Autore:
Prof.ssa Maria Rita Lo Giudice
Redattore:
Ing. Antonio Vargiu
Validatore:
Dr. Mario Mureddu

Titolo: DPIA per l'adozione di strumenti di lavoro flessibile

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Non si è ritenuto necessario richiedere un parere agli interessati, anche vista l'urgenza connessa. Qualora vi fossero suggerimenti da parte dell'utenza, l'amministrazione si impegna ad effettuare successivi aggiornamenti della presente DPIA che tengano conto delle stesse.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Questa DPIA è atta alla valutazione dell'impatto connesso all'uso di tecnologie digitali per l'adozione di modalità di lavoro agile che prevede l'utilizzo di strumentazione informatica quali tablet, smartphone e PC, personali o di proprietà dell'amministrazione, da parte del personale ATA o docente per lo svolgimento dell'attività lavorativa dal proprio domicilio. In particolare la presente DPIA si occupa dei trattamenti fatti dal personale per lo svolgimento dell'attività amministrativa o di quella di supporto alla didattica anche da parte dei docenti. I trattamenti relativi alla didattica a distanza condotta dai docenti sono invece oggetto di altra e specifica DPIA.

Nella presente DPIA sono presi in considerazione i trattamenti di dati personali operati per mezzo di tecnologie che permettono lo svolgimento di prestazioni lavorative da casa mediante:

- collegamento a piattaforme in cloud dell'amministrazione (segreteria digitale di diversi fornitori)
- collegamento a risorse locali presenti nella sede dell'istituto (server, basi dati)
- utilizzo di strumenti per la condivisione di dati ed informazioni (posta elettronica, chat, Drive, dropbox, etc.)

Si rileva che la gestione di risorse locali è di norma a carico dell'amministrazione che deve anche curare gli aspetti relativi alla sicurezza informatica e la gestione degli accessi da remoto anche se il fornitore dei servizi locali dovrà essere coinvolto comunque come responsabile del trattamento.

Le soluzioni in cloud, da privilegiare secondo le linee guida per l'informatica nella PA, sono a loro volta caratterizzate da elevati rischi che devono comunque essere gestiti in collaborazione con il fornitore del servizio, da scegliere fra quelli abilitati secondo la circolare AGID n. 2 del 9 aprile 2018, che assumerà il ruolo di responsabile del trattamento.

Quali sono le responsabilità connesse al trattamento?

La complessità delle azioni e dei possibili risvolti in termini di violazione della privacy implica una collaborazione fattiva tra le varie parti in causa. Queste sono, in particolare:

- **Il titolare del trattamento**, in questo caso l'Amministrazione Scolastica.
- **Il Dirigente Scolastico (D.S.)**, rappresentante legale dell'amministrazione, assume un ruolo centrale di supervisione e guida nei confronti dell'operato dei dipendenti. Inoltre, è compito del D.S. quello di definire un codice di condotta interno alla scuola che regoli l'utilizzo della strumentazione elettronica utilizzata, e di sorvegliare sulla sua attuazione.

- **Il direttore dei Servizi Generali e Amministrativi (DSGA),** sovrintende ai servizi amministrativo-contabili e ne cura l'organizzazione. Ha autonomia operativa e responsabilità diretta nella definizione ed esecuzione degli atti amministrativo-contabili, di ragioneria e di economato, anche con rilevanza esterna.
- **Gli Assistenti Amministrativi (A.A.),** hanno compiti amministrativi, di supporto alla didattica, di contabilità all'interno della segreteria scolastica. I compiti specifici di ciascun A.A. sono definiti da D.S. e D.S.G.A. all'interno delle loro funzioni.
- **I docenti**. In questa DPIA si affrontano i trattamenti nei quali i docenti utilizzano strumenti di lavoro a distanza e di collaborazione anche in cloud all'interno di commissioni o gruppi di lavoro. I trattamenti relativi alle attività di didattica a distanza e BYOD sono invece oggetti di altra DPIA specifica.
- **Il Responsabile della Protezione dei Dati (RPD)** ha il compito di fornire supporto a titolare, docenti e interessati, per tutte quelle questioni concernenti la protezione dei dati personali all'interno dell'ambito di applicazione del trattamento.
- **I responsabili del trattamento,** quali i provider di servizi elettronici utilizzati per lo svolgimento delle attività di lavoro agile devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato. Particolare attenzione va posta nei confronti dei fornitori di servizi cloud, ove richiesti. In questo caso, è necessario prestare particolare attenzione alle loro policy sulla cessione dei dati a organismi terzi e all'eventuale salvataggio di dati su server extra-UE. Per questo motivo, sarà necessario effettuare una valutazione preventiva dei provider di servizi cloud sulla base della loro compliance nei confronti della normativa in essere. Inoltre, sarà necessario procedere alla nomina formale dei fornitori di tali servizi quali responsabili del trattamento ai sensi dell'Art. 28, comma 3 del GDPR. Si ricorda inoltre che, sulla base di quanto previsto dalla circolare AGID n. 2 del 9 aprile 2018, le Pubbliche amministrazioni possono avvalersi esclusivamente di servizi cloud abilitati, la cui lista aggiornata può essere trovata sul sito dell'AGID.
- **Eventuali amministratori di sistema**: nominati dal DS quali responsabili del trattamento relativamente alla gestione dei sistemi informatici, collaborano con l'RPD e il DS nel fornire consulenze e pareri relativamente allo stato delle risorse informatiche dell'amministrazione.

Ci sono standard applicabili al trattamento?

Attualmente non sono stati rinvenuti standard, certificazioni o codici di condotta applicabili al problema in esame.

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Lo svolgimento di attività lavorative in modalità lavoro agile avviene tramite una/più piattaforma/e elettronica/e che facilitano la condivisione dei dati e l'organizzazione del lavoro di gruppo. Per la gestione delle comunicazioni e dei flussi tali piattaforme, che spesso fanno utilizzo di tecnologie *cloud*, trattano e conservano le informazioni necessarie per identificare univocamente coloro che operano sulla piattaforma (dati di servizio).

Le tecnologie prese in considerazione permettono quindi di effettuare da casa quelle attività lavorative richieste per garantire il perseguimento dei fini istituzionali dell'amministrazione scolastica e che prevedono il trattamento di:

- Dati personali degli alunni e delle famiglie per consentire l'assolvimento degli obblighi di istruzione e di formazione
- Dati personali dei dipendenti per garantire la gestione del rapporto di lavoro

Tali dati personali potranno essere anche di natura sensibile (dati particolari e relativi a condanne penali e reati secondo gli artt. 9 e 10 del GDPR) secondo quanto previsto dal Regolamento per il trattamento dei dati sensibili e giudiziari emanato dal MIUR (decreto n. 305 del 7/12/2006).

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

Il ciclo di vita dei dati personali trattati per mezzo degli strumenti di lavoro a distanza è il medesimo dei trattamenti operati presso la sede di lavoro. In particolare i dati personali oggetto di trattamento devono essere conservati secondo le indicazioni delle Regole tecniche in materia di conservazione digitale degli atti definite da AGID e nel rispetto dei tempi e dei modi indicati dalle Linee Guida per le Istituzioni scolastiche e dai Piani di conservazione e scarto degli archivi scolastici definiti dalla Direzione Generale degli Archivi presso il Ministero dei Beni Culturali;

La procedura di archiviazione deve essere svolta secondo le modalità definite dall'amministrazione scolastica tramite le modalità messe a disposizione dal software di segreteria digitale, accessibile in modalità cloud a tutti gli incaricati, o altri strumenti eventualmente adottati dalla amministrazione per l'accesso remoto alle risorse locali. L'archiviazione dovrà essere effettuata in modo tale da rendere accessibile l'eventuale documentazione riservata soltanto al personale autorizzato che ha necessità del documento per svolgere il proprio lavoro. Gli interessati che richiedono di avere accesso ai dati o ne richiedono la modifica, rettifica o cancellazione, possono farlo solamente tramite richiesta scritta che non limiti le finalità del trattamento, orientate al corretto svolgimento dell'attività didattica.
Il ciclo di vita dei dati di servizio relativi agli utenti e alle attività da essi svolte deve essere quello necessario a consentire le operazioni di gestione delle prestazioni lavorative svolte dal dipendente (punto E direttiva n.3/2017 lavoro agile del Presidente del Consiglio dei Ministri).

Se in fase sperimentale e/o emergenziale, ai fini di limitare i rischi connessi al trattamento dei dati c.d. "particolari" o giudiziari, come definiti dagli Artt. 9 e 10 del Reg. UE 679/2016, si consiglia di effettuare il loro trattamento con modalità da remoto solamente su esplicita indicazione del Titolare, tramite indicazioni specifiche una tantum o deleghe specifiche al personale autorizzato, purché esso sia stato adeguatamente formato sulle modalità e gli strumenti di trattamento utilizzati.

Quali sono le risorse di supporto ai dati?

Solitamente, ci si avvale di servizi, facenti utilizzo di tecnologie *cloud*, che permettono la condivisione e organizzazione dei compiti assegnati. Tali tecnologie possono, talvolta, basarsi su server extra-ue, e in tal caso è di fondamentale importanza verificarne la compliance alla normativa europea sul trattamento dei dati.

A causa delle qualità *cross-platform* di questi servizi, essi vengono fruiti dagli interessati tramite una grande varietà di strumentazione informatica che può comprendere tablet, pc e smartphone, che a loro volta possono essere basati su diversi sistemi operativi e permettere la fruizione dei servizi tramite diversi browser o app.

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento prevede l'utilizzo di tecnologie innovative atte allo svolgimento dell'attività lavorativa da remoto secondo la modalità di lavoro agile prevista dalla Legge 22/5/2017 N. 81 e richiamata

dal dpcm dell'8 marzo 2020 come strumento utile a ridurre gli spostamenti del personale e per contenere quindi la diffusione del virus COVID-19.
I trattamenti operati per mezzo degli strumenti di lavoro a distanza sono quelli previsti dalla normativa nazionale relativi all'esecuzione dei compiti istituzionali della Scuola.
Le informazioni relative alle attività didattiche ed amministrative possono contenere dati personali "particolari" e "giudiziari" ex artt. 9 e 10 del Reg. UE 2016/679, il cui trattamento con modalità da remoto dovrà, in via precauzionale, essere limitato il più possibile in relazione alle esigenze e alle possibilità organizzative e lavorative dell'amministrazione.

Quali sono le basi legali che rendono lecito il trattamento?

L'utilizzo degli strumenti di lavoro a distanza viene adottato in base ai seguenti riferimenti normativi:

- Legge 22 maggio 2017, n. 81 (Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato)
- dpcm dell'8 marzo 2020 (Misure per il contrasto e per il contenimento sull'intero territorio nazionale del diffondersi del virus COVID-19)
- Nota MIUR 8 marzo 2020 N. 279

La base giuridica dei trattamenti operati per mezzo degli strumenti di lavoro a distanza è data dallo svolgimento di attività di interesse pubblico rilevante per l'istruzione e la formazione in ambito scolastico e alla gestione del rapporto di lavoro con i dipendenti, anche in adempimento di obblighi di legge.

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

Il personale incaricato è invitato a raccogliere, conservare (e archiviare) la quantità minima di informazioni necessaria al corretto svolgimento delle loro funzioni.

A tal fine, è bene ricordare che è fondamentale la vigilanza del titolare del trattamento affinché l'insieme dei dati trattati non esuli dalle sole esigenze formative connesse all'ambito strettamente didattico.

I dati sono esatti e aggiornati?

La procedura di raccolta e conservazione dei dati prevede la creazione spesso cooperativa di contenuti, perciò potrebbe presentarsi il caso in cui un elaborato venga deliberatamente modificato da eventuali collaboratori durante il suo processo di creazione. In tal caso, è preferibile utilizzare uno strumento che tenga traccia delle modifiche apportate alla documentazione, tramite ad esempio soluzioni di backup e di cronologia delle modifiche.

Una volta terminati, gli elaborati possono essere considerati documentazione amministrativa. Per questo motivo, essa non può essere modificata o cancellata neppure su richiesta degli interessati per il periodo prescritto dalla legge, salvo in casi particolari e su intervento diretto del D.S. e, se necessario del R.P.D.

Qual è il periodo di conservazione dei dati?

I tempi di conservazione sia cartacei che telematici sono stabiliti dalla normativa di riferimento per le Istituzioni scolastiche in materia di Archivistica, e parimenti rispettati dall'Istituto Scolastico:

- ovvero DPR 445/2000;
- Decreto Legislativo 22 gennaio 2004 n. 42 Codice dei beni culturali e del paesaggio
- Legge 6 luglio 2002, n. 137, art 10 (G.U. n. 45 del 24 febbraio 2004, s.o. n. 28).

Gli stessi, in particolare, sono stati definiti seguendo le linee guida per gli archivi delle Istituzioni scolastiche e il relativo Piano di conservazione e scarto, pubblicati dalla Direzione Generale degli Archivi del Ministero per i Beni e le attività Culturali.

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati vengono informati del trattamento precedentemente all'inizio dello stesso, tramite somministrazione di informativa ex Art. 13 del Reg. UE 206/679. L'informativa viene somministrata ad alunni e genitori degli stessi tramite una combinazione più completa possibile dei canali disponibili alla scuola, che includono, a titolo esemplificativo e non esaustivo:

- La pubblicazione di una circolare;
- L'invio della stessa agli indirizzi mail indicati da genitori, alunni e dipendenti (si sottolinea anche qui l'importanza di utilizzare il campo ccn per l'invio, che a differenza del campo "a" e "cc" consente l'invio a più destinatari senza condividerne gli indirizzi);
- L'utilizzo delle modalità di comunicazione scuola famiglia messe a disposizione dal registro elettronico.

L'informativa dovrà contenere un riferimento alla policy scolastica sull'utilizzo delle strumentazioni elettroniche e sull’adozione di strumenti per l’adozione di modalità di lavoro flessibile. Nella policy dovrà essere specificato che tale modalità di svolgimento dell’attività lavorativa avverrà per mezzo di servizi considerati "sicuri" forniti da società che verranno nominate responsabili del trattamento. Inoltre, sarà necessario rendere edotti gli interessati sui diritti di accesso, rettifica e cancellazione, ponendo preventivamente attenzione sui tempi necessari al trattamento dei dati. Particolare attenzione dovrà essere posta sul fatto che, una volta prodotti, i dati non potranno essere cancellati per un periodo ben definito dalle indicazioni della direzione generale per gli archivi, in quanto atti amministrativi (o che verranno utilizzati a scopo di archivio, qualora la situazione lo preveda)

Ove applicabile: come si ottiene il consenso degli interessati?

Non è previsto.

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

La scuola mette a disposizione degli interessati un modulo di esercizio dei propri diritti. Gli interessati posso sempre rivolgersi all'amministrazione tramite la modalità da loro preferita per l'esercizio degli stessi.

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

La scuola mette a disposizione degli interessati un modulo di esercizio dei propri diritti. Gli interessati posso sempre rivolgersi all'amministrazione tramite la modalità da loro preferita per l'esercizio degli stessi.

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

La scuola mette a disposizione degli interessati un modulo di esercizio dei propri diritti. Gli interessati posso sempre rivolgersi all'amministrazione tramite la modalità da loro preferita per l'esercizio degli stessi.

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

I servizi utilizzati sono stati selezionati anche sulla base della presenza di un contratto d'uso (fosse anche visualizzato e accettato in forma elettronica) che descriva l'ambito delle rispettive responsabilità e specifica gli obblighi loro incombenti.
Nel caso in cui questo contratto non sia disponibile, il titolare provvederà a stipulare un contratto di nomina del responsabile.

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

L'elenco dei servizi ammessi prevede solamente e ove fosse necessario l'utilizzo di server posti negli Stati Uniti d'America o nella Svizzera, che garantiscano misure di sicurezza comparabili con quelli previsti dalla normativa di riferimento.

Rischi

Misure esistenti o pianificate

Crittografia

I dati sono trattati tramite l'utilizzo di meccanismi di conservazione e comunicazione cifrati, ai fini di garantire la minimizzazione del rischio di acceso agli stessi.

Controllo degli accessi logici

L'accesso alle funzionalità del delle piattaforme utilizzate deve essere regolato da un sistema di attivazione di account con permessi specifici, protetti da password, attivabili e disattivabili dall'amministratore del software (il D.S. o un suo delegato).

Archiviazione

Tutta la documentazione relativa all'attività Istituzionale dell'Amministrazione è regolata dalla normativa vigente in materia di archiviazione nella pubblica amministrazione, contenente indicazioni specifiche per la pubblica istruzione.

Minimizzazione dei dati

I dati vengono trattati e archiviati in forma minima, per quanto previsto dalla normativa vigente

Lotta contro il malware

I sistemi scolastici sono protetti da malware con modalità di protezione sia hardware che software (firewall e antivirus). È inoltre opportuno fornire agli utilizzatori delle linee guida sull’utilizzo sicuro delle risorse elettroniche e digitali, che includano le istruzioni per una efficace lotta al malware.

Backup

I sistemi di didattica da remoto utilizzati per il trattamento devono essere provvisti di una modalità di backup.

Manutenzione

Viene effettuata regolarmente una attività di manutenzione nei confronti dei sistemi hardware scolastici. Il responsabile del trattamento garantisce inoltre il corretto funzionamento del software cloud di didattica da remoto.

Contratto con il responsabile del trattamento

I responsabili del trattamento devono essere nominati tali tramite la stipula di un contratto, ai sensi degli Artt. 28 e 29 del Reg. Ue 679/2016

Politica di tutela della privacy

L'amministrazione ha messo in atto una serie di misure orientate all'adeguamento della stessa alla normativa vigente. I dipendenti sono stati nominati incaricati al trattamento ai sensi dell’Art. 2-quaterdecies del D.Lgs. 196/2003, per l’esercizio delle loro funzioni.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

L'amministrazione ha emesso un regolamento interno per la gestione dei data breach, al cui interno sono specificate le modalità di gestione di tali fenomeni.

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?
Violazione della riservatezza di dati personali comuni e/o sensibili
Quali sono le principali minacce che potrebbero concretizzare il rischio?
Accesso abusivo ai sistemi
Quali sono le fonti di rischio?
Un dipendente che si renda responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione. Terzi che fanno un accesso abusivo ai sistemi
Quali misure fra quelle individuate contribuiscono a mitigare il rischio?
Tutte le misure esistenti o pianificate individuate.
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?
La quantità e la rilevanza dei dati personali detenuti, anche di natura sensibile comporta una gravità di rischio che può essere considerata massima. La divulgazione di dati personali di cui la scuola è titolare, anche ex Art. 9 e 10 GDPR, potrebbe avere importanti conseguenze negative sulla vita delle vittime. Ciò potrebbe arrivare a causare disturbi psicologici a lungo termine o permanenti.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?
Limitata, L'attivazione di sistemi di vigilanza interna e l'adozione e attuazione del regolamento, unito ad attività di sensibilizzazione possono essere in grado di limitare violazioni ad alto impatto.

La limitazione a priori del trattamento di dati ex Art. 9 e 10, con deroghe in particolari condizioni su istruzione e permesso limitato da parte del titolare, permette di limitare i potenziali rischi connessi ad una loro diffusione illecita.

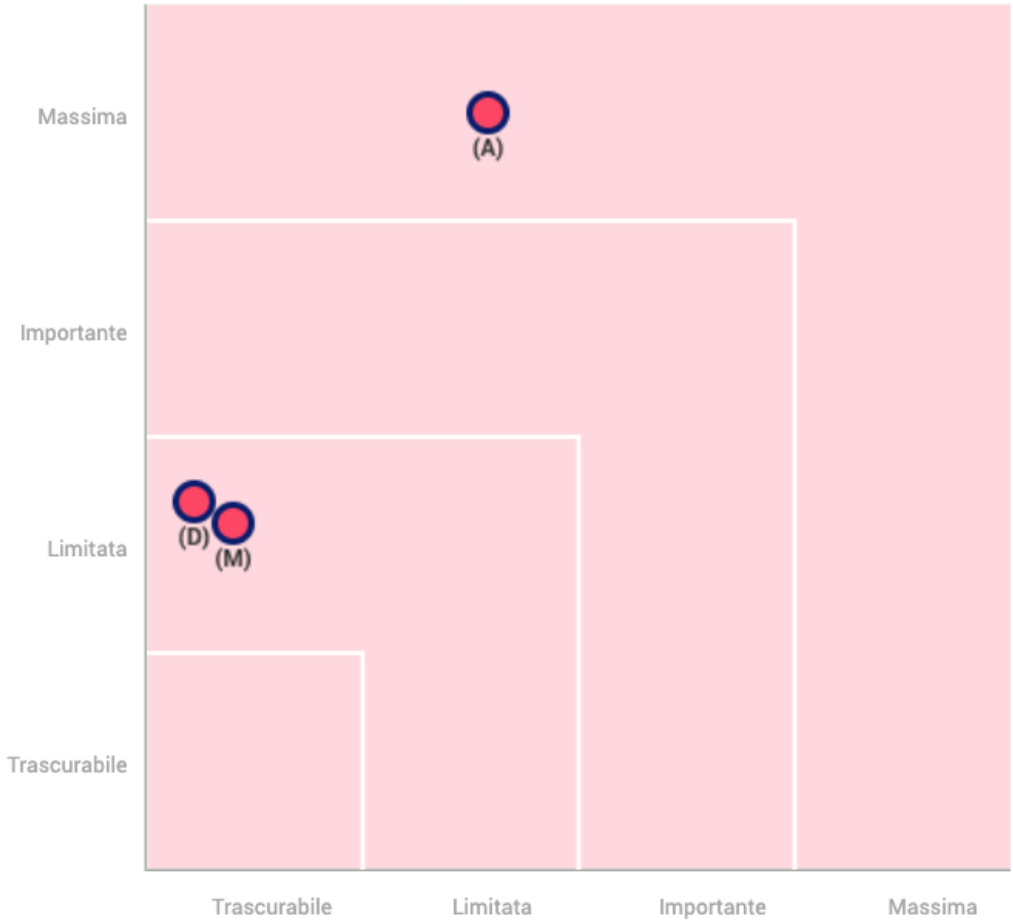
Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?
Potrebbe limitare le possibilità di intervento dell'amministrazione o, successivamente, dell'autorità giudiziaria relativamente alle attività formative e di supporto alla didattica istituzionali.
Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?
Accesso illecito ai dati e modifica degli stessi
Quali sono le fonti di rischio?
Errore umano, Fonti umane interne, che intervengano nella modifica dei dati
Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?
Tutte le misure esistenti o pianificate individuate.
Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?
Limitata, Sebbene la violazione potrebbe portare ad una errata o inefficace prestazione del servizio, le misure di backup e controllo degli accessi logici permetterebbero il recupero delle informazioni e la potenziale identificazione delle fonti di modifica.
Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?
Trascurabile, Appare impossibile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti, purché si proceda alla corretta archiviazione della documentazione, perlomeno per quanto riguarda la versione finale della stessa.

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?
Mancata o rallentata esecuzione dei compiti istituzionali dell’amministrazione.
Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?
Distruzione dei server del servizio, Perdita dell'accesso ai documenti, errore umano
Quali sono le fonti di rischio?
Fonti umane interne, Fonti umane esterne (incaricati del responsabile del trattamento o dei sub-responsabili), Eventi naturali che possano influire sui dispositivi fisici di archiviazione.
Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?
Tutte le misure esistenti o pianificate individuate.
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?
Limitata, Possibile errata o rallentata gestione dell’attività didattica o di supporto alla stessa, a causa dell'incompletezza delle informazioni a disposizione dell’amministrazione.
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?
Trascurabile, Appare impossibile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti, purché si proceda alla corretta esecuzione delle procedure di archiviazione della documentazione.

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