DATA PROTECTION IMPACT ASSESSMENT

VIDEOSORVEGLIANZA

COMUNE DI LEGNANO

GESTIONE DEGLI ACCESSI ZTL & CORSIA PREFERENZIALE.

REVISIONE DEL DOCUMENTO:

	Ruolo	Nominativo	Data
Autori	Responsabile Ufficio Polizia Locale	Com. Dott. Daniele Ruggeri	19/03/2026
Revisore	Data Protection Officer	Trust Data Solutions Srl	20/03/2026
Validato	Rappresentante legale del titolare	Sindaco dott. Lorenzo Radice	20/03/2026
	Ruolo	Nominativo	Data

Elenco delle Revisioni:

Versione	Data emissione	Sintesi
Rev 1.0	20/03/2026	

Richiesta del parere degli interessati:

Non è stato richiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati:

La richiesta di un parere degli interessati non è stata considerata opportuna nel procedimento di valutazione del sistema di videosorveglianza comunale, dal momento che il Comune di Legnano ha deciso di realizzare il sistema di videosorveglianza sulla base di disposizioni di legge che ne permettono la realizzazione e sulla base di valutazioni effettuate in consiglio comunale, organo rappresentante dei cittadini, nonché in base a valutazioni effettuate dalla giunta comunale, organo di indirizzo politico e amministrativo dell'Ente. Tali organi comunali hanno valutato la necessità della predisposizione di un sistema di videosorveglianza per finalità di polizia amministrativa e stradale in ottemperanza a norma di legge che ne permettevano l'utilizzo.

SOMMARIO

PREMESSA E METODOLOGIA UTILIZZATA

PREMESSA

La Dpia (Data Protection Impact Assesment) è una procedura prevista dall'articolo 35 del Regolamento (UE) 2016/679. Serve a descrivere un trattamento di dati per valutarne la necessità, la proporzionalità e i relativi rischi, con l'obiettivo di stabilire misure idonee ad affrontare i rischi per i diritti e le libertà delle persone fisiche di cui si effettua il trattamento dei dati.
Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.

Il Regolamento fa riferimento all'obbligo del titolare di tenere conto dei rischi che i trattamenti possono comportare per i diritti e le libertà delle persone:

- Nell'art.24, indicando che il Titolare deve sempre essere in grado di dimostrare di aver adottato tutte le misure necessarie affinché il trattamento sia conforme al Regolamento;
- Nell'art.35, che prevede una specifica valutazione di impatto quando i trattamenti possono presentare rischi elevati per gli interessati, specifica i casi in cui è necessaria e procedimentalizza le modalità da seguire e gli elementi da tenere in considerazione. Prevede inoltre un ruolo rilevante delle Autorità di controllo;
- Nell'art.36 che stabilisce la consultazione preventiva obbligatoria dell'Autorità di controllo quando il titolare ritiene che i trattamenti richiedano misure specifiche per attenuarne i rischi.

Per ogni trattamento è quindi necessario effettuare un'analisi dei rischi (art.24) per decidere se il rischio per i cittadini sia elevato e quindi se è necessario procedere con una valutazione di impatto (art. 35) per individuare le misure specifiche da adottare per minimizzare il rischio. Se del caso, successivamente procedere con una consultazione preventiva dell'Autorità di controllo.
Le linee guida del WP29 forniscono preziose indicazioni su come va effettuata una DPIA:

- L'analisi dei rischi va fatta prima che il trattamento inizi e rispetto a ciascun singolo trattamento;
- Deve essere prestata attenzione anche alle componenti tecnologiche utilizzate;
- Deve tenere conto dei casi di cui all'art. 35 e delle specifiche indicate ai punti 71, 75 e 91 dei Considerando;
- Deve essere svolta con una metodologia che tenga conto dei criteri e degli elementi indicati.

Se al termine dell'analisi il titolare, sentito il DPO, ritiene che non sussistano rischi elevati può limitarsi a dare applicazione a quanto richiesto dall'art. 24. Tuttavia deve comunque giustificare per iscritto le valutazioni fatte e tenere un registro dei trattamenti svolti.
Quando invece risultino rischi elevati, il titolare deve adottare misure tecniche adeguate a minimizzare il rischio. Spetta al titolare individuarle, sentito il DPO. Può anche consultare gli interessati o i loro rappresentanti.
È bene anche indicare nel documento della DPIA i soggetti che hanno svolto l'analisi e individuato le misure necessarie.
Le linee guida fissano i criteri da seguire per individuare le misure idonee a diminuire i rischi, distinguendo tra quelle finalizzate a ridurre il rischio e quelle a dimostrare la conformità con il Regolamento.
La consultazione preventiva dell'Autorità di controllo è necessaria solo quando il titolare non riesce a individuare misure sufficienti per ridurre i rischi a un livello accettabile.

- L'applicazione del Regolamento si basa sul principio di accountability, che pone l'accento sulla "responsabilizzazione" di titolari e responsabili nell'adozione di misure proattive per assicurare l'applicazione del regolamento;
- Il Regolamento non richiede una valutazione d'impatto per ciascun trattamento che può presentare rischi, ma solo qualora possa presentare un "rischio elevato";
- Il WP29 raccomanda comunque di effettuare la DPIA in tutti i casi in cui non è chiaro se sia richiesta, in quanto è uno strumento utile per rispettare la legge;
- L'articolo 35 del Regolamento fornisce esempi di casi nei quali un trattamento "possa presentare rischi elevati", tra cui la sorveglianza sistematica su larga scala di una zona accessibile al pubblico;
- Il Garante italiano ha chiarito che quando un trattamento può comportare un rischio elevato (ad es. per monitoraggio sistematico, gran numero di soggetti, dati sensibili), il Regolamento obbliga a svolgere una valutazione di impatto prima di iniziarlo. Ciò esprime la responsabilizzazione dei titolari;
- Le linee guida del WP29 precisano quando una valutazione di impatto è obbligatoria, oltre ai casi espressamente indicati dal Regolamento, e quando non è richiesta. Indicano che costituisce una buona prassi al di là dei requisiti di legge, permettendo di realizzare la protezione dei dati fin dalla progettazione di qualsiasi trattamento.

I criteri specifici individuati dal WP29 per determinare quando la DPIA è obbligatoria includono:

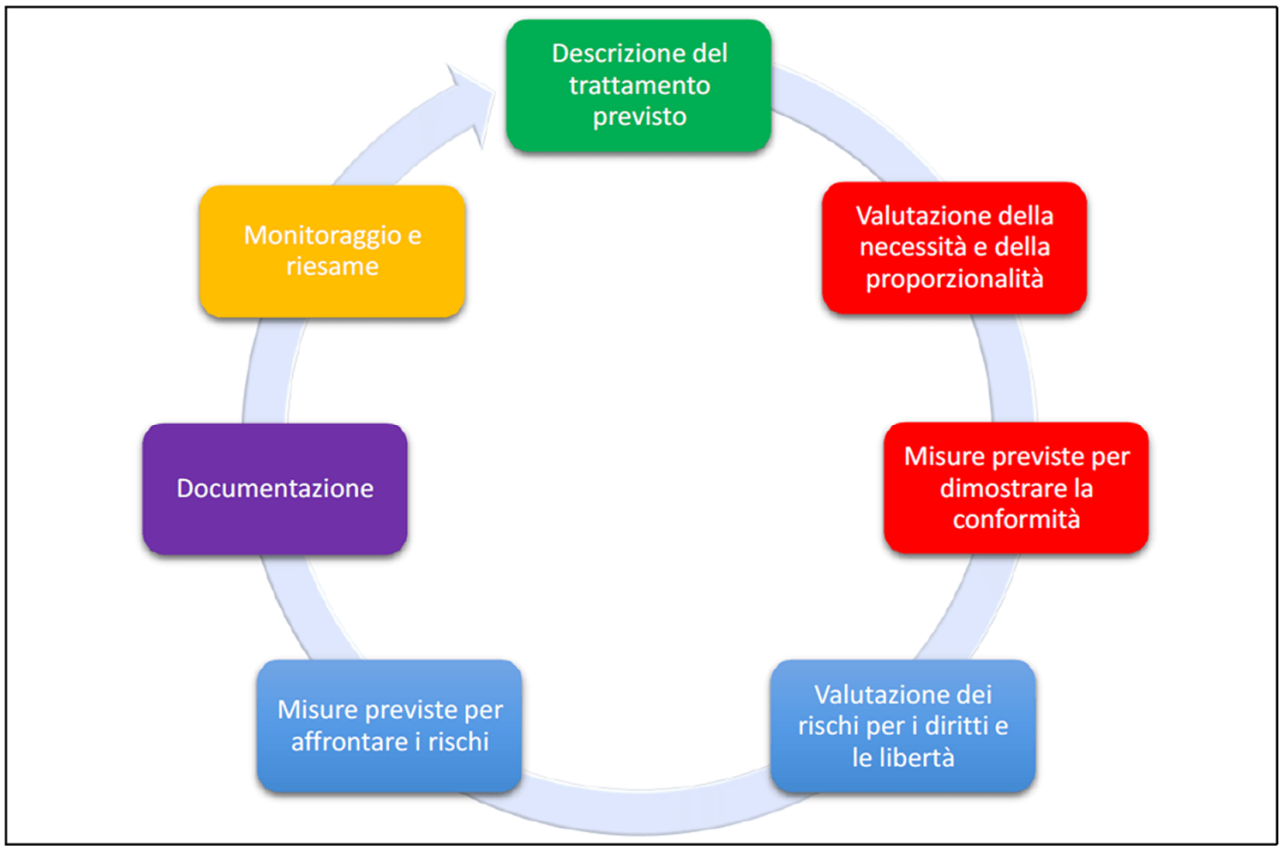
- Monitoraggio sistematico (es: videosorveglianza), specie su larga scala di zone accessibili al pubblico;
- Dati sensibili o dati aventi carattere altamente personale;
- Trattamenti di dati personali su larga scala;
- Dati relativi a interessati vulnerabili.

La DPIA è necessaria in presenza di almeno due di questi criteri, ma il titolare può decidere di condurla anche se ne ricorre solo uno.
Alla luce di quanto disposto dal Regolamento e chiarito dal Garante italiano e dal WP29, è da ritenersi necessario effettuare una DPIA circa il rischio elevato per i diritti e le libertà delle persone che può presentare l'adozione di un sistema di videosorveglianza comunale ai fini di sicurezza urbana.
Tale sistema infatti può realizzare una "sorveglianza sistematica su larga scala di una zona accessibile al pubblico" e quindi può definirsi un trattamento che "possa presentare rischi elevati ai sensi dell'articolo 35 del Regolamento".
Considerando i criteri del WP29, nel caso di un impianto di videosorveglianza comunale ai fini di sicurezza urbana sono rilevabili almeno due di questi criteri, potendosi compiere:

- Un monitoraggio sistematico;
- Di dati sensibili o dati aventi carattere altamente personale;
- Su larga scala;
- Che possono comprendere anche dati relativi a interessati vulnerabili;
- E che potrebbero comprendere utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

Il regolamento generale sulla protezione dei dati definisce le caratteristiche minime di una valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 7, e considerando 84 e 90):

- "una descrizione dei trattamenti previsti e delle finalità del trattamento";
- "una valutazione della necessità e proporzionalità dei trattamenti";
- "una valutazione dei rischi per i diritti e le libertà degli interessati";
- "le misure previste per
    - "affrontare i rischi";
    - "dimostrare la conformità al presente regolamento".



Nel valutare l'impatto di un trattamento va tenuto conto (articolo 35, paragrafo 8) del rispetto di un codice di condotta (articolo 40). Ciò può essere utile per dimostrare che sono state scelte o messe in atto misure adeguate, a condizione che il codice di condotta sia adeguato all'operazione di trattamento interessata. Devono essere presi in considerazione anche certificazioni, sigilli e marchi al fine di dimostrare la conformità rispetto al regolamento generale sulla protezione dei dati dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento (articolo 42), nonché rispetto alle norme vincolanti d'impresa.

Il considerando 90 del regolamento generale sulla protezione dei dati delinea una serie di elementi costituivi della valutazione d'impatto sulla protezione dei dati che si sovrappone a elementi ben definiti della gestione del rischio (ad esempio norma ISO 31000). In termini di gestione dei rischi, una valutazione d'impatto sulla protezione dei dati mira a "gestire i rischi" per i diritti e le libertà delle persone fisiche, utilizzando i seguenti processi:

- stabilendo il contesto: "tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio";
- valutando i rischi: "valutare la particolare probabilità e gravità del rischio";
- trattando i rischi: "attenuando tale rischio" e "assicurando la protezione dei dati personali", e "dimostrando la conformità al presente regolamento".

Si potrebbe ricorrere a metodologie diverse per contribuire all'attuazione dei requisiti essenziali stabiliti nel regolamento generale sulla protezione dei dati. Per quanto il titolare del trattamento abbia la possibilità di applicare approcci distinti, consentendo comunque di rispettare il regolamento

generale sulla protezione dei dati, sono stati individuati dei criteri comuni. Detti criteri possono essere utilizzati per dimostrare che una particolare metodologia di valutazione d'impatto sulla protezione dei dati soddisfa i parametri imposti dal regolamento generale sulla protezione dei dati.

Criteri per una valutazione d'impatto sulla protezione dei dati accettabile

Il WP29 propone i seguenti criteri che i titolari del trattamento possono utilizzare per stabilire se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno oppure se una metodologia per lo svolgimento di una tale valutazione sia sufficientemente completa per garantire il rispetto del regolamento generale sulla protezione dei dati:

- una descrizione sistematica del trattamento è fornita (articolo 35, paragrafo 7, lettera a)):
    - la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono presi in considerazione (considerando 90);
    - vengono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali;
    - viene fornita una descrizione funzionale del trattamento;
    - sono individuate le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea);
    - si tiene conto del rispetto dei codici di condotta approvati (articolo 35, paragrafo 8);
- la necessità e la proporzionalità sono valutate (articolo 35, paragrafo 7, lettera b)):
    - sono state determinate le misure previste per garantire il rispetto del regolamento (articolo 35, paragrafo 7, lettera d) e considerando 90):
        - misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:
            - finalità determinate, esplicite e legittime (articolo 5, paragrafo 1, lettera b));
            - liceità del trattamento (articolo 6);
            - dati personali adeguati, pertinenti e limitati a quanto necessario (articolo 5, paragrafo 1, lettera c));
            - limitazione della conservazione (articolo 5, paragrafo 1, lettera e));
        - misure che contribuiscono ai diritti degli interessati:
            - informazioni fornite all'interessato (articoli 12, 13 e 14);
            - diritto di accesso e portabilità dei dati (articoli 15 e 20);
            - diritto di rettifica e alla cancellazione (articoli 16, 17 e 19);
            - diritto di opposizione e di limitazione di trattamento (articoli 18, 19 e 21);
            - rapporti con i responsabili del trattamento (articolo 28);
            - garanzie riguardanti trattamenti internazionali (capo V);
            - consultazione preventiva (articolo 36).
- i rischi per i diritti e le libertà degli interessati sono gestiti (articolo 35, paragrafo 7 lettera c)):

- l'origine, la natura, la particolarità e la gravità dei rischi (cfr. considerando 84) o, più in particolare, per ciascun rischio (accesso illegittimo, modifica indesiderata e scomparsa dei dati) vengono determinate dalla prospettiva degli interessati:
  - si considerano le fonti di rischio (considerando 90);
  - sono individuati gli impatti potenziali per i diritti e le libertà degli interessati in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati;
  - sono individuate minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati;
  - sono stimate la probabilità e la gravità (considerando 90);
- sono determinate le misure previste per gestire tali rischi (articolo 35, paragrafo 7, lettera d) e considerando 90);

- le parti interessate sono coinvolte:
  - si consulta il responsabile della protezione dei dati (articolo 35, paragrafo 2);
  - si raccolgono le opinioni degli interessati o dei loro rappresentanti, ove opportuno (articolo 35, paragrafo 9).

METODOLOGIA UTILIZZATA

La valutazione d'impatto sulla protezione dei dati deve tenere conto del rischio complessivo che il trattamento previsto può comportare per i diritti e le libertà degli interessati, alla luce dello specifico contesto.
Pertanto, il concetto di rischio non si esaurisce nella considerazione delle possibili violazioni o minacce della sicurezza dei dati.
È quindi un processo complesso che deve tenere in considerazione e valutare i diversi aspetti tecnici ed organizzativi necessari a minimizzare, fino a renderli accettabili, il possibile impatto sulle persone del trattamento che si intende effettuare, in relazione ai loro diritti e alle loro libertà.
Per effettuare la valutazione di impatto si è seguito il metodo definito dalla CNIL – Autorità francese per la protezione dei dati – con il supporto del software di ausilio ai titolari per l'effettuazione della valutazione d'impatto sulla protezione dei dati (DPIA) messo a punto dalla stessa autorità.
Il software offre un percorso guidato alla realizzazione della DPIA, secondo una sequenza conforme alle indicazioni fornite dal WP29 nelle Linee-guida sulla DPIA.

Gli Art 24, 25 e 32 introducono e richiedono l'effettuazione dell'analisi dei rischi. L'analisi dei rischi è un elemento fondamentale del GDPR, che responsabilizza titolari e responsabili del trattamento nella gestione dei dati personali.
L'analisi dei rischi è il primo passo verso l'adozione di adeguate misure di sicurezza per la protezione dei dati personali.

Il processo di valutazione dei rischi sul trattamento dei dati personali è orientato a valutare – e mitigare, se non ridurre al minimo – tutti i rischi per i diritti e le libertà dell'interessato che si possono verificare a fronte di un trattamento di dati personali.

Se poi, a valle di una valutazione dei rischi si ottiene un rischio elevato per i diritti e le libertà dell'interessato, allora sarà necessario condurre anche una valutazione di impatto sul trattamento che è risultato di rischio elevato. Questo al netto delle altre condizioni che possono portare a condurre comunque una valutazione di impatto, come imposto dal GDPR stesso e dalle indicazioni dei Garanti nazionali.

Per essere coerenti con quanto disposto dal Regolamento occorre valutare i rischi analizzandone gravità delle conseguenze e probabilità di accadimento, come ci indica l'articolo 32.

Un buon modo per affrontare la valutazione dei rischi è sicuramente costituito dall'opportunità di riferirsi a standard internazionali per la valutazione dei rischi, come le norme della serie ISO 31000 (cfr. UNI ISO 31000:2018 – Gestione del rischio – Principi e linee guida).

Nel processo di risk assessment privacy vengono considerati i seguenti attributi dei dati personali (o degli archivi, banche dati di dati personali):

Riservatezza: il dato deve essere accessibile solo a chi è autorizzato a conoscerlo.
Integrità: i dati devono essere integri, esatti e coerenti.
Disponibilità: i dati devono essere sempre disponibili alle persone autorizzate quando necessario.

Pertanto, tutti i rischi che possono derivare da trattamenti non conformi ai requisiti normativi sulla protezione dei dati personali possono essere indirizzati ad una o più dei suddetti attributi delle informazioni personali gestite.

In ambito privacy sono considerati solo i rischi relativi al trattamento dei dati personali che hanno impatto sugli interessati (danni materiali ed immateriali). Sono escluse dal contesto tutte le conseguenze di rischi che non hanno impatti sui dati personali.

Le sorgenti di rischio nell'ambito del trattamento di dati personali possono riguardare:

- personale interno all'organizzazione: dipendenti, collaboratori, ecc…;
- persone esterne all'organizzazione: fornitori, concorrenti, terze parti, ecc…;
- risorse tecnologiche: virus informatici, malfunzionamenti e crash di sistemi, ecc…;
- eventi naturali e non naturali (causati dall'uomo): terremoti, incendi, alluvioni, ecc…;

Il processo di valutazione dei rischi comprende le seguenti fasi, descritte nel seguito del presente documento:

- Identificazione dei rischi

- Analisi e ponderazione dei rischi
- Identificazione e valutazione delle opzioni per il trattamento dei rischi
- Attuazione di controlli per il trattamento dei rischi
- Accettazione/Trattamento dei rischi residui.

Al di là della teoria molto estesa disponibile sull'argomento (le metodologie di risk assessment sono molto diffuse in diversi settori ed ambiti), per effettuare l'analisi dei rischi è stato utilizzato il modello VERA (Very easy risk assessment).
Il modello applicato da VERA si basa su un approccio semplificato pensato per le PMI, adatto anche alle pubbliche amministrazioni locali, per aiutarle a valutare i relativi rischi per la sicurezza.
VERA permette di analizzare il rischio relativo alla sicurezza delle informazioni a livello soprattutto tattico, ossia a livello di processo e di organizzazione in generale

Tabella allegati:

- Regolamento della videosorveglianza comunale
- Informativa estesa – Rilevatori semaforici
- Addendum contrattuale del Soggetto manutentore degli impianti
- Nomine interne

CONTESTO

PANORAMICA DEL TRATTAMENTO

Quale è il trattamento in considerazione?

- ✓ Gestione degli accessi tramite ZTL & corsia preferenziale (Legnano, Via Liguria).

Con riguardo alle esigenze istituzionali e organizzative, l'attività di monitoraggio attraverso sistema di videosorveglianza ha le seguenti finalità conformi alle funzioni istituzionali attribuite al Comune:

- ✓ tutela della sicurezza stradale;
- ✓ polizia amministrativa.

L'utilizzo del sistema di videosorveglianza per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, con sistematico accesso da parte delle forze di polizia di cui all'art. 16 della legge n. 121/1981, a competenza generale e quindi con la condivisione dei dati e individuazione delle finalità deve essere specificamente disciplinato in conformità alle disposizioni del D. Lgs. n. 51/2018.

Quali sono le responsabilità connesse al trattamento?

- ✓ Titolare del trattamento ai sensi dell'art. 4 n. 7) del Regolamento (UE) 2017/679 è il Comune di Legnano;
- ✓ Responsabili del trattamento ai sensi dell'art. 28 del Regolamento (UE) 2017/679 sono le aziende manutentrici degli impianti: REPLA srl con sede in VIA ALESSANDRO VOLTA 176 - 20030 - SENAGO (MI), P.IVA 11400200967, indirizzo e-mail: replasrl@legalmail.it (ZTL e corsia preferenziale L.go Tosi) e Traffic Technology con sede in VIA GIANNI CECCHIN 2 - 36063 - MAROSTICA (VI), P.IVA 03298520242, indirizzo e-mail: trafficteclogyspa@pec.it (Corsia Preferenziale via Liguria;
- ✓ Sub-responsabile del trattamento ai sensi dell'art. 28 del Regolamento (UE) 2017/679 del Responsabile del Trattamento che gestisce la manutenzione degli impianti ZTL e preferenziale L.go Tosi è Sismic Sistemi S.r.l. con sede in VIA MARIA MALIBRAN 51 - 50127 - FIRENZE (FI), P.IVA 04403120480, indirizzo e-mail: sismic@pec.it;

- ✓ Titolari autonomi: le autorità pubbliche che svolgono attività di Polizia Giudiziaria e di Pubblica sicurezza e che possono avere accesso ai e/o ricevere i dati dei sistemi di videosorveglianza in base alle leggi vigenti;
- ✓ Soggetti designati o autorizzati: Il responsabile dell'ufficio di Polizia Locale ed eventuali dipendenti del corpo di Polizia Locale che possono trattare i dati personali e che hanno accesso al sistema di videosorveglianza, ai sensi dell'articolo 29 del Regolamento (UE) 2016/679 e dell'art. 2-quaterdecies del decreto legislativo n. 196/2003.

Valutazione: Accettabile
Commento di valutazione: La descrizione generale del trattamento è esaustiva.

DATI, PROCESSI E RISORSE DI SUPPORTO

Quali sono i dati trattati?

- ✓ Immagini di contesto acquisitE tramite rilevatori varchi e numeri di targa dei veicoli che transitano in prossimità degli impianti senza essere in possesso di correlata autorizzazione per l'accesso e/o il transito.

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

Acquisizione:

I dispositivi acquisiscono immagini di contesto, accompagnate da altre informazioni quali targhe di autoveicoli che vengono ripresi quando transitano in prossimità dei rilevatori, con i relativi riferimenti temporali senza essere in possesso di correlata autorizzazione per l'accesso e/o il transito.
I dati dei veicoli presenti all'interno delle c.d. white list non vengono memorizzati dal sistema.

Trasmissione:

La trasmissione dei dati recuperati tramite impianti (ZTL) in favore del Data center avviene tramite rete mobile (VPN SSL).
La trasmissione dei dati recuperati tramite impianti (ZTL) in favore dei Client ubicati presso il comando di Polizia Locale avviene tramite rete mobile (VPN SSL).
La rete è dedicata.
La trasmissione dei dati recuperati tramite impianti (Corsia preferenziale) in favore del Data center avviene tramite rete mobile (VPN SSL).
La trasmissione dei dati recuperati tramite impianti (Corsia preferenziale) in favore dei Client ubicati presso il comando di Polizia Locale avviene tramite rete mobile (VPN SSL).
La rete è dedicata.

Memorizzazione:

La memorizzazione dei dati provenienti dagli impianti (ZTL e preferenziale L.go Tosi) avviene in Cloud.
La memorizzazione dei dati provenienti dagli impianti relativi a Corsia Preferenziale Via Liguria avviene in Cloud.

Conservazione:

- ✓ I dati raccolti mediante impianti (ZTL & Corsia preferenziale) vengono conservati unicamente per il periodo connesso al procedimento amministrativo che ne ha giustificato l'utilizzo e/o per la gestione di eventuali ricorsi. A tal riguardo, vengono unicamente raccolti i dati dei veicoli che transitano in prossimità dell'impianto contravvenendo alle norme del Codice della Strada e/o atti amministrativi generali.
- ✓ La conservazione potrà essere prorogata oltre i termini temporali sopra esposti per esigenze di indagine / polizia giudiziaria e/o in presenza di eventuali obblighi di legge gravanti sul Titolare del trattamento dati.

Cancellazione:

I dati sono sovrascritti automaticamente una volta decorso il periodo di conservazione.

Quali sono le risorse di supporto ai dati?

Il sistema è composto dalle seguenti componenti:

- ✓ Sistemi di acquisizione: composti da varchi ZTL (n.9) e Corsia preferenziale (n.1);
- ✓ Sistemi di trasmissione: composti da rete mobile (VPN);
- ✓ Sistemi di memorizzazione: Cloud;
- ✓ Sistemi di consultazione: n. 4 pc client ubicati presso il Comando di Polizia Locale (ufficio verbali). Il software di analisi sono Sismic (ZTL e preferenziale L.go Tosi) e Traffic Gate (Corsia Preferenziale via Liguria)

Valutazione: Accettabile
Commento di valutazione: La descrizione dell'infrastruttura è esauriente.

PRINCIPI FONDAMENTALI

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?
Le finalità del trattamento e i dati trattati:

- ✓ Sono conformi al principio di minimizzazione dei dati acquisiti e trattati, sono esplicitati nelle informative rese agli interessati, mediante cartellonistica (codice della strada) e informativa estesa presente sul sito web comunale e a disposizione su richiesta in formato cartaceo;
- ✓ Sono legittime in quanto supportate da idonea base giuridica;
- ✓ Sono legittime in quanto perseguono finalità di interesse pubblico.

Il trattamento dei dati personali è conforme al principio di limitazione della finalità di cui all'art. 5 par. 1 lett. b) del GDPR.
In particolare, le finalità del trattamento sono:

- ✓ Specifiche ed esplicite: le finalità del trattamento sono indicate specificamente nell'informativa di primo livello (cartellonistica), nell'informativa di secondo livello (informativa estesa sul sito internet dell'ente) e nel regolamento comunale sulla videosorveglianza;
- ✓ Legittime: le finalità del trattamento sono supportate da idonea base giuridica, rappresentata nello specifico dall'art. 6 par. 1 lett. e) del GDPR.

La proporzionalità del trattamento rispetto alle finalità perseguite è giustificata dal fatto che si verificano periodicamente episodi di vandalismo, di criminalità in genere e di danneggiamento al patrimonio comunale, oltre a episodi di illecito smaltimento dei rifiuti sul medesimo territorio.

Valutazione: Accettabile
Commento di valutazione: Gli scopi del trattamento sono specifici, espliciti e legittimi. Inoltre, lo scenario descritto giustifica l'adozione dei sistemi di videosorveglianza per aumentare il livello di deterrenza rispetto a comportamenti illeciti sul territorio comunale.

Quali sono le basi giuridiche che rendono lecito il trattamento?

- ✓ La base giuridica che legittima il trattamento è rappresentata dall'art. 6 lett. e) del Regolamento UE 2016/679 secondo cui il trattamento è svolto per l'esecuzione di un compito di interesse pubblico o comunque connesso all'esercizio di pubblici poteri.

Valutazione: Accettabile
Commento di valutazione: Le basi giuridiche del trattamento sono correttamente individuate.

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

I dati trattati sono esclusivamente quelli necessari per le finalità perseguite dal sistema di videosorveglianza.

- ✓ L'inquadramento delle riprese è circoscritto all'area di interesse per la finalità perseguita, in modo da escludere zone non rilevanti per la finalità della videosorveglianza.
- ✓ La proporzionalità è stata applicata in ogni fase o modalità del trattamento, stabilendo che:
  - l'impianto rilevi dati correlati a quei veicoli che violano il codice della strada accedendo a zone e/o tratte stradali senza essere in possesso di correlata autorizzazione al transito e/o sosta;
  - la durata dell'eventuale conservazione tiene conto della necessità da parte del titolare di gestire eventuali ricorsi.

Valutazione: Accettabile
Commento di valutazione: I dati raccolti sono adeguati, pertinenti e limitati. Il principio di minimizzazione è adeguatamente attuato dal titolare del trattamento.

I dati sono esatti e aggiornati?

Le immagini raccolte e/o le targhe raccolti/e sono esatti e aggiornati. In caso di estrapolazione dei dati, vengono applicate tecniche per garantire la riconoscibilità e autenticità del dato (hashing).

Valutazione: Accettabile
Commento di valutazione: I principi di esattezza e di aggiornamento dei dati sono adeguatamente attuati dal titolare del trattamento.

Qual è il periodo di conservazione dei dati?

Come previsto nel Regolamento comunale sulla videosorveglianza, i termini di conservazione dei dati sono stabiliti in conformità alla normativa applicabile sia europea sia di livello nazionale (GDPR, D.lgs. n. 51 del 2018, Provvedimenti Garante Privacy, eventuale normativa o provvedimenti o circolari speciale per casistiche specifiche). I termini di conservazione delle immagini e delle videoriprese sono determinati considerando ciascuna finalità in concreto perseguita e sulla base del principio di limitazione della conservazione di cui all'art. 5 par. 1 lett. e) del Regolamento (UE) 2016/679 e di cui all'art. 3 comma 1 lett. e) del D.lgs. n. 51/2018 attuativo della Direttiva (UE) 2016/680.

- ✓ I dati raccolti mediante rilevatori semaforici vengono conservati unicamente per il periodo connesso al procedimento amministrativo che ne ha giustificato l'utilizzo e/o per la gestione di eventuali ricorsi. A tal riguardo, vengono unicamente raccolti i dati dei veicoli che transitano in prossimità dell'impianto contravvenendo alle norme del Codice della Strada e/o atti amministrativi generali.

La conservazione potrà essere prorogata oltre i termini temporali sopra esposti per esigenze di indagine / polizia giudiziaria e/o in presenza di eventuali obblighi di legge gravanti sul Titolare o Contitolari o Designato Responsabile al trattamento dati.

Valutazione: Accettabile
Commento di valutazione: I periodi di conservazione delle immagini sono individuati correttamente in conformità al principio di limitazione della conservazione.

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

- ✓ Cartellonistica di primo livello;
- ✓ Informativa estesa reperibile sul sito web istituzionale;
- ✓ Informativa estesa su modulo cartaceo presso gli uffici comunali.

Valutazione: Accettabile
Commento di valutazione: Il Titolare del trattamento ottempera adeguatamente ai propri obblighi informativi ai sensi dell'art. 13 del Regolamento (UE) 2016/679 e dell'art. 10 del D. Lgs. n. 51/2018.

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

L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere le informazioni di cui all'art. 15 del Regolamento (UE) 2016/679 e l'accesso ai dati personali nel rispetto delle condizioni prescritte nel regolamento comunale sulla videosorveglianza, e fermi restando eventuali limiti al loro esercizio, in particolare con riferimento all'art. 23 del Regolamento (UE) 2016/679
Le modalità per esercitare il diritto di accesso sono disciplinate dal regolamento comunale in materia di videosorveglianza. Quest'ultimo disciplina anche le modalità per l'accesso ai filmati di videosorveglianza sulla base dell'art. 22 della legge n. 241/1990.
Il diritto alla portabilità non può essere esercitato dal momento che il trattamento in questione è effettuato in esecuzione di un compito di interesse pubblico o comunque correlato all'esercizio di pubblici poteri.

Valutazione: Accettabile
Commento di valutazione: Gli interessati possono esercitare il diritto di accesso riconosciuto dall'art. 15 del Regolamento (UE) 2016/679, e all'interno del Regolamento comunale sulla videosorveglianza è indicata una procedura specifica in materia di diritto di accesso che possa essere seguita dagli interessati per l'accesso ai filmati di videosorveglianza, anche sulla base dell'art. 22 della legge n. 241/1990.

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

Il diritto alla rettifica non può essere esercitato data la tipologia del trattamento effettuato.
Il diritto di cancellazione dei dati conservati può essere fatto valere dall'interessato attraverso comunicazione inviata al Titolare del trattamento oppure al Responsabile della protezione dei dati.
Il diritto alla cancellazione può essere limitato qualora sussistano le condizioni di cui all'art. 17 del Regolamento (UE) 2016/679.

Valutazione: Accettabile
Commento di valutazione: Il regolamento sulla videosorveglianza e l'informativa estesa sul trattamento dei dati relativo alla videosorveglianza specificano le modalità per esercitare il loro diritto di cancellazione, fermi restando i limiti al suo esercizio nei termini di cui all'art. 17 del Regolamento (UE) 2016/679.

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

I diritti di limitazione e opposizione possono essere esercitati compatibilmente con i limiti di cui all'art. 23 del Regolamento (UE) 2016/679.

Come previsto nell'informativa di primo e secondo livello, è possibile inoltrare una richiesta al titolare del trattamento mediante PEC o mediante lettera Raccomandata.

Valutazione: Accettabile
Commento di valutazione: Il Titolare del trattamento riconosce adeguate modalità di effettivo esercizio dei diritti di limitazione e opposizione, fermi restando eventuali limiti al loro esercizio compatibili con quanto stabilito dall'art. 23 del Regolamento (UE) 2016/679.

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

- ✓ La manutenzione degli impianti di videosorveglianza è regolamentata da apposito contratto o atto di nomina.

Tale atto è adottato dal Titolare del trattamento e contiene gli elementi minimi di cui all'art. 28 par. 3 del GDPR.
All'interno del contratto o atto di nomina sono indicate le modalità operative per effettuare la manutenzione.

Valutazione: Accettabile
Commento di valutazione: L'atto di nomina a responsabile del trattamento adottato permette di definire correttamente ed in trasparenza ruoli e responsabilità connesse al trattamento. L'adozione delle clausole contrattuali standard elaborate dalla Commissione europea ai sensi dell'art. 28 par. 7 del Regolamento (UE) 2016/679 garantisce un elevato standard di conformità alle disposizioni del Regolamento europeo.

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 o dello Spazio economico europeo (SEE).

Valutazione: Accettabile
Commento di valutazione: Il mancato trasferimento dei dati verso Paesi al di fuori dell'UE, dello SEE o presso organizzazioni internazionali determina uno scenario di conformità rispetto alle

disposizioni Regolamento (UE) 2016/679 per quanto riguarda i trasferimenti dei dati personali trattati.

RISCHI

Misure esistenti o pianificate

Crittografia

- ✓ La trasmissione dei dati recuperati tramite impianti (ZTL) in favore del Data center avviene tramite rete mobile (VPN SSL).
  La trasmissione dei dati recuperati tramite impianti (ZTL) in favore dei Client ubicati presso il comando di Polizia Locale avviene tramite rete mobile (VPN SSL).
  La rete è dedicata.
- ✓ La trasmissione dei dati recuperati tramite impianti (Corsia preferenziale) in favore del Data center avviene tramite rete mobile (VPN SSL).
- ✓ La trasmissione dei dati recuperati tramite impianti (Corsia preferenziale) in favore dei Client ubicati presso il comando di Polizia Locale avviene tramite rete mobile (VPN SSL).
- ✓ La rete è dedicata.

Valutazione: Accettabile
Commento di valutazione: La misura di sicurezza adottata è idonea a proteggere adeguatamente i dati personali trattati, ai sensi dell'art. 32 del Regolamento (UE) 2016/679.

Controllo degli accessi logici

- ✓ La piattaforma di consultazione dei dati raccolti tramite impianti ZTL è Sismic;
- ✓ La piattaforma di consultazione dei dati raccolti tramite impianti correlati alla gestione della Corsia preferenziale è Traffic Gate;
- ✓ I profili di accesso alle piattaforme sono nominali.
- ✓ Ad ogni utente vengono assegnati credenziali d'accesso.
- ✓ Ogni utente è dotato di apposito profilo che va a caratterizzare le attività che possono o non possono essere effettuate.

Valutazione: Accettabile
Commento di valutazione: La misura di sicurezza adottata è idonea a proteggere adeguatamente i dati personali trattati, ai sensi dell'art. 32 del Regolamento (UE) 2016/679 e in conformità al principio di privacy by design di cui all'art. 25 par. 1 del Regolamento (UE) 2016/679.

Tracciabilità

- ✓ I sistemi sono dotati di sistema di registrazione degli accessi (Log).
- ✓ Il log accessi correlato alla piattaforma Sismic viene conservato per 180 giorni.
- ✓ Il log accessi correlato alla piattaforma Traffic Gate viene conservato per 180 giorni.

Valutazione: Accettabile
Commento di valutazione: La misura di sicurezza adottata è idonea ad assicurare il monitoraggio dei soggetti che accedono al sistema di videosorveglianza, in modo da consentire di conoscere se soggetti non autorizzati hanno effettuato l'accesso al sistema. In tal senso, la misura adottata contribuisce a proteggere i dati personali trattati, ai sensi dell'art. 32 del Regolamento (UE) 2016/679.

Archiviazione

- ✓ I dati sono memorizzati in Cloud qualificato ACN.

Valutazione: Accettabile
Commento di valutazione: La misura di sicurezza adottata è idonea a proteggere adeguatamente i dati personali trattati, ai sensi dell'art. 32 del Regolamento (UE) 2016/679.

Vulnerabilità

- ✓ Il firmware degli impianti viene aggiornato all'occorrenza;
- ✓ L'acceso alla sala deputata ad ospitare gli apparati è regolato da serratura: tale accesso è consentito alle sole persone autorizzate;
- ✓ La consultazione degli stream avviene tramite appositi Client dedicati che vengono costantemente aggiornato;
- ✓ Gli accessi al software deputati alla visione degli stream video sono regolati da user e password e relativi profili;
- ✓ Il Sistema viene regolarmente sottoposto a Vulnerability Assessment (cadenza annuale).

Valutazione: Accettabile
Commento di valutazione: Le misura di sicurezza adottate sono idonee a proteggere adeguatamente i dati personali trattati, ai sensi dell'art. 32 del Regolamento (UE) 2016/679.

Manutenzione

- ✓ La manutenzione del Sistema è regolata da apposito contratto sottoscritto dal Titolare e dal Responsabile del trattamento;
- ✓ Il soggetto manutentore può effettuare manutenzione solo previa autorizzazione e supervisione da parte di personale incaricato. Nel dettaglio, è stato installato apposito software che garantisce la teleassistenza presidiata.

Valutazione: Accettabile
Commento di valutazione: Le misura di sicurezza adottate sono idonee a proteggere adeguatamente i dati personali trattati, ai sensi dell'art. 32 del Regolamento (UE) 2016/679.

Controllo degli accessi fisici

- ✓ Il locale deputato ad ospitare i client è accessibile ai soli autorizzati ed è chiuso con apposita chiave.
- ✓ Il sistema non è dotato di controllo degli accessi e di sistema di registrazione degli stessi.

Valutazione: Accettabile
Commento di valutazione: La misura di sicurezza adottata è idonea a proteggere adeguatamente i dati personali trattati, ai sensi dell'art. 32 del Regolamento (UE) 2016/679.

Sicurezza dell'hardware

- ✓ È presente l'inventario Hardware e Software, che viene regolarmente aggiornato.

Valutazione: Accettabile
Commento di valutazione: Le misura di sicurezza adottate sono idonee a proteggere adeguatamente i dati personali trattati, ai sensi dell'art. 32 del Regolamento (UE) 2016/679.

Politica di tutela della privacy

- ✓ L'organizzazione dell'Ente prevede la nomina del Responsabile per la protezione dei dati personali.

- ✓ È stato redatto un regolamento per la videosorveglianza.
- ✓ È stata predisposta una informativa estesa sul trattamento dei dati personali nell'ambito del sistema di videosorveglianza.
- ✓ Il personale interno del Comando di Polizia Locale è stato debitamente istruito mediante atto di designazione scritto.

Valutazione: Accettabile
Commento di valutazione: Le misure adottate sono idonee a proteggere adeguatamente i dati personali trattati, ai sensi dell'art. 32 del Regolamento (UE) 2016/679, e sono idonee a garantire i diritti e le libertà degli interessati.

Gestione delle politiche di tutela della privacy

- ✓ Le policy per la tutela della privacy vengono costantemente monitorate e aggiornate con il supporto del Responsabile della protezione dei dati personali.
- ✓ La Valutazione d'impatto (DPIA) viene revisionata a cadenza annuale.

Valutazione: Accettabile
Commento di valutazione: Le misure adottate sono idonee a proteggere adeguatamente i dati personali trattati, ai sensi dell'art. 32 del Regolamento (UE) 2016/679, e sono idonee a garantire i diritti e le libertà degli interessati.

Gestione dei rischi

- ✓ Sono stati debitamente mappati i trattamenti tramite apposito registro. La costituzione della presente DPIA include l'analisi del rischio per i diritti e le libertà degli interessati nel contesto della videosorveglianza.

Valutazione: Accettabile
Commento di valutazione: Le misure adottate sono idonee a proteggere adeguatamente i dati personali trattati, ai sensi dell'art. 32 del Regolamento (UE) 2016/679, e sono idonee a garantire i diritti e le libertà degli interessati.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

- ✓ L'Ente si è dotato di apposita policy per la gestione delle violazioni di dati personali (c.d. Data Breach).
- ✓ Il personale è stato debitamente formato per la gestione delle suddette violazioni.

Valutazione: Accettabile
Commento di valutazione: Le misure di sicurezza adottate sono idonee a proteggere adeguatamente i dati personali trattati, ai sensi dell'art. 32 del Regolamento (UE) 2016/679.

Gestione del personale

- ✓ È stata effettuata adeguata formazione del personale in materia di protezione dei dati personali.
- ✓ Vengono effettuate sessioni formative specifiche in base all'evoluzione della normativa in materia.

Valutazione: Accettabile
Commento di valutazione: Le misure di sicurezza adottate sono idonee a proteggere adeguatamente i dati personali trattati, ai sensi dell'art. 32 del Regolamento (UE) 2016/679.

Gestione dei terzi che accedono ai dati

- ✓ L'accesso ai sistemi di videosorveglianza per finalità di manutenzione tecnica viene appositamente regolamentato e avviene mediante teleassistenza presidiata.
- ✓ L'accesso da parte di soggetti terzi privati a dati raccolti mediante sistemi di videosorveglianza è disciplinato dal regolamento comunale sulla videosorveglianza.

Valutazione: Accettabile
Commento di valutazione: Le misure di sicurezza adottate sono idonee a proteggere adeguatamente i dati personali trattati, ai sensi dell'art. 32 del Regolamento (UE) 2016/679.

Vigilanza sulla protezione dei dati

- ✓ Il sistema di Videosorveglianza è stato sottoposto a Vulnerability Assessment a cadenza annuale.

- ✓ Annualmente, il Titolare del trattamento effettua una revisione delle politiche di gestione dei dati con il supporto del Responsabile della protezione dei dati personali.

Valutazione: Accettabile
Commento di valutazione: Le misure di sicurezza adottate sono idonee a proteggere adeguatamente i dati personali trattati, ai sensi dell'art. 32 del Regolamento (UE) 2016/679.

RISCHI

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?
Compromissione della riservatezza degli interessati.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

- Accesso abusivo al sistema dell'Ente;
- Furto o smarrimento dei supporti di memorizzazione;
- Accesso non autorizzato da parte del Responsabile del trattamento;
- Malware;
- Obsolescenza e/o mancato aggiornamento dei dispositivi;
- Accesso di personale interno non autorizzato.

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?

- Crittografia;
- Sicurezza dei canali informatici;
- Manutenzione;
- Controllo degli accessi fisici;
- Controllo degli accessi logici;
- Tracciabilità;
- Sicurezza dell'hardware;
- Gestione dei rischi;
- Contratto con il Responsabile del trattamento;
- Gestione del personale.

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

✓ Limitata. L'accesso illegittimo potrebbe comportare un danno reputazionale nei confronti degli interessati causato da una perdita di riservatezza. L'adozione di molteplici misure di attenuazione del rischio mitigano la gravità del rischio stesso.

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

- ✓ Trascurabile, Alla luce delle misure tecniche e organizzative adottate, si stima che la probabilità del rischio sia trascurabile, al netto del possibile impatto sui diritti e sulle libertà degli interessati qualora dovesse verificarsi una violazione di dati personali.

Valutazione: Accettabile
Commento di valutazione: Pur essendo limitata la rilevanza della gravità del rischio, al netto del verificarsi delle minacce in grado di determinare una violazione di dati personali, l'adozione di molteplici misure di sicurezza permette di circoscrivere notevolmente la probabilità che l'evento si verifichi.

MODIFICHE INDESIDERATE DEI DATI

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

- Alterazione delle targhe degli automezzi e conseguente sanzione a carico di ignoti;
- Impossibilità di perseguire il reato commesso ai danni del cittadino in caso di alterazione delle immagini;
- Impossibilità di tutelare diritti degli interessati o di perseguire reati commessi a danno degli interessati;
- Danno reputazionale nei confronti degli interessati.

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

- Alterazione delle immagini;
- Malware;
- Accesso abusivo al sistema dell'Ente;
- Accesso non autorizzato da parte del Responsabile del trattamento;
- Accesso di personale interno non autorizzato;
- Malfunzionamento software.

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?

- Crittografia;
- Controllo degli accessi logici;
- Tracciabilità;
- Controllo degli accessi fisici;
- Gestione del personale.

✓

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

✓ Limitata. L'adozione di molteplici misure di attenuazione del rischio mitigano la gravità del rischio stesso.

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

- ✓ Trascurabile. Alla luce delle misure tecniche e organizzative adottate, si stima che la probabilità del rischio sia trascurabile, al netto del possibile impatto sui diritti e sulle libertà degli interessati qualora dovesse verificarsi una violazione di dati personali.

Valutazione: Accettabile
Commento di valutazione: Pur essendo limitata la rilevanza della gravità del rischio, al netto del verificarsi delle minacce in grado di determinare una violazione di dati personali, l'adozione di molteplici misure di sicurezza permette di circoscrivere notevolmente la probabilità che l'evento si verifichi.

PERDITA DI DATI

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

Mancata impossibilità di tutelare i diritti degli interessati o di perseguire reati commessi a danno degli interessati.

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

- Eventi naturali;
- Guasti hardware;
- Malfunzionamento software;
- Manomissione delle telecamere;
- Interruzione dei canali di trasmissione;
- Malware;
- Manomissione dell'infrastruttura.

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 fisici;
- Controllo degli accessi logici;
- Tracciabilità;
- Archiviazione;
- Manutenzione;
- Sicurezza dell'hardware;
- Contratto con il Responsabile del trattamento;
- Gestione del personale.

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

✓ Limitata. L'adozione di molteplici misure di attenuazione del rischio mitigano la gravità del rischio stesso.

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

- ✓ Trascurabile. Alla luce delle misure tecniche e organizzative adottate, si stima che la probabilità del rischio sia trascurabile, al netto del possibile impatto sui diritti e sulle libertà degli interessati qualora dovesse verificarsi una violazione di dati personali.

Valutazione: Accettabile
Commento di valutazione: Pur essendo limitata la rilevanza della gravità del rischio, al netto del verificarsi delle minacce in grado di determinare una violazione di dati personali, l'adozione di molteplici misure di sicurezza permette di circoscrivere notevolmente la probabilità che l'evento si verifichi.

PIANO D'AZIONE

Principi fondamentali

Il piano d'azione cui si impegna il titolare è finalizzato a conformare il trattamento in questione ai principi e alle norme applicabili in materia di videosorveglianza e trattamento dei dati personali, in modo tale che le criticità evidenziate siano rimediate e che l'impianto possa essere rimesso in funzione.
In seguito al contributo di analisi del DPO, dunque, il titolare si impegna ad adottare le misure indicate nella sezione sottostante.

Misure pianificate

Piano d'azione:

- ✓ Procedere nuovamente a effettuare una DPIA per stabilire un rischio adeguato per i diritti e le libertà degli interessati;
- ✓ Mantenere costantemente adeguato il sistema informatico;
- ✓ Effettuare una verifica annuale dell'infrastruttura IT attraverso l'effettuazione di un vulnerability assessment.

Parere DPO/RPD

- ✓ In allegato.

ANALISI DEI RISCHI E AZIONI PER MITIGARE

Per effettuare l'analisi dei rischi è stato utilizzato il modello VERA (Very easy risk assessment).
Il modello applicato da VERA si basa su un approccio semplificato pensato per le PMI adatto anche alle pubbliche amministrazioni locali, per aiutarle a valutare i relativi rischi per la sicurezza.
VERA è progettato per la valutazione del rischio nella sicurezza delle informazioni, particolarmente adatto alle esigenze delle PMI e alle pubbliche amministrazioni locali. Questo metodo si basa sull'identificazione delle minacce, l'analisi delle misure di controllo esistenti e la determinazione delle azioni necessarie per mitigare i rischi.
Il metodo VERA mantiene la conformità agli standard ISO/IEC 27001 e soddisfa i requisiti di vari audit, rendendolo uno strumento versatile e prezioso.
VERA eccelle nell'analisi a livello tattico e organizzativo, permettendo una valutazione complessiva dei processi di sicurezza. La sua flessibilità consente di adattarsi a diverse esigenze e standard
Nonostante la sua semplicità, VERA richiede competenze in sicurezza informatica per un utilizzo ottimale e un'interpretazione accurata dei risultati. Questo equilibrio tra facilità d'uso e profondità di analisi rende VERA uno strumento efficace per le organizzazioni che cercano un approccio pratico ma completo alla valutazione del rischio informatico.

CALCOLO DEL RISCHIO PRIVACY

Ambito	Categoria	Minaccia	Veros.	Parametri RID	Rischio Privacy						Liv. rischio
					Distruzione non aut.	Perdita non aut.	Modifica non aut.	Divulgazione non aut.	Accesso n/a a dati trasmessi	Accesso n/a a dati conservati	
Sicinfo	Danni fisici	Incendio	1	ID	X	X					3,00
Sicinfo	Danni fisici	Allagamento	1	D	X	X					3,00
Sicinfo	Danni fisici	Polvere, corrosione, congelamento.	1	D	X	X					3,00
Sicinfo	Danni fisici	Distruzione di strumentazione da parte di malintenzionati o per errore (disattenzione)	2	D	X	X					6,00
Sicinfo	Danni fisici	Attacchi (bombe, terroristi)	1	D	X	X					3,00
Sicinfo	Eventi naturali	Fenomeni climatici (uragani, nevicate)	1	D	X	X					3,00
Sicinfo	Eventi naturali	Terremoti, eruzioni vulcaniche	1	D	X	X					3,00
Sicinfo	Eventi naturali	Fulmini e scariche atmosferiche	2	D	X	X					6,00
Sicinfo	Perdita di servizi essenziali	Guasto aria condizionata o sistemi di raffreddamento	2	D	X	X					6,00
Sicinfo	Perdita di servizi essenziali	Perdita di energia (o sbalzi di tensione)	2	D	X	X					6,00

Ambito	Categoria	Minaccia	Veros.	Parametri RID	Rischio Privacy						Liv. rischio
					Distruzione non aut.	Perdita non aut.	Modifica non aut.	Divulgazione non aut.	Accesso n/a a dati trasmessi	Accesso n/a a dati conservati	
Sicinfo	Perdita di servizi essenziali	Malfunzionamento nei componenti di rete	2	RID	X	X	X		X		24,00
Sicinfo	Perdita di servizi essenziali	Errori di trasmissione (incluso il misrouting)	1	ID		X		X	X		3,00
Sicinfo	Perdita di servizi essenziali	Interruzione nei collegamenti di rete (inclusi danni alle linee di TLC)	2	D		X		X	X		6,00
Sicinfo	Perdita di servizi essenziali	Eccesso di traffico sulla rete	2	D							
Sicinfo	Perdita di servizi essenziali	Interruzione di servizi erogati riconducibili ai fornitori esterni (inclusi ISP, CSP, DR site, supporto tecnico specialistico, esternalizzazione attività). Per esempio a causa di fallimento, chiusura, incidenti.	1	D		X					3,00
Sicinfo	Perdita di servizi essenziali	Indisponibilità di personale (malattie, sciopero, eccetera)	1	D							

Ambito	Categoria	Minaccia	Veros.	Parametri RID	Rischio Privacy						Liv. rischio
					Distruzione non aut.	Perdita non aut.	Modifica non aut.	Divulgazione non aut.	Accesso n/a a dati trasmessi	Accesso n/a a dati conservati	
Sicinfo	Disturbi	Disturbi elettromagnetici	1	ID	X	X	X				3,00
Sicinfo	Compromissione di informazioni	Intercettazione (inclusa analisi del traffico)	1	R					X		12,00
Sicinfo	Compromissione di informazioni	Furto di documenti o supporti di memorizzazione	1	R	X	X			X	X	12,00
Sicinfo	Compromissione di informazioni	Furto di apparati o componenti	2	RD	X	X		X		X	24,00
Sicinfo	Compromissione di informazioni	Recupero di informazioni da media (principalmente memorie di massa) dismessi.	1	R				X		X	12,00
Sicinfo	Compromissione di informazioni	Rivelazione di informazioni (da parte del personale o fornitori)	2	R				X			24,00
Sicinfo	Compromissione di informazioni	Ricezione dati da origini non affidabili	1	I							
Sicinfo	Compromissione di informazioni	Infiltrazione nelle comunicazioni	1	RID		X	X	X	X		12,00
Sicinfo	Compromissione di informazioni	Ripudio dei messaggi	1	I							

Ambito	Categoria	Minaccia	Veros.	Parametri RID	Rischio Privacy						Liv. rischio
					Distruzione non aut.	Perdita non aut.	Modifica non aut.	Divulgazione non aut.	Accesso n/a a dati trasmessi	Accesso n/a a dati conservati	
Sicinfo	Compromissione di informazioni	Accesso non autorizzato alle informazioni	2	RID	X	X	X				24,00
Sicinfo	Problemi tecnici	Fault o malfunzionamento della strumentazione IT	2	ID	X	X	X			X	6,00
Sicinfo	Problemi tecnici	Saturazione dei sistemi IT	2	ID							
Sicinfo	Problemi tecnici	Malfunzionamenti software applicativi sviluppati per i clienti	1	RID	X	X	X	X	X	X	12,00
Sicinfo	Problemi tecnici	Malfunzionamenti pacchetti software usati internamente	1	RID	X	X	X	X	X	X	12,00
Sicinfo	Problemi tecnici	Malfunzionamenti software applicativi sviluppati per uso interno	1	RID	X	X	X	X	X	X	12,00
Sicinfo	Problemi tecnici	Errori di manutenzione hardware e software di base	1	ID	X	X	X	X	X	X	3,00
Sicinfo	Azioni non autorizzate	Uso non autorizzato o negligente della strumentazione	2	RID	X	X	X	X	X	X	24,00

Ambito	Categoria	Minaccia	Veros.	Parametri RID	Rischio Privacy						Liv. rischio
					Distruzione non aut.	Perdita non aut.	Modifica non aut.	Divulgazione non aut.	Accesso n/a a dati trasmessi	Accesso n/a a dati conservati	
Sicinfo	Azioni non autorizzate	Importazione o esportazione illegale di software (copia illegale di software o uso di software illegale)	2	RID							
Sicinfo	Azioni non autorizzate	Alterazione volontaria e non autorizzata di dati di business	1	RID	X	X	X				12,00
Sicinfo	Azioni non autorizzate	Virus (malware, anche per mobile)	2	RID	X	X	X	X		X	24,00
Sicinfo	Azioni non autorizzate	Accesso non autorizzato alla rete (anche tramite AP wireless non autorizzati)	2	RID	X	X	X	X	X	X	24,00
Sicinfo	Azioni non autorizzate	Uso non autorizzato della rete da parte degli utenti o abuso delle autorizzazioni	2	RID	X	X	X	X	X	X	24,00
Sicinfo	Azioni non autorizzate	Trattamento (volontario o inconsapevole) non consentito di dati (personali)	1	RI	X	X	X	X			12,00

Ambito	Categoria	Minaccia	Veros.	Parametri RID	Rischio Privacy						Liv. rischio
					Distruzione non aut.	Perdita non aut.	Modifica non aut.	Divulgazione non aut.	Accesso n/a a dati trasmessi	Accesso n/a a dati conservati	
Sicinfo	Compromissione di funzioni	Errori degli utenti di business	1	RID	X	X	X	X	X	X	12,00
Sicinfo	Compromissione di funzioni	Uso dei servizi da parte di persone non autorizzate o elevamento di privilegi.	1	RID	X	X	X	X	X	X	12,00
Sicinfo	Compromissione di funzioni	Degrado dei media (memorie di massa)	2	ID	X	X					6,00
Sicinfo	Compromissione di funzioni	Uso di servizi in modo non autorizzato	2	RID	X	X	X	X	X	X	24,00
Sicinfo	Compromissione di funzioni	Furto identità	2	RID			X	X			24,00
Privacy	Trattamento dati personali	Eccessiva raccolta di dati personali	1	R				X			4,00
Privacy	Trattamento dati personali	Collegamenti o raffronti inappropriati o non autorizzati di dati personali	1	R				X			12,00
Privacy	Trattamento dati personali	Divulgazione o riuso per finalità diverse dei dati personali senza la consapevolezza e/o il consenso degli interessati	2	R				X		X	24,00

Ambito	Categoria	Minaccia	Veros.	Parametri RID	Rischio Privacy						Liv. rischio
					Distruzione non aut.	Perdita non aut.	Modifica non aut.	Divulgazione non aut.	Accesso n/a a dati trasmessi	Accesso n/a a dati conservati	
Privacy	Trattamento dati personali	Conservazione immotivamente prolungata dei dati personali	1	R				X		X	4,00
Privacy	Trattamento dati personali	Inesattezza o mancato aggiornamento dei dati personali	1	I			X				1,00
Privacy	Trattamento dati personali	Violazione delle istruzioni ricevute in materia di dati personali	2	RID	X	X	X	X	X	X	24,00
Privacy	Trattamento dati personali	Trasferimento dati personali extra UE senza garanzie di adeguatezza	1	RID				X			4,00

LIVELLO DI RISCHIO PER LA PIA E CONSULTAZIONE PREVENTIVA

Per la PIA deve essere indicato se il rischio è elevato per avviare la consultazione preventiva.
In questo caso, il rischio è "elevato" se massimo per valore delle informazioni (valore 4) e per verosimiglianza della minaccia (valore 3, senza considerare le misure attuate).

	Valore delle informazioni		
Informazioni	Riservatezza	Integrità	Disponibilità
Totale valore informazioni	4	1	1

Ambito	Categoria	Minaccia	Verosimiglianza	Rischio "Puro"	Rischio "puro" qualitativo
Sicinfo	Danni fisici	Incendio	1	1	Basso
Sicinfo	Danni fisici	Allagamento	1	1	Basso
Sicinfo	Danni fisici	Polvere, corrosione, congelamento.	1	1	Basso
Sicinfo	Danni fisici	Distruzione di strumentazione da parte di malintenzionati o per errore (disattenzione)	2	2	Basso
Sicinfo	Danni fisici	Attacchi (bombe, terroristi)	1	1	Basso
Sicinfo	Eventi naturali	Fenomeni climatici (uragani, nevicate)	1	1	Basso
Sicinfo	Eventi naturali	Terremoti, eruzioni vulcaniche	1	1	Basso
Sicinfo	Eventi naturali	Fulmini e scariche atmosferiche	2	2	Basso
Sicinfo	Perdita di servizi essenziali	Guasto aria condizionata o sistemi di raffreddamento	2	2	Basso
Sicinfo	Perdita di servizi essenziali	Perdita di energia (o sbalzi di tensione)	2	2	Basso
Sicinfo	Perdita di servizi essenziali	Malfunzionamento nei componenti di rete	2	8	Medio
Sicinfo	Perdita di servizi essenziali	Errori di trasmissione (incluso il misrouting)	1	1	Basso
Sicinfo	Perdita di servizi essenziali	Interruzione nei collegamenti di rete (inclusi danni alle linee di TLC)	2	2	Basso
Sicinfo	Perdita di servizi essenziali	Eccesso di traffico sulla rete	2	2	Basso

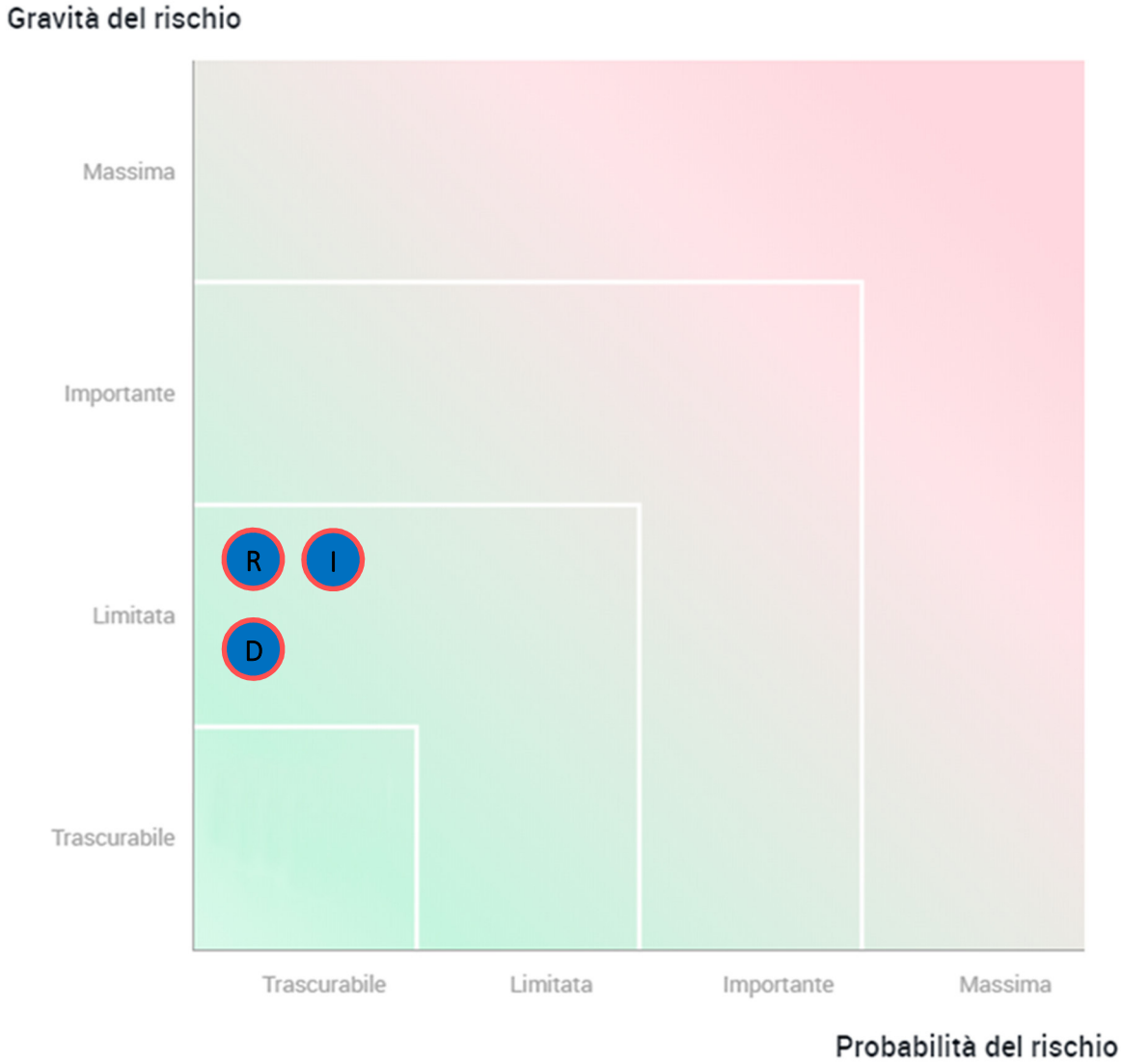
Ambito	Categoria	Minaccia	Verosimiglianza	Rischio "Puro"	Rischio "puro" qualitativo
Sicinfo	Perdita di servizi essenziali	Interruzione di servizi erogati riconducibili ai fornitori esterni (inclusi ISP, CSP, DR site, supporto tecnico specialistico, esternalizzazione attività). Per esempio a causa di fallimento, chiusura, incidenti.	1	1	Basso
Sicinfo	Perdita di servizi essenziali	Indisponibilità di personale (malattie, sciopero, eccetera)	1	1	Basso
Sicinfo	Disturbi	Disturbi elettromagnetici	1	1	Basso
Sicinfo	Compromissione di informazioni	Intercettazione (inclusa analisi del traffico)	1	4	Basso
Sicinfo	Compromissione di informazioni	Furto di documenti o supporti di memorizzazione	1	4	Basso
Sicinfo	Compromissione di informazioni	Furto di apparati o componenti	2	8	Medio
Sicinfo	Compromissione di informazioni	Recupero di informazioni da media (principalmente memorie di massa) dismessi.	1	4	Basso
Sicinfo	Compromissione di informazioni	Rivelazione di informazioni (da parte del personale o fornitori)	2	8	Medio
Sicinfo	Compromissione di informazioni	Ricezione dati da origini non affidabili	1	1	Basso
Sicinfo	Compromissione di informazioni	Infiltrazione nelle comunicazioni	1	4	Basso
Sicinfo	Compromissione di informazioni	Ripudio dei messaggi	1	1	Basso
Sicinfo	Compromissione di informazioni	Accesso non autorizzato alle informazioni	2	8	Medio
Sicinfo	Problemi tecnici	Fault o malfunzionamento della strumentazione IT	2	2	Basso
Sicinfo	Problemi tecnici	Saturazione dei sistemi IT	2	2	Basso
Sicinfo	Problemi tecnici	Malfunzionamenti software applicativi sviluppati per i clienti	1	4	Basso
Sicinfo	Problemi tecnici	Malfunzionamenti pacchetti software usati internamente	1	4	Basso

Ambito	Categoria	Minaccia	Verosimiglianza	Rischio "Puro"	Rischio "puro" qualitativo
Sicinfo	Problemi tecnici	Malfunzionamenti software applicativi sviluppati per uso interno	1	4	Basso
Sicinfo	Problemi tecnici	Errori di manutenzione hardware e software di base	1	1	Basso
Sicinfo	Azioni non autorizzate	Uso non autorizzato o negligente della strumentazione	2	8	Medio
Sicinfo	Azioni non autorizzate	Importazione o esportazione illegale di software (copia illegale di software o uso di software illegale)	2	8	Medio
Sicinfo	Azioni non autorizzate	Alterazione volontaria e non autorizzata di dati di business	1	4	Basso
Sicinfo	Azioni non autorizzate	Virus (malware, anche per mobile)	2	8	Medio
Sicinfo	Azioni non autorizzate	Accesso non autorizzato alla rete (anche tramite AP wireless non autorizzati)	2	8	Medio
Sicinfo	Azioni non autorizzate	Uso non autorizzato della rete da parte degli utenti o abuso delle autorizzazioni	2	8	Medio
Sicinfo	Azioni non autorizzate	Trattamento (volontario o inconsapevole) non consentito di dati (personali)	1	4	Basso
Sicinfo	Compromissione di funzioni	Errori degli utenti di business	1	4	Basso
Sicinfo	Compromissione di funzioni	Uso dei servizi da parte di persone non autorizzate o elevamento di privilegi.	1	4	Basso
Sicinfo	Compromissione di funzioni	Degrado dei media (memorie di massa)	2	2	Basso
Sicinfo	Compromissione di funzioni	Uso di servizi in modo non autorizzato	2	8	Medio
Sicinfo	Compromissione di funzioni	Furto identità	2	8	Medio
Privacy	Trattamento dati personali	Eccessiva raccolta di dati personali	1	4	Basso
Privacy	Trattamento dati personali	Collegamenti o raffronti inappropriati o non autorizzati di dati personali	1	4	Basso

Ambito	Categoria	Minaccia	Verosimiglianza	Rischio "Puro"	Rischio "puro" qualitativo
Privacy	Trattamento dati personali	Divulgazione o riuso per finalità diverse dei dati personali senza la consapevolezza e/o il consenso degli interessati	2	8	Medio
Privacy	Trattamento dati personali	Conservazione immotivamente prolungata dei dati personali	1	4	Basso
Privacy	Trattamento dati personali	Inesattezza o mancato aggiornamento dei dati personali	1	1	Basso
Privacy	Trattamento dati personali	Violazione delle istruzioni ricevute in materia di dati personali	2	8	Medio
Privacy	Trattamento dati personali	Trasferimento dati personali extra UE senza garanzie di adeguatezza	1	4	Basso

Mappatura del rischio

Questo grafico rappresenta la mappatura del rischio per gli indicatori R (Riservatezza), I (Integrità) e D (Disponibilità). Visualizza il livello di rischio per ciascun indicatore, mostrando la relazione tra la gravità potenziale e la probabilità di occorrenza. I punti nel grafico indicano la posizione di ogni indicatore, consentendo una rapida valutazione e confronto dei rischi associati prima e dopo l'applicazione delle misure correttive.



Mappatura del rischio con le misure esistenti

Mappatura del rischio considerando le misure correttive proposte

R	Riservatezza	I	Integrità	D	Disponibilità