Informazioni sulla PIA

Nome della PIA
(COPY) DPIA Procedura Interna Whistleblowing

Nome autore
Comune di Esempio

Nome valutatore
Responsabile Protezione Dati

Nome validatore
Designato Interno Privacy

Data di creazione
06/10/2023

Nome del DPO/RPD
Dott. Simone Carmignani

Parere del DPO/RPD
Il trattamento non presenta eccessivi rischi per gli interessati e quindi può essere implementato.

Richiesta del parere degli interessati
Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati
Non è stati richiesto il parere agli interessati per l'alto numero dei soggetti potenzialmente interessati ma ne è stata data adeguata pubblicità tramite la pubblicazione dul sito web dell'Ente.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

In attuazione della Direttiva (UE) 2019/1937, è stato emanato il d.lgs. n. 24 del 10 marzo 2023 riguardante "la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali", il decreto è entrato in vigore il 30 marzo 2023 e le disposizioni ivi previste sono efficaci dal 15 luglio 2023, si applica ai soggetti del settore pubblico e del settore privato.

Gli enti tenuti a rispettare la disciplina. La protezione dei segnalanti prevista dal D.lgs. n. 24/2023, impone l'obbligo di predisporre canali di segnalazione a carico dei seguenti soggetti del settore pubblico:
• le amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165
• le autorità amministrative indipendenti di garanzia, vigilanza o regolazione
• gli enti pubblici economici, gli organismi di diritto pubblico di cui all'articolo 3, comma 1, lettera d), del decreto legislativo 18 aprile 2016, n. 50
• i concessionari di pubblico servizio, le società a controllo pubblico e le società in house, così come definite, rispettivamente, dall'articolo 2, comma 1, lettere m) e o), del decreto legislativo 19 agosto 2016, n. 175, anche se quotate.

Segnalazioni, cosa si può segnalare. Comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato e che consistono in:
• illeciti amministrativi, contabili, civili o penali;
• condotte illecite rilevanti ai sensi del decreto legislativo 231/2001, o violazioni dei modelli di organizzazione e gestione ivi previsti;
• illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali relativi ai seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;
• atti od omissioni che ledono gli interessi finanziari dell'Unione;
• atti od omissioni riguardanti il mercato interno;
• atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione.

Canali di segnalazione:
• interno (nell'ambito del contesto lavorativo);
• esterno (ANAC);
• divulgazione pubblica (tramite la stampa, mezzi elettronici o mezzi di diffusione in grado di raggiungere un numero elevato di persone);
• denuncia all'Autorità giudiziaria o contabile.

Quali sono le responsabilità connesse al trattamento?

Protezione dei dati personali:
• Il trattamento di dati personali relativi al ricevimento e alla gestione delle segnalazioni, sia nei canali interni che esterni, è effettuato dai soggetti del settore pubblico e privato, nonché da ANAC, in qualità di titolari del trattamento, nel rispetto dei princìpi europei e nazionali in materia di protezione di dati personali, fornendo idonee informazioni alle persone segnalanti e alle persone coinvolte nelle segnalazioni, nonché adottando misure appropriate a tutela dei diritti e delle libertà degli interessati.
• Inoltre, i diritti di cui agli articoli da 15 a 22 del regolamento (UE) 2016/679 possono essere esercitati nei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196.
• Le segnalazioni interne ed esterne e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui alla normativa europea e nazionale in materia di protezione di dati personali.

Ci sono standard applicabili al trattamento?

Al momento non sono contemplati standard da applicare direttamente al trattamento, esiste la procedura informatica prevista dall'ANAC per la segnalazione esterna di whistleblowing.

Valutazione : Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Operazioni informatizzate di trattamento di dati personali relative alla raccolta e conservazione dei dati necessari per la realizzazione dell'attività di whistleblowing, dati identificativi e di contatto dei referenti del Titolare, dati eventualmente contenuti nelle segnalazioni e in atti e documenti ad essa allegati, eventuali dati relativi a condanne penali e reati.

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Il ciclo di vita dei dati prevede i seguenti trattamenti acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione ed eventuale trasferimento a soggetti autorizzati.

Quali sono le risorse di supporto ai dati?

Operazioni informatizzate di trattamento di dati personali relative alla raccolta e conservazione dei dati necessari per la realizzazione dell'attività di whistleblowing, dati identificativi e di contatto dei referenti del Titolare, dati eventualmente contenuti nelle segnalazioni e in atti e documenti ad essa allegati, eventuali dati relativi a condanne penali e reati. Le attività previste sono:

• Attivazione della piattaforma dedicata;
• Configurazione della piattaforma;
• Fase d'uso della piattaforma con caricamento delle segnalazioni da parte dei segnalanti e accesso alle stesse da parte dei riceventi preposti;
• Fase di dismissione della piattaforma al termine del contratto e alla scadenza degli obblighi di legge per finalità amministrative e contabili con conseguente cancellazione sicura dei dati da parte del fornitore.

Il Responsabile esterno del trattamento è _____ che offre il Software di whistleblowing professionale dedicato, _____, pubblicato sul sito dell'Ente al link: _____

Valutazione : Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento dei dati personali nella procedura di segnalazione si svolge nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale. Garantisce al contempo il rispetto dei diritti delle persone giuridiche e di ogni altro Ente o associazione coinvolti nel trattamento.

Le segnalazioni devono essere effettuate nell'interesse pubblico o nell'interesse alla integrità dell'amministrazione pubblica o dell'ente privato, i motivi che hanno indotto la persona a segnalare, denunciare o divulgare pubblicamente sono irrilevanti ai fini della sua protezione.

Il trattamento dei dati personali si svolge nel pieno rispetto dei principi di liceità, finalità, limitazione pertinenza e proporzionalità, sanciti dal Codice Privacy novellato e dal Reg. UE2016/679.

In attuazione dei principi di liceità e finalità, il trattamento dei dati personali acquisiti mediante l'utilizzo della piattaforma dedicata è effettuato dall'Ente esclusivamente per lo svolgimento delle funzioni istituzionali assegnate per legge.

Il trattamento di dati personali relativi al ricevimento e alla gestione delle segnalazioni è effettuato dai soggetti del settore pubblico e privato, nonché da ANAC, in qualità di titolari del trattamento, nel rispetto dei princìpi europei e nazionali in materia di protezione di dati personali, fornendo idonee informazioni alle persone segnalanti e alle persone coinvolte nelle segnalazioni, nonché adottando misure appropriate a tutela dei diritti e delle libertà degli interessati.

Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Valutazione : Accettabile

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

I dati raccolti ed elaborati vengono lititati e minimizzati unicamente alle informazioni strettamente necessarie all'a realizzazione dell'attività prevista.

Valutazione : Accettabile

I dati sono esatti e aggiornati?

I dati vengono verificati per ogni procedura attivta e aggiornati all'occorrenza.

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

Le segnalazioni interne ed esterne e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui alla normativa europea e nazionale in materia di protezione di dati personali.

Valutazione : Accettabile

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

L'informativa breve specifica viene sempre resa a tutti gli utenti in modalità telematica, è disponibile sul sito web dell'Ente l'informativa estesa che illustra anche il trattamento dei cookie.

Valutazione : Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Essendo l'Ente una pubblica amministrazione che eroga servizi pubblici legalmente attribuiti e da corso ad adempimenti di legge non è tenuto all'acquisizione del consenso al trattamento dei dati, nei casi diversi in cui questo sia dovuto viene esplicitamente acquisito per iscritto.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

In relazione al trattamento dei dati personali l'interessato, dietro presentazione di apposita istanza, ha diritto:
a. Di ottenere la conferma dell'esistenza di trattamenti di dati che possono riguardarlo;
b. Di essere informato sugli estremi identificativi del titolare e del responsabile oltre che sulle finalità e le modalità del trattamento cui sono destinati i dati;
c. Di richiedere su richiesta avanzata prima dello spirare del termine massimo di conservazione del dato e di ottenere, senza ritardo e comunque non oltre 30 giorni dal responsabile designato:
• La conferma dell'esistenza o meno di dati personali che lo riguardano, nonché della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, delle modalità e delle finalità su cui si basa il trattamento;
• La cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati, valutate le preminenti esigenze di polizia giudiziaria e di indagine.
d. Di opporsi, in tutto o in parte, per motivi legittimi qualora sia possibile, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.
Le istanze di cui al presente articolo possono essere trasmesse al designato responsabile della procedura mediante il portale dedicato o anche lettera raccomandata o indirizzo di posta elettronica personale, nel caso di esito negativo alla istanza l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.
Possono essere adottate misure legislative intese a ritardare, limitare o escludere la comunicazione di informazioni all'interessato e per il tempo in cui ciò costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata al fine di:
1. Non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari;
2. Non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali;
3. Proteggere la sicurezza pubblica;
4. Proteggere la sicurezza nazionale;
5. Proteggere i diritti e le libertà altrui.
Inoltre, i diritti di cui agli articoli da 15 a 22 del regolamento (UE) 2016/679 possono essere esercitati nei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Per esercitare il diritto alla cancellazione, se possibile in ragione dell'obbligo dell'ente di conservazione delle informazioni, gli interessati possono contattare direttamente il designato responsabile della procedura mediante il portale dedicato, la posta elettronica certificata o anche lettera raccomandata, inviando una mail tarmite l'indirizzo di posta elettronica personale.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Per esercitare il diritto di limitazione o oppoesizione, se possibile, gli interessati possono contattare direttamente il titolare o il designato del trattamento dei dati recandosi direttamente presso l'ente, a mezzo raccomandata o posta elettronica certificata.

Valutazione : Accettabile

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Gli obblighi di ogni singolo responsabile del trattamento sono definiti nei contratti di appalto dei relativi servizi o con specifica comunicazione.
Il responsabile del trattamento che opera per conto del Titolare si impegna a informare lo stesso tempestivamente e controllare eventuali sub responsabili incaricati per lo svolgimento della procedura nel pieno rispetto della normativa vigente, in tema di protezione dei dati personali.

Valutazione : Accettabile

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

I dati non vengono trasferiti al di fuori dell'Unione Europea.

Valutazione : Accettabile

Rischi

Misure esistenti o pianificate

Crittografia

I dati relativi all'identità vengono sempre pseudonimizzati e trattati in maniera riservata unicamente dal personale strettamente necessario e a questo specificatamente autorizzato, a norma di leggevengono sempre resi anonimi se pubblicati o comunicati:
• L'identità del segnalante non può essere rivelata a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni;
• La protezione riguarda non solo il nominativo del segnalante ma anche tutti gli elementi della segnalazione dai quali si possa ricavare, anche indirettamente, l'identificazione del segnalante;
• La segnalazione è sottratta all'accesso agli atti amministrativi e al diritto di accesso civico generalizzato;
• La protezione della riservatezza è estesa all'identità delle persone coinvolte e delle persone menzionate nella segnalazione fino alla conclusione dei procedimenti avviati in ragione della segnalazione, nel rispetto delle medesime garanzie previste in favore della persona segnalante.
Il responsabile del trattamento dichiara che l'applicativo implementa uno specifico protocollo crittografico. Ogni informazione scambiata viene protetta. Ogni informazione circa le segnalazioni e i relativi metadati registrata dal sistema viene protetta con specifici sistemi di protezione digitale. Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento. I dati sono integralmente cifrati e conservati in backup remoto.

Valutazione : Accettabile

Controllo degli accessi logici

Ogni autorizzato utilizza una login e password univoca di accesso.

Valutazione : Accettabile

Tracciabilità

I flussi documentali avvengono esclusivamente tramite il sistema di comunicazione interno utilizzando il sofware gestionale specifico dedicato, lasciando traccia del flusso, tutte le comunicazioni ufficiali all'esterno dovute avvengono invece per mail istituzionale, pec o raccomandata.

Valutazione : Accettabile

Archiviazione

Ogni designato alla procedura controlla l'eventuale archiviazione dei dati gestiti dall'ufficio in una cartella non condivisa su una postazione informatica protetta da password, mentre gli archivi generali dell'ente sono conservati su un server remoto dedicato il cui accesso è limitato e controllato. Per quanto riguarda l'eventuale archiviazione cartacea questa avviene all'interno degli uffici che trattano i dati e viene garantito l'anonimato delle informazioni contenute, per quanto riguarda i particolari tipi di dati vengono previste delle misure di protezione ulteriori e specifiche come armadietti con chiusura a chiave o casseforti.

Valutazione : Accettabile

Sicurezza dei documenti cartacei

Normalmente non è prevista la produzione di documenti cartacei.

Valutazione : Accettabile

Minimizzazione dei dati

Vengono raccolti e conservati unicamente i dati necessari alla relaizzazione dell'attività prevista.

Valutazione : Accettabile

Vulnerabilità

Il responsabile del trattamento garantisce che l'applicativo e la relativa metodologia di fornitura sono sicure e adeguatamente protette, sono periodicamente soggetti ad audit di sicurezza indipendenti di ampio respiro su base almeno annuale.

Valutazione : Accettabile

Lotta contro il malware

Tutti i computer del personale di Whistleblowing e degli eventuali sub-responsabili nominati eseguono firewall e antivirus come da policy aziendale e il personale riceve continua e aggiornata formazione al passo con lo stato dell'arte in materia di lotta contro i malware. Parimenti le utenze del servizio di whistleblowing vengono sensibilizzate sulla tematica tramite formazione diretta o documentazione online.

Valutazione : Accettabile

Backup

I sistemi sono soggetti a backup remoto giornaliero con policy di data retention di 7 giorni necessari per finalità di disaster recovery.

Valutazione : Accettabile

Manutenzione

E' prevista manutenzione periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza. Per i server applicativi virtuali che realizzano il servizio di whistleblowing è prevista una modalità di manutenzione accessibile al solo personale autorizzato attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti. Per i sistemi che compongono l'infrastruttura fisica, di backup e firewall è prevista una modalità di manutenzione accessibile al solo personale autorizzato e del relativo fornitore attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti.

Valutazione : Accettabile

Sicurezza dei canali informatici

Tutte le connessioni sono protette.

Valutazione : Accettabile

Controllo degli accessi fisici

Gli accessi fisici agli uffici sono limitati e controllati.

Valutazione : Accettabile

Sicurezza dell'hardware

I datacenter del fornitore dispongono di un'infrastruttura dotata di controllo degli accessi, procedure di monitoraggio, sistema di allarme e barriere fisiche presidiate.

Valutazione : Accettabile

Prevenzione delle fonti di rischio

Gli uffici dell'ente risultano rispettare le previsioni normative in materia di salute e protezione sui luoghi di lavoro.

Valutazione : Accettabile

Politica di tutela della privacy

È stato regolarmente incaricato il responsabile della protezione dei dati e la nomina comunicata al garante sulla protezione dei dati.

Valutazione : Accettabile

Gestione dei rischi

Sono stati redatti e approvati i registri sul trattamento, la valutazione e l'impatto sui dati personali.

Valutazione : Accettabile

Gestione del personale

I dipendenti sono regolarmente invitati a partecipare alle giornate di aggiornamento e formazione, una volta che cessa il rapporto di lavoro vengono cambiati gli identificativi di accesso e le password.

Valutazione : Accettabile

Gestione dei terzi che accedono ai dati

I collaboratori e i partner esterni sono sottoposti alle stesse regole e controlli del personale dipendente per l'accesso ai dati.

Valutazione : Accettabile

Specifiche misure di sicurezza

Ai sensi di quanto previsto dall'articolo 24 del Reg. UE 2016/679, i dati personali acquisiti mediante l'utilizzo della piattaforma dedicata sono protetti da misure di sicurezza tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato e trattamento non consentito o non conforme alle finalità di cui all'articolo 3 del presente Regolamento.
Ai sensi dell'art. 29 c. 2 della Direttiva UE 2016/680 il Titolare del trattamento, previa valutazione dei rischi, mette in atto misure volte a:
- Vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento («controllo dell'accesso alle attrezzature»);
- Impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate («controllo dei supporti di dati»);
- Impedire che i dati personali siano inseriti senza autorizzazione e che i dati personali conservati siano visionati, modificati o cancellati senza autorizzazione («controllo della conservazione»);
- Impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati («controllo dell'utente»);
- Garantire che le persone autorizzate a usare un sistema di trattamento automatizzato abbiano accesso solo ai dati personali cui si riferisce la loro autorizzazione d'accesso («controllo dell'accesso ai dati»);
- Garantire la possibilità di verificare e accertare gli organismi ai quali siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione di dati («controllo della trasmissione»);

- Garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il momento della loro introduzione e la persona che l'ha effettuata («controllo dell'introduzione»);
- Impedire che i dati personali possano essere letti, copiati, modificati o cancellati in modo non autorizzato durante i trasferimenti di dati personali o il trasporto di supporti di dati («controllo del trasporto»);
- Garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati («recupero»);
- Garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati («affidabilità») e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema («integrità»).

Valutazione : Accettabile

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Impatto limitato, Impatto significativo

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Perdita di dati, uso improprio di dati, diffusione di dati riservati o sensibili.

Quali sono le fonti di rischio?

Fonti di rischio interne ed esterne anche non umane.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Tracciabilità, Archiviazione, Minimizzazione dei dati, Lotta contro il malware, Backup, Sicurezza dei canali informatici, Controllo degli accessi fisici, Sicurezza dell'hardware, Gestione del personale, Gestione dei terzi che accedono ai dati

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Importante, il rischio è trascurabile o limitato

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata, il rischio è trascurabile o limitato

Valutazione : Accettabile

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Impatto significativo

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Errore materiale, evento doloso o abuso di ufficio da parte degli addetti ai lavori, accesso ai dati da parte di soggetti esterni non competenti e non autorizzati.

Quali sono le fonti di rischio?

Fonti umane interne, fonti umane esterne, fonti non umane.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Tracciabilità, Archiviazione, Sicurezza dell'hardware, Controllo degli accessi fisici, Minimizzazione dei dati, Lotta contro il malware, Backup, Gestione del personale, Sicurezza dei canali informatici, Gestione dei terzi che accedono ai dati

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Importante, limitato o importante

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

Limitata, limitato

Valutazione : Accettabile

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Impatto significativo

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Errore materiale, evento doloso o abuso di ufficio da parte di addetti ai lavori, accesso ai dati da parte di soggetti esterni non competenti e non autorizzate.

Quali sono le fonti di rischio?

Fonti umane interne, fonti umane esterne, fonti non umane.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Tracciabilità, Archiviazione, Vulnerabilità, Lotta contro il malware, Backup, Manutenzione, Sicurezza dei canali informatici, Sicurezza dell'hardware, Prevenzione delle fonti di rischio, Controllo degli accessi fisici, Gestione dei rischi, Gestione del personale, Gestione dei terzi che accedono ai dati

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

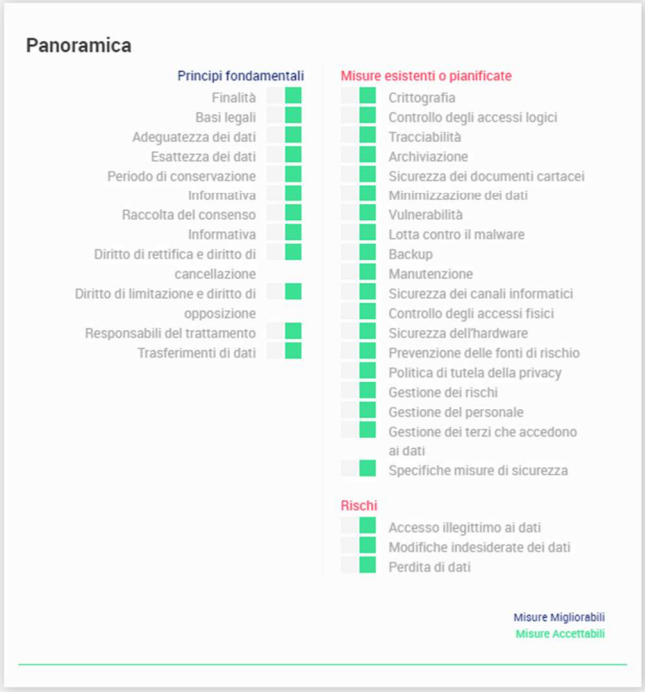
Importante, limitato o importante

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

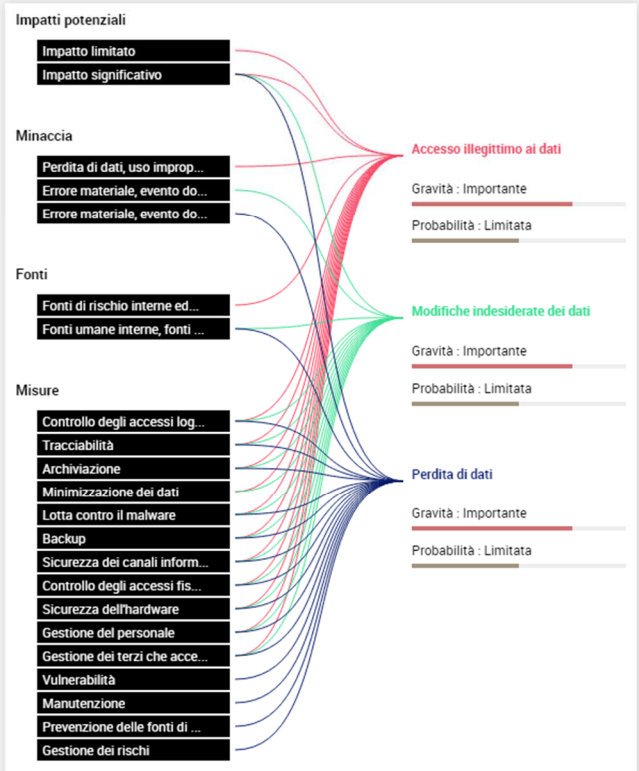
Limitata, trascurabile o limitato

Valutazione : Accettabile

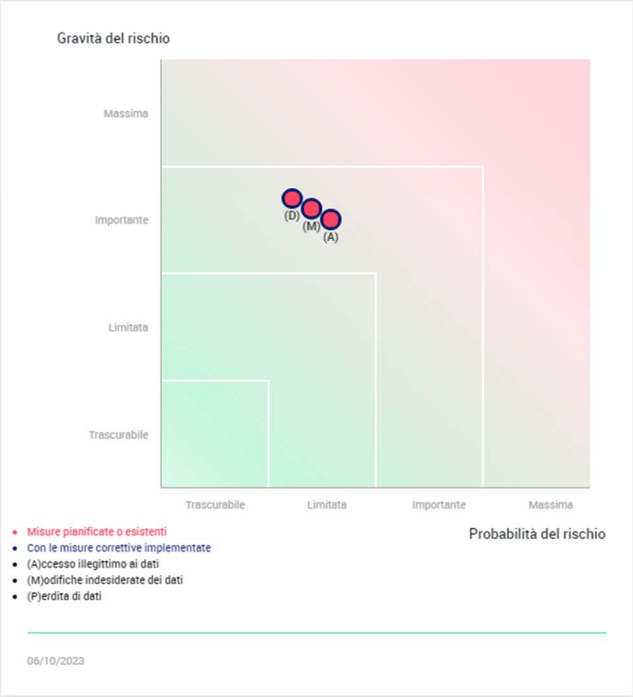
Piano d'azione



Panoramica dei rischi



Mappaggio dei rischi



- Misure pianificate o esistenti
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

06/10/2023