PROCEDURA SEGNALAZIONE ILLECITI

Approvata in data 12 ottobre 2021

Sommario

1. Premessa.

L'istituto giuridico del *Whistleblowing*, ovvero del dipendente pubblico che segnala comportamenti che possono costituire illeciti, in particolare di natura corruttiva, è stato introdotto con l'articolo 1 comma 51 della Legge 190/2012 - *Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione*.

In particolare, il comma sopracitato ha inserito l'articolo 54-*bis* all'interno del D.lgs. 165/2001 - *Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche*. Tale norma prevede un regime di tutela del dipendente pubblico che segnala condotte illecite di cui sia venuto a conoscenza in ragione del rapporto di lavoro.

Successivamente, l'articolo 54-bis è stato modificato dal D.L. 24 giugno 2014, n. 90, convertito in legge 11 agosto 2014, n. 114 ed in ultimo completamente riformulato dall'articolo 1 della Legge 179/2017 - *Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato*.

Sulla normativa sopra richiamata è intervenuta anche A.N.AC. (Autorità Nazionale Anticorruzione) prima con la Determinazione n. 6 del 28 aprile 2015 *Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d. whistleblower)* e recentemente con la Delibera n. 469 del 9 giugno 2021 *Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis, del d.lgs. 165/2001*.

La ratio della norma iniziale e degli aggiornamenti che via via si sono succeduti, nonché degli interventi di A.N.AC., è quella non solo di favorire le segnalazioni di comportamenti illeciti ma di evitare che il dipendente ometta di effettuare segnalazioni di illecito - fatti salvi gli obblighi di denuncia derivanti eventualmente dal proprio incarico/mansione e dalla propria qualifica di pubblico ufficiale o incaricato di pubblico servizio - per il timore di subire conseguenze pregiudizievoli nella ed alla sua attività lavorativa.

Inoltre, A.N.AC. in entrambe le linee guida ha ritenuto che l'applicazione delle disposizioni in materia di tutela del dipendente che segnala illeciti vada estesa anche agli enti di diritto privato in controllo pubblico di livello nazionale e locale ed ha fornito indicazioni in ordine alle concrete misure di tutela della riservatezza dell'identità del dipendente che gli enti devono approntare, misure idonee ad evitare un'esposizione ad atti discriminatori conseguenti alla segnalazione degli illeciti da parte del dipendente stesso.

2. La Procedura per la segnalazione degli illeciti.

Genova Parcheggi S.p.A. (in seguito la Società) si è dotata fin dal 2017 di una procedura per la segnalazione degli illeciti, procedura che, successivamente, è stata aggiornata in data 7 maggio 2019.

Il presente documento, costituisce una nuova revisione della procedura per tenere conto:

- delle indicazioni, precisazioni ed aggiornamenti di cui alla Delibera n. 469 del 9 giugno 2021 Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis, del d.lgs. 165/2001;
- del fatto che, per garantire la riservatezza del segnalante, si è deciso di procedere all'informatizzazione delle segnalazioni ed ai colloqui tra Responsabile della Prevenzione della Corruzione e della Trasparenza (in seguito R.P.C.T.) di Genova Parcheggi S.p.A. (in seguito Società) e lo stesso segnalate mediante l'acquisizione di apposita piattaforma certificata AgID (Agenzia per l'Italia Digitale) e denominata PAWhistleblowing (società fornitrice ISWEB S.p.A.) nonché con le caratteristiche di cui alle linee guida A.N.AC. già citate.

Pertanto, la presente procedura si conforma alle indicazioni dell'A.N.AC. e costituisce parte integrante del Piano Triennale della Prevenzione della Corruzione e della Trasparenza adottato dalla Società.

3. Scopo della Procedura.

Lo scopo della Procedure è quello di fornire al segnalante (così detto *whistleblower*) precisazioni, indicazioni in merito all'oggetto, ai contenuti, al/i destinatario, alle modalità di inoltro delle segnalazioni nonché le forme di tutela che gli vengono offerte dall'ordinamento, contrastando ogni possibile discriminazione nei suoi confronti, ed individuando e rimuovendo i possibili fattori che potrebbero in qualche modo impedire o rallentare il ricorso all'istituto della denuncia di illeciti nel pubblico interesse.

4. Destinatari della Procedura.

4.1 I Segnalanti.

I destinatari della Procedura, ai sensi dell'articolo 54-bis del D.lgs. 165/2001, e che, conseguentemente, usufruiscono della relativa tutela, possono essere così individuati:

- i dipendenti della società;
- i componenti degli Organi Sociali;
- i collaboratori, liberi professionisti con qualsiasi tipo di contratto ed incarico con la Società;
- i dipendenti ed i collaboratori di imprese fornitrici di beni o servizi o che realizzano opere a favore della Società anche al di fuori dell'ambito di applicazione del Codice dei contratti pubblici (D.lgs. 18 aprile 2016, n. 50).

Si ritiene opportuno evidenziare che rimane fermo l'obbligo, da parte dei dipendenti della Società che rivestono la qualità di pubblico ufficiale o di incaricato di pubblico servizio, i quali, nell'esercizio o a causa delle loro funzioni abbiano notizia di un reato perseguibile d'ufficio, di presentare denuncia all'Autorità Giudiziaria pure in presenza di segnalazione interna effettuata sulla base della presente Procedura.

Si precisa che secondo le Linee Guida di cui alla Delibera A.N.AC. 469/2021 precedentemente citata, sono escluse dall'applicazione della Procedura, e dalle relative tutele, particolari figure di lavoratori della Società (ad esempio stagisti, tirocinanti) che, pur svolgendo attività di lavorativa a favore della società non godono dello *status* di dipendente sebbene la Direttiva UE n. 2019/1937, da recepire nella legislazione nazionale entro il 17 dicembre 2021, preveda che tutti i soggetti che si trovino anche solo temporaneamente in rapporti lavorativi con l'amministrazione, pur non avendo la qualifica di dipendenti pubblici, devono essere ricompresi nella tutela prevista per i *whistleblower*.

Al contrario, rientrano nei destinatari della procedura coloro che, in caso di trasferimento, comando, distacco (o situazioni analoghe) presso un'altra società o amministrazione, vengano a conoscenza di fatti accaduti e direttamente appresi nell'espletamento di mansioni presso un'amministrazione o società diversa da quella in cui presta servizio al momento della segnalazione. In tale ipotesi la segnalazione va inoltrata al Responsabile della Prevenzione della Corruzione e della Trasparenza dell'amministrazione alla quale si riferiscono i fatti o ad A.N.AC.

4.2 Destinatari della segnalazione.

La segnalazione deve essere inoltrata **esclusivamente** e, ad almeno uno, delle quattro tipologie di destinatari indicati al comma 1 dell'articolo 54-bis, e precisamente:

1. Responsabile della Prevenzione della Prevenzione della Corruzione e della Trasparenza della Società (in seguito R.P.C.T.);
2. Autorità Giudiziaria ordinaria;
3. Autorità Giudiziaria contabile;
4. Autorità Nazionale Anti Corruzione (A.N.AC.) accedendo al sito web istituzionale della stessa o cliccando alla pagina dedicata Whistleblowing (https://www.anticorruzione.it/-/whistleblowing).

Si precisa che:

1. la segnalazione, se indirizzata al R.P.C.T. deve essere inviata esclusivamente mediante la piattaforma informatica messa a disposizione della Società al link di cui al paragrafo *10 – La Piattaforma per le Segnalazioni;*
2. nel caso in cui la segnalazione pervenga ad un soggetto diverso (ad esempio superiore gerarchico, dirigente) è indispensabile che quest'ultimo indichi al segnalante che le segnalazioni volte ad ottenere la tutela del *whistleblower* devono essere rivolte al R.P.T.C. della Società utilizzando il sistema informatico messo a disposizione.

In questa sede si anticipa che per quanto riguarda le *"comunicazioni di misure ritorsive"* la norma prevede che le stesse siano trasmesse esclusivamente ad ANAC (articolo 54-*bis*, comma. 1).
Nel caso in cui la comunicazione di misure ritorsive pervenga al R.P.C.T. della Società lo stesso informerà il segnalante che la comunicazione deve essere inoltrata ad A.N.AC. al fine di ottenere le tutele previste.

Nel caso in cui le segnalazioni riguardino il R.P.T.C. della Società il segnalante dovrà rivolgersi direttamente ad A.N.AC: con le modalità indicate sul sito web istituzionale dell'Autorità alla pagina dedicata e poco sopra richiamata.

5. Caratteristiche delle Segnalazioni.

5.1 Le condotte illecite

Ai fini della disciplina in esame, occorre rifarsi ad un concetto di corruzione da intendersi in senso lato, in quanto comprensivo delle varie situazioni in cui si riscontri l'abuso da parte di un soggetto del potere a lui affidato al fine di ottenere vantaggi privati. Le situazioni che danno luogo alla procedura di segnalazione regolamentata con il presente atto sono quindi più ampie delle fattispecie penalmente rilevanti di cui agli articoli 318, 319 e 319-*ter* del Codice Penale e sono tali da comprendere non solo l'intera gamma dei delitti contro la pubblica amministrazione di cui al Libro Secondo Titolo II Capo I sempre del Codice Penale ma anche le situazioni in cui - a prescindere dalla rilevanza penale del fatto – nel corso dell'attività amministrativa, si riscontrino comportamenti impropri di un funzionario che, anche al fine di curare un interesse proprio o di terzi, assuma o concorra all'adozione di una decisione che devia dalla cura imparziale dell'interesse pubblico.

Si pensi, inoltre, a titolo meramente esemplificativo, ai casi di sprechi, nepotismo, ripetuto mancato rispetto dei tempi procedimentali, assunzioni non trasparenti, irregolarità contabili, false dichiarazioni, violazione delle norme ambientali e di sicurezza sul lavoro.

Si evidenzia, altresì, che a parere di A.N.AC. (sempre Linee Guida approvate con Delibera A.N.AC. 469/2021) possono formare oggetto di segnalazione attività illecite non ancora compiute ma che il *whistleblower* ritenga ragionevolmente possano accadere in presenza di elementi precisi e concordanti.

Da quanto sopra risulta evidente l'oggetto della segnalazione meritevole di tutela è ampio e comprende azioni od omissioni, commesse o tentate, che:

- costituiscono reato, per esempio, contro la Società e/o la Pubblica Amministrazione, contro la persona, contro il patrimonio;
- poste in essere in violazione del Modello di Organizzazione e Gestione adottato ai sensi del D.lgs. 231/2001, delle disposizioni del "Codice Etico" allegato al Modello citato, ovvero del "Codice di Comportamento del personale dipendente di Genova Parcheggi S.p.a.";
- suscettibili di arrecare un pregiudizio patrimoniale a danno di Genova Parcheggi S.p.a.;
- suscettibili di arrecare un pregiudizio all'immagine di Genova Parcheggi S.p.a.;
- suscettibili di arrecare pregiudizio ai dipendenti o ad altri soggetti.

5.2 Elementi caratteristici delle segnalazioni.

Nella segnalazione è necessario che risultino definite:

- le circostanze di tempo e di luogo in cui si è verificato il fatto oggetto della segnalazione;
- la descrizione del fatto;

- le generalità o altri elementi che consentano di identificare il soggetto cui attribuire i fatti segnalati.

A tal fine, sarà utile che il segnalante alleghi documenti che forniscano elementi di fondatezza dei fatti nonché l'indicazione di altri soggetti potenzialmente a conoscenza dei fatti. A questo scopo la società mette a disposizione la procedura informatica indicata, unitamente al link d'accesso, di cui al paragrafo *10 – La Piattaforma per le Segnalazioni* comprensiva di un questionario per il caricamento delle informazioni di dettaglio e dei documenti.

Non sono meritevoli di tutela le segnalazioni fondate su meri sospetti o così dette *"voci di corridoio"*, alle segnalazioni d'informazioni che sono di dominio pubblico.

Inoltre, il segnalante non dovrà utilizzare l'istituto in argomento per scopi meramente personali o per effettuare rivendicazioni o ritorsioni che rientrano nella più generale disciplina del rapporto di lavoro o dei rapporti con il superiore gerarchico o con i colleghi, per le quali occorre fare riferimento alla disciplina ed alle procedure di competenza di altri organismi o uffici.

5.3 Le Segnalazioni anonime.

La segnalazione anonima, vale a dire priva di elementi che consentano di identificarne l'autore, anche se recapitata con le modalità previste nel presente documento, non verrà presa in considerazione nell'ambito della procedura volta a tutelare il dipendente che segnala illeciti, ma verrà trattata alla stregua delle altre segnalazioni anonime e presa in considerazione per ulteriori verifiche solo se relativa a fatti di particolare gravità e con un contenuto che risulti adeguatamente dettagliato e circostanziato.

D'altra parte l'articolo. 54-*bis* non include nel proprio campo di applicazione le segnalazioni anonime e cioè quelle del soggetto che non fornisce le proprie generalità e che il R.P.C.T. non ha la possibilità di verificare se il segnalante rientri nelle figure indicate al paragrafo *4.1 – I Segnalanti.*

Tuttavia, se da una sommaria ricognizione delle informazioni presenti sulla segnalazione e dei relativi allegati R.P.C.T. riscontrasse una qualche interesse R.P.C.T. inviterà il segnalante a fornire le proprie generalità nelle forme e nei modi previsti dalla piattaforma informatica di cui al paragrafo *10 - La Piattaforma per le Segnalazioni* al fine di verificare se ricorrano i casi per le tutele di cui all'articolo 54-*bis*.

Identica modalità di trattamento sarà applicata a segnalazioni provenienti da cittadini, associazioni, organizzazioni estranei alle figure previste al paragrafo *4.1 – I Segnalanti.*

Resta comunque fermo il fatto che non saranno prese in considerazione segnalazioni pervenute al di fuori dalla piattaforma informatica di cui al paragrafo *10 - La Piattaforma per le Segnalazioni.*

6. Responsabilità del *Whisteblower*.

La presente procedura lascia impregiudicata la responsabilità penale, civile e disciplinare del segnalante nell'ipotesi di segnalazione calunniosa o diffamatoria ai sensi del codice penale.

Sono altresì fonte di responsabilità, in sede disciplinare e nelle altre competenti sedi, eventuali forme di abuso della presente procedura, quali per esempio le segnalazioni manifestamente opportunistiche e/o effettuate al solo scopo di danneggiare il denunciato o altri soggetti, e ogni altra ipotesi di utilizzo improprio o di intenzionale strumentalizzazione dell'istituto oggetto della presente procedura.

Nelle ipotesi di segnalazione nelle forme e nei limiti di cui agli articoli 54-*bis* D.lgs. 165/01 e 6 D.lgs. 231/01, il perseguimento dell'interesse all'integrità della Società, nonché alla prevenzione e alla repressione degli *"illeciti",* costituisce giusta causa di rivelazione di notizie coperte dall'obbligo di segreto di cui agli articoli 326, 622 e 623 del codice penale e all'articolo 2105 del codice civile.

La disposizione di cui al comma precedente non si applica nel caso in cui l'obbligo di segreto professionale gravi su chi sia venuto a conoscenza della notizia in ragione di un rapporto di consulenza professionale, o di assistenza con l'ente, l'impresa o la persona fisica interessata.

Quando notizie e documenti che sono comunicati all'organo deputato a riceverli siano oggetto di segreto aziendale, professionale o d'ufficio, costituisce violazione del relativo obbligo di segreto la rivelazione con modalità eccedenti rispetto alle finalità dell'eliminazione dell'illecito e, in particolare, la rivelazione al di fuori del canale di comunicazione specificatamente predisposto a tal fine.

7. Tutela del *Whistleblower* e relative condizionalità e limitazioni.

La legge 179/2017 riconosce al *whistleblower* di tre tipi di tutela:

- la tutela della riservatezza dell'identità del segnalante e della segnalazione;
- la tutela da eventuali misure ritorsive o discriminatorie eventualmente adottate dall'ente a causa della segnalazione effettuata;
- l'esclusione dalla responsabilità nel caso in cui il *whistleblower* (nei limiti previsti dall'articolo 3 della Legge 179/2017) sia in ambito pubblico (ex art. 54-*bis*, D.lgs. 165/2001) che privato (ex art. 6 D.lgs. 231/2001) sveli, per giusta causa, notizie coperte dall'obbligo di segreto d'ufficio, aziendale, professionale, scientifico o industriale (artt. 326, 622, 623 c.p.) ovvero violi l'obbligo di fedeltà (art. 2105 c.c.).

In questa sede sono approfondite le prime due tutele essendo la terza irrilevante per quanto attiene la Società. Pertanto, al fine di eventuali approfondimenti si rimanda al paragrafo *3.3 -La «giusta causa» di rivelazione di notizie coperte dall'obbligo di segreto* delle citate Linee Guida deliberate da A.N.AC. che, in ogni caso, sono parte integrante del presente documento.

7.1 Tutela della riservatezza.

L'identità del segnalante viene protetta in ogni contesto successivo alla segnalazione. Inoltre, al fine di garantire la riservatezza dell'identità, la stessa include la documentazione allegata alla segnalazione se da questa, anche indirettamente, si possa risalire all'identità del segnalante.

La violazione dell'obbligo di riservatezza è fonte di responsabilità disciplinare, fatte salve ulteriori forme di responsabilità previste dall'ordinamento.

Ne consegue che la segnalazione e la documentazione ad essa allegata è sottratta al diritto di accesso agli atti amministrativi previsto dagli articoli. 22 e seguenti della Legge 241/1990 *Nuove norme sul procedimento amministrativo* (comma 4, articolo. 54-*bis*, D.lgs. 165/2001). Inoltre A.N.AC. nelle proprie Linee Guida ritiene, altresì, che la segnalazione e relativa documentazione debbano essere escluse *dall'accesso civico generalizzato* di cui all'articolo 5 comma 2 del D.lgs. 33/2013.

Anche la normativa di protezione dei dati, e specificatamente l'articolo 2-undecies del D.lgs. 196/2003, stabilisce che, nell'ambito di una segnalazione *whistleblowing*, il soggetto segnalato, presunto autore dell'illecito, con riferimento ai propri dati personali trattati dalla Società, non può esercitare i diritti previsti dagli articoli da 15 a 22 del Regolamento(UE) n. 2016/67922.

In merito a quanto precisato nell'ultimo capoverso resta ferma la possibilità per il soggetto segnalato, presunto autore dell'illecito, di esercitare i propri diritti con le modalità previste dall'art. 160 d.lgs. n. 196/2003.

Nel caso in cui il R.P.T.C., trasmetta la segnalazione alle Autorità giudiziarie competenti, tutelando la riservatezza dell'identità del segnalante, evidenzierà che si tratta di una segnalazione pervenuta da un soggetto cui l'ordinamento riconosce la tutela della riservatezza ai sensi dell'art. 54-bis del d.lgs. 165 del 2001. Successivamente, nel caso in cui l'Autorità giudiziaria o contabile richiedesse tale identità il R.P.C.T. la fornirà previa notifica al segnalante.

La tutela della riservatezza del segnalante riguarda anche il corso dei procedimenti giudiziari e disciplinari. In particolare:

1. nell'ambito del procedimento penale, l'identità del segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 c.p.p. Tale disposizione prevede l'obbligo del segreto sugli atti compiuti nelle indagini preliminari «fino a quando l'imputato non ne possa avere conoscenza e, comunque, non oltre la chiusura delle indagini preliminari» (il cui relativo avviso è previsto dall'art. 415-bis c.p.p.)25;
2. nel procedimento dinanzi alla Corte dei Conti l'obbligo del segreto istruttorio è previsto sino alla chiusura della fase istruttoria. Dopo, l'identità del segnalante potrà essere svelata dall'autorità contabile al fine di essere utilizzata nel procedimento stesso (articolo. 67 D.lgs. 174/2016);
3. nel procedimento disciplinare attivato dall'amministrazione contro il presunto autore della condotta segnalata, l'identità del segnalante può essere rivelata solo dietro consenso di quest'ultimo. Nel caso in cui l'identità del segnalante risulti indispensabile

alla difesa del soggetto cui è stato contestato l'addebito disciplinare, la Società non potrà procedere con il procedimento disciplinare se il segnalante non acconsente espressamente alla rivelazione della propria identità. A tal proposito si ritiene utile riproporre l'ultimo periodo del comma 3 del più volte citato articolo 54-*bis.* Ovvero *"Nell'ambito del procedimento disciplinare l'identità del segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza di consenso del segnalante alla rivelazione della sua identità."*

Con riferimento al sopra indicato al punto (3) sopra indicato il R.P.C.T. comunicherà, al Dirigente Responsabile del Personale della Società mediante posta elettronica con *"richiesta di conferma di lettura",* in tempi successivi alla trasmissione all'Autorità competente, l'esistenza di una segnalazione *"di illecito" nonché informazioni o documenti, opportunamente filtrati per non disvelare alcuna notizia utile all'individuazione del segnalante.*

7.2 Condizioni per la tutela e limitazioni.

Per quanto attiene le condizioni di tutela previste dall'art. 54-*bis* nei confronti del segnalante si richiama, ampliando e precisando, quanto già evidenziato nel paragrafo *6 - Responsabilità del Whisteblower*, si ritiene utile sottolineare quanto segue:

1. le tutele previste dall'art. 54-*bis* nei confronti del segnalante cessano in caso di sentenza, anche non definitiva di primo grado, che accerti nei confronti dello stesso la responsabilità penale per i reati di calunnia o diffamazione o comunque per reati connessi alla denuncia, ovvero la sua responsabilità civile, per aver riferito informazioni false riportate intenzionalmente con dolo o colpa;
2. nel caso in cui la sentenza di primo grado, sfavorevole per il segnalante, non venga confermata nei successivi gradi di giudizio, sarà applicabile, sia pur tardivamente, la protezione del segnalante prevista dall'articolo. 54-*bis* per le eventuali ritorsioni subite a causa della segnalazione.
3. qualora il *whistleblower* si sia rivolto, oltre che all'amministrazione o ad ANAC, anche all'autorità giudiziaria, laddove il procedimento penale che si è instaurato in seguito alla sua denuncia venga archiviato, egli conserva comunque le tutele previste dall'art. 54-bis. Ciò in quanto l'archiviazione non comporta alcun accertamento della responsabilità penale del *whistleblower* per i reati di cui al comma. 9 dell'articolo. 54-*bis*;
4. con riferimento alla responsabilità civile di cui al comma. 9 ultimo periodo, resta fermo che il danno derivante da reato deve essere stato causato dal convenuto con dolo o colpa grave. La sussistenza della colpa lieve, benché fonte di responsabilità civile accertata dal giudice, non comporta il venir meno delle tutele di cui all'articolo 54-*bis.*

7.3 Divieto di discriminazione del Whislteblower.

Il più volte richiamato articolo 54-bis del D.lgs. 165/71 ai commi 1, 6 e 7 stabilisce che il *whistleblower* non possa essere sanzionato, demansionato, licenziato, trasferito, o sottoposto ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro.

È importante ribadire, innanzi tutto, che **se il *Whislteblower* ritiene di aver subito azioni discriminatorie deve segnalare il fatto ad A.N.AC** accedendo al sito web istituzionale della stessa o cliccando alla pagina dedicata Whistleblowing (https://www.anticorruzione.it/-/whistleblowing avendo cura di fornire riferimenti oggettivi dai quali sia possibile dedurre la consequenzialità tra segnalazione effettuata e lamentata ritorsione.

In questa sede si richiama come A.N.AC., dopo lunga dissertazione (vedere Parte Prima paragrafo *3.2 - Tutela da misure discriminatorie o ritorsive* della Delibera 469/2021), ritenga come la *"misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro"* si configuri non solo in atti e provvedimenti ma anche in comportamenti o omissioni posti in essere dalla Società nei confronti del dipendente/segnalante, volti a limitare e/o comprimere l'esercizio delle funzioni proprie del lavoratore in modo tale da disvelare un intento vessatorio o comunque da peggiorare la situazione lavorativa.

A tal proposito A.N.AC. ha ritenuto utile elencare possibili misure ritorsive riscontrate nella propria prassi come, ad esempio:

- irrogazione di sanzioni disciplinari ingiustificate;
- proposta di irrogazione di sanzioni disciplinari ingiustificate;
- graduale e progressivo svuotamento delle mansioni;
- pretesa di risultati impossibili da raggiungere nei modi e nei tempi indicati;
- valutazione della performance artatamente negativa;
- mancata ingiustificata attribuzione della progressione economica o congelamento della stessa;
- revoca ingiustificata di incarichi;
- ingiustificato mancato conferimento di incarichi con contestuale attribuzione ad altro soggetto;
- reiterato rigetto di richieste (ad es. ferie, congedi);
- mancata ingiustificata ammissione ad una procedura e/o mancata ingiustificata aggiudicazione di un appalto (ad esempio, nel caso di un'impresa individuale, già fornitrice della Società, ove è avvenuto il fatto segnalato, quando si tratta dei soggetti di cui all'art. 54-*bis*, comma 2, ultimo periodo);
- per i lavoratori e i collaboratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione pubblica le ritorsioni possono consistere in: ingiustificata risoluzione o ingiustificato annullamento del contratto di servizi, della licenza o del permesso, ingiustificata perdita di opportunità commerciali determinata dalla mancata ingiustificata ammissione ad una procedura e/o mancata ingiustificata aggiudicazione di un appalto (ad esempio, nel caso di un'impresa individuale, già

fornitrice della p.a., ove è avvenuto il fatto segnalato, quando si tratta dei soggetti di cui all'art 54-*bis*, comma2, ultimo periodo.

Si ritiene utile mettere l'accento sul fatto che:

- Il legislatore ha optato per un'inversione dell'onere probatorio stabilendo, al comma 7 dell'articolo. 54-*bis,* che nel caso in cui il segnalante dimostri di avere effettuato una segnalazione di illeciti e di aver subito, a causa della segnalazione, una misura ritorsiva o discriminatoria, l'onere della prova grava sulla persona che ha posto in essere tale misura. È quest'ultima, quindi, che è tenuta a dimostrare che l'azione intrapresa non è in alcun modo connessa alla segnalazione;
- Nel caso in cui l'Autorità accerti la natura ritorsiva di atti adottati dall'amministrazione o dall'ente, ne discende che questi sono nulli e A.N.AC. ne dichiara la nullità. In caso di licenziamento, al lavoratore spetta la reintegra nel posto di lavoro ai sensi dell'articolo 2 del D.lgs. 23/2015, n. 23. L'ordine di "reintegro" resta di esclusiva competenza della magistratura.

Qualora venga accertata, nell'ambito dell'istruttoria condotta dall'A.N.AC, l'adozione di misure discriminatorie, fermi restando gli altri profili di responsabilità, l'A.N.AC. applica al responsabile che ha adottato tale misura una sanzione amministrativa pecuniaria da 5.000 a 30.000 euro. Qualora venga accertata l'assenza di procedure per l'inoltro e la gestione delle segnalazioni ovvero l'adozione di procedure non conformi a quelle indicate nelle linee guida dell'A.N.AC., applica al responsabile la sanzione amministrativa pecuniaria da 10.000 a 50.000 euro. Qualora venga accertato il mancato svolgimento, da parte del responsabile, di attività di verifica e analisi delle segnalazioni ricevute, si applica al responsabile la sanzione amministrativa pecuniaria da 10.000 a 50.000 euro. L'A.N.AC. determina l'entità della sanzione tenuto conto delle dimensioni dell'ente cui si riferisce la segnalazione.

8. Ruolo del R.P.C.T.

La legge 179/2016 assegna al R.P.C.T. un ruolo fondamentale nella gestione delle segnalazioni. Il R.P.C.T., oltre a ricevere e prendere in carico le segnalazioni, pone in essere gli atti necessari a una prima "attività di verifica e di analisi delle segnalazioni ricevute", da ritenersi obbligatoria in base al comma 6 dell'art. 54-*bis*, pena le sanzioni pecuniarie dell'Autorità (commi 1 e 6, art. 54-*bis*).

Tale ruolo si esplica nell'esercizio di alcune funzioni che, con specifico riguardo alla gestione delle segnalazioni all'interno della Società ovviamente quando il segnalante abbia scelto di utilizzare il canale di inoltro della segnalazione implementato dalla medesima, sono attribuite dalla legge al R.P.C.T..

Il R.P.C.T. è pertanto il soggetto legittimato, per legge, a trattare i dati personali del segnalante e, eventualmente, e coincide con il *custode dell'identità*.

Dapprima, spetta al R.P.C.T. la valutazione in ordine alla sussistenza dei requisiti essenziali contenuti nel comma 1 dell'art. 54-*bis* per poter accordare al segnalante le tutele ivi previste, requisiti già evidenziati al paragrafo *4.1 –I Segnalanti.*

Per quanto attiene la valutazione dei requisiti della segnalazione e della successiva sussistenza di quanto rappresentato A.N.AC., nelle proprie Linee Guida di cui alla Delibera 469/2021 suggerisce che R.P.C.T. utilizzi gli stessi criteri dalla stessa Autorità nel proprio Regolamento e precisamente:

a) manifesta mancanza di interesse all'integrità della pubblica amministrazione;
b) manifesta incompetenza dell'Autorità sulle questioni segnalate;
c) manifesta infondatezza per l'assenza di elementi di fatto idonei a giustificare accertamenti;
d) manifesta insussistenza dei presupposti di legge per l'esercizio dei poteri di vigilanza dell'Autorità;
e) accertato contenuto generico della segnalazione di illecito tale da non consentire la comprensione dei fatti, ovvero segnalazione di illeciti corredata da documentazione non appropriata o inconferente;
f) produzione di sola documentazione in assenza della segnalazione di condotte illecite o irregolarità;
g) mancanza dei dati che costituiscono elementi essenziali della segnalazione di illeciti indicati al comma 2 dell'art. 8 del Regolamento sull'esercizio sanzionatorio (Delibera n. 690/2020).

Sempre R.P.C.T., nei casi di cui alle lettere c) e g) potrà richiedere al *whislteblower* informazioni e documenti integrativi tramite l'applicazione informatica adottata dalla Società e, una volta valutata l'ammissibilità avvia l'istruttoria sui fatti o sulle condotte segnalate.

A tal proposito si precisa che spetta a R.P.C.T. un'attività di *verifica ed analisi* e non di accertamento sull'effettivo accadimento di quanto segnalato.

Per lo svolgimento dell'istruttoria, il R.P.C.T. può avviare un dialogo con il *whistleblower*, chiedendo allo stesso chiarimenti, documenti e informazioni ulteriori, sempre tramite il canale della piattaforma informatica. Ove necessario, può anche acquisire atti e documenti da altri uffici della Società, avvalersi del loro supporto, coinvolgere terze persone tramite audizioni e altre richieste, avendo sempre cura che non sia compromessa la tutela della riservatezza del segnalante e del segnalato.

Se, a seguito dell'attività svolta, il R.P.C.T. ravvisa elementi di manifesta infondatezza della segnalazione, ne dispone l'archiviazione con adeguata motivazione comunicando ciò al *whislteblower;* al contrario, se ritiene la segnalazione presenti elementi di fondatezza rivolgerà agli organi interni e/o esterni ognuno secondo le proprie competenze.

Non spetta al R.P.C.T. accertare le responsabilità individuali qualunque natura esse abbiano, né svolgere controlli di legittimità o di merito su atti e provvedimenti adottati dalla Società a pena di sconfinare nelle competenze dei soggetti a ciò preposti all'interno della stessa ovvero della

magistratura. Ciò in linea con le indicazioni già fornite nella Delibera ANAC n. 840 del 2 ottobre 2018 concernente in generale i poteri del R.P.C.T..

9. Fasi della Procedura.

È possibile individuare due fasi nell'attività se svilupperà il Responsabile della Prevenzione della Corruzione e Trasparenza nell'esame della segnalazione.

La prima fase consiste nell'esame preliminare della segnalazione, esame che consiste nella verifica che la segnalazione stessa sia di interesse per la Società completa e ben definita ovvero non rientri nei casi indicati dalla lettera a) alla lettera g) elencati al paragrafo *8 - Ruolo del R.P.C.T.*

Sebbene A.N.AC., nelle proprie Linee Guida, preveda, per questo primo esame, un termine di 15 giorni lavorativi dal ricevimento della segnalazione, poiché il R.P.C.T. della Società ha altri incarichi che prevedono l'elaborazione e la trasmissione di informazioni economiche verso i vertici della Società e all'Azionista tale termine è fissato in 45 giorni lavorativi sempre dal ricevimento della segnalazione.

La seconda fase si riferisce all'esame vero e proprio della documentazione pervenuta, compreso la richiesta di chiarimenti al *whistlebower* nonché con uffici e personale della Società, al termine della quale il R.P.C.T. procede all'archiviazione motivata della segnalazione o all'inoltro alle Autorità Competenti.

La presente procedura fissa il termine di 60 giorni lavorativi per la durata di questa istruttoria termine prorogabile di ulteriore 30 giorni in caso di necessità.

10. La Piattaforma per le Segnalazioni.

La Società, ha adottato una piattaforma informatica al fine di tutelare il *whistleblower* fin dall'inizio delle prime fasi della segnalazione.

La piattaforma utilizzata, per il caricamento della segnalazione, degli allegati e per il dialogo tra il R.P.C.T. ed il *whisteblower* è denominata *PAWhistleblowing* ed è fornita dalla società ISWEB-S.p.A. ed è utilizzata da numerose e primarie istituzioni e società dell'ambito pubblico.

La piattaforma risponde alle caratteristiche previste dalle Linee Guida di A.N.AC. di cui alla Delibera 469/2021.

In allegato è fornita documentazione sugli standard e misure di sicurezza sul prodotto.

Si ritiene utile riaffermare ai fini della tutela del *whisteblower* che lo stesso:

- rimuova riferimenti all'identità del segnalante dalla segnalazione e dai suoi allegati;

- utilizzi il canale informatico per tutte le comunicazioni successive da inviare all'Ente.

Il Responsabile della Prevenzione della Corruzione della Società prenderà in considerazione esclusivamente le segnalazioni pervenute attraverso la piattaforma informatica.

La piattaforma informatica è raggiungibile al seguente link:

https://genovaparcheggi.pawhistleblowing.it

Ancora una volta si evidenzia come le segnalazioni relative ad atti e comportamenti discriminatori nei confronti devono essere inoltrati dal *whisleblower* direttamente ad A.N.AC. accedendo al sito web istituzionale della stessa o cliccando alla pagina dedicata Whistleblowing (https://www.anticorruzione.it/-/whistleblowing

11. Riferimenti Normativi.

Legge 190/2012 - *Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione*

Decreto Legislativo 165/2001 - *Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche*

Decreto Legislativo 196/2003 - *Codice in materia di protezione dei dati personali*

Decreto Legislativo 175/2016 - *Testo unico in materia di società a partecipazione pubblica*

Legge 179/2017 - *Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato*

Decreto Legislativo – 231/2001 - *Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300*

Determinazione A.N.AC. 6/2015 - *Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d. whistleblower)*

Delibera A.N.AC. 1134/2017 - *Nuove linee guida per l'attuazione della normativa in materia di prevenzione della corruzione e trasparenza da parte delle società e degli enti di diritto privato controllati e partecipati dalle pubbliche amministrazioni e degli enti pubblici economici.*

Delibera A.N.AC. 840/2018 – *Compiti del Responsabile della Prevenzione della Corruzione e della Trasparenza*

Delibera A.N.AC. 690/2020 – *Regolamento per la gestione delle segnalazioni e per l'esercizio del potere sanzionatorio in materia di tutela degli autori di segnalazioni di illeciti o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro di cui all'articolo 54-bis del Decreto legislativo 165/2001*

Delibera A.N.AC. 469/2021 - *Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'articolo 54-bis, del D.lgs. 165/2001 (c.d. whistleblowing)*

12. Allegati.

Articolo 54-bis Decreto Legislativo 165/2001 *"Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche".*

ISWEB S.p.A. – *Caratteristiche PAWhistleBlowing*

ISWEB S.p.A - *Dichiarazione sulle misure di sicurezza applicate*

DECRETO LEGISLATIVO 30 marzo 2001 , n. 165

Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche.

Vigente al: 3-11-2021

Titolo IV
RAPPORTO DI LAVORO

Art. 54-bis.

(((Tutela del dipendente pubblico che segnala illeciti).))

((1. Il pubblico dipendente che, nell'interesse dell'integrita' della pubblica amministrazione, segnala al responsabile della prevenzione della corruzione e della trasparenza di cui all'articolo 1, comma 7, della legge 6 novembre 2012, n. 190, ovvero all'Autorita' nazionale anticorruzione (ANAC), o denuncia all'autorita' giudiziaria ordinaria o a quella contabile, condotte illecite di cui e' venuto a conoscenza in ragione del proprio rapporto di lavoro non puo' essere sanzionato, demansionato, licenziato, trasferito, o sottoposto ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro determinata dalla segnalazione. L'adozione di misure ritenute ritorsive, di cui al primo periodo, nei confronti del segnalante e' comunicata in ogni caso all'ANAC dall'interessato o dalle organizzazioni sindacali maggiormente rappresentative nell'amministrazione nella quale le stesse sono state poste in essere. L'ANAC informa il Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri o gli altri organismi di garanzia o di disciplina per le attivita' e gli eventuali provvedimenti di competenza.

2. Ai fini del presente articolo, per dipendente pubblico si intende il dipendente delle amministrazioni pubbliche di cui all'articolo 1, comma 2, ivi compreso il dipendente di cui all'articolo 3, il dipendente di un ente pubblico economico ovvero il dipendente di un ente di diritto privato sottoposto a controllo pubblico ai sensi dell'articolo 2359 del codice civile. La disciplina di cui al presente articolo si applica anche ai lavoratori e ai collaboratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione pubblica.

3. L'identita' del segnalante non puo' essere rivelata. Nell'ambito del procedimento penale, l'identita' del segnalante e' coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 del codice di procedura penale. Nell'ambito del procedimento dinanzi alla Corte dei conti, l'identita' del segnalante non puo' essere rivelata fino alla chiusura della fase istruttoria. Nell'ambito del procedimento disciplinare l'identita' del segnalante non puo' essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identita' del segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sara' utilizzabile ai fini del procedimento disciplinare solo in presenza di consenso del segnalante alla rivelazione della sua identita'.

4. La segnalazione e' sottratta all'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, e successive modificazioni.

5. L'ANAC, sentito il Garante per la protezione dei dati personali, adotta apposite linee guida relative alle procedure per la presentazione e la gestione delle segnalazioni. Le linee guida prevedono l'utilizzo di modalita' anche informatiche e promuovono il ricorso a strumenti di crittografia per garantire la riservatezza dell'identita' del segnalante e per il contenuto delle segnalazioni e della relativa documentazione.

6. Qualora venga accertata, nell'ambito dell'istruttoria condotta

dall'ANAC, l'adozione di misure discriminatorie da parte di una delle amministrazioni pubbliche o di uno degli enti di cui al comma 2, fermi restando gli altri profili di responsabilita', l'ANAC applica al responsabile che ha adottato tale misura una sanzione amministrativa pecuniaria da 5.000 a 30.000 euro. Qualora venga accertata l'assenza di procedure per l'inoltro e la gestione delle segnalazioni ovvero l'adozione di procedure non conformi a quelle di cui al comma 5, l'ANAC applica al responsabile la sanzione amministrativa pecuniaria da 10.000 a 50.000 euro. Qualora venga accertato il mancato svolgimento da parte del responsabile di attivita' di verifica e analisi delle segnalazioni ricevute, si applica al responsabile la sanzione amministrativa pecuniaria da 10.000 a 50.000 euro. L'ANAC determina l'entita' della sanzione tenuto conto delle dimensioni dell'amministrazione o dell'ente cui si riferisce la segnalazione.

7. E' a carico dell'amministrazione pubblica o dell'ente di cui al comma 2 dimostrare che le misure discriminatorie o ritorsive, adottate nei confronti del segnalante, sono motivate da ragioni estranee alla segnalazione stessa. Gli atti discriminatori o ritorsivi adottati dall'amministrazione o dall'ente sono nulli.

8. Il segnalante che sia licenziato a motivo della segnalazione e' reintegrato nel posto di lavoro ai sensi dell'articolo 2 del decreto legislativo 4 marzo 2015, n. 23.

9. Le tutele di cui al presente articolo non sono garantite nei casi in cui sia accertata, anche con sentenza di primo grado, la responsabilita' penale del segnalante per i reati di calunnia o diffamazione o comunque per reati commessi con la denuncia di cui al comma 1 ovvero la sua responsabilita' civile, per lo stesso titolo, nei casi di dolo o colpa grave)).

pawhistleblowing

le segnalazioni interne a norma di legge

Il servizio **certificato AgID** per la gestione delle **segnalazioni interne,**
sempre in linea con la normativa

15-09-2020 - PAWhistleBlowing - ISWEB - Caratteristiche

AGID Cloud Marketplace

isweb
www.isweb.it

ISWEB S.p.A.
Via Tiburtina Valeria Km. 112,500
67068 Cappelle dei Marsi (AQ)
Via Fiume Giallo 3 - 00144 Roma

ISO 9001-2015 - RINA
Sistema di gestione della
qualità certificato RINA
Certificato n° 14770/06/S

Numero Verde Gratuito
800 97 34 34

Indice

PREMESSA

Il presente documento di approfondimento è relativo ai servizi di avvio e manutenzione della soluzione applicativa denominata “PAWhistleBlowing”, nella sua versione dedicata al contesto pubblico.

PAWhistleBlowing è la soluzione applicativa dedicata alla gestione delle segnalazioni degli illeciti implementata da ISWEB sulla base del software Open Source Globaleaks, grazie all’esperienza acquisita in oltre 20 anni di collaborazione con la Pubblica Amministrazione e con le Aziende private nello specifico contesto della trasparenza amministrativa e del contrasto alla corruzione

PAWhistleblowing è la soluzione certificata dall’Agenzia per l’Italia Digitale (AgID) ed è disponibile in versione SaaS sul Cloud Marketplace, canale di approvvigionamento obbligatorio per la PA, al seguente indirizzo: https://cloud.italia.it/marketplace/service/548

La soluzione PAWhistleBlowing è implementata da ISWEB S.p.A., da 20 anni al servizio della Pubblica Amministrazione e delle Aziende Private nel processo di trasformazione digitale.

ISWEB S.p.A. annovera tra le centinaia di utilizzatori delle soluzioni dedicate al whistleblowing, anche la stessa **Agenzia per l’Italia Digitale (AgID, Presidenza del Consiglio dei Ministri)**, l’**Avvocatura dello Stato**, le società del **Gruppo MEDIASET**.

Come di consueto ISWEB S.p.A. garantisce la costante aderenza tecnica e normativa, garantendo tempestivi aggiornamenti rispetto all’evolversi della soluzione applicativa e del quadro legislativo di riferimento.

Caratteristiche PAWhistleblowing

In questa sezione del documento sono descritte le caratteristiche della soluzione applicativa PAWhistleblowing.

Caratteristiche generali

- ✓ **Certificato da AgID** e disponibile sul Marketplace tra le soluzioni SaaS, le uniche acquistabili dalla PA in ottemperanza alle "Linee Guida di acquisizione e riuso del software";
- ✓ Utilizzata da oltre 400 organizzazioni tra cui, **AgID, Avvocatura dello Stato, AGCom e il gruppo Mediaset;**
- ✓ Erogato da ISWEB SpA, che vanta oltre **20 anni di esperienza** e che serve oltre **800 organizzazioni**;
- ✓ **Basato su Globaleaks**, la piattaforma open source di riferimento a livello mondiale in ambito whistleblowing;
- ✓ Garantisce i **massimi livelli di sicurezza e riservatezza,** in un contesto applicativo progettato specificatamente per eccellere in termini di protezione del dato;
- ✓ Assicura la **compliance al GDPR** grazie ai principi di *privacy by design* e *configurable data retention policies*;
- ✓ Assicura il **massimo grado di tutela per tutti i soggetti coinvolti** nel processo di segnalazione e di gestione, offrendo strumenti e procedure di semplicissimo utilizzo, volte a garantire il corretto utilizzo del sistema nel rispetto della normativa;
- ✓ **Personalizzabile** nella struttura del modulo di segnalazione e nelle procedure di acquisizione e gestione delle informazioni;
- ✓ Garantito da **SLA di primo livello**, per offrire la massima raggiungibilità del servizio (nel rispetto del Codice dell'Amministrazione Digitale);
- ✓ **Assistita** da supporto tecnico e normativo dedicato su numero verde gratuito;
- ✓ Disponibilità dei **log di sistema**: garantisce la completa tracciabilità delle operazioni svolte sulla piattaforma;
- ✓ Possibilità di installazione e manutenzione su **server indicati dal Committente**;
- ✓ Possibilità di attivazioni o installazioni dedicate volte a soddisfare le **esigenze di unioni di enti**.

Personalizzazione del sistema

- ✓ Configurabilità dei **contenuti descrittivi e di supporto**,
- ✓ Personalizzazione del **modulo di segnalazione**, con possibilità di abilitare **moduli multipli**;
- ✓ Personalizzazione del **processo di acquisizione e gestione delle segnalazioni**;
- ✓ Possibilità di abilitare **diversi utenti gestori** delle segnalazioni;
- ✓ **Possibilità di acquisire anche segnalazioni anonime** integrabili successivamente dal segnalante con i propri dati anagrafici;
- ✓ Raggiungibilità dal **dominio scelto dall'ente**;

Caratteristiche ambiente di segnalazione

- ✓ Ambiente di **semplicissimo utilizzo**, realizzato come **webapp** basandosi sulle ultime tecnologie disponibili. Comportamento **responsive** sui vari dispositivi;
- ✓ Accesso all'interfaccia di monitoraggio della propria segnalazione mediante il "**codice segnalazione**", attribuito alla fine del processo di segnalazione;
- ✓ Se desiderato dall'ente offre la possibilità di inserire i **dati anagrafici anche successivamente all'invio della segnalazione**;
- ✓ Strumenti volti alla **comunicazione diretta tra il segnalante e il gestore delle segnalazioni** sempre disponibili anche successivamente all'invio della segnalazione;
- ✓ Piena rispondenza al modello del **W3C Accessible Rich Internet Applications (WAI-ARIA) 1.0** grazie all'utilizzo del modulo ngAria per comportamenti e funzioni avanzate dedicate all'accessibilità.

Caratteristiche ambiente di amministrazione

- ✓ **Semplicissima da utilizzare** in quanto caratterizzata da un ambiente di gestione di ultima generazione con molteplici strumenti e **funzionalità dedicate**, volte a guidare i responsabili durante la fase di gestione delle segnalazioni ricevute, al fine di garantire a questi ultimi il **massimo livello di protezione** in riferimento al rispetto del quadro normativo di riferimento;
- ✓ **Strumenti dedicati che supportano i responsabili nello svolgimento delle fasi più delicate** del processo di gestione della segnalazione, mettendolo al riparo da violazioni involontarie della norma;
- ✓ **Strumenti dedicati all'interazione con il segnalante;**
- ✓ Funzionalità specifiche dedicate al RPCT per la **visualizzazione dei dati del segnalante** e l'accoppiamento con la segnalazione;

- ✓ Possibilità di abilitare la procedura dedicata alla **visualizzazione dell'identità del segnalante** con eventuale delega della valutazione delle motivazioni di accesso al dato anagrafico (**Custode dell'identità**), in conformità a quanto previsto dalle linee guida ANAC;
- ✓ Continua **aderenza al quadro normativo** di riferimento;
- ✓ **Supporto normativo**;
- ✓ **Personalizzazione del modulo di segnalazione**;
- ✓ Possibilità di **gestire più organizzazione** con una unica attivazione;
- ✓ Sistema automatico di **scadenza della segnalazione** e relative notifiche, configurabile sulla base delle specifiche esigenze del committente.

Caratteristiche di sicurezza

La soluzione applicativa WhistleBlowing garantisce il massimo livello di protezione del dato in funzione della sua specifica infrastruttura applicativa, progettata per raggiungere questo specifico scopo.

Sicurezza applicativa

- ✓ **Privilegi ridotti:** a livello OS, l'ambiente viene eseguito con privilegi ridotti ed esclusivi all'ambito applicativo;
- ✓ **Firewall integrato**: la piattaforma dispone di un firewall integrato con regole estremamente rigide, che permettono l'utilizzo del servizio solamente nella configurazione scelta;
- ✓ **Session management OSWASP compliant:** la gestione delle sessioni sulla piattaforma segue le linee guida di sicurezza indicate da OWASP Session Management Cheat Sheet;
- ✓ **Validazioni input utente**: la piattaforma è basata su un approccio di validazione input dell'utente che viene verificato sia a livello client che a livello server seguendo regole estremamente rigide;
- ✓ **Prevenzione XSRF**: tutte le richieste gestite dalla piattaforma sono protette da un token XSRF;
- ✓ **Header avanzati per la sicurezza**: tutte le richieste vengono trattate con l'ausilio di header avanzati per la sicurezza applicativa, come Strict-Transport-Security e X-Content-Security-Policy;
- ✓ **HTTP Link Referrer Privacy**: al fine di garantire la privacy utente, sono state prese adeguate contromisure per l'accesso a risorse esterne dall'interno della piattaforma, integrando comportamenti di oscuramento del referrer applicativo;
- ✓ **Utilizzo di SSL**: l'utilizzo del servizio di whistleblowing può avvenire esclusivamente tramite Secure Sockets Layer;
- ✓ **Protezione da attacchi bruteforce**: la piattaforma utilizza meccanismi di ritardo automatico delle risposte dei propri servizi nel caso di un elevato numero di tentativi di accesso in intervalli temporali ridotti.

Sicurezza del dato

- ✓ **Crittografica PGP sui file differenziata per singolo amministratore abilitato**: con procedura di configurazione diretta e individuale da parte degli utenti amministratori senza necessità di intervento del reparto tecnico o degli amministratori di sistema;

- ✓ **UUIDv4 Casuale**: i dati relativi a segnalazioni, e file sono identificati attraverso l'assegnazione di identificativi assegnati in forma randomica (utilizzo di os.urandom) secondo lo standard UUID in versione 4;

- ✓ **Crittografia Password Amministratori**: tutte la password memorizzate nel database sono criptate attraverso funzione di derivazione script;

- ✓ **Eliminazione sicura dei dati:** per i dati che vengono eliminati dal sistema, la piattaforma utilizza metodi di cancellazione finalizzati a rendere impossibile il recupero dei dati;

- ✓ **TLS per notifiche SMTP**: per tutte le notifiche inviate attraverso SMTP viene utilizzato un canale cifrato TLS utilizzando SMTP/TLS o SMTPS a seconda della configurazione scelta.

Trasparenza e Anticorruzione: competenze ed esperienza ai vertici

Grazie alla collaborazione continuativa con centinaia di enti pubblici, ISWEB ha acquisto negli anni una specifica competenza nel contesto della Trasparenza e dell'Anticorruzione.
Nell'ambito della suite applicativa ePOLIS, dedicata alla PA, particolare riscontro hanno avuto le soluzioni dedicate a questo contesto. In particolare, la soluzione applicativa dedicata alla gestione degli obblighi derivanti dal D.lgs. 33/2013 e dalla L. 190/2012, in funzione delle sue particolari caratteristiche, è stata scelta dall'Agenzia per l'Italia Digitale (AgID) per la realizzazione del proprio portale della trasparenza (area "Amministrazione trasparente" del sito istituzionale), avvalendosi delle competenze tecniche e organizzative di ISWEB. L'AgID stessa ha ritenuto opportuno rendere disponibile a tutte le PA la soluzione applicativa, rendendola disponibile al riuso gratuito.
In questo contesto normativo è stato di recente rilasciato il Modulo Anticorruzione e la soluzione dedicata al Whistleblowing, descritta nel presente documento.

Contatti

ISWEB S.p.A.

Azienda certificata UNI EN ISO 9001:2008 - RINA
"Progettazione e sviluppo applicativi software per ambienti di rete"

Sede legale e factory:
via Tiburtina Valeria Km. 112,500 - 67068 - Cappelle dei Marsi (AQ)
Unità locale (commerciale):
via Fiume Giallo, 3 - 00144 - Roma

NUMERO VERDE
800.97.34.34

Tel. +39.0863.441163
Fax. +39.0863.444757

e-mail: info@isweb.it
pec: pec@pec.isweb.it
Sito web: http://www.isweb.it
Sito web Suite ePOLIS: http://www.smartpolis.it

Registro delle Imprese di L'Aquila
P.IVA, C.F. e numero d'iscrizione: 01722270665
Capitale Sociale euro 50.000,00 i.v.

Dichiarazione sulle misure di sicurezza applicate

Servizi ambito Whistleblowing

Ultimo aggiornamento 09/09/2020

www.isweb.it

ISWEB S.p.A.
Via Tiburtina Valeria Km. 112,500
67068 Cappelle dei Marsi (AQ)
Via Fiume Giallo 3 - 00144 Roma

ISO 9001-2015 - RINA
Sistema di gestione della
qualità certificato RINA
Certificato n° 14770/06/S

Numero Verde Gratuito
800 97 34 34

Indice

Premessa

Nell'erogazione dei propri servizi, ISWEB si impegna ad osservare le misure di sicurezza che seguono, anche ai sensi della Circolare AGID 18 aprile 2017, n. 2/2017, in quanto applicabili e indicate nel presente documento.

Sicurezza delle piattaforme software

Sviluppo

Il servizio Whistleblowing, è basato sul software opensource Globaleaks (*https://github.com/globaleaks/GlobaLeaks*), sviluppato secondo le line guida OWASP per lo sviluppo di applicazione sicure.
Per ogni approfondimento tecnico, è disponibile un'ampia documentazione sui principi di architettura e di security applicativa utilizzati per lo sviluppo del software, all'interno della documentazione di piattaforma disponibile all'indirizzo *https://docs.globaleaks.org/en/main/*

Verifiche periodiche di vulnerabilità

Il codice della piattaforma Globaleaks è periodicamente verificato dalla stessa community nel durante del ciclo di sviluppo, e dal reparto tecnico ISWEB all'interno delle procedure di upgrade dei servizi offerti.
Il repository della piattaforma rende disponibili anche la documentazione relativa a test di vulnerabilità svolti periodicamente e realizzati da organismi indipendenti.

Patch management

Le patch di sicurezza vengono applicate con tempestività sulla base dei rilasci ufficiali nel repository di piattaforma.
Le patch che non incidono sulla sicurezza vengono rilasciate secondo la calendarizzazione del reparto tecnico, con cadenza comunque mai superiore ad un semestre.

Sicurezza dell'accesso alle piattaforme software da parte di personale ISWEB

Tracciamento degli accessi utente e utenze

ISWEB individua specificamente i propri utenti e le relative utenze abilitate agli accessi alle piattaforme che trattano dati personali dei clienti in funzione degli specifici privilegi di accesso.
In particolare, sono individuati nominativamente gli amministratori di sistema, ai quali sono impartite specifiche istruzioni sul rispetto delle misure di sicurezza dirette a preservare confidenzialità, integrità e attendibilità dei dati ai quali hanno accesso.
Gli accessi sono configurati a livello applicativo in modo che gli utenti non possano alterare i log.

Formazione degli utenti

Gli utenti ricevono adeguata formazione in materia di sicurezza informatica e rispetto delle prescrizioni di cui alla normativa sulla protezione dei dati personali

Continuità operativa e disaster recovery

Ripristino attività a seguito di criticità della piattaforma

ISWEB utilizza i servizi di facility management di primari data-center italiani che prevedono politiche di backup e continuità operativa in grado di ripristinare la disponibilità dei dati e dei servizi entro 24 ore dalla criticità, salvi eventi di gravità tale da non consentire il rispetto del termine suindicato.

Ripristino attività a seguito di criticità dell'infrastruttura

Benché ISWEB si impegni al rispetto dei termini di cui al precedente paragrafo, in caso di criticità relativa all'infrastruttura di facility management i tempi di ripresa dell'erogazione dei servizi dipenderanno da quelli impiegati dal data-center per ritornare all'operatività.

Si precisa che soluzioni dedicate di DR sono disponibili su progetto.

Misure anti-intrusione

L'infrastruttura di facility management prevede la presenza di firewall e antivirus perimetrali.

Allegato 1 – Misure minime di sicurezza ICT-PA

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Tutte le risorse attive sono censite all'interno dei repository del reparto tecnico ISWEB sia con modalità manuali sia con modalità automatiche garantite dagli apparati di rete
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Tutte le risorse attive sono censite all'interno dei repository del reparto tecnico ISWEB sia con modalità manuali sia con modalità automatiche garantite dagli apparati di rete
1	2	1	S	Implementare il "logging" delle operazioni del server DHCP.	Il server DHCP effettua il log di ogni operazione all'interno della rete aziendale.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	I repository dei dispositivi sono aggiornati automaticamente ad ogni modifica
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Gli apparati di rete utilizzano modalità automatiche per il censimento dei dispositivi
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Gli apparati di rete che censiscono i dispositivi, memorizzano anche l'indirizzo IP sia nel caso di assegnazione dinamica sia nel caso di assegnazione statica.
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	L'inventario dei dispositivi è sempre formato da queste informazioni

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server,	Il reparto tecnico ISWEB mantiene un elenco dei software utilizzabili da ogni dispositivo

				workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	I sistemi sono monitorati automaticamente dai sistemi protezione software utilizzati e dal sistema operative stesso

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Tutti I dispositivi utilizzati applicano le configurazioni di sicurezza standard
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Tutti I dispositivi utilizzati applicano le configurazioni di sicurezza standard
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Nel caso di verifica di compromissione di un sistema o di un dispositivo, si procede con un completo ripristino e con l'applicazione delle configurazioni standard
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Tutte le immagini di installazione utilizzate sono sempre disponibili anche offline in repository locali o su supporti fisici
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	Tutte le operazioni che richiedono una gestione remota, sono sempre eseguite tramite canali sicuri come SSH, SFTP e HTTPS
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	Sono attivi servizi di monitoraggio continuo
3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	I servizi di monitoraggio producono alert e log
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del	Tutti I dispositivi utilizzano la verifica della firma digitale dei software

				sistema, delle variazioni dei permessi di file e cartelle.	tramite le funzionalità garantite dai produttori dei sistemi operativi utilizzati. Anche I software antivirus e firewall utilizzati nelle configurazioni standard effettuano un monitoraggio di questo tipo.

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	Le verifiche vengono svolte sia come procedura stessa del ciclo di sviluppo dell'applicativo Globaleaks, sia periodicamente dal nostro reparto tecnico con cadenza al massimo annuale. La piattaforma è inoltre periodicamente verificata anche da organismi indipendenti con periodicità stabilita dagli sviluppatori.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Le verifiche vengono svolte sia come procedura stessa del ciclo di sviluppo dell'applicativo Globaleaks, sia periodicamente dal nostro reparto tecnico con cadenza al massimo annuale. La piattaforma è inoltre periodicamente verificata anche da organismi indipendenti con periodicità stabilita dagli sviluppatori.
4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	Tutte le attività di verifica vengono svolte dal solo personale autorizzato e con strumenti validati ed autorizzati.
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente	I software utilizzati per le verifiche vengono continuamente aggiornati con modalità sia automatiche che manuali quando necessario.

				aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	I software utilizzati per le verifiche vengono continuamente aggiornati con modalità sia automatiche che manuali quando necessario.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Tutte le postazioni utilizzano le procedure di aggiornamento automatiche previste dal sistema operativo utilizzato. Per le componenti applicative del servizio, le modalità di aggiornamento possono variare in funzione dell'applicazione stessa.
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	Non sono utilizzati sistemi separate dalla rete.
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	Tutte le eventuali vulnerabilità software vengono verificate all'interno dei cicli di sviluppo del software e nelle attività di verifica interne
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	Il piano di gestione dei rischi, ed in generale lo scenario e la matrice degli utilizzatori sono stati definiti durante il design del software e vengono aggiornati sulla base di ogni modifica allo scenario (https://docs.globaleaks.org/en/main/security/index.html)

4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	Tutte le operazioni di patching e di upgrade dei software sono sempre associate alle eventuali vulnerabilità rilevate o alla segnalazione di bug.
4	9	1	S	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	Nel caso di vulnerabilità non risolvibili in tempi brevi, vengono sempre applicate misure alternative temporanee per la mitigazione della stessa fino alla risoluzione effettiva
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	Tutti I cili di sviluppo software e le relative verifiche vengono effettuate in ambienti di collaudo separati da quelli di produzione

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	Le utenze di amministrazione del servizio sono in disponibilità esclusiva al reparto tecnico ISWEB ed ai referenti individuati dal committente
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Tutti gli accessi utente, anche quelli non riusciti, vengono registrati nel log delle attività dell'applicazione e nei log di servizio. Si specifica che gli accessi amministrativi utilizzati dagli operatori ISWEB, non consentono la visualizzazione o gestione dei dati delle segnalazioni Whistleblowing, ma solo gli aspetti di configurazione dell'ambiente, utilizzati per la predisposizione dei requisiti funzionali richiesti dal committente.

5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	L'ambiente applicativo utilizza un Sistema ACL modulare per l'assegnazione dei permessi all'utente. Si specifica che gli accessi amministrativi utilizzati dagli operatori ISWEB, non consentono la visualizzazione o gestione dei dati delle segnalazioni Whistleblowing, ma solo gli aspetti di configurazione dell'ambiente, utilizzati per la predisposizione dei requisiti funzionali richiesti dal committente.
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Tutte le operazioni amministrative effettuate vengono registrate nel log delle attività dell'applicazione, che si occupa anche di registrare eventuali eccezioni o anomalie delle funzioni disponibili.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	L'ambiente applicativo dispone di una funzione dedicata alla gestione delle utenze amministrative.
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	Tutti i dispositivi vengono configurati in fase iniziale secondo gli utilizzi.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Tutte le operazioni amministrative effettuate vengono registrate nel log delle attività dell'applicazione.
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Tutti gli accessi utente, sia quelli tentati che quelli riusciti, vengono registrati nel log delle attività dell'applicazione
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	L'autenticazione a due fattori è supportata ed attivabile sul servizio Whistleblowing dietro richiesta da parte del committente.
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	L'autenticazione a due fattori è supportata ed attivabile sul servizio Whistleblowing. La piattaforma supporta inoltre ulteriori regole per la costruzione di password robuste.
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Le password vengono valutate in tre livelli: forte, accettabile, inutilizzabile. Una password forte deve essere

					formata da lettere maiuscole, lettere minuscole, numeri e simboli, essere lunga almeno 12 caratteri e includere una varietà di almeno 10 input diversi. Una password accettabile dovrebbe essere formata da almeno 3 input diversi su lettere maiuscole, lettere minuscole, numeri e simboli, contenere almeno 10 caratteri e includere una varietà di almeno 7 input diversi.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	La piattaforma richiede alle utenze un cambio password periodico (configurabile su richiesta)
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	L'ambiente applicativo controlla che ogni nuova password impostata non sia uguale a quella già utilizzata dall'utente
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	L'ambiente applicativo utilizza un Sistema ACL estremamente modulare per l'assegnazione dei permessi all'utente. Gli account sono sempre indipendenti sulla base dei relativi ACL.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Questo aspetto è gestito dal committente, tramite l'individuazione dei propri operatori e dei relativi account.
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	Gli accessi amministrativi a livello servizio vengono utilizzati esclusivamente quando strettamente necessario al tipo di operazioni. Le utenze di questo tipo sono assegnate esclusivamente all'operatore responsabile del servizio, ed eventualmente alle figure individuate come backup.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le password non sono mai memorizzate in chiaro sul sistema, ma vengono memorizzate con un hash costruito da un salt randomico a 128bit e l'algoritmo Argon2
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non vengono utilizzati certificati digitali

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	Tutte le postazioni utilizzate dispongono di software antivirus aggiornati automaticamente.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Tutte le postazioni utilizzate dispongono di software Firewall ed IPS aggiornati automaticamente con il sistema operativo. Sono anche presenti sistemi firewall hardware nella rete.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Gli operatori ISWEB utilizzano esclusivamente dispositivi autorizzati.
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	Tutte le postazioni ed i dispositivi consentiti sono configurati con funzionalità DEP e di controllo dell'account.
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	Le funzionalità sono incluse negli strumenti software antivirus e firewall utilizzati. In termini infrastrutturali, sono garantite dagli apparati e le policy infrastrutturali.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Le funzioni sono disabilitate di default nei software utilizzati
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Le funzioni sono disabilitate di default nei software utilizzati
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Le funzioni sono disabilitate nei servizi utilizzati
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Le funzioni sono disabilitate di default nei software utilizzati
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Le funzionalità sono incluse negli strumenti software antivirus e firewall utilizzati da ogni postazione utilizzata
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	Le funzioni sono incluse nei servizi utilizzati
8	9	2	M	Filtrare il contenuto del traffico web.	Le funzionalità sono incluse negli strumenti software antivirus e firewall utilizzati

8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	Le funzioni sono incluse nei servizi utilizzati e negli strumenti software antivirus e firewall utilizzati da ogni postazione
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Le funzionalità sono incluse negli strumenti software antivirus e firewall utilizzati

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Le funzionalità sono incluse nelle policy di business continuity. Inoltre le funzionalità di DR sono attivabili in modalità dedicata sul singolo progetto
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	Le informazioni riservate contenute dal servizio sono crittografate nativamente dall'ambiente applicativo.
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	I dati relativi ai backup non sono mai disponibili su servizi normalmente esposti

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	Nell'ambito del servizio Whistleblowing, l'analisi è stata effettuata già a monte del software design (https://docs.globaleaks.org/en/main/security/index.html)

13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Le funzionalità sono garantite dagli apparati firewall e dai software antivirus utilizzati.

Contatti

ISWEB S.p.A.

Azienda certificata UNI EN ISO 9001:2015 - RINA
"Progettazione e sviluppo applicativi software per ambienti di rete"

Sede legale e factory:
via Tiburtina Valeria Km. 112,500 - 67068 - Cappelle dei Marsi (AQ)
Unità locale (commerciale):
via Fiume Giallo, 3 - 00144 - Roma

NUMERO VERDE
800.97.34.34

Tel. +39.0863.441163
Fax. +39.0863.444757

e-mail: info@isweb.it
pec: pec@pec.isweb.it
Sito web: http://www.isweb.it

Registro delle Imprese di L'Aquila
P.IVA, C.F. e numero d'iscrizione: 01722270665