TO TRANSLATE - Preview

modifica pia

100%

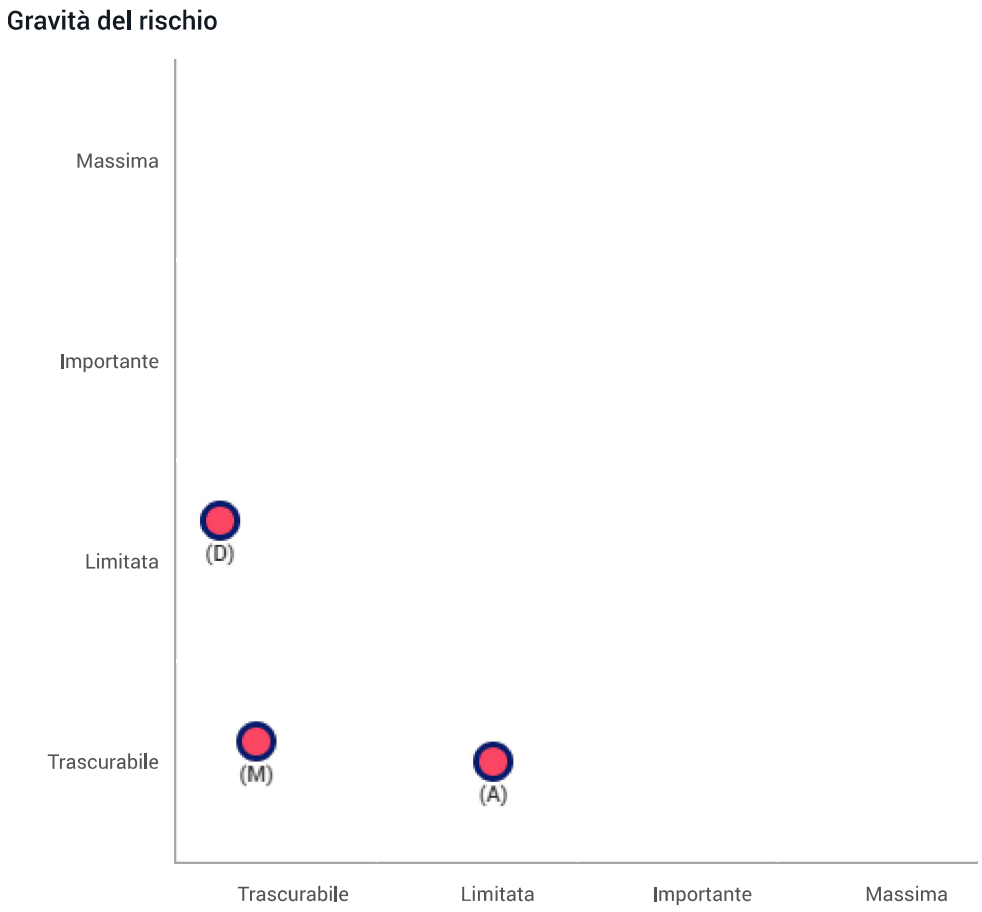
TO TRANSLATE - GENERAL INFORMATION

Anteprima

TO TRANSLATE - Editing :	Madrigali Nicola	**TO TRANSLATE - Status :**	Validata
TO TRANSLATE - Evaluation :	Madrigali Nicola		
TO TRANSLATE - Validation :	Madrigali Nicola		

TO TRANSLATE - Validation

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

07/08/23

TO TRANSLATE - Validation

Piano d'azione

Panoramica

Principi fondamentali

Finalità
Basi legali
Adeguatezza dei dati
Esattezza dei dati
Periodo di conservazione
Informativa
Raccolta del consenso
Diritto di accesso e diritto alla portabilità dei dati
Diritto di rettifica e diritto di cancellazione
Diritto di limitazione e diritto di opposizione
Responsabili del trattamento
Trasferimenti di dati

Misure esistenti o pianificate

Archiviazione
Controllo degli accessi logici
Crittografia
Politica di tutela della privacy
Gestione del personale

Rischi

Accesso illegittimo ai dati
Modifiche indesiderate dei dati
Perdita di dati

Misure Migliorabili
Misure Accettabili

Principi fondamentali

Nessun piano d'azione registrato.

Misure esistenti o pianificate

Nessun piano d'azione registrato.

Rischi

Nessun piano d'azione registrato.

TO TRANSLATE - Validation

TO TRANSLATE - DPO and data subjects opinion

Nome del DPO/RPD

Nicola Madrigali

Posizione del DPO/RPD

Il trattamento può essere implementato.

Parere del DPO/RPD

si, in quanto il rischio residuo è inferiore a quello intrinseco

Richiesta del parere degli interessati

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

non era necessario nello scenario in oggetto

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Il Comune di Casteggio (PV) si doterà di un sistema di WhistleBlowing.

Con il termine whistleblower si intende il dipendente pubblico che segnala illeciti nell' interesse generale, dei quali sia venuto a conoscenza in ragione del rapporto di lavoro, in base a quanto previsto dall'art. 54 bis del d.lgs. n. 165/2001 così come modificato dalla legge 30 novembre 2017, n. 179.

La Valutazione d'Impatto sulla Protezione dei Dati (di seguito "DPIA) è un processo che il Titolare del trattamento deve effettuare, in via preventiva, ogni qual volta un trattamento di dati personali, in particolare connesso all'impiego di nuove tecnologie, in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone.

Il processo di DPIA è ritenuto uno degli aspetti di maggiore rilevanza nel nuovo quadro normativo definito dal Regolamento Generale sulla Protezione dei Dati (Regolamento UE 2016/679), in quanto esprime chiaramente la responsabilizzazione (c.d. accountability) del titolare nei confronti dei trattamenti dallo stesso effettuati.

Il Titolare del trattamento, infatti, è tenuto non solo a garantire l'osservanza delle disposizioni regolamentari, quanto anche a dimostrare adeguatamente in che modo egli garantisca tale osservanza.

Whistleblowing Solutions, nel suo ruolo di Responsabile del trattamento per la gestione del sistema di whistleblowing, con il presente documento intende fornire tutti gli elementi ai Titolari per svolgere la valutazione di impatto così come previsto dall'art. 35 del Regolamento.

Quali sono le responsabilità connesse al trattamento?

Riservatezza

Ci sono standard applicabili al trattamento?

Si, procedure standard relative alla segnalazione di illeciti amministrativi protetti da riservatezza.

PA, Ente o Organizzazione > Titolare del trattamento
Whistleblowing Solutions > Responsabile del trattamento per la fornitura e la gestione del sistema di whistleblowing
Seeweb > Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la gestione dell'infrastruttura (IaaS)
Transaparency International Italia > Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la collaborazione nella gestione del sistema di whistleblowing

Conformità normativa:
- ISO27001 "Erogazione di Servizi SaaS di Whistleblowing Digitale su base GlobaLeaks"
- ISO27017 controlli di sicurezza sulle informazioni basati sulla per i servizi Cloud
- ISO27018 per la protezione dei dati personali nei servizi Public Cloud
- Qualifica AGID

● Certificazione CSA Star

Valutazione : Accettabile

Contesto

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 l'erogazione dei servizi in modalità SaaS così come pattuito tra le parti.

Dati di registrazione

Dati identificativi e di contatto dei referenti del Titolare che attivano il servizio di digital whistleblowing (es. Responsabile Anticorruzione).

Categorie particolari di dati

Dati eventualmente contenuti nelle segnalazioni e in atti e documenti ad essa allegati.

Dati relativi a condanne penali e reati

Dati eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati.

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

Ciclo di vita del trattamento e dei dati

1) Attivazione della piattaforma

2) Configurazione della piattaforma

3) Fase d'uso della piattaforma con caricamento delle segnalazioni da parte dei segnalanti e accesso alle stesse da parte dei riceventi preposti

4) 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

Policy di data retention di default delle segnalazioni di 18 mesi, prorogabili al doppio sulle singole segnalazioni per scelta precisa del soggetto ricevente, con cancellazione automatica sicura delle segnalazioni scadute.

Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio.

Quali sono le risorse di supporto ai dati?

Software di whistleblowing professionale GlobaLeaks

Infrastruttura IaaS e SaaS privata basata su tecnologie:

- Dettaglio Hardware

- VMWARE (virtualizzazione)

- Debian Linux LTS (sistema operativo)

- VEEAM (backup)

- OPNSENSE (firewall)

- OPENVPN (vpn)

Valutazione : Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il software di whistleblowing raccoglie segnalazioni secondo i migliori questionari predisposti in ambito di whistleblowing in collaborazione con importanti enti di ricerca in materia di whistleblowing e anticorruzione e messi a punto da Transparency International Italia in relazione alla normativa vigente in materia.

Nel rispetto del principio di privacy by design tutti i dispositivi utilizzati quali applicativo GlobaLeaks, log di sistema e firewall sono configurati per non registrare alcun tipo di log di informazioni lesive della privacy e dell'anonimato del segnalante quali per esempio indirizzi IP, User Agents e altri Metadata.

L'applicativo GlobaLeaks vede abilitata la possibilità di navigazione tramite Tor Browser per finalità accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.

Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Il Whistleblowing è un fondamentale strumento di compliance aziendale, tramite il quale i dipendenti oppure terze parti (per esempio un fornitore o un cliente) di un'azienda possono segnalare, in modo riservato e protetto, eventuali illeciti riscontrati durante la propria attività.

Nel contesto del whistleblowing, sono essenzialmente due le base giuridiche sulle quali si può fondare un trattamento dei dati personali: l'adempimento ad un obbligo legale, l'esecuzione di un compito di interesse pubblico e il perseguimento dell'interesse legittimo del titolare del trattamento.

L'articolo 54bis del D.Lgs. n. 165/2001 che impone l'istituzione di sistemi di whistleblowing da parte delle pubbliche amministrazioni per i tipi di illeciti in esso indicati sarà nella maggior parte dei casi la base giuridica del trattamento di dati nel contesto whistleblowing in ambito pubblico.

Già nel 2006, il Gruppo art 29 precisava così:

"L'istituzione di un sistema di segnalazione dovrebbe avere l'obiettivo di soddisfare un obbligo giuridico imposto dal diritto comunitario o degli Stati membri e, più specificamente, un obbligo giuridico destinato a stabilire procedure di controllo interno in settori ben definiti."[5]

Dello stesso parere sembrano essere il Garante nella sua decisione sopra citata a riguardo delle linee guide ANAC, così come il Garante francese per la protezione dei dati (CNIL) nelle sue linee guida relative al trattamento dei dati destinati all'attuazione di sistemi di segnalazione di illeciti in ambito professionale pubblicate nel 2019.

Nel settore privato, invece, non vi è nessun obbligo di istituire tali sistemi. La loro attuazione, infatti, non è altro che una delle possibilità per un'azienda di limitare la sua responsabilità per i reati commessi nel suo interesse dai suoi dipendenti.[6]

In questo caso, quindi, si potrebbe ricorrere al legittimo interesse del titolare. Quì ancora, il Gruppo 29 – e confermato dalla CNIL nelle sue linee guida 2019 – precisava:

"L'istituzione di sistemi di segnalazione può essere ritenuta necessaria ai fini di un interesse legittimo perseguito dal responsabile del trattamento o dalla terza parte a cui i dati vengono comunicati."[7]

Il D.Lgs. 231/2001, inoltre, prevede che i canali di whistleblowing sono istituiti per permettere di presentare segnalazioni di condotte illecite a tutela dell'integrità dell'ente.[8] Questo non sembra quindi rappresentare altro che la tutela degli interessi dell'azienda.

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)?

Per la registrazione e attivazione del servizio sono richiesti unicamente i seguenti dati: Nome, Cognome, Ruolo, Telefono, Email di ruolo dell'utente che effettua la registrazione e i dati relativi all'ente (nome, indirizzo, CF e PI).

Valutazione : Accettabile

I dati sono esatti e aggiornati?

Si

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

Il periodo massimo di conservazione è pari a 15 giorni dalla data di disattivazione.

Valutazione : Accettabile

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Informativa opportuna ex art.13 GDPR.

Valutazione : Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Il Decreto espressamente richiama al rispetto della disciplina in tema di protezione dei dati personali e sottolinea l'esigenza di perseguire il principio di minimizzazione dei dati trattati, uno dei cardini del

e sottolinea l'esigenza di perseguire il principio di minimizzazione dei dati trattati, uno dei cardini del GDPR. Ne emerge un rafforzato impianto normativo anche relativamente ai temi della tutela dell'identità della persona segnalante e della riservatezza quale strumento per incoraggiare il soggetto che viene a conoscenza di illeciti a trasmettere la relativa segnalazione

In particolare:

l'identità della persona segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale informazione non possono essere rivelate, senza il consenso espresso della stessa persona segnalante, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, espressamente autorizzate a trattare tali dati;

la documentazione inerente ciascuna segnalazione deve essere conservata per il tempo necessario e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione;

di ogni segnalazione resa oralmente (in colloqui oppure mediante linee telefoniche registrata o meno) va fatta trascrizione con il consenso della persona segnalante; questa deve anche poter leggere e approvare quanto trascritto;

la segnalazione e la documentazione allegata è sottratta al diritto di accesso ai documenti amministrati;

le segnalazioni non possano essere utilizzate per scopi diversi, ne rivelate a persone diverse da quelle specificamente competenti, autorizzate ed istruite in assenza del suo consenso espresso;

nell'ambito del procedimento penale, l'identità del segnalante è coperta da segreto ai sensi dell'articolo 329 c.p.p.; nel procedimento dinanzi alla magistratura contabile essa non può essere rivelata sino alla chiusura della fase istruttoria; nell'ambito del procedimento disciplinare, invece, l'identità del segnalante non può essere rivelata ove la contestazione dell'illecito disciplinare si fondi su accertamenti distinti e ulteriori rispetto alla segnalazione mentre occorre il consenso se la stessa sia indispensabile per la difesa dell'incolpato;

l'identità delle persone coinvolte e di quelle menzionate nella segnalazione è garantita sino alla conclusione dei relativi procedimenti, con il rispetto delle stesse garanzie accordate al segnalante;

la conservazione delle segnalazioni interne ed esterne e della relativa documentazione è consentita per il tempo necessario alla loro definizione e, comunque, per oltre 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione;

viene inoltre precisato che la registrazione delle segnalazioni (in caso di segnalazione effettuata oralmente, mediante linea telefonica o incontro con il personale addetto), previo consenso della persona segnalante, è documentata a cura del personale addetto mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto, mediante trascrizione integrale, oppure mediante verbale; e che in caso di trascrizione, la persona segnalante può verificare, rettificare o confermare il contenuto della trascrizione mediante la propria sottoscrizione.

Valutazione : Accettabile

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

Contattando direttamente il Titolare che comunica loro la mail personale.

Valutazione : Accettabile

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

Contattando direttamente il Titolare che comunica loro la mail personale.

Valutazione : Accettabile

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

Contattando direttamente il Titolare che comunica loro la mail personale.

Valutazione : Accettabile

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

Definiti chiaramente tramite lettera di incarico a responsabile Esterno, controfirmata e/o inviata via PEC.

Valutazione : Accettabile

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

Nessun trasferimento all'estero è previsto.

Valutazione : Accettabile

Rischi

Misure esistenti o pianificate

Archiviazione

L'applicativo GlobaLeaks implementa un database SQLite integrato acceduto tramite ORM.

Le configurazioni effettuate sono tali da garantire elevate garanzie di sicurezza grazie al completo controllo da parte dell'applicativo delle funzionalità sicurezza del database e delle policy di data retention e cancellazione sicura.

Valutazione : Accettabile

Controllo degli accessi logici

L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali.

Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password.

Il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo

Il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238.

Gli accessi privilegiati alle risorse amministrative sono protetti tramite accesso mediato via VPN.

Valutazione : Accettabile

Crittografia

Viene garantito il rispetto delle normative legate alla Privacy grazie all'elevato grado di security:

L'applicativo GlobaLeaks implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing in collaborazione con l'Open Technology Fund di Washington.

Ogni informazione scambiata viene protetta in transito da protocollo TLS 1.2= con SSLLabs rating A=.

Ogni informazione circa le segnalazioni e i relativi metadati registrata dal sistema viene protetta con chiave asimmetrica personale e protocollo a curve ellittiche per ciascun utente avente accesso al sistema e ai dati delle segnalazioni.

Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento

Il sistema è installato su sistema operativo Linux su cui è attiva Full Disk Encryption (FDE) a garanzia di maggiore tutela dei sistemi integralmente cifrati in condizione di fermo e in condizione di backup remoto.

Protocollo crittografico: https://docs.globaleaks.org/en/main/security/EncryptionProtocol.html

Valutazione : Accettabile

Politica di tutela della privacy

L'applicativo GlobaLeaks implementa un sistema di audit log sicuro e privacy preserving atto a registrare le attività effettuate dagli utenti e dal sistema in compatibilità con la massima confidenzialità richiesta dal processo di whistleblowing.

I log delle attività del segnalante sono privi delle informazioni identificative dei segnalanti quali indirizzi IP e User Agent.

I log degli accessi degli amministratori di sistema vengono registrati tramite moduli syslog e registri remoti centralizzati.

Valutazione : Accettabile

Gestione del personale

La formazione del personale addetto dovrà prevedere:
Formazione per gli operatori addetti che dovranno essere in grado di gestire tutte le funzionalità del sistema; Formazione su normative e regolamentazioni in merito all'utilizzo di sistemi di WB, con particolare riferimento al tema della Privacy e del trattamento dei dati; Formazione sulle funzionalità generali del sistema (overview) al management. In tale sede sarà fornito un set di documentazione tecnica comprendente manuali tecnici e utente.

Valutazione : Accettabile

Rischi

Accesso illegittimo ai dati

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

Comunicazioni non gradite da parte della concorrenza.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Data Breach da operatori interni e collaboratori.

Quali sono le fonti di rischio?

Chiavi USB e supporti rimovibili

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Archiviazione

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

Trascurabile, Tutti gli strumenti adottati sono sufficienti a garantire tale livello.

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

Limitata, Tutti gli strumenti adottati sono sufficienti a garantire tale livello.

Valutazione : Accettabile

Rischi

Modifiche indesiderate dei dati

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

Problemi legati alla comunicazione ed all'efficacia dei servizi.

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

Mancato controllo degli accessi da parte di collaboratori., Infiltrazione dall'esterno (poco probabile)

Quali sono le fonti di rischio?

Data breach da supporti rimovibili.

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

Archiviazione, Controllo degli accessi logici

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

Trascurabile, Tutti gli strumenti adottati sono sufficienti a garantire tale livello.

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

Trascurabile, Tutti gli strumenti adottati sono sufficienti a garantire tale livello.

Valutazione : Accettabile

Rischi
Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?
Impossibilità di finalizzare le forniture e le relative fatturazioni.

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?
Attacco hacker dall'esterno di tipo distruttivo (sabotaggio), Memorizzazione dei dati in un'unica copia.

Quali sono le fonti di rischio?
Negligenza interna e attacco esterno.

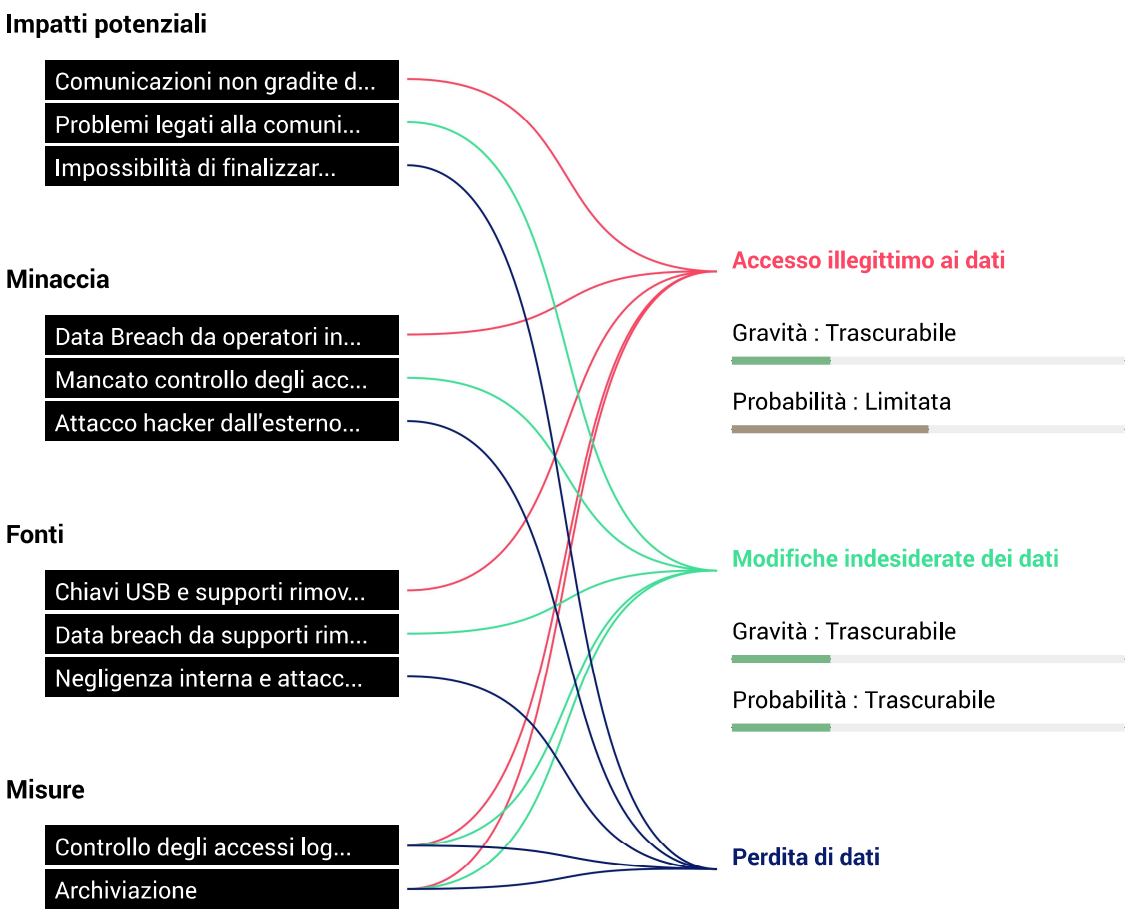
Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?
Archiviazione, Controllo degli accessi logici

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?
Limitata, Tutti gli strumenti adottati sono sufficienti a garantire tale livello.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?
Trascurabile, Tutti gli strumenti adottati sono sufficienti a garantire tale livello.

Valutazione : Accettabile

Rischi
Panoramica dei rischi



Gravità : Limitata

Probabilità : Trascurabile

Firmato digitalmente da: MADRIGALI NICOLA
Motivo: DPIA WhistleBlowing
Luogo: Bologna
Data: 07/08/2023 16:49:56