A.N.AC.

Autorità Nazionale Anticorruzione

# Allegato 3

# Requisiti Utente

# Sistema di gestione delle segnalazioni di condotte illecite (c.d. *Whistleblowing*)

| | | | |
|---|---|---|---|
| Codice del Progetto | tbd | | |
| Ufficio Committente | Specificare l'Ufficio richiedente | Referente committente | Specificare il nome del Referente per l'Uffcio richedente |
| Versione documento | 1.0 | Versione template | Specificare la versione del template utilizzato |
| Data creazione documento | gg mese anno | Data ultimo aggiornamento | gg mese anno |

| ANAC | | FORNITORE | |
|---|---|---|---|
| Redattore | Indicare il nome del redattore | Società | n.a. |
| Responsabile della fase di raccolta dei requisiti | REG-UAFI | Referente | n.a. |

| APPROVAZIONE | | |
|---|---|---|
| Visto | Approvato | Data |
| | | |

*<History con descrizione puntuale delle modifiche apportate, in termini di requisiti e casi d'uso>*

| **Ver.** | **Elabora** | **Verifica** | **Approva** | **Data emissione** | **Descrizione delle modifiche** |
|---|---|---|---|---|---|
| 1.0 | | | | | Prima versione del documento |

Sommario

## 1. Definizioni, acronimi e riferimenti

DEFINIZIONI ED ACRONIMI

*La presenza nel documento dell'abbreviazione [**tbd**] (to be defined) indica una parte per la quale non si hanno elementi sufficienti per procedere ad una completa definizione; come tale sarà subordinata ad un'ulteriore definizione in una successiva versione del documento.*

*La presenza nel documento dell'abbreviazione [**tbc**] (to be confirmed) indica una parte per la quale sono stati assunti elementi che debbono essere confermati; come tale sarà subordinata ad una conferma in fase successiva.*

*La presenza nel documento dell'abbreviazione [**na**] (non applicabile) indica che un argomento previsto nello standard di struttura di questo documento, risulta privo di significato nel contesto di questo sistema.*

| TERMINE/ACRONIMO | DESCRIZIONE |
|---|---|
| **A.N.AC.** | **Autorità Nazionale Anticorruzione**<br><br>Organo collegiale che previene la corruzione nell'ambito delle amministrazioni pubbliche, nelle società partecipate e controllate anche mediante l'attuazione della trasparenza in tutti gli aspetti gestionali, nonché mediante l'attività di vigilanza nell'ambito dei contratti pubblici, degli incarichi e comunque in ogni settore della pubblica amministrazione che potenzialmente possa sviluppare fenomeni corruttivi, evitando nel contempo di aggravare i procedimenti con ricadute negative sui cittadini e sulle imprese, orientando i comportamenti e le attività degli impiegati pubblici, con interventi in sede consultiva e di regolazione. |
| **RPC** | **Responsabile della Prevenzione della Corruzione** |
| **WB** | **WHISTLEBLOWING**<br><br>Sistema di segnalazione, da parte del dipendente pubblico, secondo il dettato dell'art. 54-bis del d.lvo n. 165 del 2001 introdotto dalla Legge n. 190/2012 |
| **CAD** | DECRETO LEGISLATIVO 7 marzo 2005, n. 82: Codice dell'amministrazione digitale |
| **e-prot** | Sistema per il protocollo informatico in uso presso l'ANAC |
| *web-services* | sistemi software progettati per supportare l'interoperabilità tra diversi ambiti applicativi |

Tabella 1 - Acronimi e Definizioni

RIFERIMENTI

| IDENTIFICATIVO DEL DOCUMENTO | TITOLO/DESCRIZIONE |
|---|---|
| Determinazione A.N.AC. n. 6 del 28 aprile 2015 | Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d. Whistleblowing) |
| D.L. 90/2014 | Misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza degli uffici giudiziari |
| Legge n. 190/2012 | Legge anticorruzione |
| D.lgs. n. 165/2001 | Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche |
| AgID: Linee guida per l'inserimento ed il riuso di programmi informatici o parti di essi pubblicati nella Banca dati dei programmi informatici riutilizzabili | linee guida sul "riuso di programmi informatici o parti di essi" che prevedono la possibilità per una pubblica amministrazione di riutilizzare gratuitamente programmi informatici o parti di essi, sviluppati per conto e a spese di un'altra amministrazione adattandoli alle proprie esigenze ai sensi dell'art. 69 del CAD.<br><br>http://www.agid.gov.it/agenda-digitale/pubblica-amministrazione/riuso-software |

Tabella 2 – Documenti di riferimento

## 2. Scenario di riferimento

### Premessa e scopo del documento

L'art. 1, comma 51, della legge 190/2012 (cd. legge anticorruzione) ha inserito un nuovo articolo, il 54-bis, nell'ambito del d.lgs. 165/2001, rubricato "tutela del dipendente pubblico che segnala illeciti", in virtù del quale è stata introdotta nel nostro ordinamento una misura finalizzata a favorire l'emersione di fattispecie di illecito, nota nei paesi anglosassoni come whistleblowing. Con l'espressione whistleblower si fa riferimento al dipendente di un'amministrazione che segnala violazioni o irregolarità commesse ai danni dell'interesse pubblico agli organi legittimati ad intervenire. La segnalazione, in tale ottica, è un atto di manifestazione di senso civico, attraverso cui il segnalante contribuisce all'emersione e alla prevenzione di rischi e situazioni pregiudizievoli per l'amministrazione di appartenenza e, di riflesso, per l'interesse pubblico collettivo.

Il decreto legge 24 giugno 2014, n. 90 (Misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza degli uffici giudiziari), convertito nella legge 11 agosto 2014, n. 114 ha modificato, con l'art. 31, il testo dell'art. 54-bis del d.lgs. n.165/2001 introducendo l'A.N.AC. quale soggetto destinatario delle segnalazioni, e (con l'art. 19, co. 5) ha stabilito che l'A.N.AC. è chiamata a gestire, oltre alle segnalazioni provenienti dai propri dipendenti per fatti illeciti avvenuti all'interno della propria struttura, anche le segnalazioni che i dipendenti di altre amministrazioni possono indirizzarle ai sensi del suddetto art. 54 bis del d. lgs. n.165/2001.

La novità legislativa impone, dunque, all'A.N.AC. di disciplinare le procedure attraverso le quali l'Autorità riceve e gestisce tali segnalazioni. Occorre sottolineare che l'art. 54-bis si riferisce esclusivamente ai dipendenti pubblici e presuppone l'identificazione del soggetto segnalante il cui nominativo deve essere, comunque, mantenuto riservato. L'Autorità può, in ogni caso ricevere segnalazioni anonime, su cui peraltro fonda una buona parte della propria attività di vigilanza, ma le modalità per la ricezione e la gestione di queste segnalazioni avranno trattamenti diversi rispetto a quelli specificamente previsti dall'art. 54-bis a tutela del dipendente pubblico.

Scopo del presente documento è descrivere i requisiti utente relativi alla realizzazione di un sistema informatico a supporto delle attività degli Uffici dell'Autorità per la ricezione e la gestione dello stato di avanzamento delle segnalazioni di condotte illecite effettuate da parte di dipendenti pubblici coerentemente alle *Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d. Whistleblowing)* emanate dall'Autorità con Determinazione n. 6 del 28 aprile 2015 (pubblicata nella Gazzetta Ufficiale serie generale n. 110 del 14 maggio 2015). Le specifiche dei requisiti contenute in questo documento riguardano anche la gestione delle segnalazioni generiche in tema di Anticorruzione.

Il sistema per la ricezione delle segnalazioni di condotte illecite (c.d. *whistleblowing*) è uno strumento di prevenzione della corruzione che si poggia sul concetto profondo che ciascun cittadino deve fare la sua parte per la salvaguardia del bene comune. Tale concetto tuttavia stenta a farsi largo nella nostra cultura mediterranea che ancora risente di un retaggio culturale che fa prevalere spesso un sentimento di timore della propria incolumità quando non addirittura di omertà e collusione. Pertanto è necessario rimuovere i fattori che possono ostacolare o disincentivare il ricorso all'istituto, quali i dubbi e le

incertezze circa la procedura da seguire e i timori di ritorsioni o discriminazioni. In tale prospettiva, l'obiettivo perseguito dalla presente procedura è quello di fornire al segnalante chiare indicazioni operative circa oggetto, contenuti, destinatari e modalità di trasmissione delle segnalazioni, nonché circa le forme di tutela che gli vengono offerte nel nostro ordinamento.

Da un punto di vista meramente operativo il sistema qui descritto riguarda gli strumenti informatici che si intende mettere a disposizione degliutilizzatori del sistema stesso e non attiene, invece, ai processi di natura istruttoria che possono derivare dall'esame delle segnalazioni raccolte ad eccezione del fatto che vengono mappati gli stati delle singole segnalazioni anche allo scopo di fornire elementi conoscitivi del fenomeno in esame attraverso elaborazioni statistiche sui dati.

### Stato dell'arte

Il sistema di ricezione di segnalazioni di condotte illecite provenienti da dipendenti pubblici, compresi quelli dell'Autorità, è attualmente gestito con strumenti che, seppur garantendo sul piano sostanziale la riservatezza del segnalante, appaiono tecnologicamente non ottimali allo scopo. In particolare le segnalazioni pervengono via Posta elettronica certificata a un sistema di protocollazione informatica il cui accesso è ristretto al Presidente dell'ANAC e alla sua Segreteria. Le istruttorie sono poi effettuate da un nucleo ristretto di funzionari i quali hanno potenzialmente libero accesso ai dati del segnalante.

### Ambito di intervento

L'ambito di intervento di tale progetto riguarda:

- la gestione delle segnalazioni di condotte illecite effettuate da dipendenti dell'Autorità (*whistleblowing* di 1° livello);
- la gestione delle segnalazioni di condotte illecite effettuate da dipendenti pubblici verso ANAC con conseguente tutela della riservatezza del segnalante (*whistleblowing* di 2° livello);

Il sistema dovrà, necessariamente, prevedere funzioni di reportistica che consentano di avere in tempo reale informazioni a livello aggregato quali ad esempio: il quadro delle segnalazioni pervenute suddivise secondo il loro stato di avanzamento, le amministrazione oggetto della segnalazione, il tipo di condotte illecita segnalata, il periodo in cui è avvenuta la condotta illecita (ad esempio mese e anno) e altre eventuali informazioni – da definire in sede di progetto - utili per la redazione di un quadro sintetico delle segnalazioni pervenute che possa rappresentare il fenomeno e consentire eventuali azioni correttive al management pubblico.

In una previsione di più ampio respiro, le funzionalità e i due sistemi descritti nel prosieguo del documento devono intendersi come istanziazione di un unico sistema che ricomprenda sia la possibilità di "costruire" schede per la raccolta di informazioni (*form builder*) sia funzionalità relative alla sicurezza e alla riservatezza dei dati raccolti applicando su di essi diversi livelli di cifratura e di visibilità in base alla loro stessa natura o in base alle finalità del trattamento che l'Autorità vorrà riservare agli stessi in ossequio alla normativa sulla privacy. Un sistema dotato della necessaria flessibilità potrebbe essere utilmente applicato ad ambiti di intervento sul tema degli obblighi di trasparenza.

## 3. Requisiti utente di gestione delle segnalazioni di condotte illecite provenienti dai dipendenti dell'ANAC (c.d. *whistleblowing* di 1° livello)

Il sistema dovrà permettere l'acquisizione delle segnalazioni di cui alla legge 190/2012 consentendo la prescritta tutela dell'identità del segnalante, i cui obiettivi fondamentali possono riassumersi in:

I. permettere ai dipendenti dell'Autorità di segnalare eventuali irregolarità, frodi e attività contrarie alle normative in materia di corruzione;

II. proteggere l'identità del segnalante;

III. permettere ad un ristretto gruppo di persone (struttura ricevente) di ricevere e analizzare le segnalazioni.

### 3.1. Descrizione delle funzionalità del sistema e dei processi

Le funzionalità del sistema possono essere descritte, ad alto livello, secondo gli schemi illustrati nelle Figure 1, 2 e 3 e tenendo conto che:

- per "struttura ricevente" si intende un ristretto gruppo di persone delegato alla ricezione e allo svolgimento dell'istruttoria relativa alle segnalazioni ricevute. Tale struttura è formalmente individuata con un atto organizzativo interno.
- per "terzo che autorizza" si intende una figura, diversa dai componenti della struttura ricevente, a cui è attribuita la funzione di autorizzare l'accoppiamento della singola segnalazione con l'identità del segnalante senza necessariamente venirne egli stesso a conoscenza, previa valutazione dell'effettiva necessità di tale operazione. Tale figura è utilmente identificata nel Presidente o nel Segretario Generale e svolge un ruolo che, in altri termini, può essere definito quale "custode delle identità".

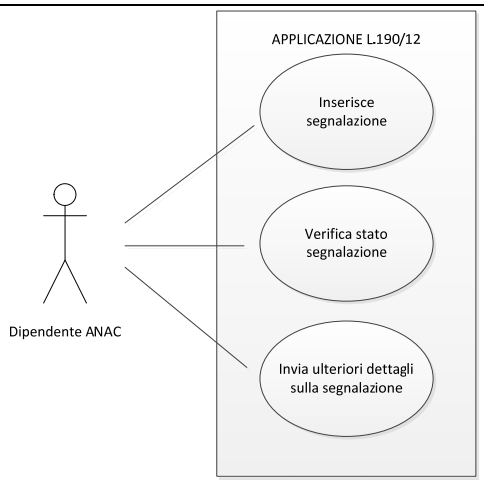



Figura 1
Funzionalità disponibili per il dipendente ANAC

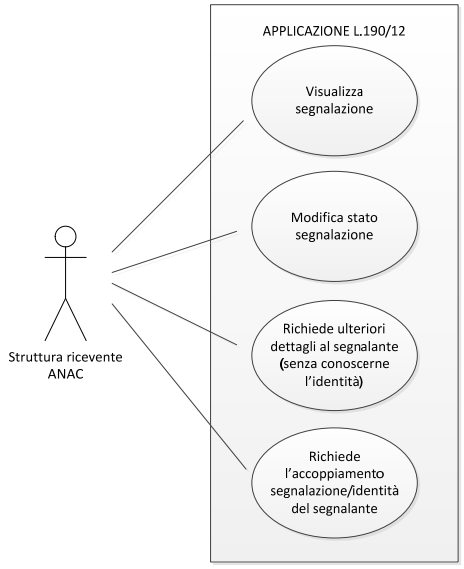



Figura 2:
Funzionalità disponibili per gli utenti appartenenti alla struttura ricevente

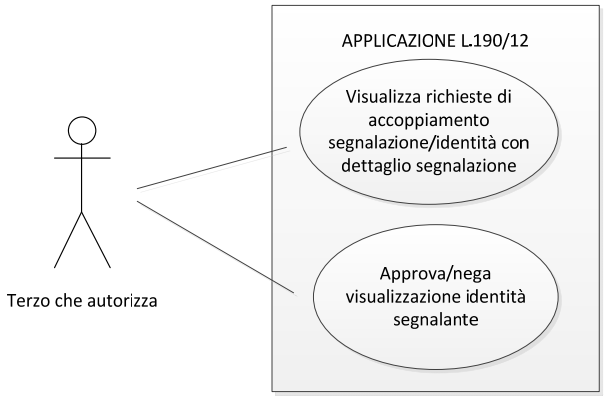



Figura 3:
Funzionalità disponibili per l'utente che autorizza l'accoppiamento segnalazione/identità del segnalante

### 3.1.1. Descrizione funzionalità DIPENDENTE ANAC

Ad un maggior livello di dettaglio le funzionalità messe a disposizione del dipendente dell'Autorità che intende sottoporre una segnalazione ai sensi della Legge 190/12, dovranno ricomprendere:

- la possibilità di visitare la pagina dell'applicazione e prendere visione del manuale d'uso, delle avvertenze riguardanti la tutela accordata, delle modalità in cui il sistema gestisce la sicurezza e la riservatezza e di ogni altra informazione che si riterrà opportuno pubblicare;
- la necessità di autenticarsi al sistema qualora voglia inserire una segnalazione;
- la possibilità di inserire una segnalazione avendo evidenza dei campi obbligatori e di quelli opzionali secondo quanto appresso specificato;
- la possibilità di allegare documenti in formato elettronico (file);
- la possibilità di ricercare una propria segnalazione unicamente attraverso il codice univoco che gli viene restituito al termine del corretto inserimento della segnalazione e avere evidenza dello stato di lavorazione della segnalazione stessa o di eventuali richieste di ulteriori informazioni da parte della struttura ricevente;
- la possibilità, su propria iniziativa o su richiesta della struttura ricevente, di fornire ulteriori informazioni in forma testuale e/o di allegare nuovi documenti in formato elettronico.

La seguente tabella riporta le informazioni che saranno rese disponibili al segnalante per la compilazione e il successivo inoltro della segnalazione. Tale elenco deve intendersi a mero scopo esemplificativo e non esaustivo, in quanto potrà essere mofìdificato in sede di analisi di dettaglio dei processi.

| Informazione | Obbligatorietà | Tipo/descrizione |
|---|---|---|
| Data o periodo del fatto | Si | data (gg.mm.aaaa) o periodo espresso in mese/anno |
| Luogo in cui si è verificato il fatto | SI | ufficio (selezionabile da una lista precaricata) o altro luogo da specificare (indicazione con testo libero) |
| Valutazione della rilevanza del fatto | NO | Scelta multipla tra:<br>□ penalmente rilevante<br>□ violazione di codici di comportamento o altre disposizioni sanzionabili in via disciplinare<br>□ pregiudizio patrimoniale all'Amministrazione o ad altro ente pubblico<br>□ pregiudizio all'immagine dell'Amministrazione<br>□ altro (specificare) |
| Descrizione sintetica del fatto | SI | testo libero (max 3.000 caratteri) |
| Autore/i del fatto | SI | testo libero |
| Altri soggetti a conoscenza del fatto e/o in grado di riferire sullo stesso | NO | testo libero |
| Documenti utili (allegati) | NO | possibilità di fare l'upload di uno o più file purché di dimensione non superiore alla dimensione massima accettata (parametrizzabile) |
| Ulteriori informazioni | NO | testo libero (solo per segnalazioni già inserite) |

### 3.1.2. Descrizione funzionalità STRUTTURA RICEVENTE

Ai componenti designati per la struttura ricevente dovrà essere consentito di:

- ricevere una mail sul proprio indirizzo di posta elettronica istituzionale all'atto dell'inserimento di una nuova segnalazione e all'atto dell'inserimento di ulteriori documenti o informazioni su una segnalazione già inserita (nella mail non devono essere contenute informazioni caratterizzanti la segnalazione come meglio specificato nel paragrafo relativo ai requisiti funzionali);
- accedere al sistema ed estrarre una lista di segnalazioni filtrate secondo lo "stato di lavorazione";
- visualizzare le informazioni della singola segnalazione incluso un ID assegnato dal sistema e data ed ora dell'inserimento della segnalazione stessa;
- modificare la stato di lavorazione della segnalazione secondo i seguenti valori:
  - Nuova (assegnato dal sistema)
  - Presa in carico
  - Istruttoria in corso

- Segnalazione all'Autorità competente
- Archiviazione

- inserire "note di lavorazione" non visibili al segnalante;
- inserire delle note, opzionali e non visibili al segnalante, contestualmente alla modifica dello stato di lavorazione;
- richiedere l'identità del segnalante con motivazione tipizzata secondo, ad esempio, la seguente casistica:

  - Verifica attendibilità della segnalazione
  - Acquisizione ulteriori elementi istruttori che può fornire solo il segnalante
  - Eventuale successivo contraddittorio
  - Verificare in quale veste il soggetto ha inoltrato la segnalazione
  - Altro (specificare)

***NB: la richiesta d'identità, in caso di diniego, potrà essere reiterata***

- inserire delle note, opzionali e non visibili al segnalante, contestualmente alla richiesta d'identità del segnalante (si precisa che la richiesta di accoppiamento segnalazione-identità del segnalante non deve mai essere visibile al segnalante);
- inserire note e/o richieste visibili al segnalante.

Tutti gli inserimenti e i cambi di stato devono essere etichettati in maniera esplicita con *timestamp* e autore (es: "*18/05/2015 12:41 – n.cognome*") a eccezione, naturalmente, degli inserimenti effettuati dal segnalante.

### 3.1.3. Descrizione funzionalità TERZO CHE AUTORIZZA

Per terzo che autorizza si intende definire un ruolo, diverso da quello assegnato ai membri della struttura ricevente, a cui si vuole affidare un compito di garanzia rispetto alla tutela dell'identità del segnalante: il suo compito sarà quello di valutare i motivi, addotti in fase di istruttoria, per i quali la struttura ricevente ritiene necessario venire a conoscenza dell'identità del segnalante per una specifica segnalazione.

Deve poter, quindi, accedere e visualizzare tutti i dati della segnalazione inclusi i documenti e i messaggi inseriti sia dal segnalante in fasi successive all'inserimento della segnalazione sia dalla struttura ricevente, incluse eventuali motivazioni di diniego da egli stesso inserite in occasione di precedenti richieste di identità relative alla medesima segnalazione.

Dovrà, dunque, sulla base degli elementi su esposti, fornire il proprio assenso o il proprio diniego motivato.

In nessun caso il terzo che autorizza dovrà conoscere l'identità del segnalante.

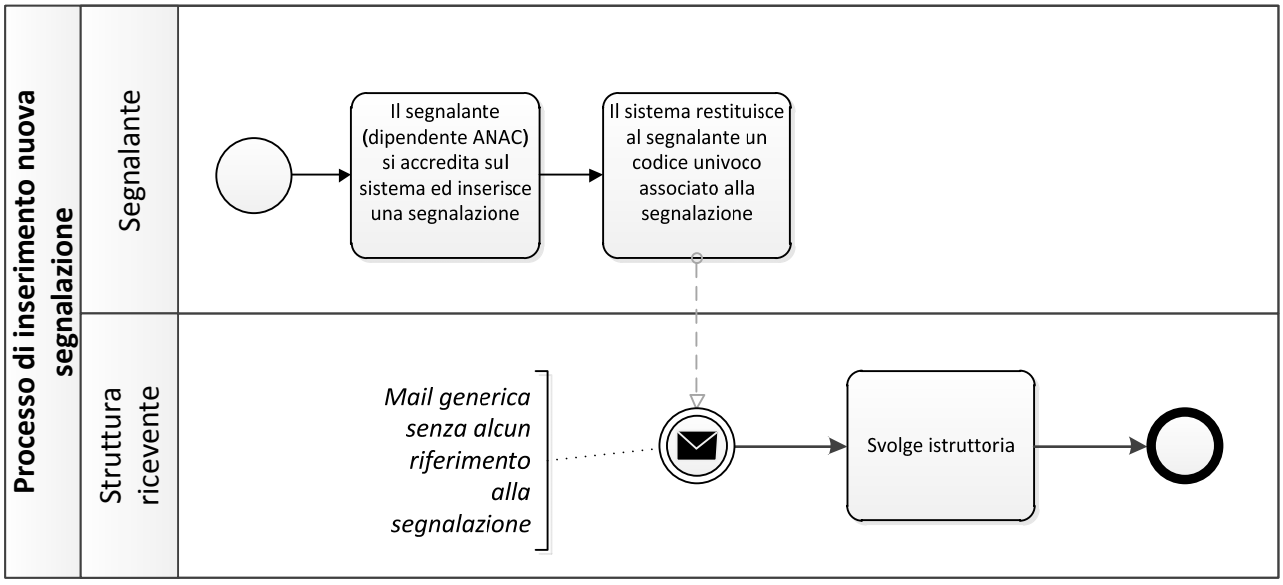
### 3.1.4. Rappresentazione dei processi

Nel presente paragrafo vengono rappresentati i principali processi che coinvolgono gli attori di cui sono state precedentemente descritte le funzionalità (segnalante, struttura ricevente e terzo che autorizza).

**A.** Inserimento nuova segnalazione

Descrive il processo attraverso il quale il dipendente ANAC (segnalante) potrà accedere al sistema e inserire una nuova segnalazione di condotta illecita. Tale inserimento scatenerà un messaggio mail verso i componenti della struttura ricevente.

Si ribadisce che ai fini del rispetto del requisito normativo di tutela dell'identità del segnalante il messaggio mail non dovrà contenere elementi utili, anche in via del tutto teorica, alla conoscenza dell'identità stessa. Tale avvertenza è applicabile a tutti i messaggi mail generati dal sistema. A titolo esemplificativo il corpo della mail potrebbe contenere esclusivamente il seguente testo: "Il sistema di whistleblowing richiede la sua attenzione".



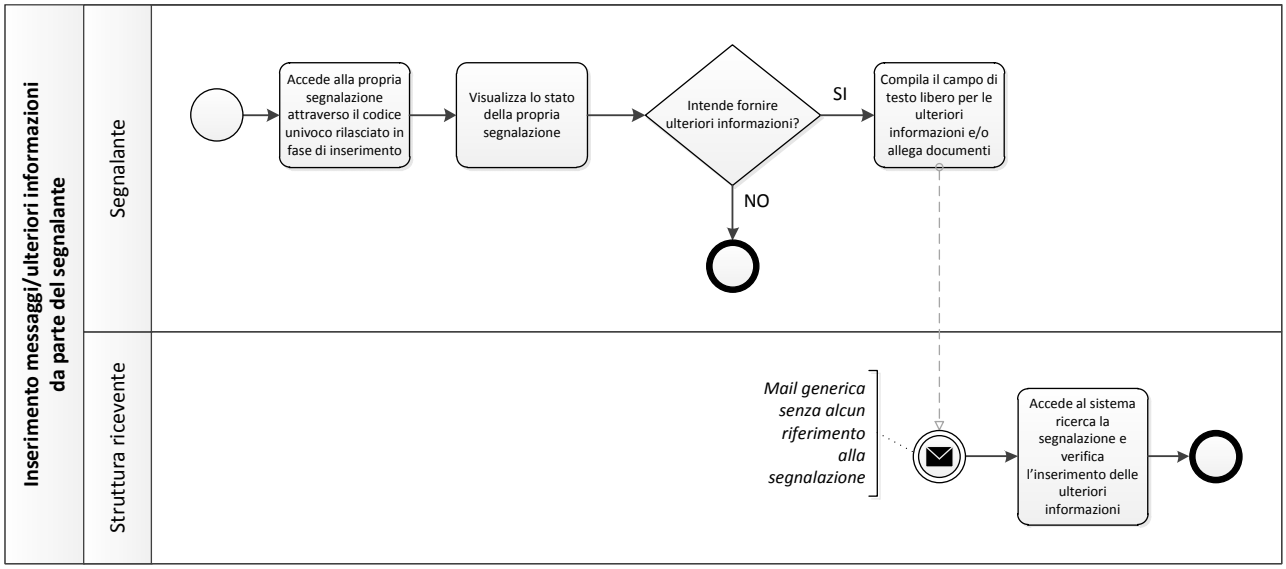
**B.** Inserimento messaggi/ulteriori informazioni da parte del segnalante

Descrive il processo attraverso il quale il segnalante potrà, su propria iniziativa, visualizzare i dati di una segnalazione e, se lo ritiene necessario, inserire nuove informazioni e/o documenti nonché inviare messaggi alla struttura ricevente.

Il segnalante non potrà in ogni caso modificare quanto già inserito, avrà conoscenza dello stato di lavorazione della sua segnalazione e potrà, al contrario, compilare un ulteriore campo di testo o allegare documentazione aggiuntiva.

Il processo potrebbe ripetersi un numero imprecisato di volte, ovvero il segnalante potrà inserire le informazioni una o più volte ed in tempi anche successivi.

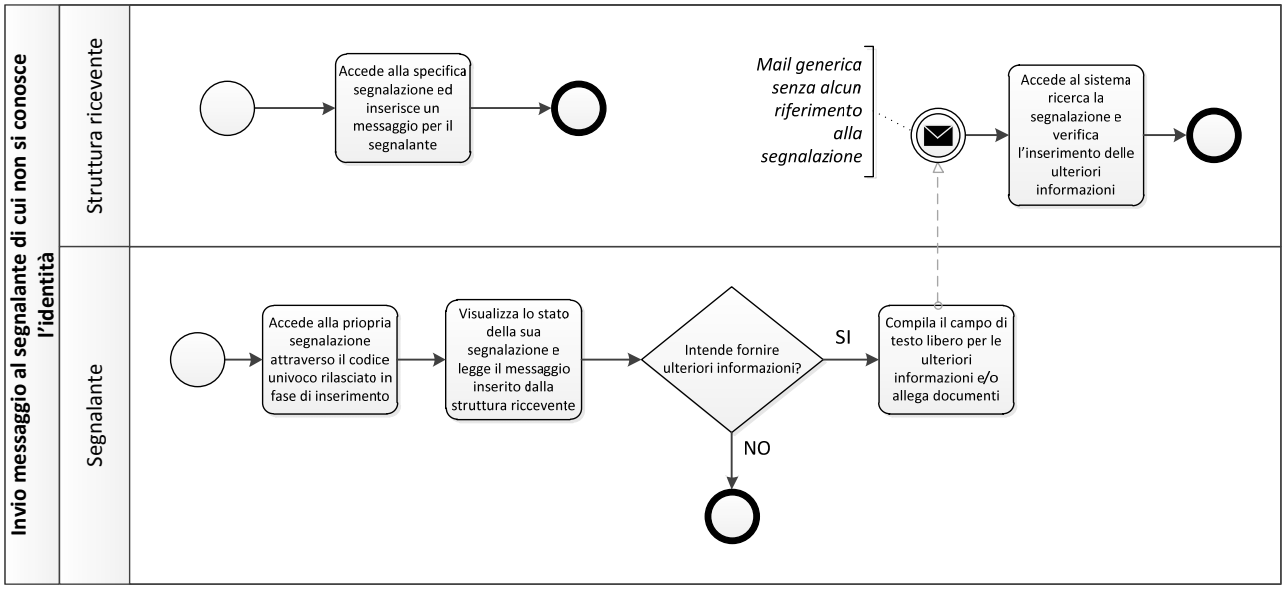
Il segnalante potrà accedere alle proprie segnalazioni, unicamente alle proprie, solo attraverso il codice univoco rilasciato dal sistema all'atto di primo corretto inserimento della segnalazione.



**C.** Invio messaggio al segnalante di cui non si conosce l'identità

Viene qui descritto il processo attraverso il quale la struttura segnalante può associare un messaggio ad una specifica segnalazione. Tale messaggio sarà visibile al segnalante, autore della segnalazione, nel caso in cui, di propria iniziativa, acceda al sistema e visualizzi la propria segnalazione che avrà a corredo il messaggio (di qualsiasi natura) inserito precedentemente da uno dei componenti della struttura ricevente.

Il segnalante, una volta venuto a conoscenza del messaggio, non ha alcun obbligo di rispondere. Nel caso in cui intenda rispondere fornendo, eventualmente, le informazioni richieste seguirà le fasi già descritte nel processo B che per completezza si riporta nella figura sottostante (corsia "Segnalante").



**D.** Richiesta identità del segnalante per una specifica segnalazione

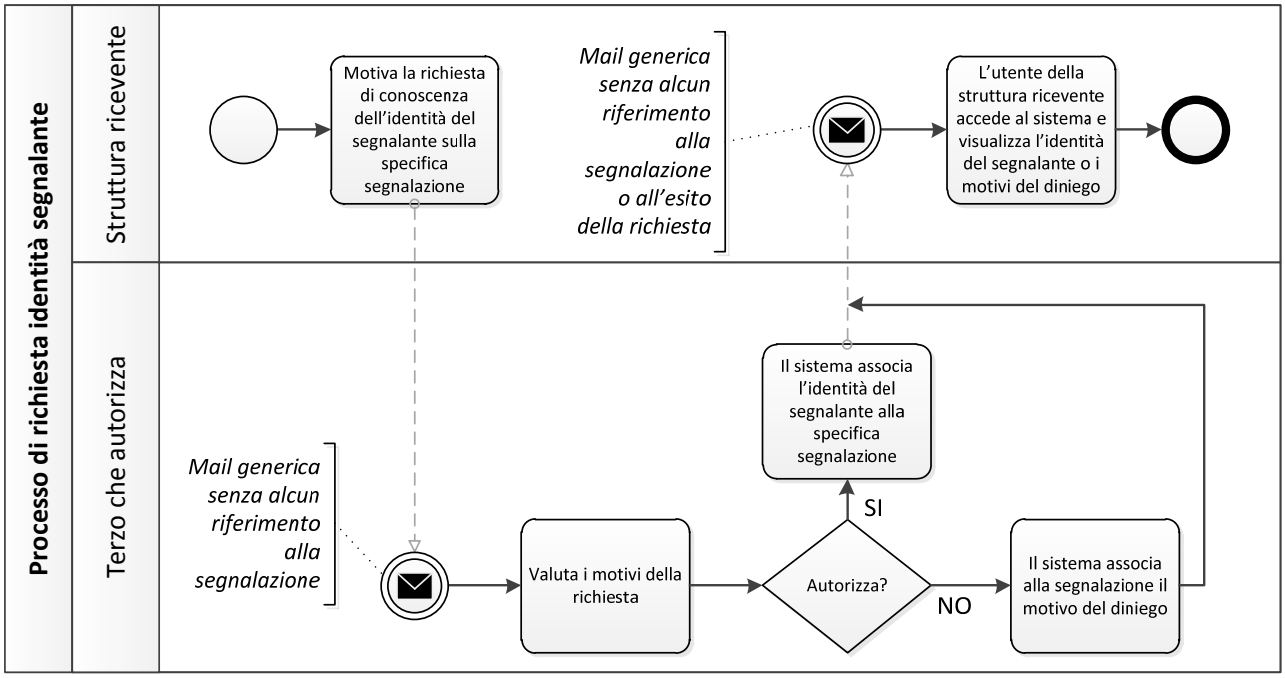
La figura che segue descrive il processo attraverso il quale uno dei componenti della struttura ricevente richiede al terzo che autorizza che alla specifica segnalazione venga associata e resa nota, ai soli componenti della struttura ricevente, l'identità del segnalante.

La richiesta deve essere obbligatoriamente motivata secondo specifiche motivazioni alle quali possono essere aggiunti ulteriori dettagli (testo libero).

Il terzo che autorizza può negare, motivando, l'autorizzazione. In ogni caso viene inviata ai componenti della struttura ricevente una mail con le caratteristiche di riservatezza più volte menzionate e comunque senza l'indicazione dell'esito della richiesta di identità.

Il terzo che autorizza non dovrà, comunque, conoscere l'identità del segnalante.

La richiesta, a seguito di diniego, può essere reiterata.



## 3.2. Requisiti utente

Si riporta di seguito la convenzione per l'identificazione dei requisiti.

Ciascun requisito è individuato da un identificativo univoco nella forma [RF_M.nn] o [RNF_M.nn], dove:

- **RF** Requisito Funzionale;
- **RNF** Requisito Non Funzionale;
- **M** identifica l'**ambito;**
- **nn** è un progressivo numerico.

**Ambito="WBANAC" segnalazioni di illecito inoltrate da dipendenti dell'Autorità Nazionale Anticorruzione**

### 3.2.1. Requisiti utente di tipo funzionale (RF_WBANAC.XX)

RF_WBANAC.01 Generalità

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | L'applicazione deve intendersi come specifica istanziazione di un sistema che consenta la predisposizione e la pubblicazione di schede di "raccolta informazioni" (*form builder*) e la gestione della sicurezza delle informazioni e della comunicazione |

RF_WBANAC.02 Disclaimer

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il sistema dovrà rendere evidente all'utente segnalante che la propria identità potrà essere estratta in caso di stretta necessità da parte degli utenti componenti della "Struttura Ricevente" (*disclaimer*) |

RF_WBANAC.03 Ambito distribuzione

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Le segnalazioni potranno essere inserite da tutti i dipendenti dell'Autorità senza alcuna limitazione e saranno inoltrate ad una "Struttura Ricevente" |

RF_WBANAC.04 Modalità di accesso

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il link all'applicazione dovrà essere reso disponibile unicamente sulla intranet e accessibile previa autenticazione. Le utenze dovranno essere quelle di dominio. |

RF_WBANAC.05 Protezione identità segnalante

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Le segnalazioni non verranno acquisite in forma anonima ma il nome del segnalante verrà nascosto fino a esplicita richiesta dei componenti della "Struttura Ricevente" vagliata dal "Terzo che autorizza". |

RF_WBANAC.06 Codice univoco segnalazione

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il sistema al momento dell'inserimento di una segnalazione assegna alla stessa un codice univoco generato in modo casuale che viene rilasciato al segnalante ed è composto da 16 caratteri alfanumerici ed esposto nella forma<br><br>xxxx-xxxx-xxxx-xxxx (sedici caratteri in gruppi da quattro) |

RF_WBANAC.07 Segnalante: inserimento segnalazione

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il segnalante potrà inserire una segnalazione contenente i dati esposti nel paragrafo 3.1.1. I dati obbligatori dovranno essere chiaramente individuabili. |

RF_WBANAC.08 Struttura ricevente: ricezione mail

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | La struttura ricevente dovrà ricevere , all'atto dell'inserimento di una nuova segnalazione o di ulteriori informazioni/documenti, una mail sul proprio account di posta elettronica istituzionale. |

RF_WBANAC.09 Riservatezza degli avvisi

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Tutte le mail di avviso alla "Struttura ricevente" e al "Terzo che autorizza" non dovranno contenere dati della segnalazione né alcun altro elemento identificativo della segnalazione stessa. |

RF_WBANAC.10 Struttura ricevente: Visualizzazione elenco segnalazioni

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | La Struttura ricevente potrà visualizzare l'elenco delle segnalazioni, filtrate in base allo "stato di lavorazione", con indicazione per ciascuna di identificativo univoco, data ed ora inserimento. |

RF_WBANAC.11 Struttura ricevente: richiesta identità segnalante

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | La Struttura ricevente potrà richiedere l'autorizzazione a conoscere l'identità del segnalante. La richiesta può essere reiterata e ciascuna richiesta/esito deve essere tracciata dal sistema. |

RF_WBANAC.12 Accoppiamento segnalazione/identità del segnalante

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Solo i componenti della "Struttura ricevente" devono poter conoscere l'identità del segnalante, evidenziandone la motivazione e previa esplicita autorizzazione puntuale sulla singola segnalazione da parte del "Terzo che autorizza" |

RF_WBANAC.13 Terzo che autorizza: ricezione mail

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il "Terzo che autorizza" dovrà ricevere all'atto dell'inserimento di una richiesta di autorizzazione a conoscere l'identità del segnalante, una mail sul proprio account di posta elettronica istituzionale. |

RF_WBANAC.14 Terzo che autorizza: identità del segnalante

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il "Terzo che autorizza" non dovrà conoscere l'identità del segnalante |

RF_WBANAC.15 Terzo che autorizza: visualizzazione segnalazione

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il "Terzo che autorizza" potrà visualizzare l'elenco delle segnalazioni per le quali è stata richiesta da parte della struttura ricevente l'autorizzazione a conoscere l'identità del segnalante con indicazione della motivazione e, cliccando su una di esse, accedere a tutte le informazioni relative. |

RF_WBANAC.16 Terzo che autorizza: concessione/diniego autorizzazione

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il "Terzo che autorizza" potrà consentire o negare, motivando, l'associazione tra la segnalazione e l'identità del segnalante. |

RF_WBANAC.17 Segnalante: ricerca propria segnalazione

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il segnalante potrà ricercare la sua segnalazione solo attraverso il codice univoco rilasciato all'atto dell'inserimento della segnalazione, potrà verificarne lo stato di lavorazione, le eventuali richieste di integrazione da parte della "Struttura ricevente" ma non potrà, in alcun caso, modificare le informazioni già trasmesse |

RF_WBANAC.18 Segnalante: criteri di ricerca delle segnalazioni

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il segnalante potrà ricercare solo le segnalazioni corrispondenti ai codici univoci a lui stesso rilasciati. Dovranno essere possibili solo ricerche puntuali. |

RF_WBANAC.19 Struttura ricevente: invio richieste/messaggi al segnalante anonimo

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | La "Struttura ricevente" potrà inviare messaggi al segnalante pur senza conoscerne l'identità. La comunicazione sarà comunque asincrona e il segnalante ne avrà notizia solo su propria iniziativa verificando lo stato della sua segnalazione. |

RF_WBANAC.20 Struttura ricevente: ricerca e visualizzazione delle segnalazioni

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | I componenti della "Struttura ricevente" potranno ricercare le segnalazioni e visualizzarne tutte le informazioni, oltreché inserendo puntualmente il codice identificativo univoco, per stato lavorazione e/o per periodo (intervallo date), per luogo in cui si è svolto il fatto e in generale imponendo filtri su tutte le informazioni di tipo strutturato idonee ad evidenziare dati aggregati per criteri di interesse. |

RF_WBANAC.21 Struttura ricevente: lavorazione segnalazioni (1)

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | I componenti della "Struttura ricevente" potranno variare lo stato di lavorazione della singola segnalazione, inserire richieste/messaggi al segnalante, inserire "note", inserire richiesta motivata di conoscenza dell'identità del segnalante. |

RF_WBANAC.22 Struttura ricevente: lavorazione segnalazioni (2)

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | I componenti della "Struttura ricevente" dovranno ricevere una mail di notifica a ogni nuova segnalazione e a ogni ulteriore messaggio inviato dal segnalante in relazione ad una specifica segnalazione. |

RF_WBANAC.23 Terzo che autorizza: valutazione opportunità dis-anonimizzazione della segnalazione

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il "Terzo che autorizza" potrà consentire o rifiutare ai componenti della "Struttura Ricevente" l'autorizzazione a conoscere l'identità del segnalante. |

RF_WBANAC.24 Segnalante: invio documenti e integrazione dati

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il segnalante potrà allegare documenti, anche in momenti successivi all'inserimento della segnalazione, e integrare, su apposito campo, le informazioni inserite precedentemente. |

RF_WBANAC.25 Reportistica

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | L'applicazione dovrà essere corredata di un sistema di reportistica in grado di fornire indicazioni di tipo statistico quali ad esempio, per un dato periodo, il numero delle segnalazioni (totali e per singolo stato - riferibili all'intera organizzazione o a una sua particolare articolazione), il tempo medio per la presa in carico di una segnalazione. Per tali dati dovranno essere previste funzioni di esportazione in formato aperto. |

RF_WBANAC.26 Stampe

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Non dovranno essere previste funzioni relative alla stampa delle informazioni gestite dall'applicazione. |

### 3.2.2. Requisiti utente di tipo non funzionale (RNF_WBANAC.XX)

Descrivono gli aspetti del sistema che non sono direttamente legati al comportamento (funzionalità) del sistema stesso.

RNF_WBANAC.01 Bonifica meta-dati dei documenti allegati

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | I documenti allegati dovranno essere bonificati da eventuali metadati presenti (autore, autore ultima modifica, data creazione, data ultima modifica, etc) nonché resi affidabili dal punto di vista della sicurezza informatica |

RNF_WBANAC.02 Sicurezza

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | In considerazione della natura delle informazioni trattate e dell'elevato grado di riservatezza che deve essere garantito, l'intera applicazione dovrà essere sottoposta ad attività di *Vulnerability Assessment & Penetration Test* con certificazione dei risultati in termini di metodologie adottate, valutazione dei rischi in base al contesto, test condotti, vulnerabilità rilevate ed azioni correttive intraprese e/o da intraprendere. |

RNF_WBANAC.03 Sicurezza delle comunicazioni (1)

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Tutti i dati inviati dall'applicazione ai PC degli utenti devono essere cifrati |

RNF_WBANAC.04 Sicurezza delle comunicazioni (2)

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Tutti i colloqui fra i server coinvolti devono essere cifrati |

RNF_WBANAC.05 Log delle attività e log applicativo

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Tutte le attività eseguite da qualunque utente (anche dagli "amministratori di sistema") devono essere tracciate. |

RNF_WBANAC.06 Sicurezza delle informazioni

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Tutte le informazioni, sia quelle proprie dell'applicazione sia quelle relative alla tracciabilità, dovranno essere memorizzate in modo cifrato |

RNF_WBANAC.07 Performance

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il sistema dovrà garantire idonei standard prestazionali, relativi ai tempi di esecuzione ed utilizzo delle risorse, per non produrre inefficienze nel contesto di esecuzione durante la sua normale attività. |

RNF_WBANAC.08 Scalabilità

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | L'architettura del sistema dovrà essere realizzata in modo tale da poter essere adattata ad esigenze future dovute all'aumento dei dati o delle richieste da elaborare. |

RNF_WBANAC.09 Affidabilità

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il sistema dovrà essere in grado di funzionare correttamente per lunghe sessioni di lavoro e dovrà garantire la consistenza dei dati elaborati nel caso di situazioni impreviste (*fault tollerance*). |

RNF_WBANAC.10 Manutenibilità

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il sistema dovrà essere dotato di un form builder al fine di poter consentire un agevole aggiornamento, anche da parte di personale non specificatamente tecnico, delle informazioni che si intendono raccogliere. |

RNF_WBANAC.11 Accessibilità

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il sistema dovrà essere realizzato nel rispetto dei requisiti di accessibilità previsti per i siti della PA |

RNF_WBANAC.12 Compatibilità WEB

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il sistema dovrà essere realizzato per essere fruito in ambiente web, seppur limitato alla rete interna dell'Autorità, ed essere indipendente dalla tipologia di browser utilizzato dall'utente. |

RNF_WBANAC.13 Riuso

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il sistema dovrà essere progettato in ottica di riuso secondo quanto previsto dalla Determinazione A.N.AC. n. 6 del 28 aprile 2015 e dalle "Linee guida per l'inserimento ed il riuso di programmi informatici o parti di essi pubblicati nella Banca dati dei programmi informatici riutilizzabili" con particolare riguardo all'utilizzo di componenti applicativi e tecnologici distribuiti con licenze *open source* e alla minimizzazione degli impatti architetturali. |

## 4. Requisiti utente Gestione delle segnalazioni di condotte illecite provenienti da dipendenti della pubblica amministrazione (c.d. *Whistleblowing* di 2° livello)

Il sistema dovrà consentire l'acquisizione delle segnalazioni di condotte illecite provenienti da dipendenti della pubblica amministrazione che intendano inoltrare tali segnalazioni direttamente all'ANAC.

Il sistema dovrà consentire il disaccoppiamento segnalazione identità del segnalante attraverso la preventiva registrazione del pubblico dipendente (che oltre a dichiarare i propri dati anagrafici e relativi al proprio rapporto di lavoro con la specifica PA dovrà fornire copia in formato elettronico di un proprio documento d'identità) al quale verranno forniti delle credenziali anonime (codice univoco utente e password).

Dovranno, inoltre, essere conciliate due diverse necessità: da un lato la tutela accordata dalla norma al pubblico dipendente che segnala una condotta illecita dichiarando la propria identità (segnalazioni *whistleblowing* in senso stretto) dall'altro lato le segnalazioni che, almeno in una fase iniziale, vengono inoltrate in forma anonima così come previsto nell'allegato 1b delle linee guida di cui alla determinazione ANAC n. 6 del 28.4.15

In corso d'istruttoria il team di gestione delle segnalazioni, di seguito denominato "Struttura ricevente PA", potrà valutare la necessità di ricondurre le segnalazioni anonime a segnalazioni whistleblowing chiedendo al segnalante anonimo di acquisire le menzionate "credenziali anonime" e di riconciliare la propria segnalazione anonima, di cui solo lui conosce il codice univoco rilasciato all'atto dell'inserimento della segnalazione stessa, alle proprie credenziali anonime.

Tutte le informazioni inserite tramite il sistema devono essere resistenti all'utilizzo di robot in grado di simulare l'interazione umana (c.d. bot); deve essere quindi previsto l'utilizzo di test, quali ad esempio i *captcha,* in grado di assicurare che la compilazione delle informazioni sia fatta da un umano.

Il sistema dovrà inoltre interfacciarsi, attraverso specifici servizi (*web-services:* sistemi software progettati per supportare l'interoperabilità tra diversi ambiti applicativi), con il protocollo informatica e-prot in uso presso l'Autorità Nazionale Anticorruzione. L'interazione tra i due sistemi dovrà ricomprendere l'assegnazione ad ogni singola segnalazione, anche anonima, di una segnatura di protocollo e la sua fascicolazione garantendo, sempre, la riservatezza sia del segnalante sia del contenuto della segnalazione (protocollo riservato).

### 4.1. Descrizione delle funzionalità del sistema e dei processi

Le funzionalità del sistema possono essere descritte, ad alto livello secondo gli schemi illustrati nelle figure che seguono e tenendo conto che:

- per "Dipendente PA" si intende il dipendente pubblico che intende inoltrare segnalazioni dichiarando la propria identità essendo in possesso di "credenziali anonime" in quanto precedentemente registrato, a esso vengono accordate le tutele previste dal dettato normativo.
- per "Segnalante PA" si intende il dipendente pubblico che inoltra una segnalazione anonima non dichiarando la propria identità.
- per "Struttura Ricevente PA" si intende l'unità organizzativa ANAC deputata alla ricezione delle segnalazioni ex Legge 190/2012. A tale profilo potranno essere comunque ricondotte tutte le figure che si vorrà far partecipare al processo di gestione delle segnalazioni secondo le peculiarità di una struttura deputata alla ricezione e alla istruzione di tali pratiche.
- per "Terzo che Autorizza PA" si intende una figura, da individuare e rendere nota a chi segnala quale garante delle tutele, a cui sarà attribuita la funzione di autorizzazione all'accoppiamento tra segnalazione e identità del "Dipendente PA".

Si precisa che il "Dipendente PA" può, in ogni momento, decidere di inoltrare segnalazioni anonime piuttosto che usare le proprie "credenziali anonime".

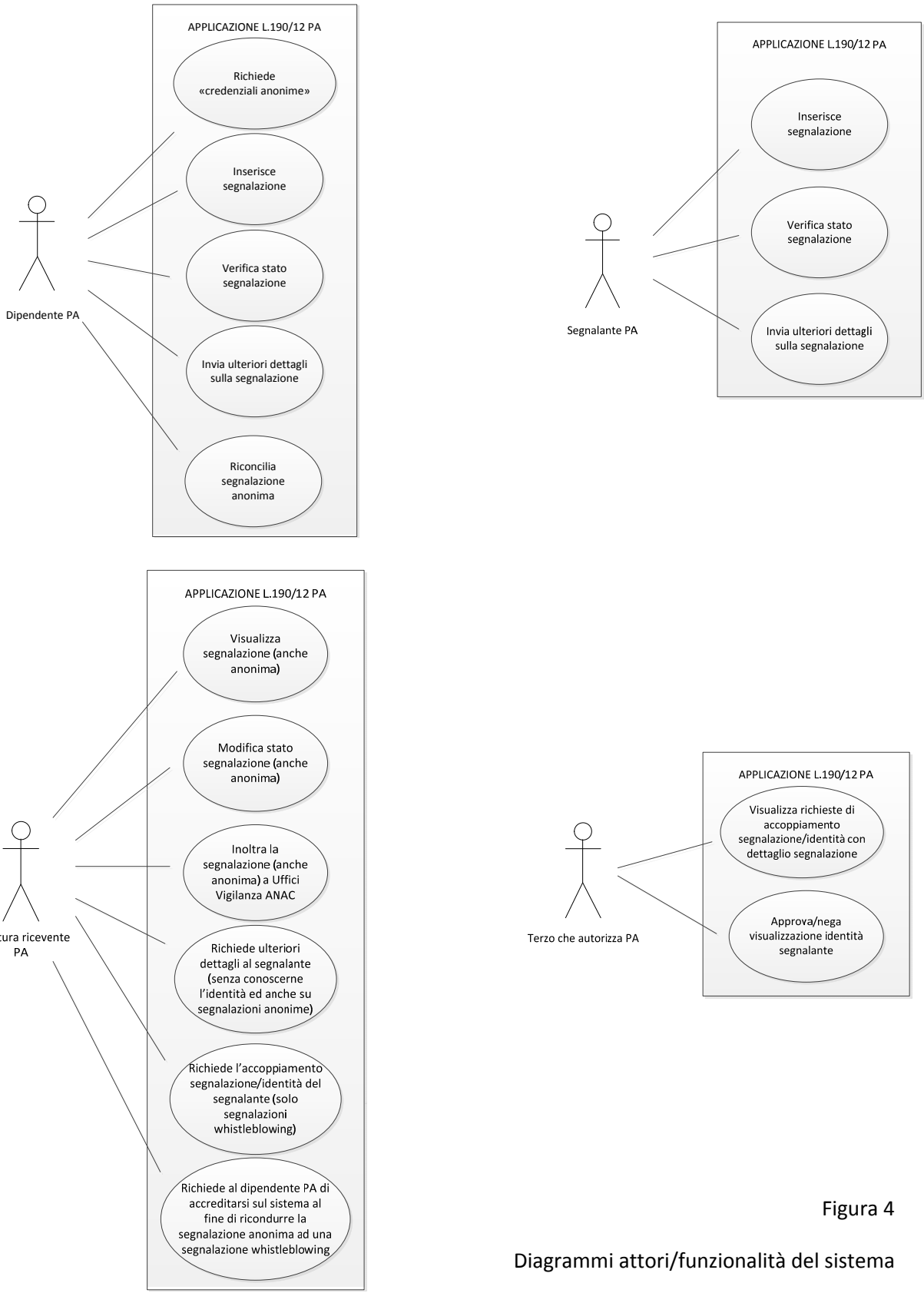



Figura 4

Diagrammi attori/funzionalità del sistema

### 4.1.1. Descrizione delle funzionalità del Dipendente PA

Il "Dipendente PA" è il dipendente pubblico che intende effettuare una segnalazione di illecito in forma non anonima e che, quindi richiede le "credenziali anonime" per l'accesso all'applicazione .

Il "dipendente PA" deve considerarsi un utente autenticato anche se le credenziali in suo possesso non consentono l'immediata identificazione della persona fisica: in questo senso vengono definite, in questo contesto, come "credenziali anonime" costituite da una coppia utente/password.

I servizi a sua disposizione devono permettergli:

- di collegarsi al sistema e avere cognizione circa:
  - le tipologie di segnalazione che possono essere inoltrate,
  - le tutele accordate e le modalità con cui viene gestita la sicurezza e la riservatezza delle informazioni,
  - l'iter delle diverse tipologie di segnalazione,
  - ogni altra informazione che si riterrà opportuno rendere nota;
- di inserire i propri dati anagrafici, i dettagli della propria posizione lavorativa e copia del documento di riconoscimento ed ottenere le "credenziali anonime" per accreditarsi al sistema ed inserire una segnalazione di illecito ai sensi della Legge 190/12;

> *A tal proposito si evidenzia che il sistema nulla garantisce rispetto all'identità del segnalante e alla sua qualificazione di "dipendente di una pubblica amministrazione".*

- di collegarsi al sistema con le proprie "credenziali anonime";
- di inserire le informazioni richieste ed inoltrare una segnalazione;
- di allegare documenti in formato elettronico;
- di ricercare una segnalazione precedentemente inoltrata unicamente attraverso il codice univoco che gli viene restituito all'atto dell'inserimento;
- di verificare lo stato della segnalazione, leggere le comunicazioni eventualmente inserite dalla "Struttura ricevente PA", inserire, in risposta o su propria iniziativa, ulteriori messaggi o informazioni (senza aver la possibilità di modificare quanto già inserito in sessioni precedenti);
- di associare alle proprie credenziali una segnalazione anonima precedentemente comunicata come "segnalante PA". In questo caso dovrà essere tracciato il passaggio da segnalazione anonima a segnalazione whistleblowing ex legge 190/.

La tabella che segue riporta le informazioni che dovranno essere inserite per le segnalazioni. Tale elenco deve intendersi a mero scopo esemplificativo e non esaustivo, in quanto potrà essere modificato in sede di analisi di dettaglio dei processi.

| Informazione | Obbligatorietà | Tipo/descrizione |
|---|---|---|
| Data o periodo del fatto | SI | data (gg.mm.aaaa) o periodo espresso in mese/anno |
| Luogo in cui si è verificato il fatto | SI | ufficio (selezionabile da una lista precaricata) o altro luogo da specificare (indicazione con testo libero) |
| Amministrazione coinvolta | SI | testo libero o elenco esaustivo |
| Unità organizzativa dell'Amministrazione coinvolta | SI | testo libero |
| Grado di coinvolgimento del segnalante nel fatto | SI | tbd (proporre eventuale tipizzazione) |
| Tipo di illecito che si vuole segnalare | SI | Scelta multipla tra:<br>- Appalti<br>- Nomine o incarichi<br>- Concorsi<br>- Gestione risorse pubbliche<br>- Altri fatti di cattiva amministrazione<br>- Reati specifici (corruzione, concussione, etc.) |
| "Appreso in adempimento di funzioni d'ufficio" | SI | si/no |
| Nominativo (cognome-nome) del Responsabile della Prevenzione della Corruzione (RPC) | SI | testo libero |
| Esistenza di un processo interno all'amministrazione per le segnalazioni di illeciti | SI | si/no, se si indicare se automatizzato |
| Valutazione della rilevanza del fatto | NO | Scelta multipla tra:<br>- penalmente rilevante<br>- violazione di codici di comportamento o altre disposizioni sanzionabili in via disciplinare<br>- pregiudizio patrimoniale all'Amministrazione o ad altro ente pubblico<br>- pregiudizio all'immagine dell'Amministrazione<br>- altro (specificare) |
| Descrizione sintetica del fatto | SI | testo libero (max 3.000 caratteri) |
| Autore/i del fatto (cognome-nome) | SI | matrice nominativo/grado o tipo di coinvolgimento |
| Fatto segnalato ad altre autorità (Procura, Corte dei conti, altre istituzioni da specificare | NO | matrice autorità/estremi segnalazione/copia segnalazione/riscontro/esito |
| Contenzioso amministrativo/civile/contabile in atto | NO | matrice tipo contenzioso/estremi/stato del ricorso/esito/documenti |
| Altri soggetti a conoscenza del fatto e/o in grado di riferire sullo stesso (cognome-nome) | NO | matrice nominativo/grado o tipo di conoscenza sul fatto (testimone oculare, ne ha riferito circostanze, etc.) |

| Informazione | Obbligatorietà | Tipo/descrizione |
|---|---|---|
| Norme violate (di qualsiasi livello) | NO | matrice: tipo norma/estremi norma/dettagli disposizione violata/copia della norma o link di pubblicazione della norma |
| Aspettative | NO | scopo della segnalazione e aspettative sull'intervento ANAC a seguito della segnalazione |
| Documenti utili (allegati) | NO | possibilità di fare l'upload di uno o più file purché di dimensione non superiore alla dimensione massima accettata (parametrizzabile) |
| Ulteriori informazioni | NO | testo libero (solo per segnalazioni già inserite) |

### 4.1.2. Descrizione delle funzionalità del Segnalante PA

Il "segnalante PA" è il dipendente di una pubblica amministrazione che non intende autenticarsi sul sistema attraverso la dichiarazione delle proprie generalità e la successiva fornitura delle c.d. "credenziali anonime" e di rimanere, quindi, totalmente anonimo.

I servizi a sua disposizione devono permettergli:

- di collegarsi al sistema e avere cognizione circa:
  - le tipologie di segnalazione che possono essere inoltrate,
  - le tutele accordate e le modalità con cui viene gestita la sicurezza e la riservatezza delle informazioni,
  - l'iter delle diverse tipologie di segnalazione,
  - ogni altra informazione che si riterrà opportuno rendere nota;
- di inserire le informazioni richieste ed inoltrare una segnalazione;
- di allegare documenti in formato elettronico;
- di ricercare una segnalazione precedentemente inoltrata unicamente attraverso il codice univoco che gli viene restituito all'atto dell'inserimento;
- di verificare lo stato della segnalazione, leggere le comunicazioni eventualmente inserite dalla "Struttura ricevente PA", inserire, in risposta o su propria iniziativa, ulteriori messaggi o informazioni (senza aver la possibilità di modificare quanto già inserito in sessioni precedenti);

Le informazioni di pertinenza delle segnalazioni anonime ricalcano quanto già descritto per le informazioni richieste nelle segnalazioni del "Dipendente PA" (tabella par. 4.1.1).

### 4.1.3. Descrizione delle funzionalità della Struttura ricevente PA

Ai componenti designati per la "struttura ricevente PA", in modo analogo a quanto previsto per la struttura ricevente deputata alla ricezione delle segnalazioni provenienti da dipendenti ANAC, dovrà essere consentito di:

- ricevere una mail sul proprio indirizzo di posta elettronica istituzionale all'atto dell'inserimento di una nuova segnalazione e all'atto dell'inserimento di ulteriori documenti o informazioni su una segnalazione già inserita (nella mail non devono essere contenute informazioni caratterizzanti la segnalazione come meglio specificato nel paragrafo relativo ai requisiti funzionali);

- accedere al sistema ed estrarre una lista di segnalazioni filtrate secondo lo "stato di lavorazione" differenziando le segnalazioni anonime da quelle effettuate ai sensi della legge 190/12;

- visualizzare le informazioni della singola segnalazione incluso un ID assegnato dal sistema e data ed ora dell'inserimento della segnalazione stessa;

- modificare la stato di lavorazione della segnalazione secondo i seguenti valori:

    - Nuova (assegnato dal sistema)
    - Presa in carico
    - Istruttoria in corso
    - Segnalazione all'Autorità competente
    - Archiviazione

- inserire "note di lavorazione" non visibili al segnalante;

- inserire delle note, opzionali e non visibili al segnalante, contestualmente alla modifica dello stato di lavorazione;

- richiedere l'identità del segnalante con motivazione tipizzata secondo, ad esempio, la seguente casistica:

    - Verifica attendibilità della segnalazione
    - Acquisizione ulteriori elementi istruttori che può fornire solo il segnalante
    - Eventuale successivo contraddittorio
    - Verificare in quale veste il soggetto ha inoltrato la segnalazione
    - Altro (specificare)

***NB: la richiesta d'identità, in caso di diniego, potrà essere reiterata***

- inserire delle note, opzionali e non visibili al segnalante, contestualmente alla richiesta d'identità del segnalante (si precisa che la richiesta di accoppiamento segnalazione-identità del segnalante non deve mai essere visibile al segnalante);

- inserire note e/o richieste visibili al segnalante;
- inoltrare, tramite mail, le segnalazioni (anche quelle anonime) agli uffici di vigilanza.

> *In questo caso il sistema dovrà comporre in modo automatico il testo della mail contenente i dati salienti della segnalazione; su tale testo il componente della struttura ricevente potrà apportare le modifiche che riterrà opportune. I dati della mail (inclusi destinatario, oggetto e corpo) dovranno essere memorizzati dal sistema.*

Tutti gli inserimenti e i cambi di stato devono essere etichettati in maniera esplicita con *timestamp* e autore (es: *"18/05/2015 12:41 – n.cognome"*) a eccezione, naturalmente, degli inserimenti effettuati dal segnalante.

### 4.1.4. Descrizione delle funzionalità del Terzo che autorizza PA

Vale quanto detto nel paragrafo 3.1.3 a proposito del terzo che autorizza in ambito whistleblowing ANAC. Si tratta comunque di ruoli separati.

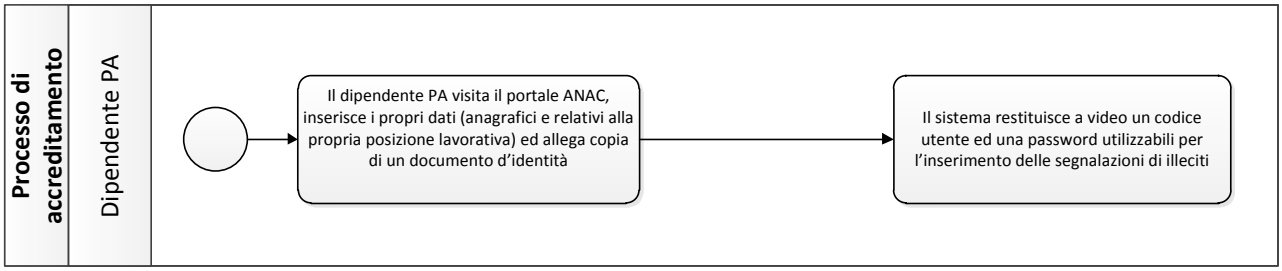
### 4.1.5. Rappresentazione dei processi

Nel presente paragrafo vengono rappresentati i principali processi che coinvolgono gli attori del sistema di cui si sono precedentemente descritte le funzionalità.

A. Richiesta credenziali anonime

Descrive il processo attraverso il quale un dipendente della pubblica amministrazione si dichiara sul sistema e ottiene una coppia utente/password utile ad autenticarsi, successivamente, sul sistema e inserire una segnalazione ai sensi della Legge 190/12.

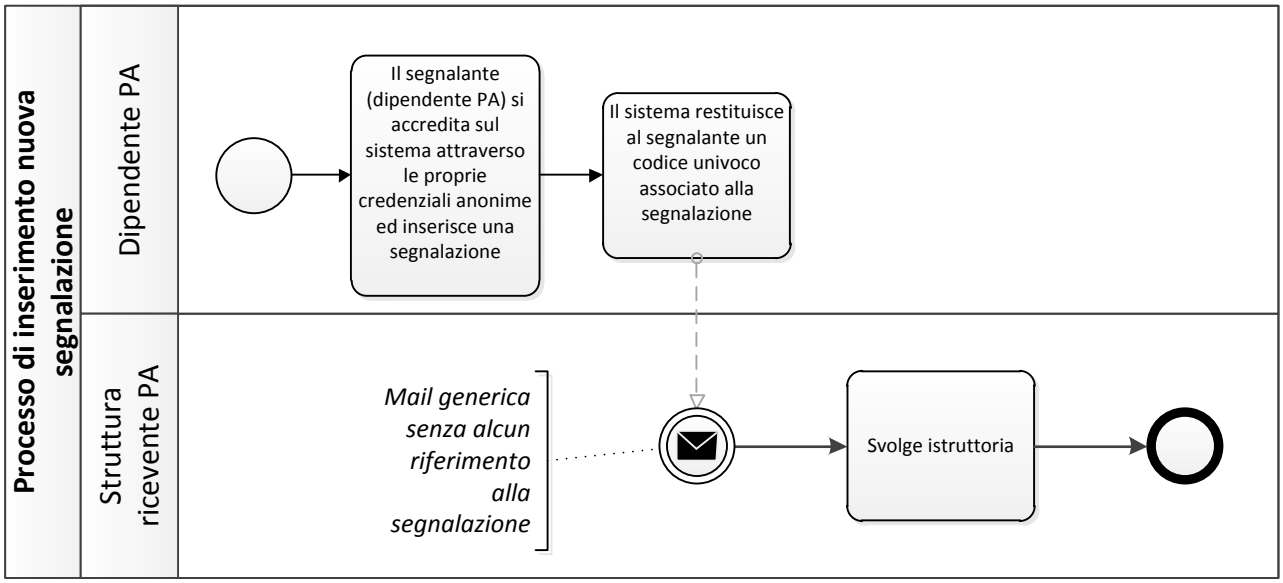
Si evidenzia che le credenziali anonime non consentono una immediata identificazione del soggetto a garanzia della tutela accordata allo stesso dalla norma



B. Inserimento nuova segnalazione ex L. 190/12

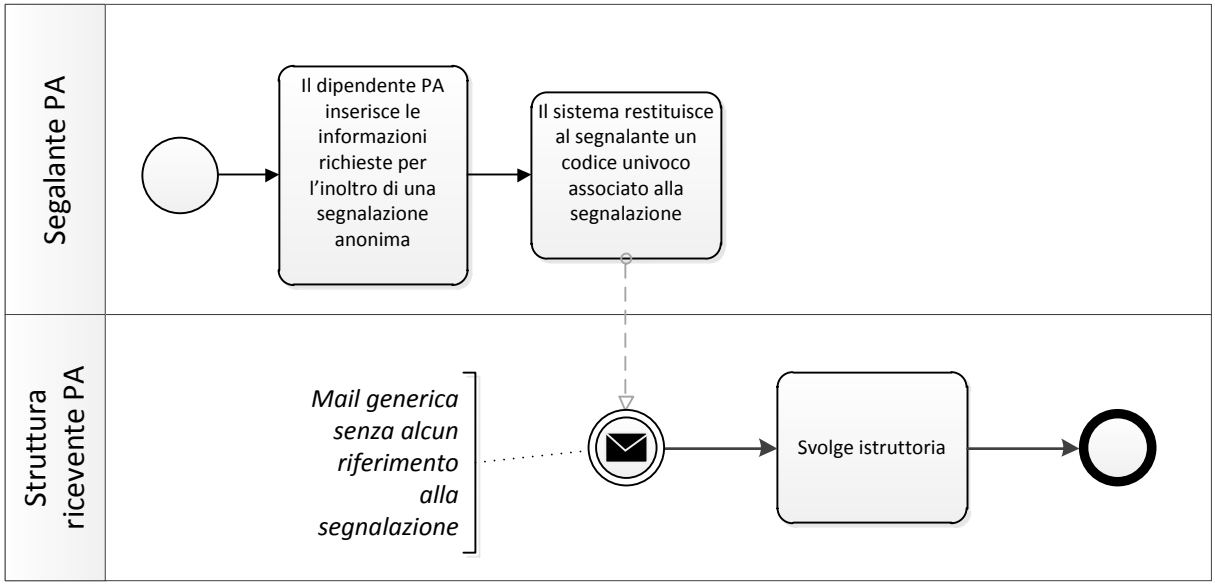
Descrive il processo attraverso il quale il dipendente di una pubblica amministrazione, dopo essersi dichiarato e aver ottenuto le "credenziali anonime", si accredita sul sistema ed inserisce una segnalazione.

La mail generata dal sistema, come già più volte evidenziato, non dovrà contenere elementi utili all'identificazione del segnalante.



C. Inserimento di una segnalazione anonima

Il segnalante PA senza autenticarsi al sistema inserisce le informazioni richieste per il completamento di una segnalazione e la inoltra. Il sistema gli restituisce un codice univoco con il quale egli stesso può verificare lo stato della segnalazione inoltrata e avere cognizione di eventuali messaggi associati alla segnalazione stessa dalla struttura ricevente PA o inserire lui stesso ulteriori informazioni, senza però aver la possibilità di modificare quanto precedentemente inoltrato.



### 4.2. Requisiti utente

Si riporta di seguito la convenzione per l'identificazione dei requisiti.

Ciascun requisito è individuato da un identificativo univoco nella forma [RF_M.nn] o [RNF_M.nn], dove:

- **RF** Requisito Funzionale;
- **RNF** Requisito Non Funzionale;
- **M** identifica l'**ambito;**
- **nn** è un progressivo numerico.

**Ambito="PA" segnalazioni di illecito inoltrate da dipendenti pubblici**

#### 4.2.1. Requisiti utente di tipo funzionale (RF_WBPA.XX)

RF_WBPA.01 Generalità

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | L'applicazione deve intendersi come specifica istanziazione di un sistema che consenta la predisposizione e la pubblicazione di schede di "raccolta informazioni" (*form builder*) e la gestione della sicurezza delle informazioni e della comunicazione |

RF_WBPA.02 Disclaimer

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il sistema dovrà rendere evidente all'utente segnalante che la propria identità potrà essere estratta in caso di stretta necessità da parte degli utenti componenti della "Struttura Ricevente PA" e le modalità di trattazione delle segnalazioni (*disclaimer*) |

RF_WBPA.03 Ambito di distribuzione

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il sistema sarà pubblicato sul portale dell'Autorità e reso disponibile sia per l'inserimento di segnalazioni anonime sia per quello di segnalazioni whistleblowing (previo inserimento delle c.d. "credenziali anonime"). |

RF_WBPA.04 Identità del segnalante

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Le segnalazioni verranno acquisite anche in forma anonima. In tal caso il segnalante sarà informato in modo esplicitò sulle modalità di trattazione delle segnalazioni anonime rispetto a quelle non anonime, della possibilità di inserire la stessa segnalazione previa acquisizione delle c.d. "credenziali anonime" e delle garanzie accordate in merito alla riservatezza in caso di segnalazioni non anonime. |

RF_WBPA.05 "Credenziali anonime"

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | L'utente che intende registrarsi preventivamente all'inserimento di una segnalzione deve forinire, in formato elettronico, copia del proprio documento d'identità e un modulo che autocertifichi la sua appartenenza all'ambito soggettivo di cui alle “Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d. whistleblower)” (parte II, punto 1) |

RF_WBPA.06 Codice univoco segnalazione

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il sistema al momento dell'inserimento di una segnalazione assegna alla stessa un codice univoco generato in modo casuale che viene rilasciato al segnalante ed è composto da 16 caratteri alfanumerici ed esposto nella forma<br><br>xxxx-xxxx-xxxx-xxxx (sedici caratteri in gruppi da quattro) |

RF_WBPA.07 Segnalante PA/Dipendente PA: Inserimento segnalazione:

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il segnalante potrà inserire una segnalazione contenente i dati esposti nel paragrafo 4.1.1. I dati obbligatori dovranno essere chiaramente individuabili. |

RF_WBPA.08 Segnalante PA/Dipendente PA: Inserimento segnalazione, segnatura di protocollo e fascicolazione

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Ad ogni segnalazione dovrà essere associata una segnatura di protocollo in modalità riservata (ovvero senza che dal sistema di protocollo sia possibile risalire all'identità del segnalante, al contenuto della segnalazione o a qualsiasi altra informazione che possa compromettere la riservatezza accordata al segnalante dalla norma di legge) e dovrà essere possibile fascicolare, anche in tempi successivi all'effettivo inserimento, le diverse segnalazioni secondo criteri dettati dall'operatività. |

RF_WBPA.09 Struttura ricevente PA: ricezione mail

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | La "struttura ricevente PA" dovrà ricevere , all'atto dell'inserimento di una nuova segnalazione o di ulteriori informazioni/documenti, una mail sul proprio account di posta elettronica istituzionale. |

RF_WBPA.10 Riservatezza degli avvisi

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Tutte le mail di avviso alla ”Struttura ricevente PA“ e al ”Terzo che autorizza PA“ non dovranno contenere dati della segnalazione né alcun altro elemento identificativo della segnalazione stessa |

RF_WBPA.11 Struttura ricevente PA: Visualizzazione elenco segnalazioni

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | La "Struttura ricevente PA" potrà visualizzare l’elenco delle segnalazioni, filtrate in base allo ”stato di lavorazione”, con indicazione per ciascuna dell'identificativo univoco della data ed ora inserimento, della segnatura di protocollo e del corrispondente fascicolo di protocollo. |

RF_WBPA.12 Struttura ricevente PA: richiesta identità segnalante

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | La "Struttura ricevente PA" potrà richiedere l’autorizzazione a conoscere l’identità del segnalante. La richiesta può essere reiterata e ciascuna richiesta/esito deve essere tracciata dal sistema. |

RF_WBPA.13 Accoppiamento segnalazione/identità del segnalante

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Solo i componenti della ”Struttura ricevente PA“ devono poter conoscere l’identità del segnalante, evidenziandone la motivazione e previa esplicita autorizzazione puntuale sulla singola segnalazione da parte del ”Terzo che autorizza PA” |

RF_WBPA.14 Terzo che autorizza PA: ricezione mail

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il ”Terzo che autorizza PA” dovrà ricevere all’atto dell’inserimento di una richiesta di autorizzazione a conoscere l’identità del segnalante, una mail sul proprio account di posta elettronica istituzionale. |

RF_WBPA.15 Terzo che autorizza PA: identità del segnalante

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il ”Terzo che autorizza PA“ non dovrà conoscere l’identità del segnalante |

RF_WBPA.16 Terzo che autorizza PA: visualizzazione segnalazione

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il "Terzo che autorizza PA" potrà visualizzare l’elenco delle segnalazioni per le quali è stata richiesta da parte della "Struttura ricevente PA" l’autorizzazione a conoscere l’identità del segnalante con indicazione della motivazione e, cliccando su una di esse, accedere a tutte le informazioni relative (a eccezione dell'identità del segnalante. |

RF_WBPA.17 Terzo che autorizza: concessione/diniego autorizzazione

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il "Terzo che autorizza PA" potrà consentire o negare, motivando, l’associazione tra la segnalazione e l’identità del segnalante. |

RF_WBPA.18 Segnalante PA/Dipendente PA: ricerca propria segnalazione

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il "segnalante PA" e il "Dipendente PA" potranno ricercare la propria segnalazione solo attraverso il codice univoco rilasciato all'atto dell'inserimento della segnalazione stessa, potrà verificarne lo stato di lavorazione, le eventuali richieste di integrazione da parte della "Struttura ricevente PA" ma non potranno, in alcun caso, modificare le informazioni già trasmesse |

RF_WBPA.19 Segnalante PA/Dipendente PA: criteri di ricerca delle segnalazioni

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il "Segnalante PA" e il "Dipendente PA" potranno ricercare solo le segnalazioni corrispondenti ai codici univoci a loro stessi rilasciati. Dovranno essere possibili solo ricerche puntuali. |

RF_WBPA.20 Struttura ricevente PA: invio richieste/messaggi al segnalante PA o al Dipendente PA

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | La "Struttura ricevente PA" potrà inviare messaggi al "Segnalante PA" o al "Dipendente PA", pur senza conoscerne l'identità. La comunicazione sarà comunque asincrona e i destinatari ne avranno notizia solo su propria iniziativa verificando lo stato della propria segnalazione. |

RF_WBPA.21 Struttura ricevente PA: ricerca e visualizzazione delle segnalazioni

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | I componenti della ”Struttura ricevente PA“ potranno ricercare le segnalazioni e visualizzarne tutte le informazioni, oltreché inserendo puntualmente il codice identificativo univoco, per stato lavorazione e/o per periodo (intervallo date), per luogo in cui si è svolto il fatto, per ente oggetto della segnalazione e in generale imponendo filtri su tutte le informazioni di tipo strutturato. |

RF_WBPA.22 Struttura ricevente PA: lavorazione segnalazioni (1)

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | I componenti della ”Struttura ricevente PA“ potranno variare lo stato di lavorazione della singola segnalazione, inserire richieste/messaggi al segnalante, inserire ”note”, inserire richiesta motivata di conoscenza dell’identità del segnalante. |

RF_WBPA.23 Struttura ricevente PA: lavorazione segnalazioni (2)

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | I componenti della ”Struttura ricevente PA“ dovranno ricevere una mail di notifica a ogni nuova segnalazione e a ogni ulteriore messaggio inviato dal segnalante in relazione ad una specifica segnalazione. |

RF_WBPA.24 Terzo che autorizza PA: valutazione opportunità dis-anonimizzazione della segnalazione

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il ”Terzo che autorizza PA“ potrà consentire o rifiutare ai componenti della “Struttura Ricevente PA” di conoscere l’identità del segnalante |

RF_WBPA.25 Segnalante PA/Dipendente PA: invio documenti e integrazione dati

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il segnalante potrà allegare documenti, anche in momenti successivi all'inserimento della segnalazione, e integrare, su apposito campo, le informazioni inserite precedentemente. |

RF_WBPA.26 Reportistica

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | L'applicazione dovrà essere corredata di un sistema di reportistica in grado di fornire indicazioni di tipo statistico quali ad esempio, per un dato periodo, il numero delle segnalazioni (totali e per singolo stato - riferibili a un'intera organizzazione o a una sua particolare articolazione), il tempo medio per la presa in carico di una segnalazione. Per tali dati dovranno essere previste funzioni di esportazione in formato aperto. |

RF_WBPA.27 Inoltro segnalazioni

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il sistema dovrà consentire l'inoltro delle segnalazioni ad altri uffici dell'Autorità competenti in materia di vigilanza: i destinatari dovranno essere raggiunti tramite mail istituzionale e si dovrà consentire il mascheramento di eventuali informazioni che la "Struttura ricevente PA" riterrà opportuno non trasmettere. |

RF_WBPA.28 Mascheramento di informazioni (omissis)

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Nel caso in cui la "Struttura ricevente PA" trasmetta la segnalazione ad altri uffici il sistema dovrà rendere disponibili funzionalità di mascheramento di informazioni puntuali e massive<br><br>Dovrà essere possibile mascherare le stringhe selezionate e dovrà essere possibile mascherare, ricercando in tutto il testo trasmesso, i caratteri che corrispondo ad una specifica stringa inserita dall'utente senza distinguere tra caratteri maiuscoli e minuscoli (esempio: maschera tutti i caratteri che corrispondono a "direttore dell'ufficio delle entrate di Roma I") |

RF_WBPA.29 Stampe

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Non dovranno essere previste funzioni relative alla stampa delle informazioni gestite dall'applicazione. |

### 4.2.2. Requisiti utente di tipo non funzionale (RNF_WBPA.XX)

Descrivono gli aspetti del sistema che non sono direttamente legati al comportamento (funzionalità) del sistema stesso.

RNF_WBPA.01 Bonifica dei meta-dati dei documenti allegati

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | I documenti allegati dovranno essere bonificati da eventuali metadati presenti (autore, autore ultima modifica, data creazione, data ultima modifica, etc) |

RNF_WBPA.02 CAPTCHA

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Dovrà essere impedito l'utilizzo dei servizi resi disponibili sul portale dell'Autorità da parte di "bot" attraverso l'obbligo di immissione di captcha o di altra metodologia similare idonea ad escludere l'impiego di processi automatici di compilazione dei dati. |

RNF_WBPA.03 Sicurezza (1)

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | In considerazione della natura delle informazioni trattate e dell'elevato grado di riservatezza che deve essere garantito, l'intera applicazione dovrà essere sottoposta ad attività di *Vulnerability Assessment & Penetration Test* con certificazione dei risultati in termini di metodologie adottate, valutazione dei rischi in base al contesto, test condotti, vulnerabilità rilevate ed azioni correttive intraprese e/o da intraprendere. |

RNF_WBPA.04 Sicurezza (2)

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Dovrà essere garantita la non tracciabilità del client dal quale viene effettuata la segnalazione. Le modalità adottate devono essere rese evidenti all'utente (vedi RF_WBPA.01: Disclaimer) |

RNF_WBPA.05 Sicurezza delle comunicazioni (1)

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Tutti i dati inviati dall'applicazione ai PC degli utenti devono essere cifrati |

RNF_WBPA.06 Sicurezza delle comunicazioni (2)

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Tutti i colloqui fra i server coinvolti devono essere cifrati |

RNF_WBPA.07 Log delle attività e log applicativo

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Tutte le attività eseguite da qualunque utente (anche dagli "amministratori di sistema") devono essere tracciate. |

RNF_WBPA.08 Sicurezza delle informazioni

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Tutte le informazioni, sia quelle proprie dell'applicazione sia quelle relative alla tracciabilità, dovranno essere memorizzate in modo cifrato |

RNF_WBPA.09 Performance

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il sistema dovrà garantire idonei standard prestazionali, relativi ai tempi di esecuzione ed utilizzo delle risorse, per non produrre inefficienze nel contesto di esecuzione durante la sua normale attività. |

RNF_WBPA.10 Scalabilità

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | L'architettura del sistema dovrà essere realizzata in modo tale da poter essere adattata ad esigenze future dovute all'aumento dei dati o delle richieste da elaborare. |

RNF_WBPA.11 Affidabilità

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il sistema dovrà essere in grado di funzionare correttamente per lunghe sessioni di lavoro e dovrà garantire la consistenza dei dati elaborati nel caso di situazioni impreviste. |

RNF_WBPA.12 Manutenibilità

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il sistema dovrà essere dotato di un form builder al fine di poter consentire un agevole aggiornamento, anche da parte di personale non specificatamente tecnico, delle informazioni che si intendono raccogliere. |

RNF_WBPA.13 Accessibilità

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il sistema dovrà essere realizzato nel rispetto dei requisiti di accessibilità previsti per i siti della PA |

RNF_WBPA.14 Compatibilità WEB

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Il sistema dovrà essere realizzato per essere fruito in ambiente web ed essere indipendente dalla tipologia di browser utilizzato dall'utente. |

RNF_WBPA.15 Protocollo

| VER. | STATO | DESCRIZIONE |
|---|---|---|
| 01 | provvisorio | Ad ogni segnalazione dovrà essere associata una segnatura di protocollo. Il sistema di protocollo non dovrà contenere alcuna informazione relativa alla segnalazione (c.d. protocollo riservato) |