Informazioni sulla PIA

Nome della PIA

Gestione Tasse Automobilistiche

Nome autore

Domenico Migali

Nome valutatore

Donatello Garcea

Nome validatore

Filippo De Cello

Data di creazione

01/08/2018

Nome del DPO/RPD

Non ancora richiesto parere DPO

Angela Stellato

Parere del DPO/RPD

Il parere del DPO deve essere ancora richiesto

Parere positivo in data 30/01/2019

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

La platea degli utenti interessati non è predeterminabile e individuabile a priori. Non è dunque possibile individuare preventivamente degli interessati.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Gestione dati sanitari contenuti nelle certificazioni delle Commissioni Mediche Integrate al fine di valutare la sussunzione dei contribuenti istanti nelle categorie di disabilità comportanti riconoscimento dell'esenzione dalla tassa automobilistica.

Quali sono le responsabilità connesse al trattamento?

I responabili del procedimento assumono cognizione dei dati sanitari dei contribuenti e dunque di dati sensibili afferenti la sfera personale di un rilevante numero di istanti. Tali dati devono essere accuratamente conservati per evitare indebite propalazioni all'esterno.

Ci sono standard applicabili al trattamento?

I responsabili di procedimento sono tenuti a garantire la riservatezza dei dati ai sensi del decreto 2755 del 2018, curando la conservazione delle pratiche cartacee e telematiche e adottando particolari cautele nella gestione dei sistemi informatici.

Valutazione : Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Dati sanitari, conservati per dieci anni successivi alla vendita o radiazione del veicolo. I dati evidenziano la sussistenza di patologie gravi ed invalidanti, tali da avere comportato il riconoscimento dello status di disabile da parte delle competenti Commissioni Mediche Integrate.

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

Le certificazioni mediche sono prodotte dagli istanti via mail, visionate dal dirigente ed assegnate al responsabile. Dunque sono memorizzate in un NAS ad accesso protetto. Analogo schema per le istanze prodotte via epistola cartacea, che sono memorizzate nel NAS previa scansione. Successivamente le mail o le epistole sono distrutte in modo da evitare ricostruzione dei dati.

Quali sono le risorse di supporto ai dati?

Le istanze arrivano via epistola cartacea ovvero via PEC su server ARUBA e sono archiviato previa scansionate o memorizzazione su NAS collegato a rete interna ad accesso riservato.

Valutazione : Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento è necessario per consentire all'Ente pubblico trattante di valutare se l'istante rientri nelle categorie di soggetti che possono beneficiare dell'esenzione tributaria. In base alle leggi tributarie, infatti, solo alcune categorie di disabili godono dell'esenzione ed è dunque necessario comprendere se l'istante rientri o meno nelle disabilità ammesse analizzando la tipologia di disabilità che il detto accusa.

Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Richiesto dalla legge (art. 8, l. 449/97; art. 50, l. 342/00; art. 30, co. 7, l. 388/00)

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)?

Non sono richiesti dati ulteriori a quelli necessari alla sussunzione nella categoria medica. Ove sia prodotto certificato recante con "omissis" nella descrizione dell'ananmesi, ma che comunque reca indicato seppur genericamente il possesso dei requisiti fiscali, la certificazione è ritenuta sufficiente e non è richiesta al contribuente la produzione di certificati con indicazione espressa della patologia.

Valutazione : Migliorabile
Piano d'azione / misure correttive :
Verificare possibilità di accesso alla banca dati I.N.P.S. al fine di assumere direttamente i dati necessari alla istruzione delle istanze.

I dati sono esatti e aggiornati?

I dati sono estrapolati da certificazioni mediche rilasciate dalle Commissioni Mediche Integrate. A campione i dati sono soggetti a verifica presso l'I.N.P.S.

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

Dieci anni dopo la perdita di possesso del veicolo. La tassa automobilistica può essere contestata dopo tre anni (atto) + due anni (cartella) + cinque anni (atto esecutivo). Potendo il contribuente proporre autotutela anche fuori termine è necessario attendere la prescrizione dell'ultimo atto prima di potere cancellare i dati. Parimenti, per le concessioni, il termine di potere di indagine della Corte dei Conti è decennale.

Valutazione : Accettabile

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Nel modulo di istanza è presente una nota esplicativa, ripetuta nel sito web.

Valutazione : Migliorabile
Piano d'azione / misure correttive :
Prevedere una informativa web più ampia e descrittiva
Commento di valutazione :
Prevedere una informativa web più ampia e descrittiva

Ove applicabile: come si ottiene il consenso degli interessati?

Con la presentazione della istanza e la produzione della certificazione medica contentente i dati, gli istanti manifestano consenso implicito al trattamento.

Valutazione : Migliorabile
Piano d'azione / misure correttive :
Valutare la possibilità di evitare il consenso al trattamento assumendo le informazioni sanitarie tramite accesso diretto alla banca dati I.N.P.S.

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

Inviando una mail al DPO

Valutazione : Migliorabile
Piano d'azione / misure correttive :
Istruire gli sportelli alla ricezione di istanze informali da parte degli utenti.

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

Inviando una mail al DPO.

Valutazione : Migliorabile
Piano d'azione / misure correttive :
Istruire gli sportelli alla ricezione di istanze informali da parte degli utenti.

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

Inviando una mail al DPO

Valutazione : Migliorabile
Piano d'azione / misure correttive :
Istruire gli sportelli alla ricezione di istanze informali da parte degli utenti

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

Obblighi a trattare i dati assicurando garanzia della riservatezza sono imposti via decreto 2755 del 2018, la cui violazione può comportare applicazione di sanzioni disciplinari.

Valutazione : Migliorabile
Piano d'azione / misure correttive :
Prevedere esplicite attribuzioni nel seno del decreto di attribuzioni delle mansioni

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

Non è previsto trasferimento di dati fuori dell'Unione Europea. E' possibile che i dati, per finalità di raffronto o controllo, siano comunicati all'I.N.P.S. e ad Agenzia delle Entrate. La trasmissione dei dati è prevista in forma puntuale e non massiva.

Valutazione : Accettabile

Rischi

Misure esistenti o pianificate

Accesso riservato da password

Il NAS è collegato a rete interna non accessibile dall'esterno ed è protetto da password e contiene cartelle criptate.
Le password di accesso ai sistemi debbono avere date caratteristiche e devono essere mutate periodicamente, come previsto dal decreto 2755 del 2018

Valutazione : Migliorabile
Piano d'azione / misure correttive :
Verificare l'implementazione di sistemi crittografici per le informazioni contenute nel NAS.

NAS con ridondanza RAID, back up di sicurezza e ridondanza su PECOrganizzer

Per evitare perdite di dati i dati sono conservati in un NAS con ridondanza RAID e riprodotti in copia di back up di sicurezza gestita direttamente dal dirigente e conservata in luogo differente dai server principali. Le istanze sono conservate anche sui server del CED regionale all'interno del sistema PECOrganizzer che archivia ogni comunicazione PEC.

Valutazione : Migliorabile
Piano d'azione / misure correttive :
Posizionamento del NAS in sede territoriale di Reggio Calabria, al fine di disaster recovery per eventuali eventi catastrofici che dovessero colpire la sede principale di Catanzaro.

Limitazione della permanenza dei dati su server esterni

Le istanze che pervengono via PEC su server ARUBA accedibile (via password) anche dall'esterno, sono detenute nel seno dello stesso solo per il tempo necessario per lo smistamento.

Valutazione : Migliorabile
Piano d'azione / misure correttive :
Ridurre la permanenza sul server di ARUBA ad un periodo inferiore ai sette giorni, al fine di contenere la diffusione di dati sensibili nella ipotesi in cui la casella mail sia violata da accessi abusivi esterni.

Accesso illegittimo ai dati

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

Dati sanitari di terzi potrebbero essere propalati, con indicazione delle patologie che i detti accusano, I soggetti i cui dati siano propalati, potrebbero essere vittime di comportamenti discriminatori

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Apprensione dei dati da accesso abusivo al NAS o da soggetti che giungano in possesso delle istanze cartacee., Apprensione dei dati da accesso abusivo al sistema informatico esterno PEC Aruba

Quali sono le fonti di rischio?

Soggetti esterni all'amministrazione che accedano abusivamente al sistema PEC ARUBA, Soggetti esterni all'amministrazione che apprendano copie delle pratiche cartacee in lavorazione, Soggetto interno all'amministrazione che violi il NAS accedibile solo da rete interna

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Limitazione della permanenza dei dati su server esterni, Accesso riservato da password

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

Importante, Sarebbero propalati dati sensibili di natura sanitaria di una vasta platea di contribuenti, anche se occorre significare che in diversi casi i contribuenti allegano certificati coperti da omissis che pur evidenziando stato di disabilità non evidenziano in modo espresso il tipo preciso di patologia accusata.

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

Trascurabile, I dati sono conservati su server accedibili solo da rete interna e comunque coperti da password e cartelle criptate.

Valutazione : Migliorabile
Piano d'azione / misure correttive :
- Verificare con frequenza la legittimazione all'accesso da parte degli operatori, al fine di evitare permanenza di utenze nella ipotesi di sopravvenuta cessazione delle mansioni relative
- Prevedere dei log di accesso per tracciare i comportamenti delle utenze abilitate all'accesso
- Limitare a massimo sette giorni la permanenza sul server esterno PEC ARUBA

Alla luce del piano d'azione, come valutate la gravità di questo rischio (Accesso illegittimo ai dati)? **Trascurabile**
Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Accesso illegittimo ai dati)? **Trascurabile**

Modifiche indesiderate dei dati

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

Sul contribuente i rischi sarebbero limitati: l'amministrazione potrebbe non riconoscere una esenzione tributaria e contestare l'omissione tributaria ma il contribuente, producendo il dato corretto sarebbe comunque in grado di fare annullare l'atto in autotutela

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

Non se ne ravvedono. La perdita dei dati è un rischo concreto ma la modificazione accidentale o dolosa dei dati è improbabile: i dati sono conservati in formato pdf immodificabile e conservati in ridondanza in un sistema tripartito. Per modificare il dato il presunto offensore dovrebbe accedere a tre sistemi differenti, uno dei quali gestito direttamente ed esclusivamente dal dirigente

Quali sono le fonti di rischio?

Non se ne ravvedono

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

NAS con ridondanza RAID, back up di sicurezza e ridondanza su PECOrganizzer, Accesso riservato da password

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

Trascurabile, I contribuenti avrebbero un rischio limitato dalla modificazione del dato: sono in grado di comprovare in autotutela o via giudiziale il contenuto corretto del dato. Essi infatti detengono il documento originale che comunque è riproducibile dall'I.N.P.S.
La P.A. potrebbe invece rischiare di emanare (o non emanare) atti sulla scorta di dati travisati.

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

Trascurabile, Non esiste possibilità di rischio di modifica dei dati. La ridondanza dei sistemi di archiviazione, la tipologia di archiviazione e l'assenza di un interesse alla modificazione rendono improbabile l'ipotesi.

Valutazione : Migliorabile
Piano d'azione / misure correttive :
Effettuare confronti a campione tra i files contenuti nei diversi archivi di back up, al fine di verificare eventuali modificazioni

Alla luce del piano d'azione, come valutate la gravità di questo rischio (Modifiche indesiderate dei dati)? **Trascurabile**
Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Modifiche indesiderate dei dati)? **Trascurabile**

Perdita di dati

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

Sugli interessati nessuno. La PA potrebbe invece dovere giustificare concessioni di beneficio non comprovabili (in caso di istanza accolta) ovvero potrebbe non potere giustificare atti di accertamento o cartelle esattoriali (in caso di istanza rigettata)

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

Problemi tecnici sui server (rotture plurime) o eventi catastrofici su sito di archiviazione.

Quali sono le fonti di rischio?

Senescenza dell0 hardware con rischio crescente di rottura., Eventi catastrofici su sito nel quale sono conservati i server

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

NAS con ridondanza RAID, back up di sicurezza e ridondanza su PECOrganizzer

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

Importante, Per il contribuente limitato: i dati restano in sua disponibilità e comunque sono detenuti anche da I.N.P.S. Ma per l'Amministrazione il rischio è alto: indimostrabilità in Corte dei Conti della legittimità dell'accoglimento ovvero in Commissione Tributaria della legittimità del diniego, con correlate possibili condanne erariali o condanne da soccombenza giudiziale.

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

Trascurabile, Sistema di archiviazione tripartito su tre archivi informatici autonomi ed indipendenti.

Valutazione : Migliorabile
Piano d'azione / misure correttive :
- Installare il NAS in luogo fisico diverso (sede territoriale di Reggio Calabria) rispetto alla sede dove sono installati i server PECOrganizzer (sede principale di Catanzaro), al fine di disaster recovery in caso di eventi catastrofici o tellurici.
- Prevedere protocollo di intesa con I.N.P.S. per il recupero dei dati eventualmente persi
- Aumentare la frequenza dei back up sul disco esterno gestito dal dirigente

Alla luce del piano d'azione, come valutate la gravità di questo rischio (Perdita di dati)? **Limitata**
Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Perdita di dati)? **Trascurabile**

Piano d'azione

Panoramica

Principi fondamentali

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

Misure esistenti o pianificate

Accesso riservato da password
NAS con ridondanza RAID, back up di sicurezza e ridondanza su PECOrganizzer
Limitazione della permanenza dei dati su server esterni

Rischi

Accesso illegittimo ai dati
Modifiche indesiderate dei dati
Perdita di dati

Misure Migliorabili
Misure Accettabili

Principi fondamentali

Adeguatezza dei dati

Piano d'azione / misure correttive :
Verificare possibilità di accesso alla banca dati I.N.P.S. al fine di assumere direttamente i dati necessari alla istruzione delle istanze.
Data prevista di implementazione : 31/12/2019
Responsabile dell'implementazione : Dirigente Settore Tasse Automobilistiche

Informativa

Piano d'azione / misure correttive :
Prevedere una informativa web più ampia e descrittiva
Commento di valutazione :
Prevedere una informativa web più ampia e descrittiva
Data prevista di implementazione : 31/12/2019
Responsabile dell'implementazione : Dirigente Settore Tasse Automobilistiche

Raccolta del consenso

Piano d'azione / misure correttive :
Valutare la possibilità di evitare il consenso al trattamento assumendo le informazioni sanitarie tramite accesso diretto alla banca dati I.N.P.S.

Data prevista di implementazione : 31/12/2019
Responsabile dell'implementazione : Dirigente Settore Tasse Automobilistiche

Informativa

Piano d'azione / misure correttive :
Istruire gli sportelli alla ricezione di istanze informali da parte degli utenti.
Data prevista di implementazione : 31/12/2019
Responsabile dell'implementazione : Dirigente Settore Tasse Automobilistiche

Diritto di rettifica e diritto di cancellazione

Piano d'azione / misure correttive :
Istruire gli sportelli alla ricezione di istanze informali da parte degli utenti.
Data prevista di implementazione : 31/12/2019
Responsabile dell'implementazione : Dirigente Settore Tasse Automobilistiche

Diritto di limitazione e diritto di opposizione

Piano d'azione / misure correttive :
Istruire gli sportelli alla ricezione di istanze informali da parte degli utenti
Data prevista di implementazione : 31/12/2019
Responsabile dell'implementazione : Dirigente Settore Tasse Automobilistiche

Responsabili del trattamento

Piano d'azione / misure correttive :
Prevedere esplicite attribuzioni nel seno del decreto di attribuzioni delle mansioni
Data prevista di implementazione : 31/12/2019
Responsabile dell'implementazione : Dirigente Settore Tasse Automobilistiche

Misure esistenti o pianificate

Accesso riservato da password

Piano d'azione / misure correttive :
Verificare l'implementazione di sistemi crittografici per le informazioni contenute nel NAS.
Data prevista di implementazione : 31/12/2019
Responsabile dell'implementazione : Fornitore informatico convenzionato

NAS con ridondanza RAID, back up di sicurezza e ridondanza su PECOrganizzer

Piano d'azione / misure correttive :
Posizionamento del NAS in sede territoriale di Reggio Calabria, al fine di disaster recovery per eventuali eventi catastrofici che dovessero colpire la sede principale di Catanzaro.
Data prevista di implementazione : 31/12/2019
Responsabile dell'implementazione : Fornitore informatico convenzionato

Limitazione della permanenza dei dati su server esterni

Piano d'azione / misure correttive :
Ridurre la permanenza sul server di ARUBA ad un periodo inferiore ai sette giorni, al fine di contenere la diffusione di dati sensibili nella ipotesi in cui la casella mail sia violata da accessi abusivi esterni.
Data prevista di implementazione : 31/12/2019
Responsabile dell'implementazione : Dirigente Settore Tasse Automobilistiche

Rischi - Accesso illegittimo ai dati

Piano d'azione / misure correttive :
- Verificare con frequenza la legittimazione all'accesso da parte degli operatori, al fine di evitare permanenza di utenze nella ipotesi di sopravvenuta cessazione delle mansioni relative
- Prevedere dei log di accesso per tracciare i comportamenti delle utenze abilitate all'accesso
- Limitare a massimo sette giorni la permanenza sul server esterno PEC ARUBA

Data prevista di implementazione : 31/12/2019
Responsabile dell'implementazione : Dirigente settore / Fornitore informatico
Alla luce del piano d'azione, come valutate la gravità di questo rischio (Accesso illegittimo ai dati)? **Trascurabile**
Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Accesso illegittimo ai dati)? **Trascurabile**

Rischi - Modifiche indesiderate dei dati

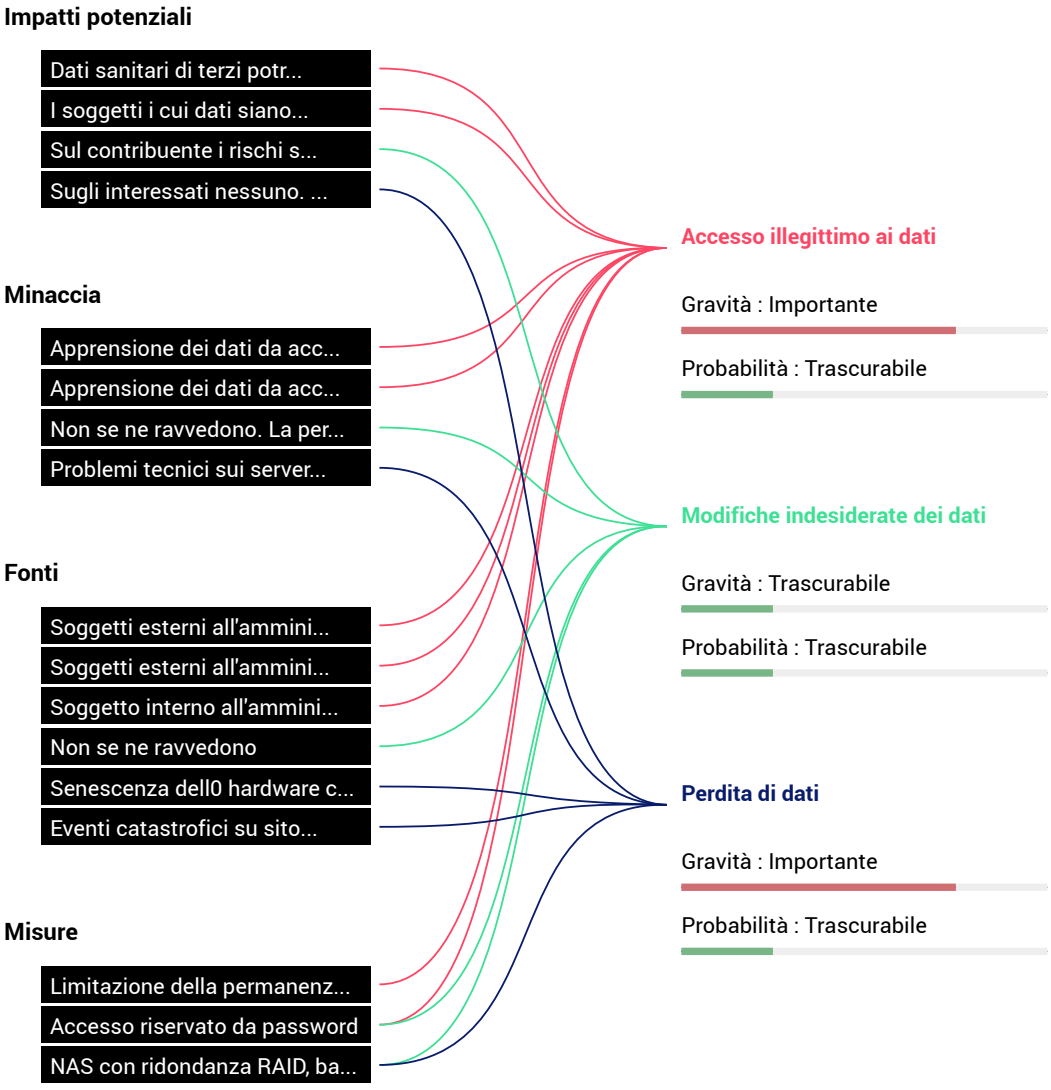
Piano d'azione / misure correttive :
Effettuare confronti a campione tra i files contenuti nei diversi archivi di back up, al fine di verificare eventuali modificazioni
Data prevista di implementazione : 31/12/2019
Responsabile dell'implementazione : Dirigente Settore Tasse Automobilistiche
Alla luce del piano d'azione, come valutate la gravità di questo rischio (Modifiche indesiderate dei dati)? **Trascurabile**
Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Modifiche indesiderate dei dati)? **Trascurabile**

Rischi - Perdita di dati

Piano d'azione / misure correttive :
- Installare il NAS in luogo fisico diverso (sede territoriale di Reggio Calabria) rispetto alla sede dove sono installati i server PECOrganizzer (sede principale di Catanzaro), al fine di disaster recovery in caso di eventi catastrofici o tellurici.
- Prevedere protocollo di intesa con I.N.P.S. per il recupero dei dati eventualmente persi
- Aumentare la frequenza dei back up sul disco esterno gestito dal dirigente

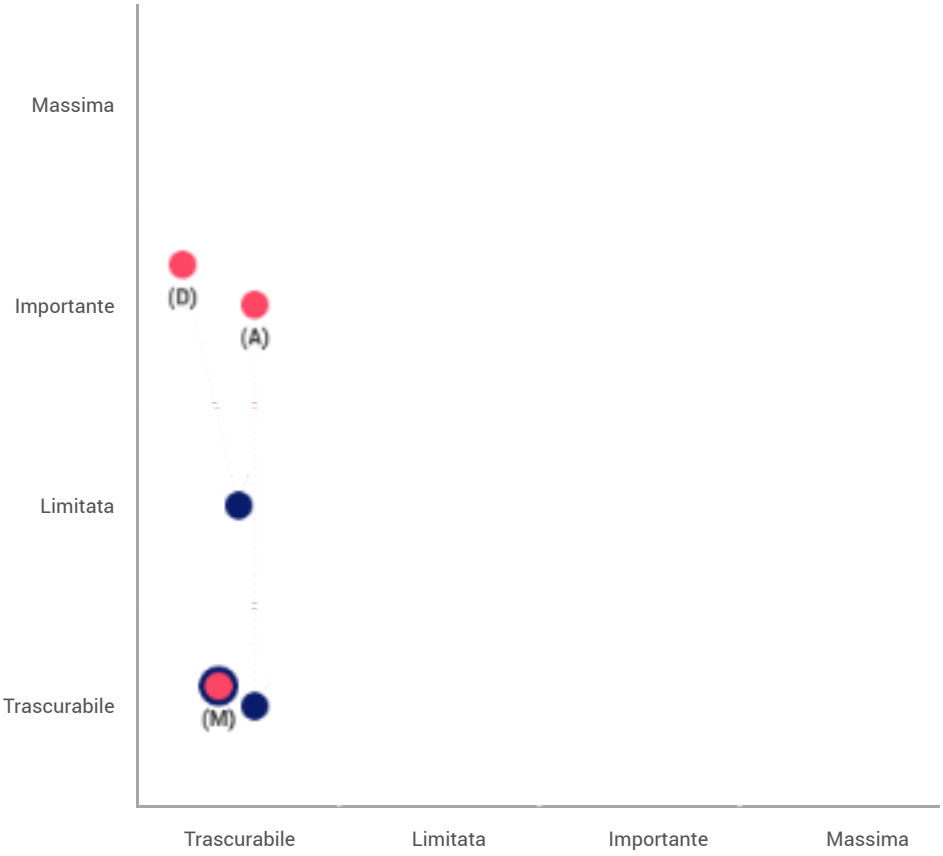
Data prevista di implementazione : 31/12/2019
Responsabile dell'implementazione : Fornitore informatico / Dirigente Settore
Alla luce del piano d'azione, come valutate la gravità di questo rischio (Perdita di dati)? **Limitata**
Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Perdita di dati)? **Trascurabile**

Panoramica dei rischi



Mappaggio dei rischi

Gravità del rischio



Probabilità del rischio

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