Valutazione d'impatto sulla protezione dei dati

Informazioni sulla PIA

Nome della valutazione di impatto: Videosorveglianza
Nome autore: dirigente scolastico
Nome valutatore: Mureddu, Mario
Nome validatore: Vargiu, Antonio
Data di creazione: 15/3/2021

Contesto

Panoramica del trattamento

Quale è la finalità del trattamento?

Questa DPIA è atta alla valutazione dell'impatto connesso all'uso della videosorveglianza negli edifici pubblici scolastici. I dati personali raccolti e trattati tramite il sistema di videosorveglianza sono le immagini di persone e cose che si trovino nel raggio di ripresa delle telecamere. Tali immagini sono trattate esclusivamente per il perseguimento delle finalità istituzionali dell'istituto e, in particolare, al fine di garantire la sicurezza e l'incolumità del personale scolastico, degli studenti e dei frequentatori degli spazi scolastici; nonché allo scopo di tutelare il patrimonio dell'istituto prevenendo e perseguendo il compimento di eventuali atti illeciti.

Quali sono i riferimenti normativi presi in considerazione?

Oltre al Regolamento 679/2016 e al D.Lgs 10 agosto 2018, n.101 nella redazione della presente valutazione di impatto sono state prese in considerazione:

- Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video emesse dal Comitato europeo per la protezione dei dati (EDPB)
- FAQ Videosorveglianza del Garante 3/12/2020

Quali sono le responsabilità connesse al trattamento?

La complessità delle azioni e dei possibili risvolti in termini di violazione della privacy implica una collaborazione fattiva tra le varie parti in causa. Queste sono, in particolare:

- **Il titolare del trattamento**, in questo caso la scuola di cui il Dirigente scolastico (DS) ne è il rappresentante legale. Essa ha il compito di definire un codice di condotta interno alla scuola che regoli l'utilizzo della videosorveglianza, e di supervisionare sulla sua attuazione.
- **Il Responsabile della Protezione dei Dati (RPD)** ha il compito di fornire supporto a titolare, docenti e interessati, per tutte quelle questioni concernenti la protezione dei dati personali all'interno dell'ambito di applicazione del trattamento.
- **I responsabili del trattamento.** Questi sono individuabili nella società esterna all'amministrazione scolastica che gestisce l'acquisizione la conservazione delle immagini e, ove è il caso, nell'amministrazione del comune nel quale ha sede la scuola, in quanto proprietario dell'immobile. Sarà necessario procedere alla nomina formale dei precedenti quali responsabili del trattamento ai sensi dell'Art. 28, comma 3 del GDPR.

- **Eventuali amministratori di sistema**: nominati dal DS quali responsabili del trattamento relativamente alla gestione dei sistemi informatici, collaborano con l'amministrazione da un punto di vista informatico.
- **Autorizzati al trattamento:** è il personale della scuola che è autorizzato dal DS ad effettuare dei trattamenti sui dati acquisiti con il sistema di videosorveglianza e che collaborano per tutte le necessità e le incombenze collegate alla corretta fruizione del servizio.

Ci sono standard applicabili al trattamento?
Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video emesse dal Comitato europeo per la protezione dei dati (EDPB)

Dati, processi e risorse di supporto

Quali sono i dati trattati?
I dati trattati sono immagini e registrazioni video, che si articolano principalmente in due categorie. La prima, raccoglie in sè tutte quelle immagini generiche dei soggetti che non ne permettono l'identificazione (ad esempio nel caso in cui il soggetto si trovasse di spalle rispetto alla telecamera) e che quindi non sono ascrivibili alla categoria "dati personali" ai sensi dell'Art. 4 comma 1 del GDPR. La seconda categoria invece, racchiude immagini e video nei quali è possibile riconoscere il soggetto ripreso dal circuito di videosorveglianza, che contengono quindi dati personali ai sensi dell'art. 4 comma 1 del GDPR. E' a questa seconda categoria che bisogna prestare particolare attenzione e per la quale è necessario ridurre al minimo la possibilità di rischi connessi alla protezione dei dati personali.

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?
Il sistema potrà essere utilizzato nelle sole aree interessate e negli orari di chiusura delle amministrazioni scolastiche. In caso di riprese esterne, si dovranno escludere dalla visuale le aree non pertinenti all'edificio. I dati andranno conservati in dispositivi adeguatamente protetti dal punto di vista informatico.

Quali sono le risorse di supporto ai dati?
Le immagini vengono caricate su dei server, locali e Cloud, che devono garantire le adeguate misure di sicurezza informatica per la protezione dei dati personali contenuti. L'azienda che si occupa dell'installazione, manutenzione e gestione dell'infrastruttura di sorveglianza deve essere nominata responsabile del trattamento ai sensi dell'Art. 28 del GDPR.

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?
Il trattamento oggetto di questa DPIA è l'utilizzo di circuiti di videosorveglianza all'interno e all'esterno degli edifici che ospitano le scuole pubbliche.
Il trattamento ha finalità di tutela delle persone e del patrimonio da atti criminosi.

Quali sono le basi legali che rendono lecito il trattamento?

Le basi giuridiche per i trattamenti operati sono:
- motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri (articolo 6, paragrafo 1, lettera e), del GDPR)
- legittimo interesse del titolare o di terzi (articolo 6, paragrafo 1, lettera f), del GDPR)

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 trattati devono rispettare il diritto alla riservatezza. A tal fine, come riportato nelle FAQ del Garante, il circuito di sorveglianza potrà essere utilizzato solo ai fini della tutela dell'edificio e dei beni scolastici. Per questo motivo, i circuiti potranno essere utilizzati nelle sole aree interessate e negli orari di chiusura delle amministrazioni scolastiche. In caso di riprese esterne, si dovranno escludere dalla visuale le aree non pertinenti all'edificio. Infine, non si potrà ricorrere alla videosorveglianza nelle ore di attività extrascolastiche che si svolgono all'interno della scuola.

Qual è il periodo di conservazione dei dati?

Per quanto riguarda il periodo di conservazione le FAQ del Garante specificano che le immagini registrate non possono essere conservate più a lungo di quanto necessario per le finalità per le quali sono acquisite. In base al principio di responsabilizzazione (art. 5, paragrafo 2, del Regolamento), spetta al titolare del trattamento individuare i tempi di conservazione delle immagini, tenuto conto del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche. Ciò salvo che specifiche norme di legge non prevedano espressamente determinati tempi di conservazione dei dati.

Se gli scopi della videosorveglianza sono la sicurezza e la protezione del patrimonio è possibile individuare eventuali danni entro uno o due giorni. Tenendo conto dei principi di minimizzazione dei dati e limitazione della conservazione, i dati personali dovrebbero essere cancellati dopo pochi giorni, preferibilmente tramite meccanismi automatici. Quanto più prolungato è il periodo di conservazione previsto (soprattutto se superiore a 72 ore), tanto più argomentata deve essere l'analisi riferita alla legittimità dello scopo e alla necessità della conservazione.

In considerazione di ciò suggeriamo di non prevedere tempi di conservazione delle registrazioni superiori alle 72 ore e di fissare tempi più ridotti se possibile (anche se periodi festivi più lunghi potrebbe comunque giustificare un periodo di conservazione più prolungato).

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati al trattamento in questione saranno informati precedentemente al trattamento stesso e tramite la cosiddetta "doppia informativa". Questa include un'informativa minima, unitamente al cartello contenente la dicitura "Area videosorvegliata", che viene posta all'accesso della zona videosorvegliata e contiene le informazioni più utili e immediate per l'interessato, quali le finalità del trattamento e l'indicazione del titolare dello stesso (utilizzare il modello di informativa minima previsto da *EDPB - Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - adottate il 29 gennaio 2020)*. L'informativa semplificata deve essere collocata prima del raggio di azione del circuito di sorveglianza e deve essere chiaramente visibile in ogni condizione ambientale diurna e notturna. L'informativa semplificata deve contenere l'indicazione alla versione completa dell'informativa (mettere URL di pubblicazione sul sito web della scuola).
L'informativa completa dovrà contenere l'identità e i dati di contatto del titolare del trattamento e del Responsabile Protezione Dati (RPD). Andranno poi indicate sia le finalità del trattamento che la

base giuridica dello stesso, nonché il periodo di conservazione dei dati. Dovrà essere inoltre presente il riferimento ai destinatari del trattamento (personale autorizzato ed eventuali soggetti esterni nominati responsabili del trattamento). Qualora i dati fossero trasferiti in verso paesi terzi o organizzazioni internazionali, bisognerà specificarlo nell'informativa completa. Parte fondamentale dell'informativa completa sono poi i diritti dell'interessato, esercitati senza formalità e devono essere ottemperati nella medesima forma della richiesta senza ingiustificato ritardo, nei limiti del periodo di conservazione degli stessi. Poiché l'informativa dovrà contenere il diritto al reclamo, è necessario inserire Autorità di Controllo e Sito Web (ad esempio, Garante Privacy - https://www.garanteprivacy.it).

Ove applicabile: come si ottiene il consenso degli interessati?

Non applicabile al presente trattamento perché la base legale del trattamento non è il consenso dell'interessato.

Come fanno gli interessati a esercitare i loro diritti di accesso?

Gli interessati potranno esercitare i loro diritti mediante apposita richiesta da inoltrare alla casella mail alic81200r@istruzione.it.

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

Nei casi relativi all'art. 17 GDPR, il titolare del trattamento dovrà procedere alla valutazione della richiesta di cancellazione di tali dati senza ingiustificato ritardo. In caso contrario, i dati seguiranno il ciclo di vita previsto dal trattamento.

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

Nei casi relativi all'art. 18 GDPR, il titolare del trattamento dovrà procedere alla valutazione della richiesta di limitazione di tali dati senza ingiustificato ritardo. In caso contrario, i dati seguiranno il ciclo di vita previsto dal trattamento. In ogni caso, sarà sempre necessario considerare i tempi di conservazione scelti dal titolare del trattamento (potrebbe essere impossibile procedere con l'esercizio di tale diritto). Per quanto riguarda il diritto all'opposizione, la scuola metterà a disposizione dell'interessato i dati di contatto dell'amministrazione stessa, tramite i quali esprimere la volontà all'esercizio del diritto all'opposizione a tale trattamento. Anche qui, vista la particolare tipologia di trattamento, potrebbe essere impossibile procedere con l'esercizio di tale diritto, poichè sarebbe impossibile definire eventuali regole di gestione dell'opposizione.

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

Ove intervengano nel trattamento dei dati soggetti esterni, il titolare del trattamento dovrà provvedere a nominarli responsabili del trattamento.
Nel contratto saranno esposti tutti gli aspetti previsti dall'art. 28 del GDPR: durata, ambito, finalità, istruzioni di trattamento documentate, autorizzazione preventiva qualora si ricorra a sub-responsabili del trattamento, fornitura di documentazione che dimostri la conformità al GDPR, notifica tempestiva di eventuali violazioni dei dati, ecc.

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

Ove fosse previsto che i servizi si appoggino su server posti al di fuori del territorio dell'Unione

Europea il titolare dovrà accertarsi che sia comunque garantito un livello di protezione equivalente a quello garantito dal GDPR.

Rischi

Misure esistenti o pianificate

Crittografia
I dispositivi di conservazione devono essere protetti con adeguate tecnologie di crittazione dei dati. Il trasferimento di dati all'interno del sistema di videosorveglianza deve avvenire tramite canali criptati.

Controllo degli accessi logici
L'accesso alle immagini conservate è reso disponibile solamente al personale autorizzato, adeguatamente formato. Devono essere implementate adeguate misure informatiche atte a garantire il controllo e monitoraggio degli accessi ai dati.

Tracciabilità
Le registrazioni devono contenere le informazioni riguardanti la data e l'ora esatta in cui sono avvenute. Gli accessi ai dati, oltre che contenere informazioni riguardanti l'identità dell'accedente, devono contenere informazioni riguardanti la data e l'ora di accesso.

Archiviazione
L'archiviazione deve avvenire esclusivamente su dispositivi criptati e il cui accesso è protetto da adeguate misure di sicurezza informatica. I dispositivi di archiviazione devono essere protetti da intrusioni malevole atte alla copia non autorizzata dei dati in essi contenuti.

Lotta contro il malware
I dispositivi che vengono utilizzati per l'accesso ai dati devono garantire un livello di sicurezza e protezione contro il malware adeguato, atto a minimizzare il rischio di violazioni dei dati personali.

Sicurezza dell'hardware
I dispositivi preposti alla gestione dei dati trattati devono garantire adeguati meccanismi di protezione anti-intrusione, sia fisici che software, e di controllo degli accessi virtuali.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali
La scuola deve essere dotata di un regolamento interno per la gestione delle violazioni di dati personali. L'autorizzato al trattamento ed il responsabile del trattamento (se nominato) sono obbligati a riferire al titolare qualunque violazione riconducibile ai dati trattati.

Accesso illegittimo ai dati

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

Le immagini conservate potrebbero essere oggetto di divulgazione non autorizzata, o di comportamenti collegati al fenomeno. I dati potrebbero essere cancellati, limitandone l'accesso agli stessi

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Bassi livelli di sicurezza informatica dei dispositivi di raccolta, trasmissione, conservazione e gestione dei dati, Errore umano.

Quali sono le fonti di rischio?

Persona esterna all'ente che accede in maniera intenzionale. Persona interna all'ente che accede in maniera accidentale o intenzionale.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Archiviazione, Lotta contro il malware, Sicurezza dell'hardware, Sicurezza dei canali informatici, Contratto con il responsabile del trattamento, Controllo degli accessi logici

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

Importante: L'accesso illegittimo ai dati potrebbe avere delle conseguenze di tipo psicologico quali grave disturbo psicologico (depressione, fobie), senso di violazione della privacy e di un danno irreparabile, esposizione a ricatti, cyberbullismo e molestie psicologiche, ecc.

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

Trascurabile: appare improbabile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti. Questi rischi includono il furto di supporti digitali conservati su dispositivi criptati, muniti di modalità di controllo logico degli accessi, intercettazione e decifrazione dei flussi di dati tra dispositivi di acquisizione e quelli di conservazione e gestione. Allo stesso modo, i dati potranno essere gestiti solamente da personale adeguatamente formato sui compiti e le responsabilità del trattamento, consapevole dell'attività di tracciamento degli accessi, e sotto la responsabilità del responsabile o del titolare del trattamento. Questo rende trascurabile la probabilità del rischio connessa ad un accesso non autorizzato, sia esso interno o esterno.

Modifiche indesiderate dei dati

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

I dati potrebbero essere modificati, portando ad una errata valutazione dei fatti accaduti durante la registrazione. I dati potrebbero essere resi inutilizzabili, parzialmente o in toto.

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

Accesso non autorizzato, Bassi livelli di sicurezza informatica dei dispositivi di raccolta, trasmissione, conservazione e gestione dei dati, Errore umano.

Quali sono le fonti di rischio?

Persona, interna o esterna all'organismo o all'ente, operante in via accidentale o intenzionale (esempio: amministratore IT, utente, attaccante esterno, concorrente), o fonte non umana (acqua, materiali pericolosi, virus informatici generici) che può essere all'origine di un rischio, virus informativi generici, atti di vandalismo nei confronti dei dispositivi fisici.

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

Crittografia, Controllo degli accessi logici, Tracciabilità, Archiviazione, Lotta contro il malware, Backup, Manutenzione, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Sicurezza dell'hardware, Gestire gli incidenti di sicurezza e le violazioni dei dati personali.

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

Limitata: Disturbo psicologico minore ma oggettivo, senso di violazione della privacy senza danni irreparabili, intimidazione sui social network ecc.

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

Trascurabile: Le misure di sicurezza informatica utilizzate, unitamente alle misure di controllo logico degli accessi e la protezione da malware, limitano la possibilità di accesso esterno ai dati conservati. L'utilizzo dei backup permette di verificare l'integrità dei dati. Le eventuali modifiche ai dati da personale interno potranno essere ugualmente tracciate tramite il controllo logico degli accessi.

Perdita di dati

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

Cancellazione di elementi probatori

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

Bassi livelli di sicurezza informatica dei dispositivi di raccolta, trasmissione, conservazione e gestione dei dati, Errore umano.

Quali sono le fonti di rischio?

Atti di vandalismo nei confronti dei dispositivi fisici, Persona interna all'amministrazione o all'azienda di gestione dei, Persona interna o esterna all'amministrazione o all'azienda di gestione del sistema di videosorveglianza che in via accidentale o intenzionale cancelli i dati, virus informativi generici, Distruzione o perdita dell'accesso ai dispositivi di conservazione.

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

Controllo degli accessi logici, Tracciabilità, Backup, Lotta contro il malware, Manutenzione, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Sicurezza dell'hardware.

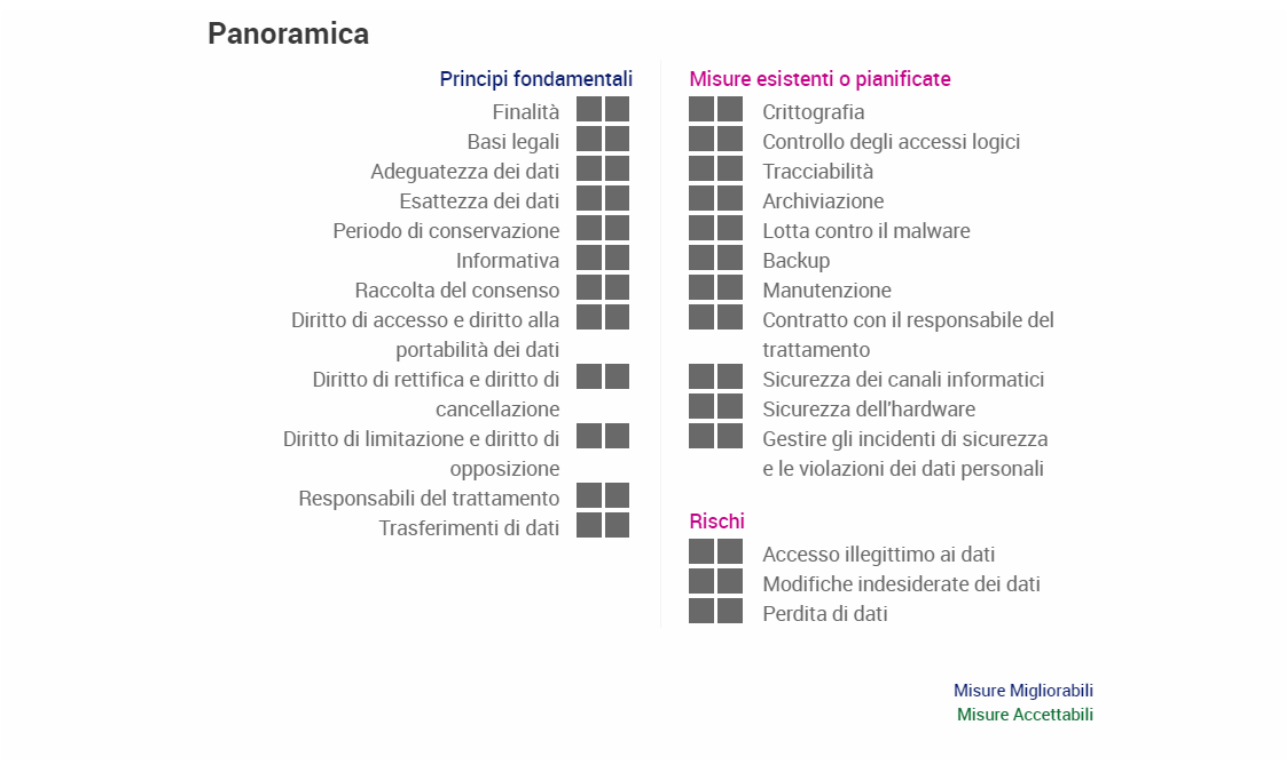
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Trascurabile: Non sono previsti rischi importanti per la libertà e i diritti delle persone fisiche.

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

Limitata: la limitazione dell'accesso a personale autorizzato, specificamente formato e informato delle policy di controllo degli accessi limita la probabilità di cancellazione accidentale o intenzionale dei dati.

Piano d'azione



Principi fondamentali

Nessun piano d'azione registrato.

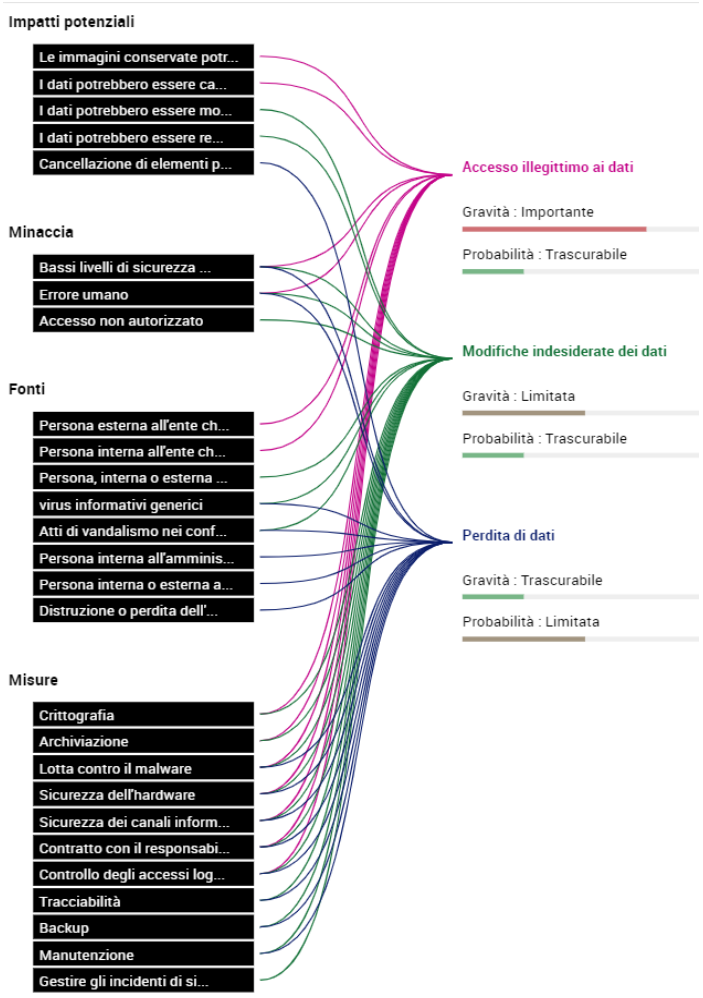
Misure esistenti o pianificate

Nessun piano d'azione registrato.

Rischi

Nessun piano d'azione registrato.

Panoramica dei rischi



Mappaggio dei rischi