

# Informazioni sulla PIA

---

**Nome della PIA**

SISTEMA P@DOC

**Nome autore**

Carraro, Nicola

**Nome valutatore**

Rampin, Daniele

**Nome validatore**

Pavone, Valeria

**Data di creazione**

08/03/2019

**Richiesta del parere degli interessati**

Non è stato chiesto il parere degli interessati.

# Contesto

## Panoramica del trattamento

### Quale è il trattamento in considerazione?

La seguente valutazione di impatto si riferisce al trattamento dei dati attraverso il sistema di protocollo informatico e di gestione documentale p@doc [riferimento processo/attività di trattamento nr. 3601]. La finalità del trattamento è l'Attività amministrativa e giudiziaria. P@doc viene utilizzato da tutta l'organizzazione e quindi diventa rilevante una analisi su tutte le entità, i processi, la banca dati e i flussi di dati tra queste.

In particolare questa valutazione si concentra sulle entità, i processi, i database e i flussi all'interno del sistema di gestione documentale.

### Quali sono le responsabilità connesse al trattamento?

Il titolare del trattamento è il **Comune di Padova** nella persona del Sindaco.

Il responsabile del trattamento è il **settore Servizi Istituzionali** nella figura del Capo settore.

Il responsabile della gestione documentale è la dott.ssa Valeria Pavone.

Nonostante la responsabilità del sistema sia stata definita all'interno del settore Servizi Istituzionali, il procedimento nr.

**3601 P@DOC - ATTIVITA DI REGISTRAZIONE DI PROTOCOLLO E DI GESTIONE DOCUMENTALE**, è una attività di trattamento che riguarda tutti i settori che utilizzano il sistema nell'ambito della propria attività amministrativa e giudiziaria.

### Ci sono standard applicabili al trattamento?

Gli standard applicabili al trattamento sono i seguenti:

- Decreto del Presidente della Repubblica 20 dicembre 2000 n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
- Decreto Legislativo 7 marzo 2005 n. 82 - Codice dell'amministrazione digitale
- Decreto Legislativo 22 gennaio 2004, n. 42 - Codice dei beni culturali e del paesaggio
- Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali
- Regolamento UE 679/2016 - General Data protection Regulation
- Legge 7 agosto 1990 n. 241 - Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi
- ISO 31000:2010 - Risk management - Principles and guidelines
- ISO/IEC 29134:2017 - Information technology - Security techniques - Guidelines for privacy impact assessment
- ISO 27000:2018 - Information technology - Security techniques - Information security management systems - Overview and vocabulary
- ISO 15489-1:2016 - Information and documentation - Record management - Part 1: Concept and principles
- ISO 15489-2:2001 - Information and documentation - Record management - Part 2: Guidelines
- MoReq2010 - Modular Requirement for Record Systems
- EAD3 - Encoding Archival Description (2015)
- ISAD - Standard internazionale di descrizione archivistica

Inoltre il Comune di Padova adotta linee guida e standard attraverso il Manuale di gestione.

**Valutazione : Accettabile**

**Commento di valutazione :**

La sezione è completa

## Dati, processi e risorse di supporto

### Quali sono i dati trattati?

L'attività prevede il trattamento delle seguenti categorie di dati:

- dati identificativi
- dati genetici

- dati relativi alla salute
- dati relativi alla vita sessuale o all'orientamento sessuale
- dati relativi all'origine razziale
- dati relativi alle opinioni politiche
- dati relativi alle convinzioni religiose o filosofiche
- dati relativi all'appartenenza sindacale
- dati relativi a condanne penali e a reati o a connesse misure di sicurezza

Come si evince dal presente elenco sono trattate categorie particolari di dati ex. articolo 9 del GDPR e dell'art. 10 del GDPR.

Gli interessati sono i cittadini, utenti, candidati a procedure concorsuali o preselettive, genitori, gruppi familiari, imprenditori, indagati o imputati, lavoratori dipendenti e collaboratori, persone disabili, persone giuridiche e altri enti, soggetti con limitata capacità di intendere e volere.

Emerge quindi la presenza di categorie di interessati definiti come vulnerabili.

Per ulteriori informazioni sull'attività di trattamento si rimanda alla descrizione del censimento e del registro delle attività di trattamento con ID 3601

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

Si rimanda l'analisi del ciclo di vita di dati al DFD p@doc allegato. Inoltre si fa riferimento al Manuale di gestione del Comune di Padova

### **Quali sono le risorse di supporto ai dati?**

Hardware:

- DBMS p@doc (Database dei metadati di p@doc)
- ProtoPEC (Server di posta elettronica, Attività schedulate di gestione posta elettronica e attività automatizzate del sistema)
- DocMGR (Repository file)
- Application server (5 in totale)
- ProtoBalancer (Bilanciatore di smistamento degli utenti)
- Serviziweb4 (Sistema single sign-on di autenticazione)
- Infrastruttura di Networking dell'organizzazione
- PDL degli utenti
- Scanner e fotocopiatori
- Mail Server (Fax server incluso) e Pec server

Software:

- PostgreSQL (DBMS p@doc)
- Software applicativo p@doc
- Doveqot (server IMAP)
- Fetch mail (attività schedulate di gestione posta elettronica)
- Simple SAML PHP (software per l'autenticazione)
- Apache (per il livello HTTPS)
- HAProxy (Software bilanciatore)
- Browser (Mozilla Firefox, Chrome)
- Client di posta (Outlook, Mozilla Thunderbird)
- Portale della pubblicazione on-line (Albo online)
- Archivia fax
- Web Mail

Persone:

- Utenti del sistema
- Amministratori del sistema
- Tecnici del sistema

Documenti cartacei:

- Documenti in entrata, Uscita, Interni su supporto analogico

**Valutazione : Accettabile**

**Commento di valutazione :**

Ok, la sezione è completa

# Principi Fondamentali

## Proporzionalità e necessità

### Gli scopi del trattamento sono specifici, esplicativi e legittimi?

Il Comune di Padova tratta i dati attraverso il sistema p@doc per il conseguimento della propria attività amministrativa o giudiziaria. Essendo uno strumento trasversale e utilizzato da tutta l'organizzazione nell'ambito delle proprie attività e dei propri procedimenti, si rimanda al registro delle attività di trattamento di ogni settore (responsabile del trattamento) per le specifiche finalità.

**Valutazione : Accettabile**

### Quali sono le basi legali che rendono lecito il trattamento?

La base giuridica del trattamento è l'adempimento e obbligo del titolare del trattamento derivante dal DPR 445/2000 e dal D.Lgs 82/2005 e s.m.i.

**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)?

La raccolta dei dati per la registrazione è limitata alle informazioni minime richieste per la registrazione di protocollo. Per quanto riguarda i documenti registrati o prodotti, è il responsabile del procedimento a definire quali informazioni siano richieste in base alla normativa che regola il procedimento amministrativo.

**Valutazione : Accettabile**

### I dati sono esatti e aggiornati?

L'esattezza dei dati va valutata in base alla fonte di provenienza. Il Comune di Padova, in qualità di pubblica amministrazione, riceve dati da:

- Cittadini e Aziende (attraverso istanze, segnalazioni o comunicazioni)
- Altre pubbliche amministrazioni (attraverso istanze, richieste, comunicazioni o attraverso l'utilizzo di banche dati certificate)

**Valutazione : Accettabile**

### Qual è il periodo di conservazione dei dati?

Il periodo di conservazione dei dati è variabile a seconda dell'unità documentaria e delle aggregazioni documentarie (fascicoli, registri e repertori). L'Ente utilizza un piano di conservazione per la definizione dei tempi di conservazione.

**Valutazione : Accettabile**

## Misure a tutela dei diritti degli interessati

### Come sono informati del trattamento gli interessati?

Gli interessati sono informati sul trattamento dei dati attraverso portale istituzionale <http://www.padovanet.it/> e attraverso apposite informative predisposte da ogni settore in base al procedimento amministrativo di competenza.

**Valutazione : Accettabile**

## Ove applicabile: come si ottiene il consenso degli interessati?

Non è prevista la raccolta del consenso da parte degli interessati.

### Valutazione : Accettabile

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

Gli interessati possono esercitare i loro diritti di accesso e di portabilità dei dati attraverso i contatti riportati all'indirizzo <http://www.padovanet.it/informazione/informativa-il-trattamento-dei-dati-personali#26961> o disponibili sull'informativa resa dai settori competenti.

Gli interessati possono esercitare i loro diritti anche attraverso le altre forme di accesso stabilite dalla normativa.

### Valutazione : Accettabile

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

Gli interessati possono esercitare i loro diritti di rettifica dei dati attraverso i contatti riportati all'indirizzo <http://www.padovanet.it/informazione/informativa-il-trattamento-dei-dati-personali#26961> o disponibili sull'informativa resa dai settori competenti. Per ogni procedimento amministrativo vengono definite apposite modalità di rettifica e modifica dei dati.

Il diritto di cancellazione (diritto all'oblio) non è esercitabile quando la conservazione del dato ha una finalità di archiviazione nel pubblico interesse, all'interno della quale si inquadra la conservazione della documentazione amministrativa registrata all'interno del sistema di protocollo informatico p@doc.

### 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 opposizione attraverso i contatti riportati all'indirizzo <http://www.padovanet.it/informazione/informativa-il-trattamento-dei-dati-personali#26961>. Il diritti di limitazione e opposizione possono essere esercitati anche ai sensi dell'art. 126, comma 2 del Codice dei beni culturali, qualora il trattamento dei dati stessi comporti un concreto pericolo di lesione della dignità, della riservatezza o dell'identità.

### Valutazione : Accettabile

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

I responsabili del trattamento vengono appositamente nominati con atto di nomina o contratto che riporta le responsabilità nell'ambito del trattamento.

### Valutazione : Accettabile

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

I dati non sono trasferiti in territori e paesi extra-UE

### Valutazione : Accettabile

# Rischi

## Misure esistenti o pianificate

### Politica di tutela della privacy

Il Comune di Padova ha istituito con Determinazione 2018/56/0001 del 04/05/2018 il **Gruppo di lavoro per la protezione dei dati personali e l'attuazione degli adempimenti richiesti dal Regolamento Europeo N.679/2016**. Il gruppo di lavoro si pone a supporto degli adempimenti privacy da parte dell'organizzazione (registro delle attività di trattamento, redazione delle informative, comunicazioni con il DPO)

Il Comune di Padova ha nominato con Determinazione 2018/34/101 del 21/05/2018 il **Responsabile della protezione dei dati**. Il RPD si identifica nella persona giuridica esterna all'organizzazione, ovvero nella ditta **IPSLAB S.R.L.**. I dati di contatto sono resi pubblici dal titolare/responsabile mediante pubblicazione sul sito web istituzionale [www.padovanet.it](http://www.padovanet.it)

**Valutazione : Accettabile**

### Gestione delle politiche di tutela della privacy

Il Comune di Padova ha messo a disposizione attraverso la propria rete intranet documenti inerenti alle attività e alla conformità del sistema privacy.

Inoltre, con la pubblicazione del nuovo Manuale di gestione del Comune di Padova, vengono definite politiche di gestione documentali conformi al Regolamento Europeo 679/2016 - General data protection regulation.

**Valutazione : Accettabile**

### Gestione dei rischi

Il Comune di Padova dispone di uno strumento di censimento dei documenti e delle istanze al quale è stato integrato il registro delle attività di trattamento. Il citato censimento rappresenta una base per il monitoraggio delle produzione documentale e viene implementato per ogni nuova attività di trattamento dai responsabili dei relativi procedimenti.

**Valutazione : Migliorabile**

#### Piano d'azione / misure correttive :

- Prevedere l'analisi dei rischi con il tool di AGID Cyber Risk Management - Tool di valutazione e trattamento del rischio cyber

#### Commento di valutazione :

- Integrare nuova attività di gestione dei rischi per p@doc

### Gestire gli incidenti di sicurezza e le violazioni dei dati personali

All'interno del Manuale di gestione è disponibile il modulo di comunicazione databreach per il garante. In caso di data breach, viene data comunicazione all'ufficio privacy del Comune di Padova, il quale chiede parere al RPD. Tuttavia non sono state formalizzate in maniera diversa procedure o piani di reazione.

**Valutazione : Migliorabile**

#### Piano d'azione / misure correttive :

- Definire le responsabilità, i piani di reazione e la caratterizzazione delle violazioni per la corretta gestione degli incidenti di sicurezza che possono influire sulle libertà e sulla riservatezza dei dati personali.

#### Commento di valutazione :

La gestione degli incidenti di sicurezza va implementata e migliorata sia dal punto di vista tecnico che organizzativo.

### Vigilanza sulla protezione dei dati

Per una visione globale dello stato di protezione dei dati è disponibile il censimento delle istanze e dei documenti. Tuttavia non sono stati definiti ulteriori strumenti che consentano una visione aggiornata e in tempo reale dei trattamenti in essere.

### **Valutazione : Migliorabile**

#### **Piano d'azione / misure correttive :**

- Integrare all'interno del sistema p@doc una codifica dei procedimenti e processi che prevedono il trattamento di dati personali [Integrazione e miglioramento Codifica oggettario]. Attraverso il collegamento con il Censimento delle istanze e dei documenti sarà possibile generare un report periodico che rilevi i flussi di dati personali in entrata / uscita.

#### **Commento di valutazione :**

La misura organizzativa, con un adeguata implementazione permetterà di avere una visione globale e aggiornata dello stato di protezione dei dati (conformità dei trattamenti, obiettivi e indicatori).

## **Formazione continua del personale**

Il Settore Risorse Umane prevede periodici momenti di formazione del personale nell'ambito della protezione dei dati personali.

Il Settore Servizi Istituzionali mette a disposizione attraverso i portali I-Wiki e I-tube strumenti e documentazione a garanzia dei requisiti di integrità e riservatezza dei dati personali.

### **Valutazione : Accettabile**

## **Crittografia**

Allo stato attuale la crittografia è applicata a livello di rete (HTTPS)

### **Valutazione : Accettabile**

#### **Commento di valutazione :**

Attuare delle politiche di crittografia sul sistema p@doc potrebbe comportare un rischio di mancata accessibilità e disponibilità del dato. Inoltre la cifratura del dato risulta essere eccessivamente dispendiosa da tutti i punti di vista.

## **Partizionamento**

Sono pianificabili alcune misure di partizionamento per la tutela dei dati personali.

### **Valutazione : Migliorabile**

#### **Piano d'azione / misure correttive :**

- In seguito ad una analisi sulla fattibilità prevedere un partizionamento dei dati solitamente descritti all'interno del campo "oggetto" del documento registrato/protocollato. Questa proposta, eventualmente applicabile a p@doc 3.0, prevede la separazione dell'azione (istanza, segnalazione, dichiarazione) dall'interessato (cittadino, utente, libero professionista), rendendo logicamente separabili i dati.

- Eseguire un analisi sulla gestione delle identità e dei vari strumenti ad oggi esistenti.

#### **Commento di valutazione :**

La misura risulta migliorabile perché allo stato attuale non sono previsti metodi di partizionamento dei dati.

## **Controllo degli accessi logici**

I profili degli utenti sono definiti in base alla UOR di appartenenza e al proprio ruolo.

Le regole per le password sono quelle definite dalle politiche aziendali e dal sistema centralizzato di autenticazione.

### **Valutazione : Migliorabile**

#### **Piano d'azione / misure correttive :**

- Documentare i maniera dettagliata i mezzi di autenticazione implementati e le regole per le password (lunghezza minima, caratteri richiesti, durata della validità, numeri di tentativi prima del blocco dell'account)  
- Integrare la documentazione relativa al controllo degli accessi logici nei sistemi di conservazione digitale.

#### **Commento di valutazione :**

Le politiche e gli strumenti per l'attribuzione dei profili degli utenti sono definiti e gestiti dal Responsabile della gestione documentale e dall'ufficio protocollo generale. Essendo la gestione delle password centralizzata a livello organizzativo, questa va documentata e aggiornata con cadenza temporale da definire.

## **Tracciabilità**

Il sistema di protocollo e di gestione documentale registra gli eventi e le operazioni eseguite dagli utenti e genera le relative tracce. Oltre alla traccia appena descritta, viene conservata anche quella sistematica per un tempo non superiore ai 12 mesi.

#### **Valutazione : Accettabile**

### **Archiviazione**

Tutte le informazioni registrate, gestite e archiviate all'interno del sistema sono correttamente classificate. Ai fini della conservazione si rimanda al Manuale della conservazione del Comune di Padova

#### **Valutazione : Accettabile**

### **Minimizzazione dei dati**

All'interno del sistema p@doc vengono richiesti esclusivamente i dati richiesti dalla normativa nazionale nell'ambito della gestione documentale e di amministrazione digitale.

Qualora fossero allegati al sistema documenti con informazioni aggiuntive queste vengono correttamente classificate secondo le politiche definite dal Manuale di gestione e la responsabilità di queste informazioni è associata al Responsabile del procedimento amministrativo.

#### **Valutazione : Accettabile**

### **Lotta contro il malware**

Tutte le PDL degli utenti del sistema p@doc sono dotati di sistemi anti-virus.

Il server di posta elettronica dell'Ente implementa un sistema di anti-spam e antivirus.

Il sistema p@doc è dotato di una funzione di alert e di blocco dei file non conformi alle politiche definite dall'organizzazione.

#### **Valutazione : Accettabile**

### **Gestione postazioni**

Esistenza del Regolamento sull'uso degli strumenti informatici redatto e condiviso nel 2010.

#### **Valutazione : Migliorabile**

#### **Piano d'azione / misure correttive :**

- Aggiornare il Regolamento sull'uso degli strumenti informatici redatto nel 2010.

#### **Commento di valutazione :**

Venne implementata una misura correttiva in quanto il regolamento sull'uso degli strumenti informatici risulta essere obsoleto.

### **Backup**

Il back-up viene fatto su rete protetta interna dell'organizzazione.

Il Database esegue una copia istantanea sul sito gemello in altra sede ogni 20 minuti.

Giornalmente viene eseguita una esportazione totale del protocollo alla fine delle attività e conservata nel sistema di backup dell'ente.

migliorabile usando una nuova versione del DataBase.

#### **Valutazione : Migliorabile**

#### **Piano d'azione / misure correttive :**

- Le operazioni di back-up possono essere migliorate con l'utilizzo della nuova versione di Database.

#### **Commento di valutazione :**

- Le operazioni di back-up possono essere migliorate con l'utilizzo della nuova versione di Database

## **Manutenzione**

La manutenzione hardware è governata dai sistemi per la parte centralizzata e dall'Help Desk per tutte le PDL degli utenti del sistema.

Per quanto riguarda la manutenzione dei software, sono nominati appositamente degli amministratori di sistema sia interni che esterni (quando il software è di un fornitore).

**Valutazione : Accettabile**

## **Contratto con il responsabile del trattamento**

Qualora fossero affidate a terzi attività all'interno del sistema p@doc, questi sono tenuti alla sottoscrizione dell'atto di nomina di responsabile del trattamento, all'interno del quale vengono specificati tutti gli obblighi di questo e viene richiesta la conformità al Regolamento UE.

**Valutazione : Accettabile**

## **Controllo degli accessi fisici**

Nell'ambito delle risorse hardware il controllo fisico è limitato dall'accesso ai locali mediante sistemi di autenticazione tramite badge e chiave.

Nell'ambito delle risorse cartacee gli utenti non hanno accesso liberamente agli archivi cartacei dell'organizzazione. Per la consultazione è deputata la sala consultazione.

**Valutazione : Accettabile**

## **Prevenzione delle fonti di rischio**

La prevenzione da fonti di rischio non umane è garantita dalle seguenti misure di sicurezza:

- Porte blindate
- Armadi ignifughi
- Impianti elettrici dedicati
- Sistemi di condizionamento per il raffreddamento delle apparecchiature
- Gruppi di continuità elettrica
- Controlli periodici su l'efficacia del gruppo elettrogeno
- Estintori
- Piano di verifica periodica sull'efficacia degli estintori
- Impianto antincendio nella sala macchine

La prevenzione da fonti di rischio umane è garantita dalle seguenti misure di sicurezza:

- Accesso ai locali mediante sistema di autenticazione tramite badge e chiave
- Impianto antiintrusione autonomo per gli accessi al locale sala macchine
- Sistema di sorveglianza
- Piano di verifica periodica sull'efficacia dei sistemi di sorveglianza
- Identificazione e autenticazione utente
- Profilazione degli accessi

**Valutazione : Accettabile**

## **Classificazione delle informazioni**

Tutte le registrazioni all'interno del sistema p@doc sono soggette a diverse tipologie di classificazione:

- Classificazione archivistica (titolario di classificazione)
- Classificazione gestionale (oggettario)
- Classificazione privacy (livello di riservatezza)

**Valutazione : Migliorabile****Piano d'azione / misure correttive :**

- Definire una nuova classificazione della riservatezza e implementarla all'interno del sistema.

**Commento di valutazione :**

- Definire una nuova classificazione della riservatezza e implementarla all'interno del sistema.

## Accesso illegittimo ai dati

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

Problemi di relazione con conoscenti privati o lavorativi (reputazione rovinata), Disagi psicologici seri (depressione, sviluppo di una fobia), Invasione della privacy con danno irreversibile, Violazione dei diritti fondamentali (discriminazione e libertà di espressione), Perdita dei legami familiari, Rischio finanziario, Impossibilità di lavorare e di ricollocamento, Suicidio

**Quali sono le principali minacce che potrebbero concretizzare il rischio?**

Visibilità dei dati per visione, modifica o diffusione non autorizzata, Penetrabilità dei dati attraverso i canali di comunicazione, Rivelazione non intenzionale di informazioni, Employe poaching, Furto di documenti

**Quali sono le fonti di rischio?**

Codici maligni (virus, malware), Hackers, Dipendenti, Organizzazioni criminali, trasgressori

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

Politica di tutela della privacy, Vigilanza sulla protezione dei dati, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Formazione continua del personale, Prevenzione delle fonti di rischio, Minimizzazione dei dati, Classificazione delle informazioni, Controllo degli accessi logici, Crittografia, Gestione postazioni, Partizionamento, Tracciabilità, Lotta contro il malware, Controllo degli accessi fisici

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

Massima, Gli interessati potrebbero sperimentare conseguenze significative, anche irrimediabili, che potrebbero non superare.

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

Limitata, Appare difficile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti

**Valutazione : Accettabile**

## Modifiche indesiderate dei dati

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

Perdita di tempo nel ripetere formalità o nell'attendere il ripristino del dato, Timore di perdere il controllo sui propri dati, Pagamenti inaspettati (tasse imposte erroneamente), Rifiuto all'accesso di servizi amministrativi, Dati non aggiornati, Danni materiali e finanziari, Perdita di accesso a infrastrutture e servizi vitali (acqua, gas, luce etc..), Trattamento di dati non corretto che genera disservizi

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

Modifiche indesiderate ai dati di un DB, Errore di aggiornamento, di configurazione o di mantenimento, Infezione da parte di codici maligni, Carico di lavoro elevato, stress e cambiamenti negativi nelle condizioni di lavoro, Alterazione volontaria e falsificazione di documenti

**Quali sono le fonti di rischio?**

Dipendenti, Dipendenti inesperti, amministratori del sistema, Hackers, staff della manutenzione, organizzazioni criminali, Codici maligni sconosciuti

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

Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Prevenzione delle fonti di rischio, Tracciabilità, Archiviazione, Crittografia, Controllo degli accessi logici, Gestione postazioni, Vigilanza sulla protezione dei dati,

Partizionamento, Formazione continua del personale, Controllo degli accessi fisici, Classificazione delle informazioni, Lotta contro il malware, Gestione dei rischi, Contratto con il responsabile del trattamento

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

Massima, Gli interessati potrebbero sperimentare conseguenze significative, anche irrimediabili, che potrebbero non superare.

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

Limitata, Appare difficile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti

**Valutazione : Accettabile**

## **Perdita di dati**

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

Perdita di controllo sui propri dati, Rifiuto di accesso a servizi amministrativi, Richio finanziario, Perdita di beni materiali, Perdita di evidenze in ambito giuridico

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

Storage sovraccarico o interruzione di elettricità, Aggiunta di hardware incompatibili che generano un malfunzionamento, Allagamento, incendio e usura delle risorse, Furto di un laptop o di un hardware, Uso inappropriato del software e cancellazione dei dati, Carico di lavoro elevato, assegnazione dell'attività ad uno staff non competente., Termine del contratto del dipendente, Perdita di integrità dei documenti informatici, Usura di documenti analogici, Sovraccarico nei processi

### **Quali sono le fonti di rischio?**

Dipendenti, manager, amministratori del sistema, Terze parti autorizzate, hackers, visitatori e utenti, trasgressori, Disastri naturali, Condutture dell'acqua, incendi, materiali infiammabili

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

Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Gestione dei rischi, Vigilanza sulla protezione dei dati, Formazione continua del personale, Backup, Manutenzione, Lotta contro il malware, Gestione postazioni, Prevenzione delle fonti di rischio, Contratto con il responsabile del trattamento, Minimizzazione dei dati, Classificazione delle informazioni, Controllo degli accessi fisici, Archiviazione

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

Massima, Gli interessati potrebbero sperimentare conseguenze significative, anche irrimediabili, che potrebbero non superare.

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

Limitata, Appare difficile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti

**Valutazione : Accettabile**

# Piano d'azione

---

## Panoramica

Principi fondamentali	Misure esistenti o pianificate
Finalità	Politica di tutela della privacy
Basi legali	Gestione delle politiche di tutela della privacy
Adeguatezza dei dati	Gestione dei rischi
Esattezza dei dati	Gestire gli incidenti di sicurezza e le violazioni dei dati personali
Periodo di conservazione	Vigilanza sulla protezione dei dati
Informativa	Formazione continua del personale
Raccolta del consenso	Crittografia
Informativa	Partizionamento
Diritto di rettifica e diritto di cancellazione	Controllo degli accessi logici
Diritto di limitazione e diritto di opposizione	Tracciabilità
Responsabili del trattamento	Archiviazione
Trasferimenti di dati	Minimizzazione dei dati

Rischi	Misure Migliorabili
Accesso illegittimo ai dati	Misure Accettabili
Modifiche indesiderate dei dati	
Perdita di dati	

---

Misure Migliorabili  
Misure Accettabili

## **Principi fondamentali**

Nessun piano d'azione registrato.

## Misure esistenti o pianificate

### Gestione dei rischi

#### Piano d'azione / misure correttive :

- Prevedere l'analisi dei rischi con il tool di AGID Cyber Risk Management - Tool di valutazione e trattamento del rischio cyber

#### Commento di valutazione :

- Integrare nuova attività di gestione dei rischi per p@doc

Data prevista di implementazione : 31/10/2019

Responsabile dell'implementazione : Gruppo di lavoro Padova PA digitale

### Gestire gli incidenti di sicurezza e le violazioni dei dati personali

#### Piano d'azione / misure correttive :

- Definire le responsabilità, i piani di reazione e la caratterizzazione delle violazioni per la corretta gestione degli incidenti di sicurezza che possono influire sulle libertà e sulla riservatezza dei dati personali.

#### Commento di valutazione :

La gestione degli incidenti di sicurezza va implementata e migliorata sia dal punto di vista tecnico che organizzativo.

Data prevista di implementazione : 31/03/2020

Responsabile dell'implementazione : Settore Servizi Informatici e Telematici

### Vigilanza sulla protezione dei dati

#### Piano d'azione / misure correttive :

- Integrare all'interno del sistema p@doc una codifica dei procedimenti e processi che prevedono il trattamento di dati personali [Integrazione e miglioramento Codifica oggettario]. Attraverso il collegamento con il Censimento delle istanze e dei documenti sarà possibile generare un report periodico che rilevi i flussi di dati personali in entrata / uscita.

#### Commento di valutazione :

La misura organizzativa, con un adeguata implementazione permetterà di avere una visione globale e aggiornata dello stato di protezione dei dati (conformità dei trattamenti, obiettivi e indicatori).

Data prevista di implementazione : 31/12/2020

Responsabile dell'implementazione : Gruppo di lavoro Padova PA digitale

### Partizionamento

#### Piano d'azione / misure correttive :

- In seguito ad una analisi sulla fattibilità prevedere un partizionamento dei dati solitamente descritti all'interno del campo "oggetto" del documento registrato/protocollato. Questa proposta, eventualmente applicabile a p@doc 3.0, prevede la separazione dell'azione (istanza, segnalazione, dichiarazione) dall'interessato (cittadino, utente, libero professionista), rendendo logicamente separabili i dati.
- Eseguire un analisi sulla gestione delle identità e dei vari strumenti ad oggi esistenti.

#### Commento di valutazione :

La misura risulta migliorabile perché allo stato attuale non sono previsti metodi di partizionamento dei dati.

Data prevista di implementazione : 31/12/2020

Responsabile dell'implementazione : Gruppo di lavoro Padova PA digitale

### Controllo degli accessi logici

#### Piano d'azione / misure correttive :

- Documentare i maniera dettagliata i mezzi di autenticazione implementati e le regole per le password (lunghezza minima, caratteri richiesti, durata della validità, numeri di tentativi prima del blocco dell'account)
- Integrare la documentazione relativa al controllo degli accessi logici nei sistemi di conservazione digitale.

#### Commento di valutazione :

Le politiche e gli strumenti per l'attribuzione dei profili degli utenti sono definiti e gestiti dal Responsabile della gestione documentale e dall'ufficio protocollo generale. Essendo la gestione delle password centralizzata a livello organizzativo, questa va documentata e aggiornata con cadenza temporale da definire.

Data prevista di implementazione : 31/03/2020

**Responsabile dell'implementazione :** Settore Servizi Informatici e Telematici

## Gestione postazioni

### Piano d'azione / misure correttive :

- Aggiornare il Regolamento sull'uso degli strumenti informatici redatto nel 2010.

### Commento di valutazione :

Viene implementata una misura correttiva in quanto il regolamento sull'uso degli strumenti informatici risulta essere obsoleto.

**Data prevista di implementazione :** 31/03/2020

**Responsabile dell'implementazione :** Settore Servizi Informatici e telematici

## Backup

### Piano d'azione / misure correttive :

- Le operazioni di back-up possono essere migliorate con l'utilizzo della nuova versione di Database.

### Commento di valutazione :

- Le operazioni di back-up possono essere migliorate con l'utilizzo della nuova versione di Database

**Data prevista di implementazione :** 31/12/2020

**Responsabile dell'implementazione :** Settore Servizi Informatici e Telematici

## Classificazione delle informazioni

### Piano d'azione / misure correttive :

- Definire una nuova classificazione della riservatezza e implementarla all'interno del sistema.

### Commento di valutazione :

- Definire una nuova classificazione della riservatezza e implementarla all'interno del sistema.

**Data prevista di implementazione :** 31/03/2020

**Responsabile dell'implementazione :** Gruppo di lavoro Padova PA digitale

## Rischi

Nessun piano d'azione registrato.



# Panoramica dei rischi

## Impatti potenziali

Problemi di relazione con c...
Disagi psicologici seri (d...
Invasione della privacy con...
Violazione dei diritti fond...
Perdita dei legami familiari
Rischio finanziario
Impossibilità di lavorare e...
Suicidio
Perdita di tempo nel ripete...
Timore di perdere il contro...
Pagamenti inaspettati (tass...
Rifiuto all'accesso di serv...
Dati non aggiornati
Danni materiali e finanziari
Perdita di accesso a infras...
Trattamento di dati non cor...
Perdita di controllo sui pr...
Rifiuto di accesso a serviz...
Rischio finanziario
Perdita di beni materiali
Perdita di evidenze in ambi...

## Accesso illegittimo ai dati

Gravità : Massima

Probabilità : Limitata

## Modifiche indesiderate dei dati

Gravità : Massima

Probabilità : Limitata

## Perdita di dati

Gravità : Massima

Probabilità : Limitata

## Minaccia

Visibilità dei dati per vis...
Penetrabilità dei dati attr...
Rivelazione non intenzional...
Employe poaching
Furto di documenti
Modifiche indesiderate ai d...
Errore di aggiornamento, di...
Infezione da parte di codic...
Carico di lavoro elevato, s...
Alterazione volontaria e fa...
Storage sovraccarico o inte...
Aggiunta di hardware incompl...
Allagamento, incendio e usu...
Furto di un laptop o di un ...
Uso inappropriato del softw...
Carico di lavoro elevato, a...
Termine del contratto del d...
Perdita di integrità dei do...
Usura di documenti analogici
Sovraccarico nei processi

## Fonti



Codici maligni (virus, malw...
Hackers
Dipendenti
Organizzazioni criminali
trasgressori
Dipendenti, Dipendenti ines...
Hackers, staff della manute...
Codici maligni sconosciuti
Dipendenti, manager, ammini...
Terze parti autorizzate, ha...
Disastri naturali, Condottu...

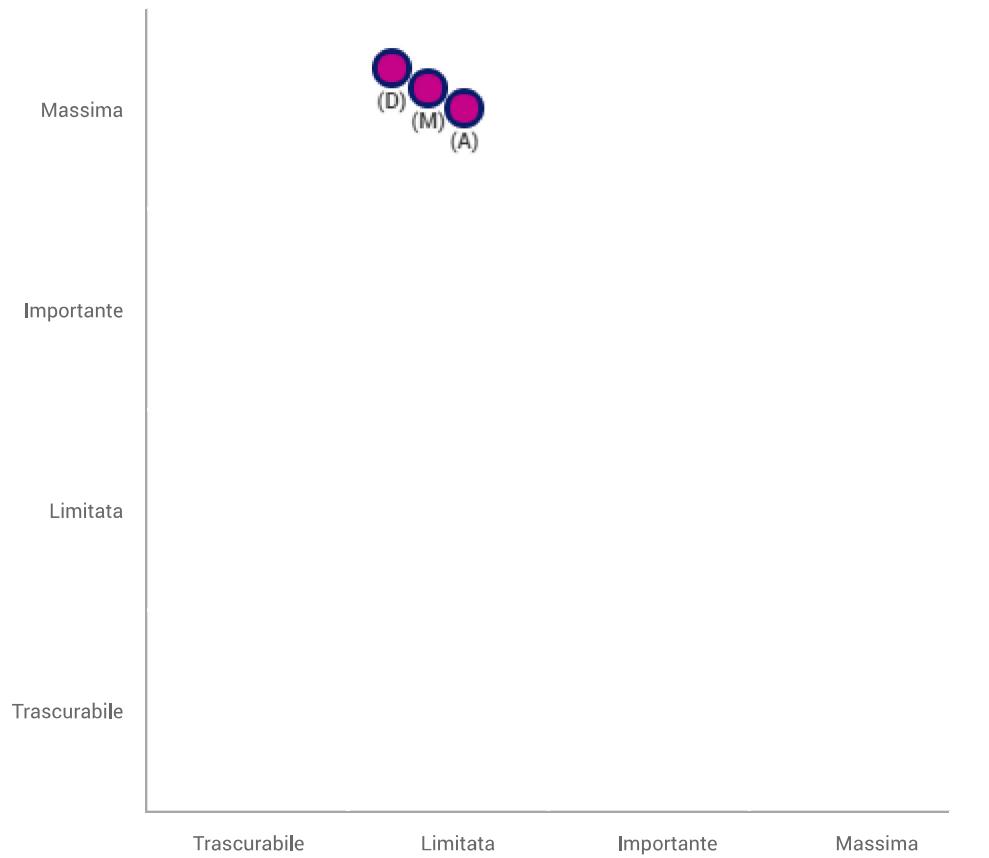
## Misure

Politica di tutela della pr...
Vigilanza sulla protezione ...
Gestire gli incidenti di si...
Formazione continua del per...
Prevenzione delle fonti di ...
Minimizzazione dei dati
Classificazione delle infor...
Controllo degli accessi log...
Crittografia
Gestione postazioni
Partizionamento
Tracciabilità
Lotta contro il malware
Controllo degli accessi fis...
Gestione delle politiche di...
Archiviazione
Gestione dei rischi
Contratto con il responsabi...
Backup
Manutenzione

# Mappaggio dei rischi

---

Gravità 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

Probabilità del rischio