STUDIO AMICA

# ALLEGATO TECNICO - SOFTWARE WHISTLEBLOWING

Segnalazione di illeciti per Aziende e PA

## Premessa

Il software di whistleblowing realizzato da STUDIO AMICA Srl è progettato per consentire di segnalare in modo sicuro e anonimo attività illegali, frodi o altre violazioni etiche all'interno di un'organizzazione. Il sistema è stato sviluppato tenendo conto delle disposizioni normative del D.Lgs. 24 del 2023, che stabilisce le linee guida per il whistleblowing in Italia.

Il software offre le seguenti caratteristiche:

1. Anonimato: Il sistema assicura la completa protezione dell'identità del segnalante. I whistleblower possono inviare le loro segnalazioni in modo anonimo, garantendo la riservatezza delle informazioni fornite.
2. Sicurezza dei dati: Il software implementa rigorose misure di sicurezza per proteggere le informazioni sensibili. I dati delle segnalazioni sono crittografati e archiviati in modo sicuro per prevenire accessi non autorizzati.
3. Facilità di utilizzo: L'interfaccia utente del software è intuitiva e user-friendly, consentendo ai whistleblower di presentare le segnalazioni in modo semplice e senza complicazioni.
4. Tracciabilità delle segnalazioni: Il sistema registra tutte le attività associate alle segnalazioni, inclusi gli aggiornamenti, i tempi di risposta e le azioni intraprese. Questo permette di monitorare e gestire efficacemente le segnalazioni nel rispetto della normativa.
5. Canali di comunicazione sicuri: Il software fornisce canali di comunicazione protetti, come criptaggio di tutte i dati e documenti, separazione delle banche dati, ecc. per garantire che le

informazioni scambiate tra il whistleblower e l'organizzazione siano al sicuro da intercettazioni o manomissioni.

6. Conformità normativa: Il software è stato sviluppato tenendo conto delle disposizioni del D.Lgs. 24 del 2023, garantendo la conformità alle normative vigenti in Italia in materia di whistleblowing.

Il software di whistleblowing si propone di fornire un ambiente sicuro e protetto per consentire ai whistleblower di segnalare violazioni senza temere ritorsioni. Rappresenta uno strumento efficace per promuovere l'integrità e la trasparenza all'interno delle organizzazioni, in conformità con la normativa vigente.

## Sicurezza e Riservatezza dei dati

### CRITTOGRAFIA

Il software di WHISTLEBLOWING implementa un sistema di crittografia avanzato per proteggere i dati delle segnalazioni e dei segnalanti: mediante l'utilizzo di una coppia di chiavi asimmetriche (di tipo RSA con una dimensione di 4096 bit) tutti i dati e documenti sono crittografati prima di essere archiviati sul disco.

La crittografia con chiavi asimmetriche coinvolge l'uso di una coppia di chiavi: una chiave pubblica e una chiave privata. La chiave pubblica viene utilizzata per crittografare i dati, mentre la chiave privata, che è strettamente custodita dal responsabile, viene utilizzata per decrittografarli.

Questo approccio crittografico robusto garantisce che solo il segnalante e il responsabile per l'anticorruzione possano accedere ai dati delle segnalazioni, mantenendo la riservatezza e la sicurezza delle informazioni durante tutto il processo di whistleblowing. L'utilizzo della crittografia con chiavi asimmetriche oltre a fornire un livello elevato di sicurezza e protezione dei dati delle segnalazioni, garantisce la confidenzialità delle stesse, riducendo al minimo il rischio di accessi non autorizzati e consentendo di verificare l'autenticità dei dati stessi.

Utilizzando chiavi RSA con una lunghezza di 4096 bit, il software garantisce un elevato livello di sicurezza nella crittografia dei dati delle segnalazioni. La dimensione della chiave offre una robusta protezione crittografica e riduce al minimo la possibilità di decrittazione senza la chiave privata corrispondente, infatti

una chiave di questa dimensione offre un elevato livello di sicurezza e rende computazionalmente difficile la decrittazione senza la chiave corrispondente.

Per tutti i processi di crittazione, il software utilizza l'algoritmo AES (Advanced Encryption Standard), un algoritmo di crittografia a blocchi che utilizza una chiave simmetrica per crittografare e decrittografare i dati. Esso offre una crittografia forte e ampiamente accettata per proteggere le informazioni sensibili. Il software implementa l'algoritmo AES con una lunghezza di chiave adeguata (AES a 256 bit) per garantire una protezione efficace dei dati e un elevato livello di sicurezza.

**ACCESSO AL SISTEMA**

L' accesso al sistema mediante username e password:

- Le password degli utenti non vengono memorizzate nel database in chiaro, ma vengono crittografate utilizzando un algoritmo di hash SHA512, che è noto per essere sicuro e resistente a violazioni.
- Oltre all'algoritmo di hash, viene utilizzato anche un salt random per aumentare la sicurezza della memorizzazione delle password. Il salt è un valore casuale univoco generato per ogni password e viene concatenato alla password prima di eseguire l'hashing. Questo rende più difficile l'individuazione delle password originali tramite attacchi di forza bruta o tabelle di lookup (rainbow table).
- Anche gli amministratori di sistema non possono risalire alle password degli utenti. La memorizzazione delle password in modalità cifrata, combinata con un salt random, garantisce che nemmeno gli amministratori di sistema possano accedere alle password degli utenti.
- Durante il processo di accesso al sistema, la password inserita dall'utente viene sottoposta allo stesso algoritmo di hash e al salt random per generare un hash crittografato. Questo hash viene quindi confrontato con quello memorizzato nel database. Se i due hash corrispondono, l'utente viene autenticato e può accedere al sistema.

L'utilizzo di un algoritmo di hash sicuro come l'SHA512 combinato con un salt random e la memorizzazione cifrata delle password nel database garantisce un alto livello di sicurezza. Anche nel caso di un potenziale furto o visualizzazione del database, le password degli utenti rimangono protette e non possono essere facilmente decifrate o utilizzate da terze parti non autorizzate.

STUDIO AMICA

**AUTENTICAZIONE A 2 FATTORI | STRONG AUTHENTICATION**

Nel software viene implementata anche l'autenticazione a due fattori (2FA) per aggiungere un ulteriore livello di sicurezza nell'accesso al sistema. L'autenticazione a due fattori richiede che gli utenti forniscano due elementi distinti per verificare la loro identità. Ecco come funziona:

1. Fattore 1: Password - Come descritto in precedenza, gli utenti inseriscono la propria password per accedere al sistema. La password è il primo fattore di autenticazione.
2. Fattore 2: Autenticazione aggiuntiva - Dopo aver inserito correttamente la password, viene richiesto all'utente di fornire un secondo fattore di autenticazione. Il secondo fattore corrisponde a un codice di verifica generato da un'applicazione di autenticazione: L'utente utilizza un'applicazione sul proprio dispositivo (come Google Authenticator o Authy) per generare un codice di verifica temporaneo. Questo codice viene inserito nell'interfaccia del software di whistleblowing per completare l'autenticazione.
3. Verifica dei due fattori: Il software di whistleblowing verifica entrambi i fattori di autenticazione prima di concedere l'accesso all'utente. La combinazione della password (primo fattore) e del secondo fattore di autenticazione (secondo fattore) fornisce un'identificazione più affidabile dell'utente e aumenta la sicurezza complessiva dell'accesso al sistema.

L'autenticazione a due fattori aggiunge una protezione significativa perché anche se qualcuno riesce a ottenere la password di un utente, non può accedere al sistema senza il secondo fattore di autenticazione, che è generato in tempo reale e di difficile duplicazione.

**INFRASTRUTTURA**

Il software di whistleblowing è fornito come servizio in modalità SaaS (Software as a Service) presso un'infrastruttura qualificata AgID (Agenzia per l'Italia Digitale). Ciò significa che il software viene ospitato su un'infrastruttura di hosting qualificata e gestita da fornitori di servizi qualificati secondo le linee guida stabilite da AgID:

1. L'infrastruttura di hosting su cui viene eseguito il software di whistleblowing è certificata e qualificata da AgID. Ciò implica che il fornitore del servizio di hosting ha soddisfatto tutti i requisiti

di sicurezza e conformità stabiliti da AgID per garantire un'adeguata protezione dei dati e un funzionamento affidabile del servizio.

2. Il software di whistleblowing viene offerto come servizio, consentendo agli utenti di accedere al sistema tramite una connessione Internet senza dover installare il software sui propri dispositivi. Gli utenti possono utilizzare il software attraverso un'interfaccia web sicura.
3. L'infrastruttura qualificata AgID implementa misure di sicurezza avanzate per proteggere i dati e garantire la continuità del servizio. Ciò includere misure come firewall, monitoraggio della sicurezza, backup regolari dei dati, autenticazione forte per gli amministratori di sistema, ecc.
4. La fornitura del software di whistleblowing in modalità SaaS presso un'infrastruttura qualificata AgID assicura che il servizio sia conforme alle linee guida e alle normative stabilite da AgID per la gestione sicura dei dati e la protezione della privacy.
5. L'infrastruttura qualificata fornisce una garanzia di affidabilità e disponibilità del servizio, riducendo al minimo i tempi di inattività e garantendo una risposta tempestiva alle richieste di supporto tecnico.

L'infrastruttura di STUDIO AMICA è protetta da firewall hardware ridondati e da un sistema di IPS (Intrution Prevention System). È inoltre prevista un'appliance VPN per il deploy e l'interazione con la macchina virtuale. Sono disponibili inoltre il servizio WAF, un sistema di archiviazione e consultazione dei Log applicativi e di sistema (SIEM), l'installazione di certificato SSL per la protezione e crittazione del traffico in ingresso e in uscita sulle macchine virtuali, un sistema di verifica anti malware, il monitoraggio attivo attraverso specifiche sonde, l'installazione tempestiva delle ultime patch di sicurezza e la manutenzione ordinaria ed evolutiva dell'infrastruttura.

Inoltre, il data center di COLT Telecom di Torino, presso il quale è ospitata la nostra infrastruttura, è realizzato attraverso anelli in fibra ottica completamente ridondati e su percorsi geografici diversi. Gli armadi server sono dotati di refrigerazione ridondata, di alimentazione protetta sia da gruppi statici sia da gruppi elettrogeni diesel a lunga autonomia.

È assicurata la sorveglianza dei locali 365/7/24 con personale proprio o esterno autorizzato o con sistemi di monitoraggio remotizzato. Tutti gli accessi alle aree di data center sono sottoposti ad audit.

**Backup e Restore**: STUDIO AMICA garantisce l'esecuzione di backup periodici dei software di base, del software applicativo e dei dati su specifici supporti e con specifiche modalità di conservazione; tutte le operazioni di backup vengono monitorate.

I backup vengono effettuati con cadenza giornaliera e con una retention di 3 anni. I backup riguardano:

- database (mysql);
- definizione di gruppi e utenti;
- configurazione dei sistemi (server e apparati di rete);
- filesystem server web.

Per il software e per i dati sono mantenute almeno 1 versione giornaliera. I backup risiedono su dispositivi fisici presso il data center COLT Telecom di Torino.

## CONTINUITÀ DEL SERVIZIO

Per i servizi vengono definiti i seguenti orari, di erogazione e di funzionamento supportato, nei quali essi vengono forniti rispettivamente senza e con presidio di supporto:

- Erogazione (orario in cui un servizio è attivo e utilizzabile dall'utente, indipendentemente dal presidio) - 24 x 7 [24 ore per 7 giorni pari a 168 h/sett.], 365 giorni all'anno
- Supporto (orario di erogazione di un servizio, con supporto) - 8 x 5 [8 ore per 5 giorni pari a 40 h/sett.]

In riferimento alla disponibilità del servizio, è garantito:

- uptime del 100% su base annuale per alimentazione elettrica e/o climatizzazione ambientale;
- uptime del 99% su base annuale di accessibilità tramite rete internet all'infrastruttura;
- uptime del 99% su base annuale per la disponibilità dei nodi fisici (server) che ospitano l'infrastruttura.

I tempi di risposta dell'applicazione sono garantiti a ≤ 2 secondi nel 97% dei casi.

La manutenzione ordinaria e straordinaria pianificata riguarda le attività svolte regolarmente per il mantenimento della funzionalità ottimale dei servizi. Le attività relative alla manutenzione ordinaria sono: backup, gestione dei log, procedure di controllo e gestione.

Tali attività sono programmate con cadenza periodica; solo alcune possono determinare discontinuità nel servizio.

Le attività relative alla manutenzione straordinaria pianificata sono: patch e/o upgrade ai sistemi operativi, modifiche e/o upgrade all'hardware, modifiche e/o upgrade alla infrastruttura di rete, upgrade ai RDBMS, patch e/o upgrade fornite dal fornitore del software applicativo, riconfigurazioni di sistema e ottimizzazioni periodiche di performance.

Tali attività, non strettamente legate ad una cadenza periodica, vengono effettuate, ove possibile, in giorni e orari prestabiliti; in caso determinino discontinuità nel servizio la relativa utenza viene avvertita con un congruo tempo di preavviso, indicato nella tabella che segue. Le attività di manutenzione straordinaria vengono, laddove possibile, concordate.

Le manutenzioni notturne sono attivate automaticamente.

In caso di manutenzione straordinaria non pianificata (emergenze, guasti ecc.) ove possibile saranno utilizzati gli stessi tempi e modalità di quelli indicati per la manutenzione straordinaria pianificata.

STUDIO AMICA, per garantire la sicurezza e la continuità del servizio anche nei casi di eventi disastrosi, si è dotata di un **Business Continuity Plan con all'interno le politiche di Disaster Recovery specifiche per il servizio offerto conformi alla clausola A.14 della ISO 27001**, che si impegna a consegnare alla committenza nel caso di aggiudicazione della gara.

**L'architettura di Business Continuity e Disaster Recovery** è costituita da server virtuali presso il data center COLT Telecom di Torino (**sito primario**) e presso il data center Seeweb di Frosinone (**sito secondario**).

La macchina virtuale ospitata presso il sito secondario ha lo stesso dimensionamento e gli stessi elementi applicativi di quella presente nel sito primario.

**La replica dei dati avviene in modalità asincrona, secondo dei cicli iterativi, utilizzando un canale crittato tra i due siti avente capacità trasmissiva pari a 70 Mb/s.**

La consistenza applicativa dei dati trasmessi è garantita dalla procedura di remotizzazione, che utilizza la tecnologia rsync per il filesystem, syslogd per i log e la funzionalità di replicazione nativa di Mysql.

I sistemi sono costituiti da un sito principale ed un sito secondario, in ognuno dei quali è presente una macchina virtuale erogata tramite infrastruttura hardware con **sistemi server e storage completamente ridondati**, in configurazione ad alta affidabilità.

Le macchine virtuali hanno le seguenti caratteristiche:

| Server sito primario | Server sito secondario |
|---|---|
| 1 "Cloud Server" CentOS 7<br>• 16GB RAM<br>• 512GB Hard Disk<br>• 8 vCpu<br>• servizio di firewalling, ips, waf, ...<br>• backup giornaliero dei dati<br>• software preinstallato: sistema operativo, Apache, Postifix, Php, Mysql<br>• situato presso il data center di Torino | 1 "Cloud Server" CentOS 7<br>• 16GB RAM<br>• 512GB Hard Disk<br>• 8 vCpu<br>• servizio di firewalling, ips, waf, ... |

La macchina virtuale primaria viene replicata in tutte le componenti dell'applicativo: filesystem, log e DB mysql.

Per il sistema operativo, la sua configurazione e la configurazione degli altri pacchetti installati, non è prevista la replica automatica dei dati, in quanto gli aggiornamenti dei sistemi operativi vengono effettuati manualmente sulle due macchine virtuali.

Entrambi i server sono collegati in rete internet, e la replica avviene tramite tunnel ssh criptato con chiavi asimmetriche e **con banda garantita di 70Mbps.**

La modalità di replica di dati tra Torino e Frosinone avviene in modalità asincrona, attraverso l'utilizzo di:

- sincronizzazione asincrona del database mysql tramite replica;
- sincronizzazione asincrona del filesystem (applicativi web) tramite rsync schedulato con frequenza pari a 5 minuti;
- sincronizzazione asincrona dei log tramite syslogd.