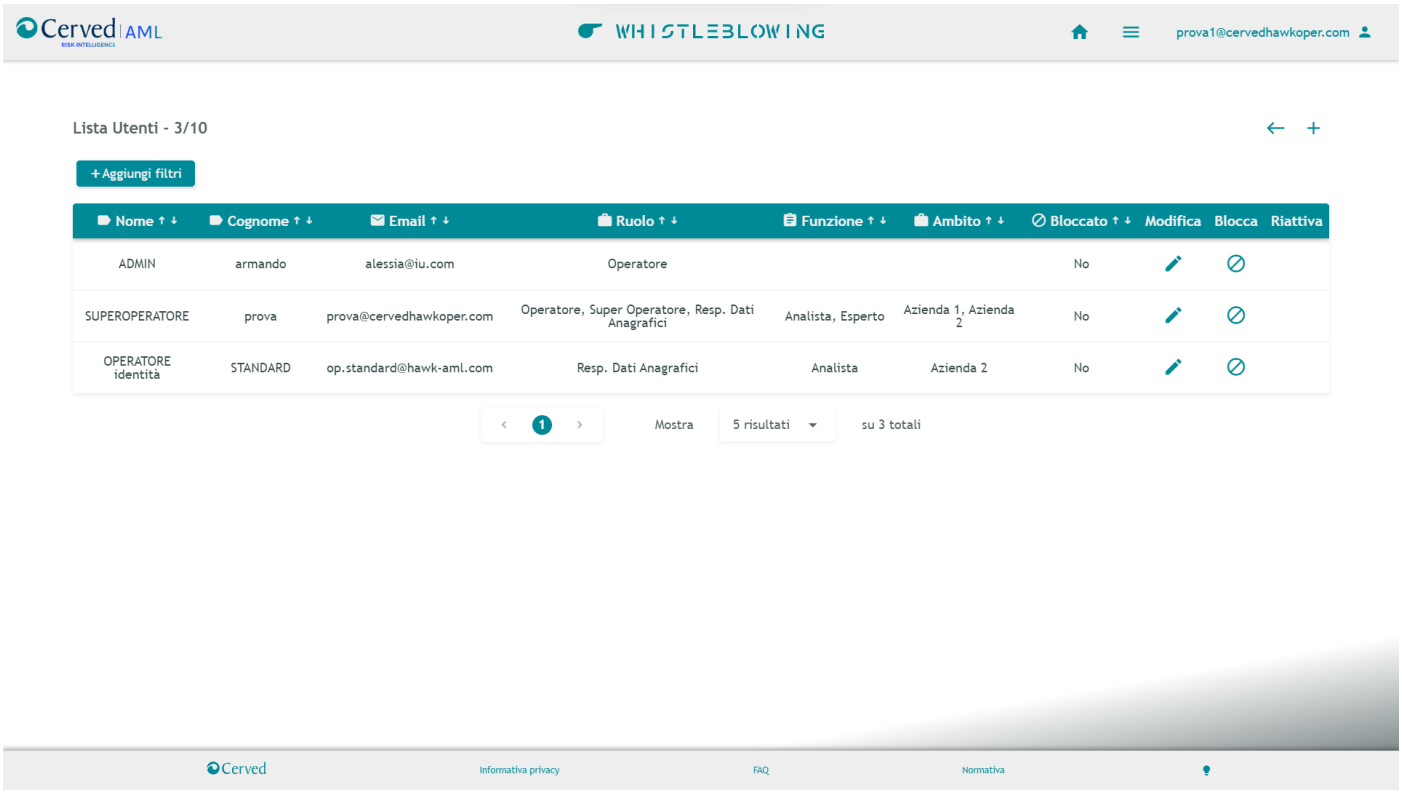

Figura 46 – Gestione Utenti

La form di inserimento per l'inserimento del "Nuovo Utente" prevede di specificare:

- Cognome*;
- nome*;
- user (email) *;
- Password*;
- ruolo*;
- funzione;
- ambito.

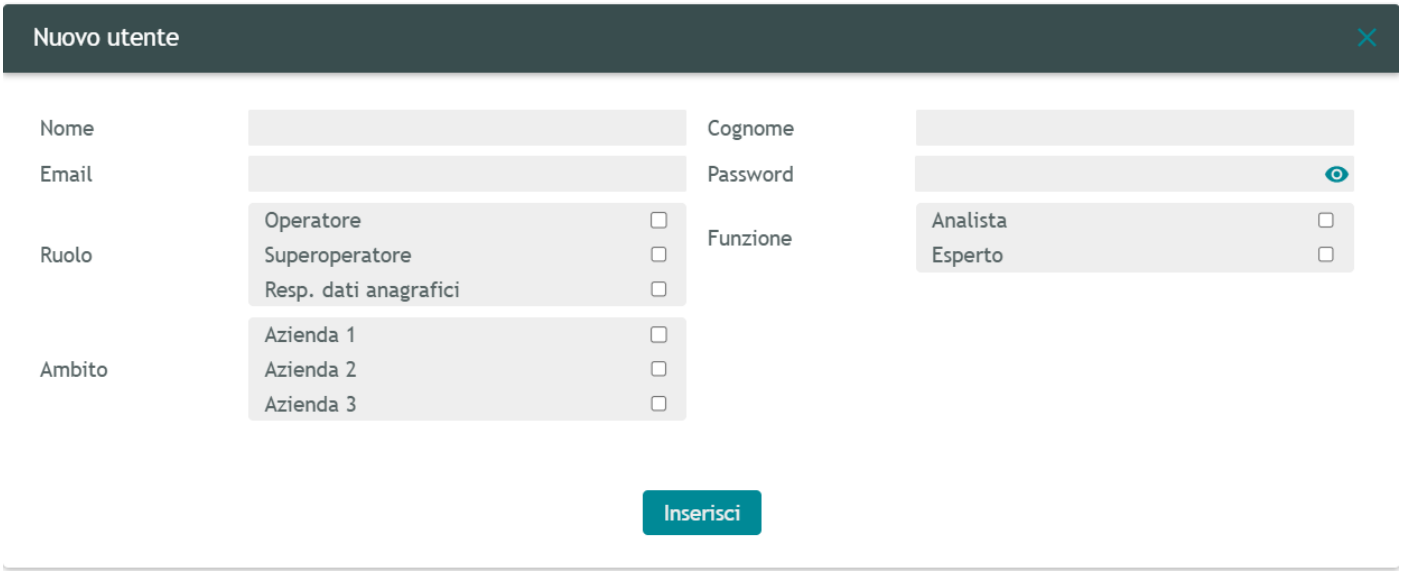

Figura 47 – Creazione nuovo utente

Il sistema prevede a fronte dell'inserimento, la creazione dell'utenza e l'assegnazione delle credenziali di accesso al sistema.

- Gestione classificazioni, Il sistema consente all'amministratore di gestire classi alla quali associare le segnalazioni
  - di aggiornare una classe già presente;
  - di modificare una classe;
  - di eliminare una classe;
  - di inserire una nuova classe.

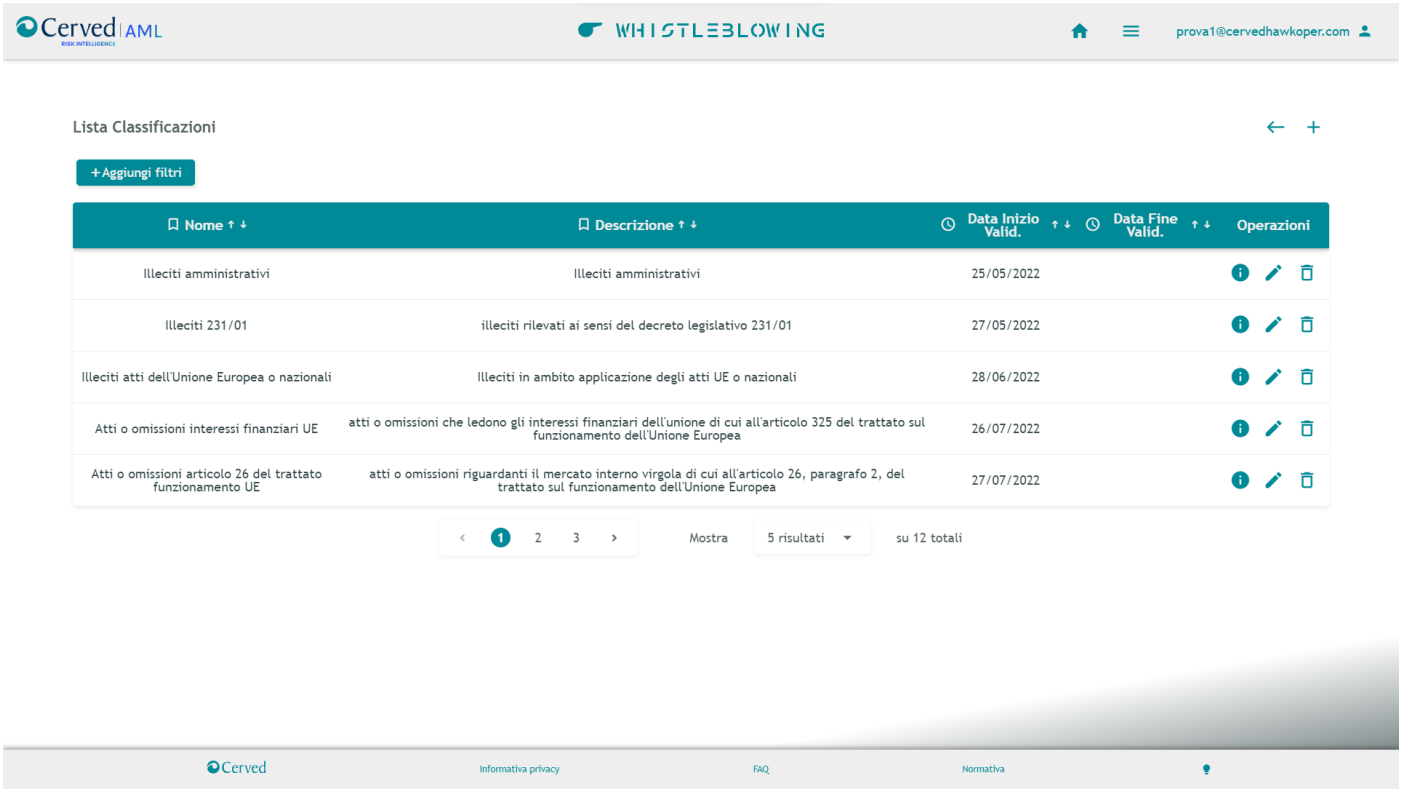

Figura 48 – Gestione Classificazione

- le modalità per la gestione delle segnalazioni di whistleblowing possono essere definite nei i tempi attraverso la configurazione scadenze, che è comunque limitata dai tempi massimo previsti dalla normativa

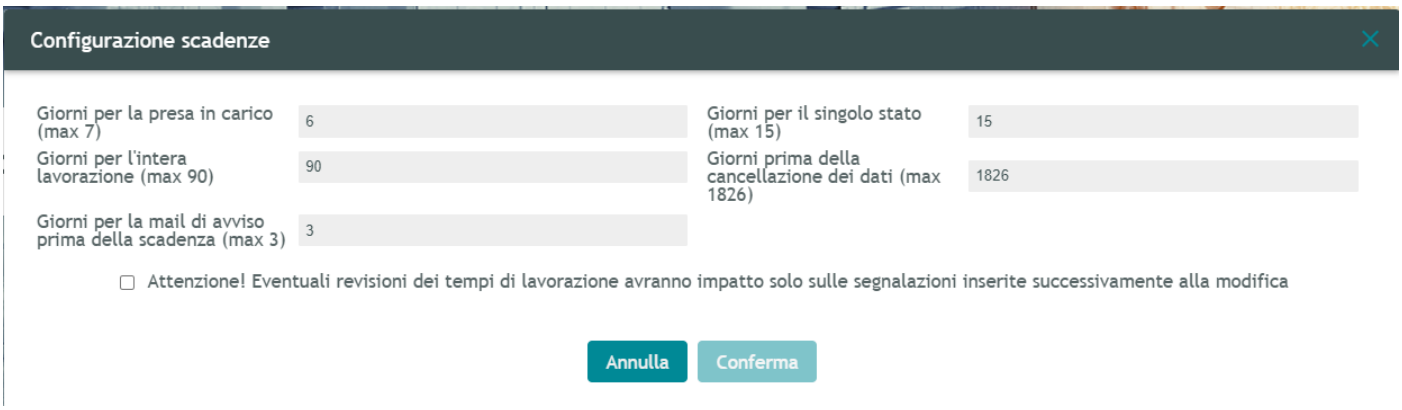

Figura 49 – Configurazione scadenze

- impostazione della lingua predefinita

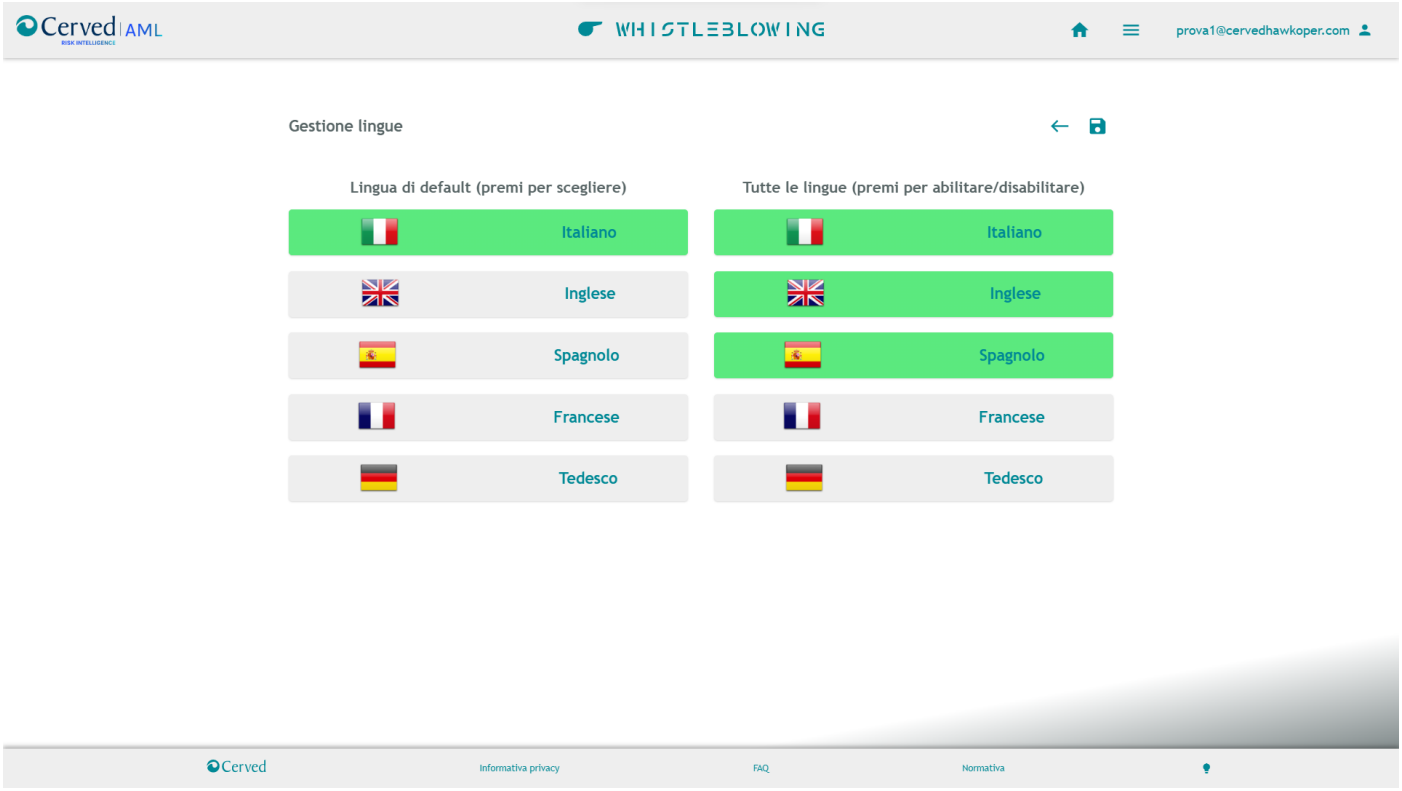

Figura 50 – Impostazione lingue

1.1.5.16 Conservazione della Documentazione

Ai fini del trattamento dati, l'Azienda conserva e censisce le segnalazioni ricevute all'interno del registro del trattamento dati Whistleblowing che provvede ad alimentarlo e tenerlo aggiornato tempestivamente, ogni qual volta pervengano delle segnalazioni o aggiornamenti. Il Registro Whistlebowing viene conservato in forma cartacea ed informatica e confluisce quale sezione opportunamente identificata nel Registro Generale dell'Azienda in qualità di Titolare del trattamento dati conservato a cura del

Referente Aziendale Privacy. Tutte le segnalazioni e la relativa documentazione sono conservate esclusivamente per il tempo necessario al trattamento e gestione della segnalazione e comunque non oltre cinque anni dalla data di comunicazione dell'esito finale della procedura di segnalazione.

2 Caratteristiche tecniche del sistema

2.1.1 Crittografia

I mezzi implementati per assicurare la confidenzialità dei dati archiviati sono Database MSSQL cifrato con TDE (Transparent Data Encrytion) nativa del prodotto.
I backup sono compressi e protetti con password.
L'accesso all'applicazione avviene in https con certificato, protocollo TLS 1.2 e chiave di cifratura a 2048 bit; Lo scambio flussi da/verso Cliente avviene con protocollo SFTP ed autenticazione con username/password e/o chiave pubblica/privata.
I dati acquisiti sono suddivisi in più DB e stoccati in cloud per proteggere i contenuti nelle segnalazioni dagli utenti.
Riguardo alla chiave asimmetrica la metodologia utilizzata recupera una chiave da codice java su uno specifico percorso, mentre l'altra chiave è generata per ogni segnalazione.

2.1.2 Anonimizzazione

Viene utilizzata una keycode, restituita a video, per ogni segnalazione inserita, unica chiave per richiamare successivamente la segnalazione inserita.
È inoltre prevista la figura del "gestore delle identità", addetto all'esclusiva gestione delle richieste di accesso ai dati anagrafici legati alla segnalazione al fine di tutelare il segnalante durante l'indagine

2.1.3 Partizionamento

I dati acquisiti vengono salvati su più database (database 1 per dati utenti e profili utente; database2 per segnalazioni; database3 gestione pratiche/segnalazioni)

2.1.4 Controllo degli accessi logici

I mezzi di autenticazione implementati prevedono una password con lunghezza minima pari a 12 caratteri alfanumerici (1 Maiuscola, 1 minuscola, 1 numerico e 1 special)
La validità della password ha una durata pari a 3 mesi standard, impostabile dal cliente e prevede tre tentativi prima del blocco dell'account.

2.1.5 Tracciabilità

La procedura traccia gli accessi, le attività, l'esecuzione dei processi e tutte le operazioni effettuate dagli utenti, con la relativa data e ora ed indirizzo IP.
Lo storico del log viene mantenuto per una durata pari alla durata del contratto.
È prevista operatività SOC H24.

2.1.6 Archiviazione

I dati anagrafici sono custoditi all'interno del database applicativo, per il quale è prevista la cifratura mediante Transparent Data Encryption (TDE).
Il database risiede in area protetta, non raggiungibile da internet, presso infrastruttura Infordata in Private Cloud.

2.1.7 Vulnerabilità

Le risorse utilizzate sono regolamentate e gestite attraverso procedure e soluzioni interne (es. versionamento, archiviazione, procedure di deploy automatici, VAPT e relativi rientri ecc.). È inoltre prevista una policy di BCDR per ridurre i rischi ai livelli minimi.

2.1.8 Lotta contro il malware

È prevista la soluzione DarkTrace per le funzionalità di controllo e contrasto delle minacce legate alla componente network e di scambio flussi.
È prevista la soluzione CyberReason per le funzionalità di controllo delle minacce.
Entrambe le soluzioni contemplano l'operatività di SOC H24.

2.1.9 Sicurezza dei siti web

L'accesso all'applicazione avviene in https con certificato, protocollo SSL/TLS 1.2 e chiave di cifratura a 2048 bit; E' prevista l'esecuzione periodica di VAPT con successiva applicazione delle contromisure atte a ripristinare i corretti livelli di sicurezza. Sono inoltre previste verifiche periodiche da parte della funzione Internal Audit e di soggetti terzi certificatori ISO27001

2.1.10 Backup

I database applicativi prevedono esecuzione di backup giornalieri con retention di una settimana. I backup vengono archiviati in forma compressa e cifrata e custoditi su sito secondario, collocato geograficamente a distanza maggiore di 300km.

2.1.11 Contratto con il responsabile del trattamento

È prevista la cifratura mediante Transparent Data Encryption.
La trasmissione delle informazioni avviene mediante protocolli HTTPS e SFTP.
È prevista la tracciatura applicativa con retention pari alla durata del contratto.
Le utenze vengono configurate e profilate in base al concetto di minima accessibilità ai dati ("least privilege" e "need to know"), compatibilmente con il ruolo assegnato.
L'autenticazione avviene mediante password gestite in base alle policy GDPR
Il Contratto stipulato con Infordata recepisce quanto riportato.

2.1.12 Prevenzione delle fonti di rischio

I dati sono in Cloud ed ubicati solo su territorio Nazionale.

2.1.13 Protezione contro fonti di rischio non umane

I dati personali risiedono presso Webfarm Infordata. La totalità delle misure riportate è recepita ed implementata dal fornitore.

FINE