CNIL. PROTÉGER les données personnelles ACCOMPAGNER l'innovation PRÉSERVER les libertés individuelles

Documento di valutazione di Impatto su Trattamenti di Dati
(DPIA.CNIL_REP Ed. 2023-2024)

Preambolo di contesto:
La nostra azienda ha svolto una valutazione dei rischi (DVR) ai sensi dell'Art. 35 del Regolamento Generale della Protezione dei Dati Personali (GDPR – Reg.679/16 e succ. Dlg.101/18). Dalla analisi commissionata dal TDT al RET (consulente esterno autorizzato al trattamento), non sono emersi trattamenti di cui al Provvedimento N. 467 11 Ottobre 2018 (Doc.web: 9058979) e suo allegato con relativa newsletter della Autorità Garante.

Ancor che non necessaria, in considerazione dei Principi di minimizzazione dei rischi informatici e delle raccomandazioni in merito alla Sicurezza Preventiva da minacce del *Cyberspace*, è stato comunque deciso di svolgere una **DPIA** confinata ai trattamenti automatizzati con particolare riferimento alla Gestione del Sistema Aziendale della Posta Elettronica.

NOTA: I contenuti del Rapporto che segue sono fedelmente riportati dal layout del SW PIA.UE riconosciuto quale standard Europeo unificato dalle Istituzioni Europee.

TDT: RS MANAGEMENT Srl
Editing : Dott.ssa Serena Borelli
Evaluation : DIP, RET
Validation : Dott.ssa Sara Borelli
Status : In corso 90% (Piano di azioni non necessario)

Mappaggio dei rischi e Piano d'azione

- **Principi fondamentali**: Nessun piano d'azione registrato.
- **Misure esistenti o pianificate**: Nessun piano d'azione registrato.
- **Rischi**: Nessun piano d'azione registrato.

Validation
DPO and data subjects opinion: No data to display.

Contesto e Panoramica del trattamento

Quale è il trattamento in considerazione?

Trattamento della posta elettronica aziendale

Quali sono le responsabilità connesse al trattamento?

Elenco di figure nominate ai sensi del GDPR e s.s.m (Es. Dlg.vo 101/2018 nell'ambito della (D-SPPD)

1. Il titolare (TDT)
2. Designato Inteno Privacy (DIP) in rappresentanza dei Co-titolari,
3. Amministratore di Sicurezza ICT per la IntraLan (ADS-Intramurale LAN)
4. Amministratore di Sicurezza ICT per la ExtraLan (ADS-siti WEB)
5. Amministratore di Sicurezza ICT per la Network (ADS-WAN Sicurezza firewall)

Ci sono standard applicabili al trattamento?

No solo Direttiva AG in merito ai meta-dati che non sono applicabili perchè il TDT non attua forme di controllo remoto dei propri Operatori Autorizzati al Trattamento (OAT) (anche Lavoratori Incaricati).

Valutazione : Accettabile
Commento di valutazione :

Questa sezione e il suo contenuto discende da una pregressa procedura formalizzata come **Documento di Valutazione dei Rischi** (DVR).

In seguito alla ricognizione di tutti i tipi di Trattamento dei Dati in questo contesto si è identificato quello relativo al **Sistema di Posta Elettronica previsto** come tipologia **di Trattamento Automatizzato ICT**.

Per il potenziale rischio di merito, è stata svolta la Valutazione degli Impatti formalizzata in questo documento (DPIA), con lo scopo di validare come accettabile e conforme il proprio Sistema Privacy e di Protezione dei Dati personali

La opportunità di redazione del DPIA è stata approvata a partire dal Piano di Adeguamento e Riedizione del Sistema Privacy e Protezione dei Dati nella transizione 2023-2024.

Il DPIA della R&S Management SrL è svolto secondo principio di "Accountability" a cura del:

Titolare del Trattamento (TDT): **Dott.ssa Serena Borelli**
Delegato Interno al Trattamento (DIP): **Dott.ssa Sara Borelli**
Responsabile Esterno del Trattamento (RET): **Dott.Salvo Reina**
NOTA: Tutti i riferimenti utili del presente DPIA sono disponibili nella documentazione di Sistema pubblicato in formato web disponibile dal sito ufficiale

www.rsmanagement.it

Contesto: Dati, processi e risorse di supporto

Quali sono i dati trattati?

Contenuti e allegati del Sistema di Posta Elettronica
NO METADATI

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

Dalla creazione di un Account per il singolo operatore assunto, successivamente tutti le comunicazione di posta elettronica sono confinate nel Server di Posta su Cloud Microsoft365 e ovviamente in locale nella stazione di lavoro del profilo utente validato con Server di LAN basato su Active Directory per evitare ogni possibile accesso estraneo.

Quali sono le risorse di supporto ai dati?

Server Exchange in Cloud, PC dedicato, Backup di sicurezza delle comunicazione INTRALAN su 2 dispositivi NAS RAID5

SEZ. - Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Si, gli scopi

a) riflettono la Politica del Sistema Privacy e Protezione dei Dati
b) sono formalizzati nella documentazione del Manuale (D-SPPD)
c) sono stati concordate con tutte le parti interessate (interne ed esterne)
d) sono stati pubblicati/comunicati a mezzo Informative

Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Nella fatti specie dell'ambito di cui in Valutazione degli Impatti di Sicurezza (D-PIA) per tutti i soggetti coinvolti/implicati nella Gestione della Posta Elettronica Aziendale le lasi legali del trattamento sono il Consenso libero e inequivocabile espresso/sottoscritto dall'Interessato.

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)?

SI

Valutazione : Accettabile

I dati sono esatti e aggiornati?

SI. Riflettono i contenuti delle comunicazioni relative alle attività di business

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

I dati del Sistema di Posta Elettronica Aziendale sono conservati in relazione alle tipologie di attività finalizzate alla missione aziendale.
Nessun contenuto viene pregiudizialmente cancellato anche per essere reso disponibile in caso di controlli. Nella circostanza di un profilo dimissionario,

Valutazione : Accettabile

Principi Fondamentali
Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Agli operatori interni all'azienda viene somministrato un Piano di Formazione e affiancamento continuo
I Clienti interessati dispongono di Informative (cartiglio email e WEB aziendale).

Ove applicabile: come si ottiene il consenso degli interessati?

Con operatori interni autorizzati al trattamento (vedi sopra OAT) il consenso è raccolto in presenza al tempo della stipola del contratto di lavoro ()

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

Tramite canale web nella apposita area per le comunicazioni e ele segnalazioni al Titolare

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

Tramite canale web nella apposita area per le comunicazioni e ele segnalazioni al Titolare

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

Tramite canale web nella apposita area per le comunicazioni e ele segnalazioni al Titolare

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

Sempre

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

Per la posta elettronica gestita nel Cloud esiste sempre la possibilità di risiedere o essere replicati fisicamente in locazione transfrontaliera. In questa situazione la sicurezza è garantita dal contratto di fornitura dell SaaS.
Per la Sicurezza delle copie di comunicazioni nei dispositivi intramurali NAS, sono programmate dagli ADS procedure automatiche (Batch e Bash) che garantiscono ridondanza, isolamento e confinamento di trasmissione dati comunque cifrate a mezzo FTPS

Rischi - Misure esistenti o pianificate

Crittografia

A tutte le forme di Copie e/o Repliche di sicurezza, siano esse
persistite su supporti di stoccaggio NAS (RAID5 e R-sync), trasmesse telematicamente nelle comunicazioni Server FTP, memorie fisiche locali nelle stazioni di ogni Operatore

Sono applicati livelli di crittografia quali:
Certificato SSH/TSL con il Server WEBmail del Provider
Credenziali HASH a 2° livello di alberatura del sito web (PHP)
Credenziali di Gestione proprietarie per la Gestione di tutti i Siti web pubblicati da TDT e Co-titolari (Piattaforma WordPress)

Chiavi PGP e/o semi full-pass per permessi multimodali e multi utenti su accesso/modifica/stampa di documentazioni sensibili
Credenziali di Gestioni amministrative degli ADS (Amministratori di Sicurezza) con autenticazzione a 2 fattori (OTP)
Cifratura Kerberos del servizio del Server Windows Active Directory INTRALAN pre le auteticazioni delle postazioni di lavoro

Sicurezza dei documenti cartacei

Eventuali versioni cartacee delle comunicazioni di Posta Elettronica e loro allegati sono conservate e securitate secondo misure logiche e organizzative quali:

confinamento e segregazione elettiva agli ambienti/locali amministrativi competenti
armadi ignifughi con serramento
impianto anti-intrusione fuori orario degli uffici

Tutto il personale elettivamente autorizzato ha ricevuto formazioni e istruzioni operative concernenti i criteri di stampa, archiviazione, condivisione e distruzione dei dati.

Controllo degli accessi logici

Tutti i mezzi di autenticazione implementati e applicabili,e le regole per la accettazione delle password degli account di Posta Elettronica (Es. lunghezza minima, caratteri richiesti, durata della validità, numero di tentativi prima del blocco dell'account, ecc.) seguono gli standard di cui al Paragrafo "CRITTOGRAFIA" sopra esposto.

Tracciabilità

Per ciò che attiene al Sistema di Gestione della Posta Elettronica aziendale **nessun tracciamento** dei log nè post-eleborazione dei meta dati delle singole comunicazione viene effettuata.
In accordo all'approccio *By-Design*, lo stesso Servizio Emails in Cloud (Microsoft365 - Exchange) non viene programmato per raccogliere elaborazioni di tracciamento a fini di controllo remoto degli operatori.

Archiviazione

Tutti gli archivi elettronici originati, conservati, archiviati dai Sistemi informativi attuano Politiche e istruzioni operative finalizzate alla validazione giuridica per il periodo richiesto dal *business* aziendale.
Nei casi di Legittimo Interesse (Es. accordi vincolanti di impresa, appalti e/o convenzioni con Enti Pubblici e/o attività di controllo delle Autorità Istituzionali) la azienda può fornire accesso selettivo (*Smart Contract*) ai repertori digitali storicizzati comunque in modo limitato e finalizzato al contesto.

Vulnerabilità e Difesa Preventiva dalle Minacce Cyber e Malware

Tutti i Sistemi Informatici sono inerentemente vulnerabili e il rischio zero non esiste. Peraltro, insieme ai *BYOD*, la posta elettronica è notoriamente il più sensibile ai fenomeni di Defacing, MITM, *Phishing* e la minaccia più temibile del *Ransonware*.

Il TDT ha quindi dotato anche il sistema di Posta Elettronica strumenti HW e SW di Sicurezza Cyber adeguati.

La nostra difesa preventiva e resiliente è basata su un sistema di *Appliance* ingegnerizzato HW nel Firewall, pertanto a livello di Difesa Perimetrale di Dominio.

In ultima analisi i dati di posta elettronica viaggiano nel flusso di connettività; in sintesi si tratta di informazione che si poggia su protocolli di *network* o trasmissione.

La adozione di questa misura preventiva non solo è efficace sul monitoraggio continuo del flusso di comunicazione (sia entrata che uscita) ma serve contestualmente come Sistema antivirus a livello di analisi TCP/IP. Questo permette un sistema IDS (di detezione e difesa da intrusione). In merito al sistema di antivirus, tutte le postazioni di lavoro ne sono dotate e il livello di configurazione è delegato elettivamente alle figure di ADS

Altro canale critico è la vulnerabilità dei dispositivi personali quali cellulare, iPad e notebook complessivamente definiti BYOD.
In merito tutti gli operatori aziendali vengono istruiti (formazioine e sensibilizzazione; Es. utilizzo dei *pendrive*) in merito alle giuste prassi di utilizzo volte a mitigare e remotizzare il più possibile attacchi di tipo *Zero Day* e *Zero Clic*

Per tutti i dispositivi/apparati di memoria di massa della rete aziendale (NAS)

Sicurezza dei siti web

La sicurezza dei siti web aziendali è contrattualizzata con il provider del dominio primario. La responsabilizzazione e l'impegno alla sicurezza informatica è pertanto trasferita al provider che controllo lo spazio web e risponde della sua integrità nei termini pattuiti con SLA e PLA.

Rischi - Accesso illegittimo ai dati

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

Nel contesto di cui in oggetto si risponde:,

1. ***Interruzione delle comunicazioni di posta elettronica,***
2. ***Potenziali disinformazioni e misinformazioni dovute a disservizio,***
3. ***Blocchi di attività di business,***
4. ***Ritardi nelle consegne e chiusure di Commesse***

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Vedi paragrafo precedente0

Quali sono le fonti di rischio?

Inadeguata formazione e affiancamento, Operatori infedeli che svolgono ruolo di insider, Operatori e/o consulenti non competenti

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Sicurezza dei documenti cartacei, Controllo degli accessi logici, Tracciabilità, Archiviazione, Vulnerabilità e Difesa Preventiva dalle Minacce Cyber e Malware, Sicurezza dei siti web

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

Trascurabile, Oggettivamente valutata sulla base del Capitolo precedente relativo alle Misure di Sicurezza adottate

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

Trascurabile, Oggettivamente valutata sulla base del Capitolo precedente relativo alle Misure di Sicurezza adottate

Rischi - Modifiche indesiderate dei dati

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

Nel contesto di cui in oggetto si risponde

1. *Interruzione delle comunicazioni di posta elettronica,*
2. *Potenziali disinformazioni e misinformazioni dovute a disservizio,*
3. *Blocchi di attività di business,*
4. *Ritardi nelle consegne e chiusure di Commesse,*

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

Vedi paragrafo precedente

Quali sono le fonti di rischio?

Inadeguata formazione e affiancamento, Operatori e/o consulenti non competenti, Operatori infedeli che svolgono ruolo di insider

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

Crittografia, Sicurezza dei documenti cartacei, Controllo degli accessi logici, Tracciabilità, Archiviazione, Vulnerabilità e Difesa Preventiva dalle Minacce Cyber e Malware, Sicurezza dei siti web

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

Trascurabile, Oggettivamente valutata sulla base del Capitolo precedente relativo alle Misure di Sicurezza adottate

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

Trascurabile, Oggettivamente valutata sulla base del Capitolo precedente relativo alle Misure di Sicurezza adottate

Rischi - Perdita di dati

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

Nel contesto di cui in oggetto si risponde:

1. Interruzione delle comunicazioni di posta elettronica,
2. Potenziali disinformazioni e misinformazioni dovute a disservizio,
3. Blocchi di attività di business,
4. Ritardi nelle consegne e chiusure di Commesse,

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

Vedi paragrafo precedente

Quali sono le fonti di rischio?

Inadeguata formazione e affiancamento, Operatori e/o consulenti non competenti, Operatori infedeli che svolgono ruolo di insider

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

Crittografia, Sicurezza dei documenti cartacei, Controllo degli accessi logici, Tracciabilità, Archiviazione, Vulnerabilità e Difesa Preventiva dalle Minacce Cyber e Malware, Sicurezza dei siti web

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

Trascurabile, Oggettivamente valutata sulla base del Capitolo precedente relativo alle Misure di Sicurezza adottate

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

Trascurabile, Oggettivamente valutata sulla base del Capitolo precedente relativo alle Misure di Sicurezza adottate

Allegati

Figura 1 - Panoramica dei rischi

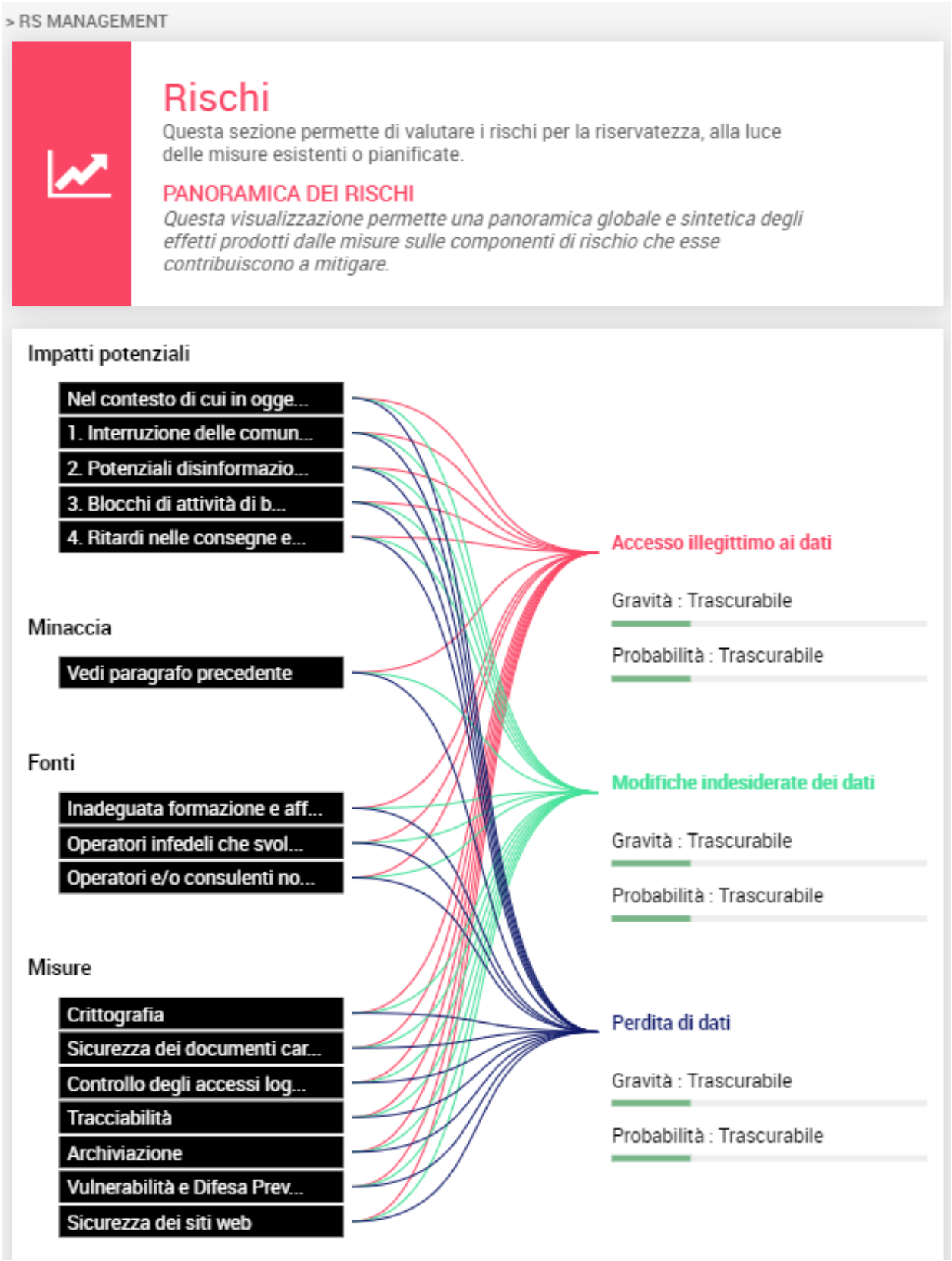

Figura 2 – Mappatura RACI del rischio per il trattamento Sistema Posta Elettronica

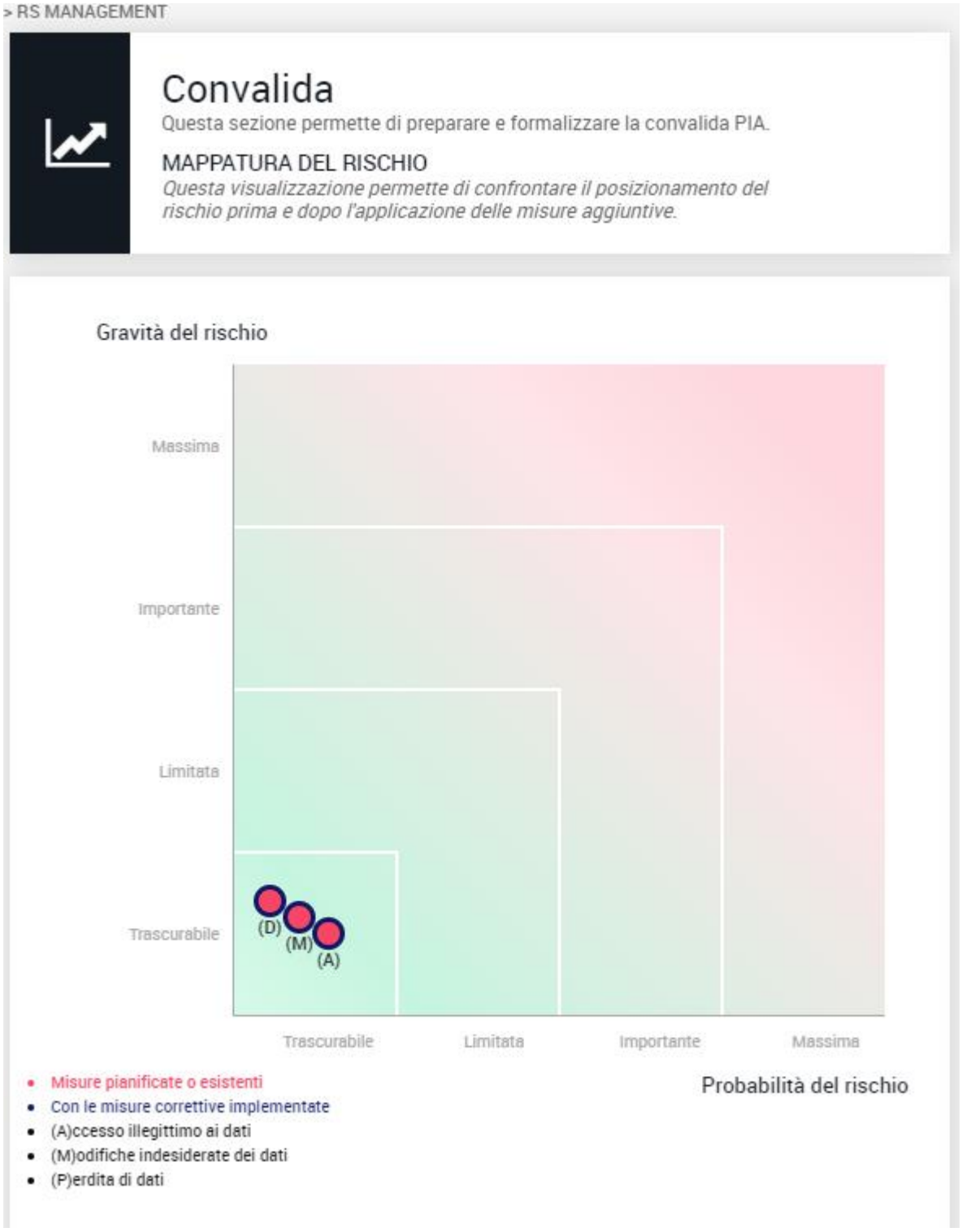

Figura 3 – Piano di azione (non necessario)