

Safira

Piattaforma per le segnalazioni di abusi e discriminazione di genere



Tecnologia OpenBlow

Nel contesto odierno, la segnalazione di comportamenti illeciti e rilevanti è diventata una necessità fondamentale per promuovere ambienti sicuri e inclusivi, oltre che per essere conformi alle normative.

La tecnologia OpenBlow, **nata in collaborazione con ANAC per le segnalazioni di whistleblowing**, rappresenta un'innovazione in questo ambito, offrendo uno strumento avanzato e accessibile per effettuare e gestire segnalazioni di illeciti, molestie sessuali, abusi in ambito sportivo o lavorativo, discriminazione di genere, bullismo scolastico e altri comportamenti inaccettabili.



Le soluzioni

Dalla tecnologia OpenBlow sono nate diverse piattaforme specializzate, per rispondere a specifiche esigenze di segnalazione in **vari ambiti**.

Ogni piattaforma garantisce **anonimato, protezione e conformità** alle normative, promuovendo ambienti più sicuri e trasparenti.



OpenBlow

OpenBlow rappresenta la soluzione centrale per il whistleblowing aziendale, utile a gestire frodi e illeciti sul posto di lavoro.



Safira

Safira si concentra sulla denuncia di abusi e discriminazioni di genere, offrendo uno spazio sicuro per segnalare molestie e violazioni dei diritti.



Butterfly

Butterfly è stata sviluppata per contrastare il bullismo nelle scuole, fornendo uno strumento anonimo per studenti e genitori.



Safeguarding

Safeguarding è pensata per combattere abusi e sfruttamenti nel mondo dello sport.

La normativa

L'evoluzione della normativa italiana degli ultimi anni in materia di violenza di genere prende le mosse dalla ratifica della **Convenzione di Istanbul dell'11 maggio 2011** sulla prevenzione e sulla lotta contro la violenza nei confronti delle donne e la violenza domestica.

A seguito della ratifica della Convenzione, avvenuta con la legge n. 77 del 2013, l'Italia ha compiuto una serie di interventi volti a istituire una **strategia integrata per combattere la violenza di genere**.



La convenzione n. 190 ILO (Organizzazione Internazionale del Lavoro)

Favorisce, previene e attua una regolamentazione per l'eliminazione della violenza e delle molestie nel mondo del lavoro, approvata a Ginevra il 21 giugno 2019 da più di 180 Paesi. In Italia è stata ratificata mediante la legge n. 4 del 15 gennaio 2021.



Il Decreto Legislativo n.198/2006 art 26 c.d. Codice delle pari opportunità

All'art. 26, comma 2, sancisce una equiparazione tra molestie sessuali e discriminazioni di genere, stabilendo che «sono, altresì, considerate come discriminazioni le molestie sessuali».



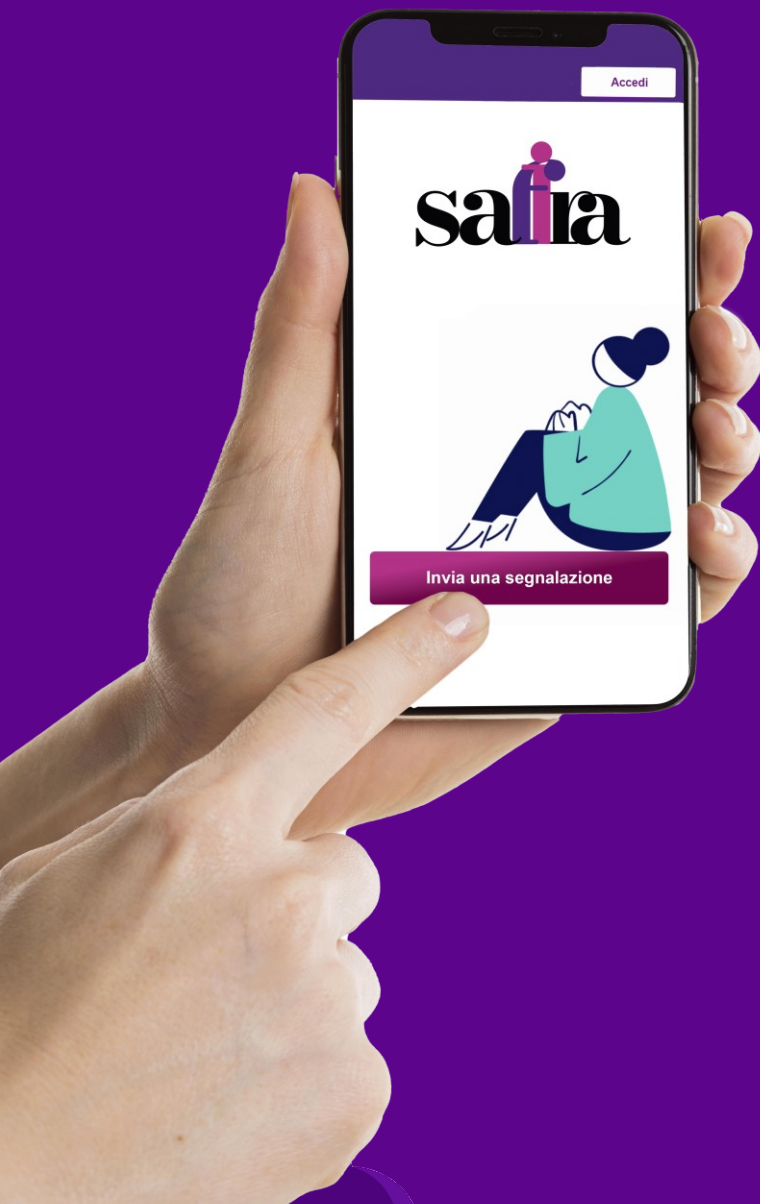
Accordo quadro sulle molestie e sulla violenza sul luogo di lavoro

Del 26 aprile 2007 delle Parti Sociali Europee, ha l'obiettivo di sensibilizzare maggiormente i datori di lavoro, i lavoratori e i loro rappresentanti e fornire un quadro di azioni concrete per individuare, prevenire e gestire le situazioni di molestie e di violenza sul luogo di lavoro.



Decreto Legislativo 24/2023 in materia whistleblowing

All'art. 17 "Divieto di ritorsione" identifica nelle molestie e nelle discriminazioni degli esempi di condotte ritorsive a danno dei soggetti che segnalano violazioni di cui sono venuti a conoscenza nel contesto lavorativo.



La piattaforma Safira

Soluzione per segnalare abusi e discriminazione di genere

Safira è la piattaforma realizzata dalla Laser Romae, che utilizza la tecnologia OpenBlow, tecnologia leader nell'ambito delle segnalazioni.

Safira è **sicura, semplice da utilizzare e personalizzabile** in funzione di qualsiasi tipo di organizzazione.

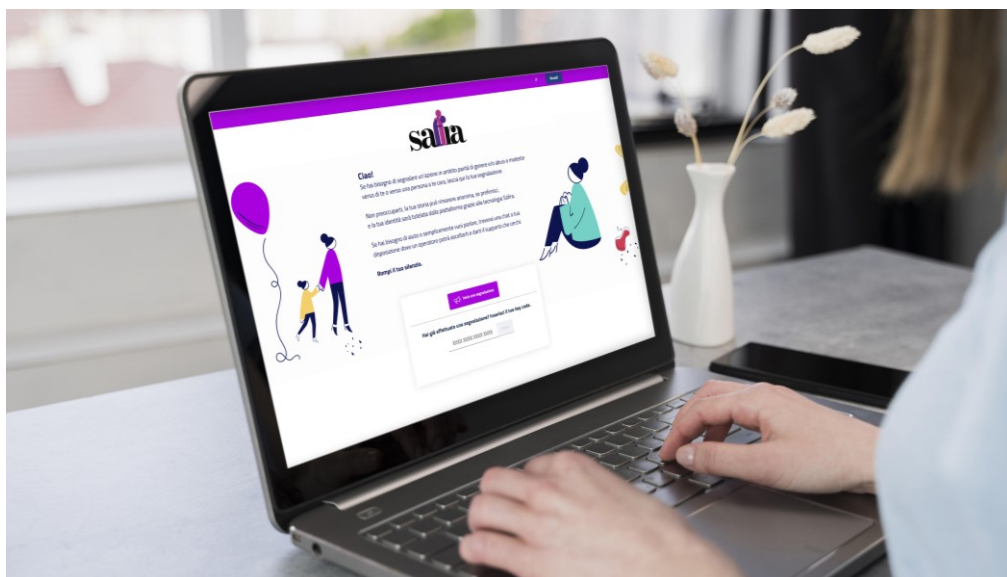
Punti di forza

- Piattaforma informatica **Web-Based**
- **Semplificazione** delle procedure di gestione delle segnalazioni
- Contenuto delle **segnalazioni riservato** durante il processo
- **Separazione dei dati** del segnalante dalla segnalazione
- Adeguate politiche di accesso e **conservazione** dei dati
- Integrazione della piattaforma all'interno delle **applicazioni**
- Gestione **multi legal entity** in modo nativo per istanze multiple, garantendo la segregazione dei dati
- Traducibile in **qualsiasi lingua**



Processo di segnalazione

Il processo di segnalazione è centralizzato sulla piattaforma, la quale garantisce una **chiara separazione dei ruoli** e la **sicurezza durante tutte le fasi** di gestione della segnalazione.



Alla ricezione di una segnalazione, la persona designata procede con i seguenti passi:

- **Ricezione** e categorizzazione della segnalazione;
- **Verifica** preliminare della segnalazione (screening della segnalazione);
- **Istruttoria** (e interazione con il Segnalante);
- **Definizione** (chiusura) con esito di archiviazione o di inoltro;
- **Trasmissione** agli Uffici Competenti e/o dipartimenti interni in caso di inoltro.

Oggetto della segnalazione

Al momento della segnalazione, potrà essere scelto se procedere con una segnalazione in ambito:

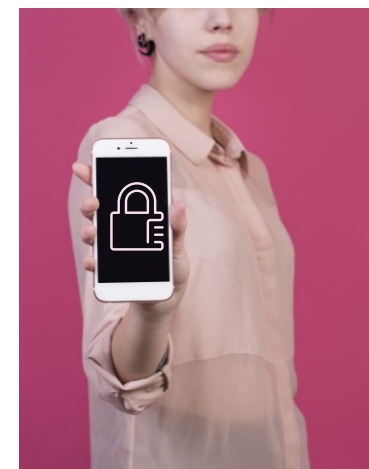
A. PARITÀ DI GENERE

B. ABUSI/MOLESTIE

Nel primo caso (A) si tratta di violazioni alla politica e alle regole del Sistema sulla Parità di genere.

Nel caso di sospetti o fatti inerenti a minacce, abusi, molestie reali o potenziali, si potrà procedere con l'invio di una segnalazione del secondo tipo (B).

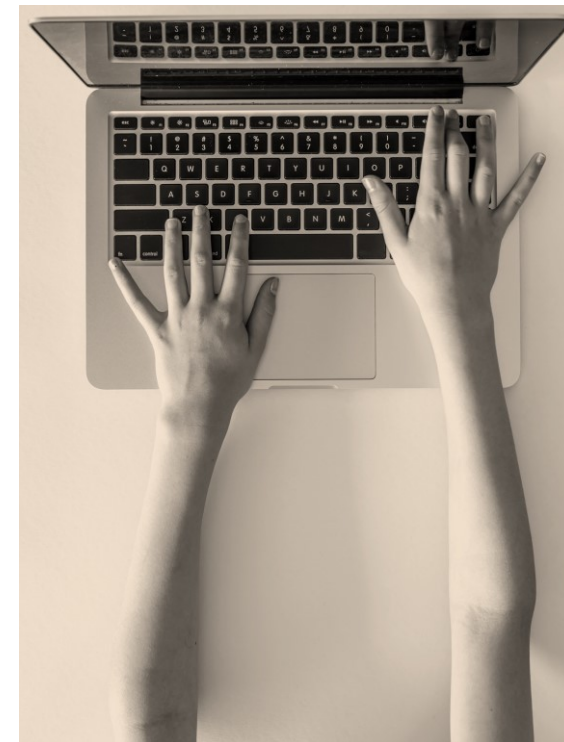
E' possibile utilizzare la piattaforma Safira anche per un solo ambito, il **livello di personalizzato elevato** permette di offrire una soluzione costruita ad hoc per ogni esigenza.



Contenuto della segnalazione

La segnalazione avviene tramite la **compilazione di un questionario**, che deve contenere:

- una chiara e completa **descrizione** dei fatti oggetto di segnalazione;
- le **circostanze** di tempo e di luogo in cui sono stati commessi i fatti segnalati;
- se conosciute, le **generalità** o altri elementi che consentano di identificare il soggetto che ha posto in essere i fatti segnalati;
- indicazione di eventuali **altri soggetti** che possono riferire sui fatti oggetto di segnalazione;
- eventuali **documenti** che possano confermare la fondatezza dei fatti riportati;
- ogni altra informazione che possa fornire un utile riscontro circa la sussistenza dei fatti segnalati.



La segnalazione può essere effettuata in forma anonima o inserendo le proprie generalità.

Qualora fossero inserite le proprie informazioni, la **piattaforma garantisce l'anonimato tramite sistemi di cifratura avanzati.**


Caratteristiche funzionali

- **Separazione dei 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;
- **Riservatezza del contenuto delle segnalazioni** durante l'intera fase di gestione della segnalazione;
- **Adozione di protocolli sicuri** per il trasporto dei dati in rete nonché l'utilizzo di strumenti di crittografia per i contenuti delle segnalazioni e dell'eventuale documentazione allegata;
- **Adozione di adeguate modalità di conservazione** dei dati e della documentazione (fisico, logico, ibrido);
- **Adozione di politiche di tutela della riservatezza** attraverso strumenti informatici (disaccoppiamento dei dati del segnalante rispetto alle informazioni relative alla segnalazione, crittografia dei dati e dei documenti allegati);
- **Adozione di politiche di accesso ai dati** (funzionari abilitati all'accesso, amministratori del sistema informatico).

Sicurezza della piattaforma


- **Server Resiliency:** configurato in modo da rendere inoffensivi attacchi di tipo D/DOS.
- **2FA e Password Policy:** il sistema supporta nativamente il 2FA e di base viene gestita la password policy (strength e scadenza) degli account.
- **Password Storage:** password memorizzate attraverso l'utilizzo di un hash generato con un salt a 128 bit casuale. Le ricevute dei segnalanti sono con Crypto.Random di Python.
- **Web content security:** comunicazione tra frontend e backend utilizza le best practice, condivise a livello internazionale.
- **Workflow di gestione:** garantisce la possibilità di definire dall'interno del sistema delle gerarchie, con il supporto di multipli livelli di autorizzazione per la messa on-line di un contenuto.
- **File Encryption:** un receiver può utilizzare la propria chiave PGP, se posseduta. Ciascun file è salvato su dicker utilizzando una chiave simmetrica casuale AES, la chiave è salvata su ramdisk.
- **GDPR:** le piattaforme sono a norma con il regolamento sulla protezione dei dati (GDPR-UE 2016/679).



 Viale Cesare Pavese 305 - Roma

 06 56 55 92 45

 sales@laserromae.it

 www.laserromae.it

