COMUE DI SANTA VITTORIA D'ALBA
Provincia di Cuneo

Valutazione d'impatto sulla protezione dei dati (DPIA) – Impianto di videosorveglianza

Sommario

Premessa 5
Informazioni sulla PIA 5
Nome della PIA 5
Nome autore 5
Nome valutatore 5
Nome validatore 5
Data di creazione 5
Nome del DPO/RPD 5
Parere del DPO/RPD 5
Richiesta del parere degli interessati 5
Motivazione della mancata richiesta del parere degli interessati 5
Allegati 6
..... 6
Diagramma ciclo di vita del dato.jpg 6
Contesto 6
Panoramica del trattamento 6
Quale è il trattamento in considerazione? 6
Quali sono le responsabilità connesse al trattamento? 7
Ci sono standard applicabili al trattamento? 7
Dati, processi e risorse di supporto 7
Quali sono i dati trattati? 7
Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)? 8
Quali sono le risorse di supporto ai dati? 8
Principi Fondamentali 8
Proporzionalità e necessità 8
Gli scopi del trattamento sono specifici, espliciti e legittimi? 8
Quali sono le basi legali che rendono lecito il trattamento? 8
I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)? 8
I dati sono esatti e aggiornati? 9
Qual è il periodo di conservazione dei dati? 9
Misure a tutela dei diritti degli interessati 9
Come sono informati del trattamento gli interessati? 9
Ove applicabile: come si ottiene il consenso degli interessati? 9
Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati? 9
Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)? 10

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione? 10
Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto? 10
In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente? 10
Rischi 10
Misure esistenti o pianificate 10
Crittografia 10
Controllo degli accessi logici 10
Tracciabilità 11
Archiviazione 11
Minimizzazione dei dati 11
Vulnerabilità 11
Lotta contro il malware 11
Gestione postazioni 11
Backup 11
Manutenzione 12
Sicurezza dei canali informatici 12
Controllo degli accessi fisici 12
Sicurezza dell'hardware 12
Politica di tutela della privacy 12
Gestione delle politiche di tutela della privacy 12
Gestire gli incidenti di sicurezza e le violazioni dei dati personali 12
Gestione del personale 12
Accessi diversificati 13
Misure antincendio 13
Accesso illegittimo ai dati 13
Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare? 13
Quali sono le principali minacce che potrebbero concretizzare il rischio? 13
Quali sono le fonti di rischio? 13
Quali misure fra quelle individuate contribuiscono a mitigare il rischio? 13
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate? 13
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate? 13
Modifiche indesiderate dei dati 14
Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare? 14
Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio? 14

Quali sono le fonti di rischio? 14
Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio? 14
Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate? 14
Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate? 14
Perdita di dati 14
Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi? 14
Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio? 14
Quali sono le fonti di rischio? 14
Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio? 14
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate? 15
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate? 15
Grafiche 16
Principi fondamentali - Misure esistenti o pianificate 16
16
Panoramica dei rischi 17
18
Mappaggio dei rischi 19

Premessa

Il **Regolamento (UE) 2016/679 sulla protezione dei dati** (GDPR), ha introdotto la previsione che i titolari del trattamento predispongano una valutazione di impatto (DPIA–*Data protection impact assessment* o anche *PIA–Privacy impact assessment*) ogni qual volta un trattamento presenti rischi elevati per i diritti e le libertà delle persone fisiche.

Ai sensi dell'art. 35 par. 3 lett c) GDPR, è necessario preventivamente predisporre una DPIA se si effettua una **sorveglianza sistematica su larga scala di una zona accessibile al pubblico**; un sistema di videosorveglianza territoriale, per definizione, presenta queste caratteristiche. Di fatto, risulta impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici.

Nell'elaborazione dell'analisi si utilizza il software open source "PIA" messo a disposizione dal CNIL (Autorità garante francese per la protezione dei dati personali), progetto a cui ha aderito successivamente l'Autorità garante italiana, inteso quale valido supporto ed indirizzo operativo.

La presente valutazione d'impatto è condotta avvalendosi anche delle Linee Guida su Data Protection Impact Assessment elaborate dal *Working Party 248 art. 29*. Per stabilire se il trattamento di dati è svolto su larga scala si deve tener conto dei seguenti fattori:

1) il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
2) il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
3) la durata, ovvero la persistenza, dell'attività di trattamento;
4) la portata geografica dell'attività di trattamento.

Visto l'allegato 1 al provvedimento del Garante n. 467 dell'11 ottobre 2018, si ritiene che la videosorveglianza costituisca un trattamento che prevede un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati (n. 3).

Il **Responsabile del trattamento dei dati**, RPS Gavuzzi srl nella persona di Paolo Barberis, ha preventivamente assistito il titolare nella stesura della valutazione *ex* art. 35 par. 2 GDPR.

Informazioni sulla PIA

Nome della PIA
Videosorveglianza territoriale Santa Vittoria d'Alba

Nome autore
Odasso Matteo

Nome valutatore
Badellino Giacomo

Nome validatore
Badellino Giacomo

Data di creazione
04/12/2018

Nome del DPO/RPD
dott. Matteo Odasso

Parere del DPO/RPD
L'analisi condotta relativa ai potenziali rischi per i diritti degli interessati ed alle probabilità di verificazione degli stessi pare completa ed esaustiva. Le misure tecniche ed organizzative adottate nel trattamento, a tutela della riservatezza dei dati personali, paiono adeguate al contesto. Durante il processo di valutazione, in cui il Titolare è stato assistito, si è potuto inoltre apprezzare l'adeguatezza del Responsabile esterno del trattamento dei dati. I rischi che potrebbero compromettere i diritti e le libertà degli interessati paiono quindi adeguatamente limitati

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

Motivazione della mancata richiesta del parere degli interessati

Il trattamento è svolto nell'ambito dell'esecuzione di un complito di pubblico interesse o connesso all'esercizio di pubblici poteri. Il parere degli interessati non è pertanto necessario in quanto è il legislatore che effettua a priori un bilanciamento degli interessi coinvolti, assegnando maggiore rilevanza a taluno di essi senza pur sacrificare del tutto i rimanenti.

Allegati

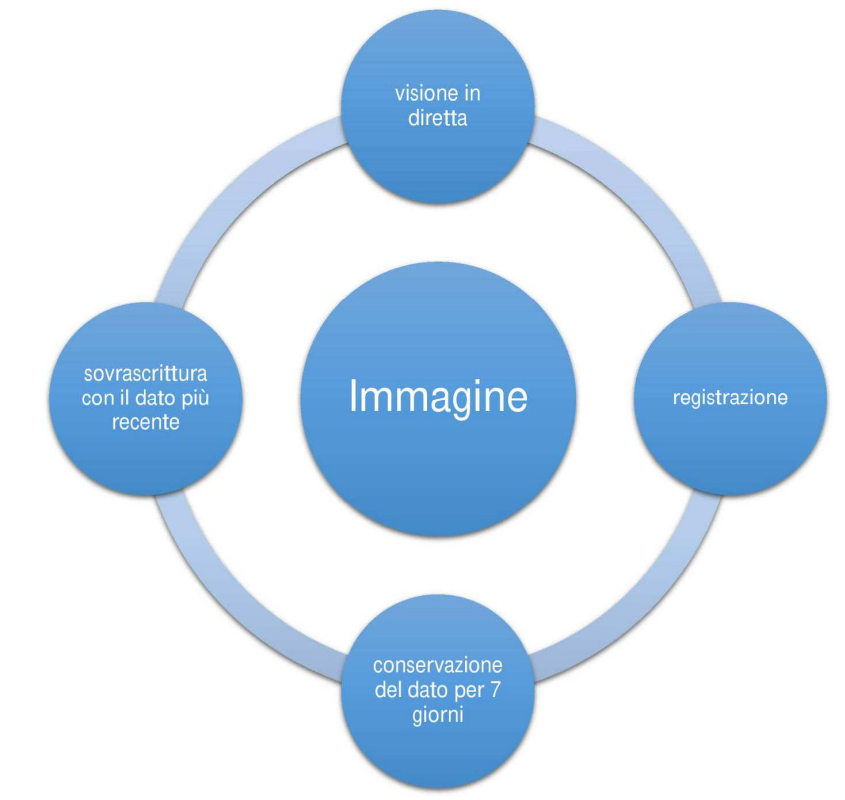


Diagramma ciclo di vita del dato.jpg

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Il Comune di Santa Vittoria d'Alba, al fine di tutelare il proprio territorio e garantire il necessario grado di sicurezza ai propri cittadini e a tutte le persone che lo attraversano, oltre che per la tutela del patrimonio, per la prevenzione, l'accertamento e la repressione dei reati, con deliberazione di Giunta Comunale n. 28 del 13.04.2012 ha disposto l'attivazione di un sistema di videosorveglianza urbana mediante l'installazione di telecamere, debitamente segnalate, nel rispetto delle prescrizioni fornite dal Garante per la protezione dei dati personali.
Con determinazione del Responsabile del Servizio manutenzione e conservazione patrimonio n. 175 del 27.12.2017 il sistema di videosorveglianza territoriale è stato integrato con nuove telecamere di tecnologia più evoluta.

Le apparecchiature sono indirizzate verso luoghi di proprietà comunale o di attraversamento pubblico, individuati in ragione delle esigenze di sicurezza delle persone fisiche o della tutela del patrimonio e sono collocate nelle seguenti località:

- Palazzo Comunale (ingresso da piazza Marone) -Telecamera di contesto;

- Palazzo Comunale (cortile interno) - Telecamera di contesto;

- Piazza Bertero (zona antistante la scuola) - Telecamera di contesto;

- Via Monticello (ingresso campo sportivo) - Telecamera di contesto;

- Via della Pianchetta (peso pubblico) - Telecamera di contesto;

- Via della Pianchetta (ingresso cimitero comunale) - Telecamera di contesto;

- Piazza Europa - Telecamera di contesto;

- Via Vers Pont du Gard (ingresso palestra comunale) Telecamera di contesto;

- Via Dei Roeri (ingresso giardino pubblico) Telecamera di contesto;

- Via Monviso (ingresso area giochi bambini) Telecamera di contesto;

- Strada Provinciale n. 171 Loc. Lussi (ingresso centro abitato) Telecamera lettura targhe;

- Strada Statale n. 231 provenienza da Bra (ingresso centro abitato) Telecamera lettura targhe;

- Strada Provinciale n. 153 (km 0 - ingresso centro abitato) Telecamera lettura targhe;

- Strada Statale n. 231 provenienza da Alba (Km 33+600) Telecamera lettura targhe

Quali sono le responsabilità connesse al trattamento?

Il **titolare del trattamento** è il Comune di Santa Vittoria d'Alba Piazza Marone n. 2 12069 Santa Vittoria d'Alba (CN) – Telefono: +39 0172/478023
Fax: +39 0172/478744, email: info@comunedisantavittoriadalba.it PEC: comune.santavittoriadalba@legalmail.it

Il **responsabile del trattamento** è R.P.S. GAVUZZI Corso Coppino, 42/A - 12051 Alba (CN) Tel. 0173 363607 - 0173 363609 fax 0173 440648 email rps@rps-sicurezza.com.

Ci sono standard applicabili al trattamento?

La **base giuridica** del trattamento è costituita dal D.L. (cosiddetto "Decreto Sicurezza") del 23 febbraio 2009 n. 11, recante misure urgenti in materia di sicurezza pubblica, convertito, con modificazioni, dall'art. 1 comma 1 della Legge del 23 aprile 2009, n. 38.
Il trattamento dei dati personali è posto in essere nel pieno rispetto del **Provvedimento dell'Autorità Garante per la protezione dei dati personali in materia di videosorveglianza** (8 aprile 2010).
Con deliberazione n. 17 del 18 aprile 2016 è stato adottato un **Regolamento comunale per l'utilizzo di sistemi di videosorveglianza**.

Valutazione: Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Sono trattate le immagini riprese dalle videocamere.
Le immagini riprese sono visualizzate e gestite da una stazione di controllo e monitoraggio ubicata presso la Centrale Operativa della Polizia Municipale ubicata nel palazzo comunale.
L'accesso alla stazione di controllo e la visione delle immagini è consentito solo a dipendenti o personale tecnico espressamente autorizzati e con diversi livelli di autorizzazione, informati sugli obblighi da rispettare e sulle responsabilità connessa in caso di violazione. I sistemi sono programmati in modo da operare la cancellazione automatica delle informazioni allo scadere del termine previsto (**7 giorni**), laddove non vi siano ragioni, per disposizione dell'autorità giudiziaria o di altre autorità competenti, che ne giustifichino la conservazione.
I dati trattati non saranno oggetto di diffusione a terzi, ad eccezione dei casi di espressa e motivata disposizione dell'**Autorità giudiziaria**.

Referente interno all'Ente è: Sindaco (Badellino Giacomo)
Personale autorizzato a visualizzare le immagini: Zanelli Simone (Vicecommissario Polizia Locale).

I tecnici della società R.P.S. GAVUZZI (responsabile del trattamento) accedono, in loco o da remoto, al sistema di videosorveglianza unicamente nella loro attività di manutenzione software ed hardware degli impianti.

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

L'immagine è raccolta attraverso telecamere 24 ore al giorno.
Gli impianti, visibili anche in presa diretta da personale incaricato, sono progettati per registrare e conservare le immagini raccolte. La conservazione del dato non supera i **7 giorni**, salvo comprovate esigenze.
Il dato più vecchio è automaticamente sovrascritto con il dato più recente senza bisogno di intervento umano.

Quali sono le risorse di supporto ai dati?

Il dato è conservato su NVR server su cui è trasmesso via radio dalla telecamera. Il sistema di registrazione è stato dimensionato per esaltare le performance di registrazione, supervisionamento e fruizione del registrato. E' dotato di due baie con chiusura a chiave, per ospitare due hard disk per un massimo di 2 Terabyte cad., microprocessore Intel.

Il link radio si basa sulla tecnologia "punto-punto" o "punto multi punto" realizzati con tecnologia 5Ghz a frequenza libera, criptatura della componente radio con protocollo WPA2/Personal e protezione mediante password dei parametri di configurazione della radio.

Valutazione: Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

La finalità del trattamento dei dati riguarda la tutela della sicurezza urbana, del territorio al fine di garantire il necessario grado di sicurezza ai cittadini e a tutte le persone che lo attraversano, oltre che la tutela del patrimonio, la prevenzione, l'accertamento e la repressione dei reati.
Si sono susseguiti in questi anni numerosi interventi legislativi statali che hanno attribuito ai Sindaci ed ai Comuni specifiche competenze in materia di tutela dell'incolumità pubblica e della sicurezza urbana.
La videosorveglianza territoriale è quindi uno strumento funzionale allo svolgimento di compiti istituzionali.
Al fine di tutelare la sicurezza e l'incolumità pubblica, non esistono, allo stato attuale, altri strumenti di vigilanza e controllo che garantiscano il risultato di un impianto di videosorveglianza, negli stessi termini di efficacia ed economicità, a fronte di un sacrificio del tutto accettabile di una parte delle libertà degli interessati. In altri termini, si ritiene che sussista un **equo bilanciamento** tra l'interesse pubblico (nella specie, la tutela della sicurezza e dell'incolumità dei cittadini), ed i diritti degli interessati.

Valutazione: Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

I dati sono trattati nell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 6 par. 1 lett. e) GDPR).

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)?

Il dato personale raccolto (immagine) è limitato allo stretto necessario ed in modo assolutamente pertinente alla finalità per cui è trattato, assicurando il pieno rispetto del principio di minimizzazione dei dati.

Valutazione: Accettabile

I dati sono esatti e aggiornati?

L'esattezza e genuinità del dato è garantita da misure tecniche che ne impediscono la modifica.

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

I dati sono conservati per **7 giorni**, salvo comprovate ragioni di giustizia avanzate dall'Autorità giudiziaria o dall'Autorità di Polizia, nel pieno rispetto del Provvedimento dell'Autorità Garante per la protezione dei dati personali in materia di videosorveglianza (8 aprile 2010).

Valutazione: Accettabile

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Nell'area di operatività di ogni videocamera è affissa apposita cartellonistica conforme al Provvedimento dell'Autorità Garante per la protezione dei dati personali in materia di videosorveglianza (8 aprile 2010).

Sul sito web istituzionale è inoltre pubblicata una informativa sul trattamento dei dati ex art. 13 Reg. 2016/679/UE comprendente un elenco della dislocazione territoriale delle videocamere. Tale documento è accessibile tramite un collegamento diretto dalla homepage.

Valutazione: Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

La base giuridica del trattamento è lo svolgimento di un compito connesso all'esercizio di un pubblico interesse o di pubblici poteri. Non è pertanto richiesto il consenso dell'interessato.

Valutazione: Accettabile

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

Non essendo possibile associare univocamente una immagine ad un interessato (non si trattano infatti dati biometrici), il diritto di accesso al dato personale non è di semplice attuazione. Il formato video di uso non comune utilizzato da un sistema professionale di videoregistrazione è altrettanto ostativo. Saranno comunque valutate, caso per caso, le singole richieste eventualmente pervenute al Titolare del trattamento, alla Polizia Locale o al Responsabile per la protezione dei dati personali (Data Protection Officer, DPO).
Alcune telecamere sono dotate di un sistema di riconoscimento delle targhe dei veicoli che transitano all'interno del raggio di azione degli impianti. In questi casi, il diritto di accesso è più facilmente esercitabile dal punto di vista tecnico.

Il diritto di portabilità dei dati non è esercitabile stante l'inapplicabilità dell'art. 20 Reg. 2016/679/UE al trattamento oggetto di valutazione.

Valutazione: Accettabile

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

Il diritto di rettifica non è concretamente esercitabile stante la natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo.

Il diritto di cancellazione è invocabile dagli interessati inoltrando apposita richiesta al Titolare del trattamento, alla Polizia Locale o al Responsabile per la protezione dei dati personali (Data Protection Officer, DPO) qualora ricorrano le condizioni di cui all'art. 17 Reg. 2016/679/UE.

Valutazione: Accettabile

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

Gli interessati possono esercitare i loro diritti di limitazione e di opposizione al trattamento contattando il Titolare del trattamento, la Polizia Locale o il Responsabile per la protezione dei dati personali (Data Protection Office, DPO).

Valutazione: Accettabile

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

Gli obblighi del Responsabile del trattamento sono assunti mediante determinazione del Responsabile del Servizio manutenzione e conservazione patrimonio n. 175 del 27.12.2017 integrata dalla deliberazioni n. 28 del 13.04.2012.

Valutazione: Accettabile

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

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

Valutazione: Accettabile

Rischi

Misure esistenti o pianificate

Crittografia

Le comunicazioni radio sono crittografate con il protocollo di sicurezza **WPA2/PSK.**

Valutazione: Accettabile

Controllo degli accessi logici

Solo utenti espressamente autorizzati possono accedere alle immagini in diretta ed alle immagini conservate sul server. Il sistema segnala all'utente l'utilizzo di una password considerata troppo debole, invitandolo così ad utilizzarne una adeguata.

Valutazione: Accettabile

Tracciabilità

Ogni operazione compiuta sui sistemi è registrata nel log degli eventi.
Il log eventi ha una durata programmabile e conserva tutti gli eventi di sistema (come, ad esempio, gli accessi da parte degli utenti). Ad oggi il sistema è programmato per salvare gli eventi degli ultimi 180 giorni.

Valutazione: Accettabile

Archiviazione

L’archiviazione sugli hard disk è fissata a 7 giorni. Successivamente, i dati più vecchi sono sovrascritti automaticamente

Valutazione: Accettabile

Minimizzazione dei dati

Sono raccolte le sole immagini di contesto, senza estrapolazione automatica dei di dati biometrici o di altre categorie particolari di dati.
Sono letti in automatico i dati relativi alle targhe dei veicoli che transitano sotto alcune telecamere più evolute (il cui elenco è rintracciabile nelle premesse del presente documento nonché nell'informativa pubblicata sul sito internet del Comune).

Valutazione: Accettabile

Vulnerabilità

I software e l'hardware sono aggiornati al bisogno durante l'attività di manutenzione compiuta dal Responsabile esterno del trattamento dei dati.

Valutazione: Accettabile

Lotta contro il malware

Il server, di tipo Linux, non è collegato direttamente alla rete internet.

Valutazione: Accettabile

Gestione postazioni

Il PC, sito nell'ufficio di Polizia locale che necessita di apposita chiave per l'accesso, è utilizzabile solo da utenti specifici muniti di credenziali di accesso personali.
Un Regolamento comunale disciplina le procedure di accesso alle postazioni.

Valutazione: Accettabile

Backup

Viene eseguita una ridondanza dei dati con metodo RAID 5 che rende il sistema resiliente alla perdita di uno o più dischi e poterli rimpiazzare senza interrompere il servizio.

Valutazione: Accettabile

Manutenzione

Il Responsabile esterno del trattamento provvede, secondo quanto stabilito da contratto, alla manutenzione programmata. L'attività è condotta in outsourcing.

Valutazione: Accettabile

Sicurezza dei canali informatici

Misure di sicurezza WPA2 e password. Il server che ospita le immagini non è allegato a internet riducendo così drasticamente i rischi di attacco da parte di cybercriminali.

Valutazione: Accettabile

Controllo degli accessi fisici

Il computer da cui si accede al server è collocato in un apposito locale chiuso a chiave, accessibile solo da specifici autorizzati al trattamento dei dati ritualmente nominati.

Valutazione: Accettabile

Sicurezza dell'hardware

La rete è isolata e non connessa a internet; oltre alle credenziali personali è presente una password sul PC di accesso al server.

Valutazione: Accettabile

Politica di tutela della privacy

Si è proceduto alla nomina del Data Protection Officer.
Il responsabile del servizio Polizia Locale vigila inoltre sulla genuinità del trattamento dei dati.

Valutazione: Accettabile

Gestione delle politiche di tutela della privacy

Il Titolare del trattamento ha predisposto un Regolamento comunale relativo alla protezione dei dati personali oltre ad uno specifico regolamento in materia di videosorveglianza.
È' stato istituito il registro dei trattamenti; il documento è periodicamente aggiornato.
L'ente ha anche predisposto una procedura operativa interna per la gestione di un eventuale data breach (deliberazione n. 80 del 15.10.2018.

Valutazione: Accettabile

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

È stato elaborato ed approvato un piano operativo per fare fronte al data breach che coinvolge diversi attori con ruoli precisi.

Valutazione: Accettabile

Gestione del personale

Il personale autorizzato al trattamento ha ricevuto una formazione di base sulla protezione dei dati personali. La nomina degli incaricati dà conto del dovere di riservatezza cui sono tenuti, in base alla normativa vigente.

Valutazione: Accettabile

Accessi diversificati

La password è diversificata tra l'utenza della Polizia Locale e del Responsabile esterno (che è il manutentore del sistema) in modo da poter identificare chi accede al sistema.

Valutazione: Accettabile

Misure antincendio

Il trattamento dei dati avviene nel pieno rispetto degli obblighi normativi in materia di prevenzione incendi.
Nella sede municipale sono presenti n. 3 estintori, di cui n. 1 posto nelle immediate vicinanze dell'ufficio preposto.

Valutazione: Accettabile

Accesso illegittimo ai dati

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

Lesione al diritto all'immagine, Lesione del diritto alla riservatezza, Percezione di insicurezza

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Attacco da remoto ai sistemi, Attacco fisico, Visione dei monitor della diretta

Quali sono le fonti di rischio?

Fonti umane interne, Fonti umane esterne

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Controllo degli accessi logici, Tracciabilità, Minimizzazione dei dati, Gestione postazioni, Lotta contro il malware, Politica di tutela della privacy, Vulnerabilità, Gestione del personale, Accessi diversificati, Gestione delle politiche di tutela della privacy, Controllo degli accessi fisici, Sicurezza dei canali informatici, Manutenzione

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

Trascurabile,

La gravità delle conseguenze di un ipotetico accesso non autorizzato agli impianti di videosorveglianza sono del tutto trascurabili. Chi accede agli impianti visiona unicamente immagini riguardanti persone e cose presenti in un pubblico spazio (territorio urbano) o, in alcuni casi, il transito di un determinato veicolo, in precise circostanze di tempo e di luogo. Non essendo impianti con caratteristiche di riconoscimento biometrico, è impossibile associare univocamente una figura umana che compare nelle immagini ad una persona fisica (a meno che l'intruso non conosca personalmente l'interessato). E' invece possibile, in via ipotetica, riscontrare passaggi di veicoli attraverso una ricerca mirata per targa. Qualora un interessato venisse a conoscenza dell'intrusione, scaturirebbero conseguenze psicologiche di bassissimo impatto quali, a titolo esemplificativo, semplice fastidio e percezione di pericolo non particolarmente intensa con riferimento all'impressione di violazione della propria riservatezza, senza pur patire un danno reale.

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

Trascurabile, Le misure di sicurezza paiono adeguate a proteggere i dati personali trattati da accessi non autorizzati in considerazione del contesto gli impianti saranno in funzione.
La probabilità di concretizzazione del rischio di accesso illegittimo ai dati è trascurabile, soprattutto per quanto concerne gli attacchi di soggetti esterni all'Ente. Il server non è collegato ad internet (riducendo drasticamente, quindi, la già scarsissima probabilità di attacco informatico esterno) e le telecamere trasmettono le immagini con segnale radio crittografato.
Trascurabile inoltre la probabilità di accesso illegittimo ai dati ad opera di fonti umane interne. Gli autorizzati al trattamento sono soggetti specifici (e numericamente limitati) in possesso di credenziali personali (e ciò è valido anche in relazione al Responsabile esterno del trattamento). La presenza di un log eventi consente di monitorare ogni accesso, tenendo così traccia anche degli accessi illeciti e non motivati. I log eventi è controllato periodicamente proprio a tal fine. L'asportazione fisica dei supporti di memorizzazione è una azione che ha anch'essa una probabilità di verificazione del tutto irrisoria: i locali che ospitano tali supporti sono inaccessibili da chiunque non sia in possesso di apposita chiave di accesso in quanto chiusi in un locale adibito *ad hoc*.

Il monitor per la visualizzazione in diretta delle immagini è sito in posizione tale da non essere visibile al pubblico, evitando così che chiunque possa visionare le immagini.

Valutazione: Accettabile

Modifiche indesiderate dei dati

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

Lesione al diritto all'immagine, Lesione all'integrità del dato personale, Impossibilità di tutela a seguito di un reato subito, Percezione di insicurezza

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

Attacco da remoto, Attacco fisico

Quali sono le fonti di rischio?

Fonti umane interne, Fonti umane esterne

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

Crittografia, Controllo degli accessi logici, Tracciabilità, Minimizzazione dei dati, Vulnerabilità, Lotta contro il malware, Gestione postazioni, Manutenzione, Sicurezza dei canali informatici, Controllo degli accessi fisici, Sicurezza dell'hardware, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Accessi diversificati, Gestione del personale

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

Limitata, Una modificazione indesiderata delle immagini comporterebbe un rischio limitato con riguardo al profilo psicologico dell'interessato. Il senso di violazione della propria riservatezza sarebbe apprezzabile, sebbene priva di danni irreparabili. Ciò potrebbe comportare un disturbo di contenuta gravità ma oggettivo, soprattutto nelle persone più suscettibili. Le immagini alterate potrebbero essere utilizzate, in linea teorica, per scherni, intimidazioni o ricatti verso gli interessati ad opera di malintenzionati.

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

Trascurabile, Sebbene il rischio zero sia da considerarsi un'utopia a carattere precipuamente teorico, la modifica dell'immagine raccolta da una telecamera di videosorveglianza è un'operazione tecnicamente molto complessa. Il rapporto costi/benefici tra i mezzi impiegati ed i risultati ottenuti per compiere l'azione illecita risulta davvero sproporzionato.
In ogni caso, le misure di sicurezza che sono state adottate contribuiscono ad abbattere drasticamente la già scarsissima probabilità di verificazione dell'evento.

Valutazione: Accettabile

Perdita di dati

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

Lesione alla integrità del dato personale, Impossibilità di tutela a seguito di un reato subito, Percezione di insicurezza

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

Attacco da remoto, Attacco fisico, Malfunzionamenti fisici dei sistemi, Eventi naturalistici

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, Archiviazione, Sicurezza dei canali informatici, Controllo degli accessi fisici, Sicurezza dell'hardware, Gestione delle politiche di tutela della privacy, Gestione del personale, Accessi diversificati, Politica di tutela della privacy, Manutenzione, Backup, Gestione postazioni, Tracciabilità, Vulnerabilità, Lotta contro il malware, Misure antincendio

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

Limitata, Una perdita indesiderata delle immagini comporterebbe un rischio limitato con riguardo al profilo psicologico dell'interessato. Il senso di violazione della propria riservatezza sarebbe apprezzabile, sebbene priva di danni irreparabili. Ciò potrebbe comportare un disturbo di contenuta gravità ma oggettivo, soprattutto nelle persone più suscettibili. La perdita del dato comporterebbe l'impossibilità di utilizzare le immagini per reprimere i reati commessi, con conseguente danno materiale e morale per l'interessato che accresce in relazione alla gravità del reato subito

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

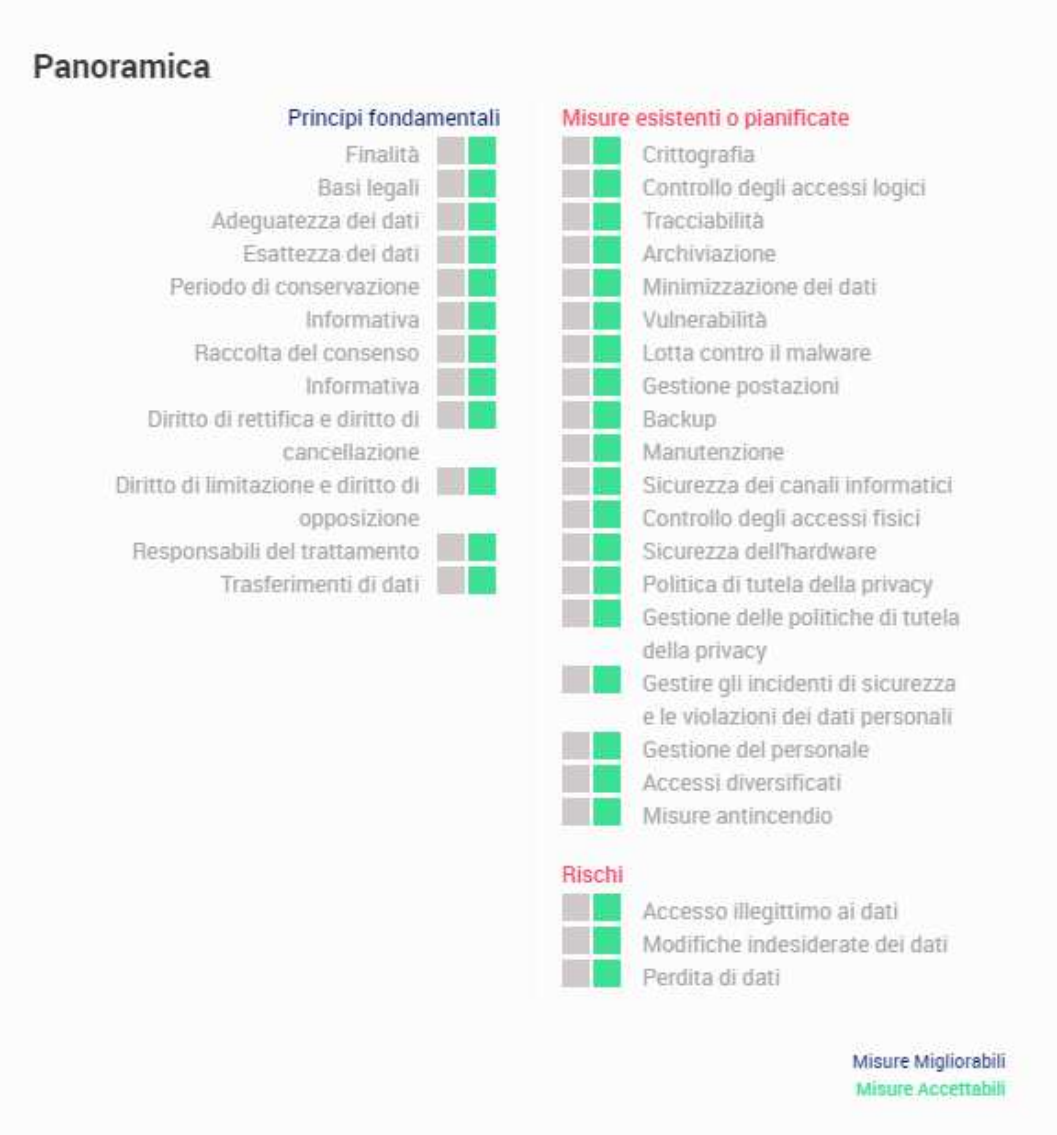
Trascurabile,

Le misure di sicurezza che sono state adottate contribuiscono ad abbattere drasticamente la probabilità di verificazione di una perdita dei dati.
Le misure antincendio, sebbene non soggette ad automatismi, sono proporzionate alle modeste dimensioni del server ospitato.
La politica di memorizzazione consente di salvare le immagini su più dischi fisici, indipendenti tra loro, e garantire una continuità operativa (grazie alla tecnologia RAID) anche nel caso venisse meno uno dei supporti e prima che esso sia sostituito.
Le misure informatiche e fisiche paiono adeguate a prevenire la perdita dei dati trattati.
La politica di manutenzione periodica contribuisce a prevenire la probabilità di verificazione della perdita indesiderata di dati a causa di malfunzionamento degli apparati tecnici.
Il rischio di terremoti, che potrebbero ipoteticamente danneggiare i supporti, è di per sé trascurabile. Secondo la classificazione del rischio sismico condotta dal Dipartimento della Protezione Civile (http://www.protezionecivile.gov.it/jcms/it/classificazione.wp) il Comune di Santa Vittoria d'Alba è sito in zona 4 (rischio molto basso).

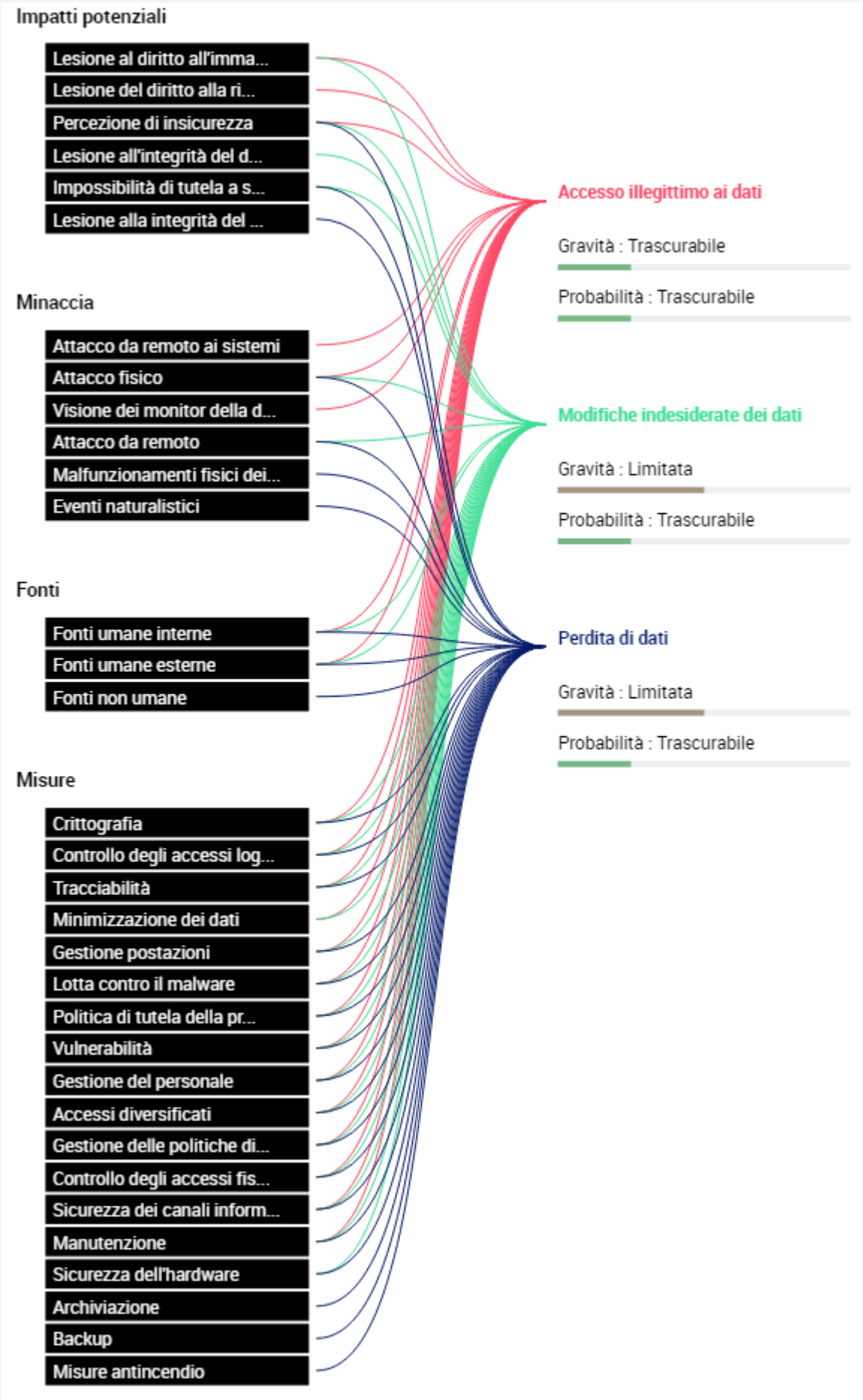
Valutazione: Accettabile

Grafiche

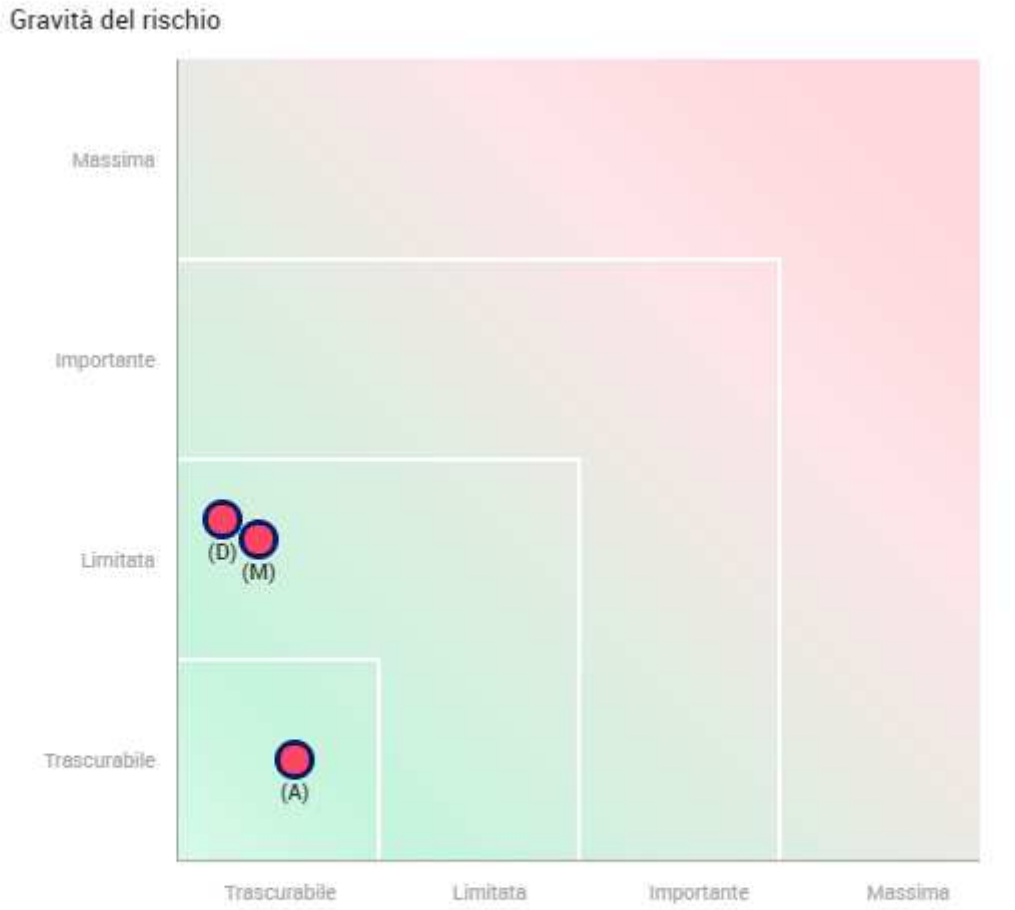
Principi fondamentali - Misure esistenti o pianificate



Panoramica dei rischi


Impatti potenziali
Lesione al diritto all'imma...
Lesione del diritto alla ri...
Percezione di insicurezza
Lesione all'integrità del d...
Impossibilità di tutela a s...
Lesione alla integrità del ...
Minaccia
Attacco da remoto ai sistemi
Attacco fisico
Visione dei monitor della d...
Attacco da remoto
Malfunzionamenti fisici dei...
Eventi naturalistici
Fonti
Fonti umane interne
Fonti umane esterne
Fonti non umane
Misure
Crittografia
Controllo degli accessi log...
Tracciabilità
Minimizzazione dei dati
Gestione postazioni
Lotta contro il malware
Politica di tutela della pr...
Vulnerabilità
Gestione del personale
Accessi diversificati
Gestione delle politiche di...
Controllo degli accessi fis...
Sicurezza dei canali inform...
Manutenzione
Sicurezza dell'hardware
Archiviazione
Backup
Misure antincendio
Accesso illegittimo ai dati
Gravità : Trascurabile
Probabilità : Trascurabile
Modifiche indesiderate dei dati
Gravità : Limitata
Probabilità : Trascurabile
Perdita di dati
Gravità : Limitata
Probabilità : Trascurabile

Mappaggio dei rischi



La presente valutazione d'impatto è aggiornata con cadenza **annuale**.

Santa Vittoria d'Alba, lì 11/02/2019

Il Titolare del trattamento

Il Data Protection Officer