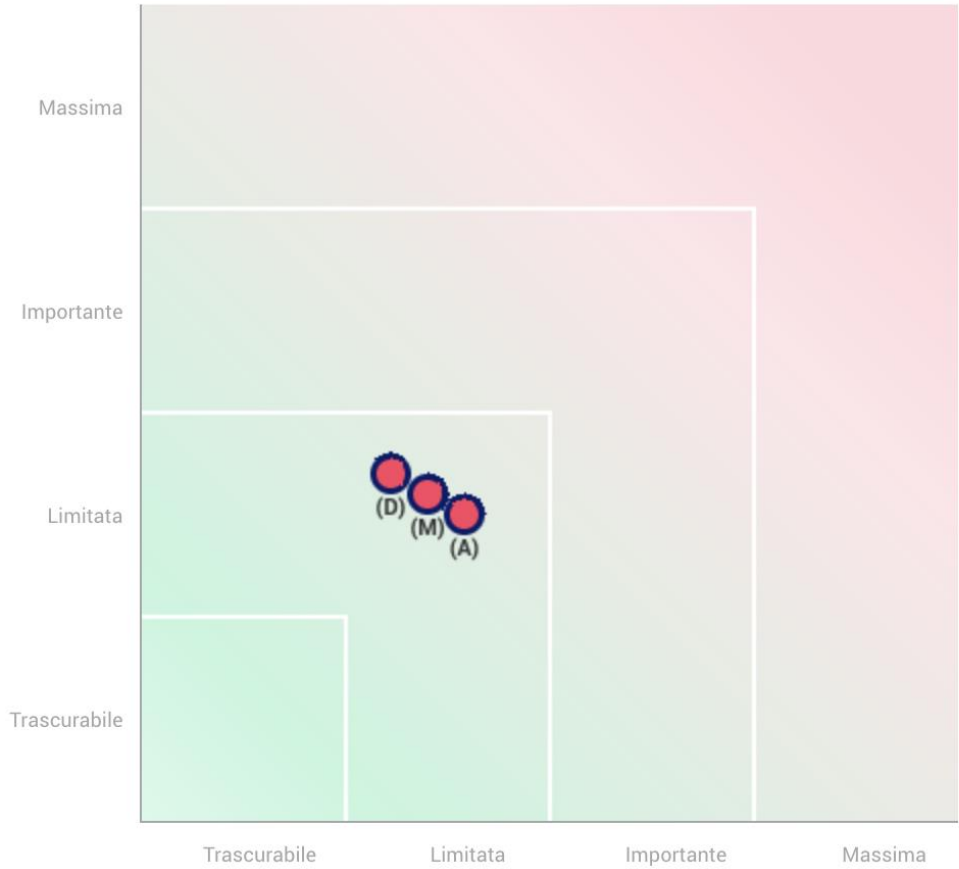


Gravità del rischio



- 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

18/10/24

TO TRANSLATE - Validation

Piano d'azione

Panoramica

Principi fondamentali

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

Misure esistenti o pianificate

		Crittografia
		Controllo degli accessi
		Monitoraggio e rilevamento delle minacce
		Backup e ripristino
		Aggiornamenti di sicurezza continui
		misure applicate ai device utilizzati

Rischi

		Accesso illegittimo ai dati
		Modifiche indesiderate dei dati
		Perdita di dati

Misure Migliorabili

Misure Accettabili

VALUTAZIONE DI IMPATTO

- **GEMINI**
- **NOTEBOOK LM**
- **APP DI TERZE PARTI VERIFICATE**

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Il trattamento dei dati relativi all'utilizzo di strumenti e applicazioni digitali basati sull'Intelligenza Artificiale può essere definito come l'insieme delle operazioni che hanno come oggetto la raccolta, la conservazione, l'elaborazione, la comunicazione, la diffusione, la cancellazione e la distruzione di dati personali degli utenti, effettuate con l'ausilio di strumenti automatizzati, finalizzato a compiti di ricerca/analisi, previsione o generazione di contenuti.

Il trattamento dei dati effettuato mediante l'utilizzo di assistenti di AI generativa (come Google Gemini), di ricerca documentale (come NotebookLM), di creazione di materiali didattici multimediali e collaborativi (come Canva for Education), di redazione collaborativa di documenti tecnici e scientifici (come Overleaf), di somministrazione di quiz interattivi e attività ludiche (come Kahoot e Wordwall) per supportare la didattica, l'apprendimento e l'efficienza amministrativa ha le seguenti finalità: migliorare la produttività del personale e offrire nuove metodologie di apprendimento agli studenti. Tali strumenti, dunque, consentono alla scuola di:

- personalizzare l'apprendimento: adattare i contenuti e le modalità di insegnamento alle esigenze individuali di ogni studente.
- Supportare l'apprendimento: fornire agli studenti strumenti per lo studio, la ricerca e la risoluzione dei problemi.

I risultati attesi dal trattamento dei dati sono molteplici:

- Miglioramento dell'efficacia didattica: grazie alla personalizzazione dell'apprendimento, gli studenti possono raggiungere risultati migliori e più rapidamente.
- Aumento della motivazione: gli studenti sono più motivati quando l'apprendimento è personalizzato e coinvolgente.
- Sviluppo di competenze digitali: l'utilizzo di strumenti digitali favorisce lo sviluppo di competenze digitali fondamentali per il futuro.
- Supporto agli insegnanti: gli insegnanti possono disporre di strumenti per monitorare i progressi dei loro studenti e personalizzare le loro attività didattiche.

Il contesto di utilizzo di Google Gemini, Notebook LM e App di Terze Parti in ambito scolastico è molto ampio e può includere:

- Piattaforme di e-learning: Google Gemini/Notebook LM possono essere integrati in piattaforme di e-learning per fornire supporto agli studenti nello studio autonomo; Canva può essere integrato con Google Classroom

per l'assegnazione di compiti creativi agli studenti ; Wordwall e Kahoot per la distribuzione di esercitazioni interattive, Overleaf per la condivisione di progetti scientifici ecc...

- Applicazioni per dispositivi mobili: Google Gemini/Notebook LM/app di terze parti verificate possono essere disponibili come app per smartphone e tablet, consentendo agli studenti di accedere ai servizi di intelligenza artificiale ovunque si trovino.
- Ambienti virtuali di apprendimento: Google Gemini/Notebook LM/ app di terze parti verificate possono essere utilizzati in ambienti virtuali di apprendimento per creare esperienze di apprendimento immersive e interattive.

Quali sono le responsabilità connesse al trattamento?

Le responsabilità principali del titolare del trattamento sono:

- Identificazione delle finalità: definire chiaramente gli scopi per cui i dati vengono raccolti e trattati (es. personalizzazione dell'apprendimento, ricerca).
- Scelta dei mezzi: determinare le modalità tecniche e organizzative per il trattamento dei dati.
- Informazione agli interessati: Informare gli interessati (studenti, genitori, insegnanti) sulle modalità del trattamento, sui loro diritti e sulle misure di sicurezza adottate.
- Nomina del responsabile (se necessario): se si delega parte del trattamento a un altro soggetto, è necessario nominare un responsabile del trattamento.
- Garanzia di conformità: assicurare che il trattamento sia conforme alla normativa sulla protezione dei dati personali.
- Gestione delle richieste degli interessati: rispondere alle richieste degli interessati relative all'esercizio dei loro diritti (accesso, rettifica, cancellazione, ecc.).

Le responsabilità principali del responsabile del trattamento sono:

- Esecuzione delle istruzioni del titolare: trattare i dati secondo le istruzioni ricevute dal titolare.
- Scelta dei mezzi: determinare i mezzi tecnici e organizzativi per il trattamento dei dati, nel rispetto delle istruzioni ricevute dal titolare.
- Assistenza al titolare: assistere il titolare nell'adempimento degli obblighi previsti dalla normativa sulla protezione dei dati personali.

Ci sono standard applicabili al trattamento?

Di seguito sono elencati alcuni degli standard più rilevanti che Google e le App di Terze parti verificate adottano e delle certificazioni che ha ottenuto:

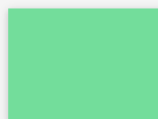
- CCPA (California Consumer Privacy Act): Similmente al GDPR, il CCPA è una legge statunitense che concede ai consumatori della California maggiori diritti sulla privacy dei loro dati personali. Google ha adeguato i suoi servizi per rispettare anche questa normativa.
- Altre normative nazionali: Google si adegua alle normative sulla privacy dei dati di numerosi altri paesi, come il Brasile (LGPD) e il Giappone (APPI).

Standard Internazionali Google Gemini e App di Terze parti verificate

- ISO 27001: Questo standard internazionale definisce i requisiti per un sistema di gestione della sicurezza delle informazioni (ISMS). Google ha ottenuto la certificazione ISO 27001 per molti dei suoi servizi, a dimostrazione del suo impegno per la sicurezza dei dati.
- ISO 27017: Questa estensione della ISO 27001 fornisce specifiche per la sicurezza delle informazioni nel cloud computing. Google ha ottenuto anche questa certificazione per i suoi servizi cloud.

- PCI DSS: Questo standard è specificamente rivolto alle aziende che gestiscono dati di carte di credito. Google, offrendo servizi di pagamento, è conforme a questo standard.
- **ISO/IEC 27018**: Codice di pratica per la **protezione dei dati personali (PII) nel cloud pubblico**, fondamentale per la privacy.
- **ISO/IEC 27701**: Estensione della 27001 e 27002 per la **gestione della privacy (PIMS)**, rilevante per la conformità GDPR.
- **ISO/IEC 42001**: Standard internazionale per i **Sistemi di Gestione dell'AI (AIMS)**, specifico per la gestione responsabile dell'AI.
- **SOC 1, SOC 2, SOC 3**: Report di audit di terze parti (Service Organization Control) sulla sicurezza, disponibilità, integrità dell'elaborazione, riservatezza e privacy.

Valutazione : Accettabile



Contesto

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Dati raccolti e trattati da Google Gemini Education , Notebook LM e da App di Terze parti verificate

Quando si utilizzano Gemini Education, Notebook LM e App di Terze Parti verificate con un account Google Workspace for Education, Google raccoglie e tratta una serie di dati per fornire il servizio e migliorare l'esperienza utente. I dati raccolti possono includere:

- Dati identificativi: nome, cognome, ID utente scolastico
- Dati di utilizzo: interazioni con i servizi, *prompt* di ricerca, documenti caricati, risultati generati dall'AI ecc..
- Informazioni sul dispositivo: Tipo di dispositivo, sistema operativo, browser, indirizzo IP, ecc.
- Informazioni sulla posizione (approssimativa): Utilizzata per personalizzare i risultati in base alla posizione geografica.

Si esclude per policy interna il trattamento di categorie particolari di dati (Art. 9 GDPR).

Periodo di conservazione

Il periodo di conservazione dei dati varia a seconda del tipo di dato e delle finalità del trattamento. In generale, Google tende a conservare i dati per il tempo necessario a fornire il servizio e per rispettare gli obblighi di legge. Tuttavia, alcuni dati potrebbero essere conservati per periodi più lunghi a fini di analisi e miglioramento del servizio.

L'Istituto Scolastico si impegna a conservare i dati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati ("principio di limitazione della conservazione", art.5, GDPR), ossia fino al termine delle attività progettuali e/o per il tempo necessario per obblighi di legge e, in ogni caso, fino alla revoca del consenso. L'Amministrazione scolastica in ogni caso procederà alla cancellazione dell'account al termine del percorso scolastico o nel caso in cui l'utente non sia più parte della comunità scolastica.

Destinatari dei dati

I soggetti destinatari dei dati generati o utilizzati tramite Google Gemini, NotebookLM e App di Terze Parti sono:

1. Istituzione Scolastica, in qualità di titolare del Trattamento. I dati (come le query dei docenti, i riassunti dei documenti scolastici, i materiali generati) sono destinati all'uso interno dell'istituto per scopi didattici e amministrativi;
2. Docenti, Personale ATA, Studenti;
3. Google LLC/Google Ireland Lt, in qualità di Responsabile Esterno del trattamento dei dati personali Google riceve i dati di *input* (ad esempio i *prompt* di Gemini, i documenti sorgente di NotebookLM immagini, testi ecc) e i dati di *output* (la risposta AI generata, progetti, risultati quiz) al solo scopo di fornire il servizio richiesto in base al contratto (Addendum DPA). I dati personali (come i *prompt* o i documenti caricati) non sono destinati a terzi non autorizzati. L'accesso è strettamente limitato.
Google può avvalersi di sub-responsabili (altre entità del gruppo Google o fornitori di servizi terzi) per l'erogazione dell'infrastruttura di base. Questi sono soggetti a contratti che impongono gli stessi obblighi di protezione dei dati (Art. 28 GDPR). Google è tenuta a mantenere un elenco di sub-responsabili e a notificare il Titolare del Trattamento (la scuola) in caso di cambiamenti.
4. I dati personali degli utenti di Workspace for Education (inclusi i *prompt* e i contenuti generati) non sono utilizzati per addestrare i modelli di intelligenza artificiale generativa e non vengono esaminati da operatori umani, salvo casi eccezionali e limitati (es. per motivi di sicurezza, tecnici o legali).

Protezione dei dati e privacy

Google e le App di Terze Parti verificate si impegnano a proteggere la privacy degli utenti e adottano una serie di misure di sicurezza per prevenire l'accesso non autorizzato ai dati. Alcune delle misure di sicurezza adottate includono:

- Crittografia: I dati vengono crittografati sia durante la trasmissione che durante la conservazione.
- Controllo degli accessi: L'accesso ai dati è limitato a un numero ristretto di persone autorizzate.
- Privacy by design: La privacy viene integrata nella progettazione e nello sviluppo dei prodotti e dei servizi Google e delle App di terze parti.

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

Descrizione Dettagliata dei Processi

1. Raccolta dei Dati:
 - Fonti: I dati vengono raccolti principalmente dalle interazioni degli utenti con Gemini Education, Notebook LM e App di terze parti verificate, inclusi gli input dell'utente, i clic, le azioni compiute, i metadati sui dispositivi e le informazioni sulla rete.
 - Tipi di Dati:
 - Dati personali: Nome utente, indirizzo email, informazioni sull'istituto scolastico.
 - Dati di utilizzo: Informazioni su come vengono utilizzati Gemini, Notebook LM, App di Terze Parti (frequenza di utilizzo, funzionalità utilizzate, ecc.).
 - Dati tecnici: Informazioni sul dispositivo, sul browser e sulla rete.
 - Modalità di Raccolta: I dati vengono raccolti in modo automatico durante l'utilizzo della piattaforma.
2. Elaborazione e Analisi:
 - De-identificazione: I dati personali vengono spesso de-identificati o pseudonimizzati per proteggere la privacy dell'utente.
 - Aggregazione: I dati vengono aggregati per identificare trend e modelli di utilizzo.
 - Analisi: I dati vengono analizzati per migliorare l'esperienza utente, sviluppare nuove funzionalità e garantire la sicurezza della piattaforma.
3. Archiviazione:
 - Database: I dati vengono archiviati in database sicuri e protetti.

- Cloud Storage: Google utilizza i propri servizi cloud per archiviare grandi volumi di dati; le App di Terze Parti verificate utilizzano provider leader che garantiscono standard di sicurezza elevati.
 - Backup: Vengono effettuati backup regolari dei dati per prevenire perdite accidentali.
4. Utilizzo dei Dati:
- Personalizzazione: I dati vengono utilizzati per personalizzare l'esperienza dell'utente, ad esempio fornendo suggerimenti personalizzati o adattando l'interfaccia utente.
 - Miglioramento del Servizio: I dati vengono utilizzati per migliorare le funzionalità di Gemini Education e di App di Terze Parti al fine di identificare bug e sviluppare nuove funzionalità.
 - Analisi: I dati vengono utilizzati per analizzare l'utilizzo della piattaforma e identificare trend e modelli.
5. Condivisione dei Dati (se applicabile):
- Condivisione interna: I dati possono essere condivisi all'interno di Google per scopi di sviluppo e miglioramento dei prodotti; per App di Terze Parti i dati possono essere condivisi all'interno delle aziende fornitrici.
 - Condivisione con terze parti: In alcuni casi, i dati possono essere condivisi con partner di fiducia, come fornitori di servizi cloud o fornitori di analisi dati.
 - Condivisione obbligatoria: Google e App di Terze Parti possono essere obbligati a condividere i dati con le autorità governative in risposta a richieste legali.
6. Distruzione dei Dati:
- Periodo di conservazione: I dati vengono conservati per un periodo di tempo limitato, in conformità con le leggi e le normative applicabili e le politiche interne di Google, nonché di App di Terze Parti
 - Cancellazione: Al termine del periodo di conservazione, i dati vengono cancellati in modo sicuro.
 - Anonimizzazione: In alcuni casi, i dati possono essere resi anonimi e conservati a fini di ricerca o statistici.

Quali sono le risorse di supporto ai dati?

Disclaimer: l'infrastruttura esatta utilizzata da Google per ospitare i dati di Gemini Education e Notebook LM è proprietaria e soggetta a modifiche. Le informazioni fornite di seguito sono basate sulla conoscenza generale delle infrastrutture cloud e delle pratiche comuni nel settore.

Tipi di Risorse Utilizzate:

Google, essendo uno dei principali fornitori di servizi cloud al mondo, si affida a una combinazione di risorse hardware e software altamente scalabili e sicure per ospitare i dati dei suoi utenti. Ecco alcune delle risorse più probabili coinvolte nel trattamento dei dati di Gemini Education, Notebook LM e App di terze parti verificate:

Infrastruttura Fisica

- Data Center: Google possiede e gestisce una vasta rete di data center in tutto il mondo. Questi centri ospitano i server fisici che memorizzano e processano i dati. Canva e Kahoot, ad esempio, utilizzano principalmente l'infrastruttura di Amazon Web Services (AWS).
- Server: I server sono i computer ad alte prestazioni che eseguono le applicazioni e memorizzano i dati. Google e App di terze parti verificate utilizzano una varietà di server, dai server standard ai server specializzati per compiti specifici, come l'elaborazione di grandi quantità di dati.
- Reti: Le reti ad alta velocità interconnettono i server e i data center, consentendo la trasmissione dei dati in modo efficiente e sicuro.

- Sistemi di Stoccaggio: I sistemi di stoccaggio sono utilizzati per memorizzare grandi quantità di dati, sia a breve che a lungo termine. Questi possono includere dischi rigidi, unità a stato solido (SSD) e sistemi di archiviazione su nastro.

Software e Sistemi Operativi

- Sistemi Operativi: Google e App di terze parti verificate utilizzano principalmente il sistema operativo Linux per i suoi server, grazie alla sua flessibilità e scalabilità.
- Database: I dati vengono memorizzati in database relazionali e non relazionali, come MySQL, PostgreSQL o BigQuery.
- Software di Virtualizzazione: La virtualizzazione consente di eseguire più sistemi operativi su un singolo server fisico, ottimizzando l'utilizzo delle risorse.
- Piattaforme Cloud: Google utilizza la propria piattaforma cloud, Google Cloud Platform (GCP), per fornire i servizi di Gemini Education. GCP offre una vasta gamma di servizi cloud, tra cui calcolo, storage, database e analisi dei dati. Canva, ad esempio, utilizza Amazon Web Services (AWS); Overleaf utilizza, principalmente, Google Cloud Platform (GCP) e AWS.
- Software di Sicurezza: Viene utilizzato un'ampia gamma di software di sicurezza per proteggere i dati da accessi non autorizzati, perdite e altre minacce.

Risorse Umane

- Ingegneri: Ingegneri software, ingegneri di rete e altri specialisti IT sono responsabili della progettazione, dello sviluppo e della manutenzione dell'infrastruttura.
- Operatori: Gli operatori si occupano della gestione quotidiana dell'infrastruttura, monitorando le prestazioni e risolvendo eventuali problemi.
- Personale addetto alla sicurezza: Il personale addetto alla sicurezza è responsabile della protezione dei dati e della conformità alle normative sulla privacy.

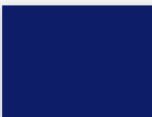
Supporti Cartacei (Minimizzati)

Sebbene l'elaborazione dei dati sia prevalentemente digitale, potrebbero esserci casi in cui vengono utilizzati supporti cartacei per scopi specifici, ad esempio per la documentazione legale o per la conservazione a lungo termine di alcuni dati. Tuttavia, l'uso di supporti cartacei è generalmente minimizzato per ridurre i rischi di perdita o danneggiamento dei dati.

Considerazioni Finali:

- Sicurezza: Google e App di terze parti verificate implementano misure di sicurezza rigorose per proteggere i dati degli utenti, tra cui la crittografia, i firewall, i sistemi di rilevamento delle intrusioni e i controlli di accesso.
- Scalabilità: L'infrastruttura di Google e delle App di terze parti verificate è progettata per essere altamente scalabile, in modo da poter gestire l'aumento del volume dei dati e degli utenti.
- Ridondanza: Vengono implementate misure di ridondanza per garantire la disponibilità dei dati anche in caso di guasti hardware o software.
- Conformità: Google e le App di terze parti verificate si impegnano a rispettare le normative sulla privacy e sulla sicurezza dei dati, come il GDPR.

Valutazione : Accettabile



Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Le finalità del trattamento dei dati in Gemini Education, Notebook LM e App di Terze parti verificate: specifiche, esplicite e legittime

Le finalità per cui Google e le App di terze parti verificate raccolgono e trattano i dati degli utenti sono definite in modo specifico, esplicito e legittimo per diverse ragioni, tra cui:

- Conformità alle normative sulla privacy: Le normative come il GDPR (Regolamento Generale sulla Protezione dei Dati) e il CCPA (California Consumer Privacy Act) richiedono che le finalità del trattamento dei dati siano chiaramente indicate agli interessati.
- Trasparenza verso l'utente: comunicando in modo chiaro le finalità del trattamento, Google e le App di terze parti verificate permettono agli utenti di comprendere come i loro dati vengono utilizzati e di esercitare i loro diritti.
- Limitazione del trattamento: Specificando le finalità, Google e le App di terze parti verificate si impegnano a trattare i dati solo per gli scopi dichiarati, evitando utilizzi impropri o eccessivi.

Esempi di finalità specifiche e legittime:

- Fornire il servizio: I dati vengono utilizzati per fornire le funzionalità di base di Gemini Education e Notebook LM, come la creazione e la gestione di contenuti educativi, nonché per il salvataggio di progetti grafici (Canva), la compilazione delle sorgenti LaTeX (Overleaf) e lo svolgimento di attività ludico-didattiche (Kahoot/Wordwall).
- Personalizzare l'esperienza utente: I dati vengono analizzati per offrire un'esperienza utente più personalizzata, ad esempio mostrando contenuti rilevanti o suggerendo attività.
- Assicurare la sicurezza della piattaforma: i dati vengono utilizzati per rilevare e prevenire attività fraudolente o dannose.
- Condurre ricerche: I dati aggregati e anonimizzati possono essere utilizzati per condurre ricerche e analisi di mercato.

Perché è importante che le finalità siano specifiche e legittime:

- Protezione della privacy: Specificando le finalità, si limita l'utilizzo dei dati a ciò per cui sono stati raccolti, riducendo il rischio di utilizzi impropri.
- Trasparenza: Gli utenti possono comprendere chiaramente come i loro dati vengono utilizzati e prendere decisioni informate.
- Conformità normativa: Il rispetto delle finalità è un requisito fondamentale per la conformità alle normative sulla privacy.

Valutazione : Accettabile

Firmato digitalmente da SAVINI ANNA ARGELLI

Quali sono le basi legali che rendono lecito il trattamento?

- Base giuridica: Ogni trattamento di dati personali deve basarsi su una base giuridica legittima. Nel caso di Gemini Education e Notebook LM, nonché di App di terze parti verificate le basi giuridiche possono includere:
 - Consenso esplicito dell'utente

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)?

- Fornire il servizio:
 - Dati di identificazione: Nome utente, email, affinità accademiche sono necessari per creare un profilo personalizzato e consentire l'accesso al servizio.
- Migliorare il servizio:
 - Dati tecnici: Informazioni sul dispositivo, sistema operativo, browser aiutano a identificare eventuali bug o incompatibilità e a ottimizzare le prestazioni.
 - Dati di utilizzo: La frequenza d'uso, le funzionalità più utilizzate permettono di capire quali aspetti del servizio sono più apprezzati e quali necessitano di miglioramenti.
- Garantire la sicurezza:
 - Dati di geolocalizzazione: In alcuni casi, possono essere utili per prevenire attività fraudolente o inappropriate.
 - Dati di accesso: Gli orari e i dispositivi utilizzati per accedere al servizio possono aiutare a rilevare accessi non autorizzati.

Valutazione : Accettabile

I dati sono esatti e aggiornati?

Raccolta e Selezione dei Dati

- Fonti affidabili: I dati utilizzati per addestrare Google Gemini for Education, e le App di terze parti verificate provengono da fonti ritenute affidabili e di alta qualità, come pubblicazioni scientifiche, libri, articoli di notizie e codici aperti, immagini.
- Filtraggio e pulizia: I dati vengono sottoposti a rigorosi processi di filtraggio e pulizia per rimuovere informazioni errate, incomplete, duplicate o contraddittorie.
- Bilanciamento dei dati: si cerca di garantire un bilanciamento adeguato dei dati, evitando bias che potrebbero influenzare i risultati del modello.

Processi di Addestramento

- Apprendimento supervisionato: Google Gemini, Notebook LM e App di terze parti verificate vengono addestrati su grandi quantità di dati etichettati, in modo da apprendere a correlare input e output specifici.
- Apprendimento per rinforzo: Il modello viene ulteriormente affinato attraverso tecniche di apprendimento per rinforzo, che permettono di ottimizzare le risposte in base a un feedback specifico.

- Valutazione continua: Le prestazioni di Google Gemini, Notebook LM e App di terze parti verificate vengono valutate continuamente su nuovi set di dati per identificare eventuali aree di miglioramento.
- Sincronizzazione in tempo reale: in Overleaf e Canva, ad esempio, la natura collaborativa permette aggiornamenti istantanei. Il "controllo di versione" (Project History) assicura che il dato sia sempre recuperabile nella sua versione corretta, eliminando errori di salvataggio.
- Valutazione continua (Feedback loop): I report di Kahoot e Wordwall, ad esempio, vengono generati immediatamente dopo l'interazione, garantendo che i dati di valutazione formativa siano specchio fedele e attuale della prestazione dello studente.

Misure di Controllo della Qualità

- Valutazione umana: esperti valutano manualmente i risultati generati da Gemini e dalle App di terze parti verificate per assicurarsi che siano corretti, pertinenti e coerenti con le richieste dell'utente.
- Metriche di valutazione: vengono utilizzate diverse metriche per misurare la qualità dei risultati, come la coerenza, la pertinenza e la comprensibilità.
- Feedback degli utenti: Il feedback degli utenti è fondamentale per identificare eventuali problemi e migliorare le prestazioni del modello.

Misure di Sicurezza dei Dati

- Privacy: Google e le App di terze parti verificate rispettano le normative sulla privacy e proteggono i dati degli utenti.
- Sicurezza: Vengono adottate misure di sicurezza rigorose per prevenire accessi non autorizzati e proteggere i dati sensibili.

Aggiornamenti Continui

- Apprendimento continuo: Google e le App di terze parti verificate sono in costante evoluzione, grazie all'apprendimento continuo da nuovi dati e feedback degli utenti.
- Aggiornamenti regolari: Il modello viene aggiornato regolarmente per migliorare le sue prestazioni e correggere eventuali errori.

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

1. Miglioramento Continuo del Servizio:

- Apprendimento automatico: Per affinare costantemente i modelli di linguaggio e fornire risposte sempre più accurate e pertinenti, è necessario conservare un campione rappresentativo delle interazioni utente. Questo permette al sistema di identificare trend, errori e aree di miglioramento.
- Analisi storica: La conservazione di dati storici permette di individuare evoluzioni nel linguaggio, nelle modalità di interazione e nelle richieste degli utenti, consentendo di adattare il servizio alle nuove esigenze.

Risoluzione di Problemi e Assistenza Clienti:

- Debugging: La conservazione dei dati relativi a eventuali errori o malfunzionamenti è essenziale per individuare le cause e implementare le correzioni necessarie.
- Supporto tecnico: La conservazione delle conversazioni e delle azioni degli utenti può essere utile per fornire un supporto tecnico più efficace in caso di problemi.

Conformità Normativa:

- Evidenza delle attività: La conservazione dei dati può essere necessaria per dimostrare la conformità a specifiche normative, come quelle sulla privacy o sulla sicurezza informatica.
- Obblighi legali: In alcuni casi, la legge può imporre un periodo di conservazione minimo per determinate tipologie di dati, ad esempio per finalità contabili o fiscali.

Ricerca e Sviluppo:

- Innovazione: La conservazione di dati anonimizzati e aggregati può essere utile per condurre ricerche e sviluppare nuove funzionalità e applicazioni.

Perché non si può stabilire un periodo di conservazione generico?

Il periodo di conservazione ottimale varia a seconda della tipologia di dato e della finalità specifica per cui viene raccolto. Ad esempio:

- Dati di log: possono essere conservati per un periodo relativamente breve, sufficiente per individuare e risolvere eventuali problemi tecnici.
- Dati di profilo utente: possono essere conservati più a lungo per personalizzare l'esperienza utente e migliorare le raccomandazioni.
- Dati relativi a transazioni: possono essere soggetti a periodi di conservazione più lunghi per motivi legali o contabili.

Salvo l'esistenza di un obbligo di legge che imponga uno specifico termine di conservazione:

- Minimizzazione dei dati: Google e le App di terze parti verificate si impegnano a conservare i dati solo per il tempo strettamente necessario al raggiungimento delle finalità del trattamento.
- Periodiche revisioni: I periodi di conservazione vengono periodicamente rivisti e aggiornati per garantire che siano sempre adeguati alle esigenze e alle normative vigenti.
- Diritto all'oblio: gli utenti hanno il diritto di richiedere la cancellazione dei propri dati, salvo che sussistano motivi legittimi per la conservazione.

Valutazione : Accettabile



Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Informativa dettagliata e formazione preventiva all'uso della piattaforma

Valutazione : Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Il Consenso è stato espressamente richiesto ai genitori e/o tutori legali dello studente e al personale ed è stato rilasciato previo rilascio dell'informativa. La mancata prestazione del consenso non ha determinato alcun limite nella fruizione dei servizi erogati dalla Scuola, ad eccezione della partecipazione al progetto specifico.

Valutazione : Accettabile

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

Gli interessati (cioè gli utenti di Google Gemini Education, Notebook LM e App di terze parti verificate) hanno il diritto di accedere ai propri dati personali e di richiederne la portabilità, in linea con le normative sulla protezione dei dati come il GDPR. Per facilitare l'esercizio di questi diritti, Gemini Education e le App di terze parti verificate dovrebbero mettere a disposizione procedure chiare e accessibili.

Modalità per esercitare i diritti:

1. Canale di richiesta dedicato:
 - Pagina web specifica: Google e le App di terze parti verificate dovrebbero fornire una pagina web dedicata all'interno del proprio portale o sito web, dove gli utenti possono trovare informazioni dettagliate sui loro diritti e un modulo per presentare le richieste; piattaforme come Canva e Overleaf offrono dashboard amministrative che consentono alla scuola di esportare i progetti di un utente.
 - Indirizzo email dedicato: Un indirizzo email specifico (es. privacy@gemini.com) dovrebbe essere messo a disposizione per ricevere le richieste degli utenti.
 - Assistenza clienti: Il servizio clienti dovrebbe essere in grado di fornire assistenza agli utenti che desiderano esercitare i loro diritti.
2. Identificazione dell'interessato:
 - Verifica dell'identità: Per motivi di sicurezza, Google dovrebbe richiedere agli utenti di fornire una prova della loro identità prima di elaborare la richiesta; per le App di terze parti verificate l'accesso avviene tramite SSO (Single Sign-On).
 - Metodi di verifica: È possibile utilizzare diversi metodi di verifica, come la richiesta di un documento d'identità o l'invio di un codice di verifica all'indirizzo email associato all'account.
3. Contenuto della richiesta:
 - Dati specifici: L'utente dovrebbe specificare i dati ai quali desidera accedere o che desidera portare.
 - Formato: l'utente dovrebbe indicare il formato desiderato per i dati (es. CSV, JSON).
4. Tempi di risposta:
 - Tempi massimi: Google e le App di terze parti verificate dovrebbero rispettare i tempi massimi di risposta previsti dalla normativa (generalmente entro un mese).
 - Comunicazione: L'utente dovrebbe essere informato sullo stato della sua richiesta e sui tempi di risposta previsti.
5. Modalità di accesso e portabilità:
 - Accesso diretto: L'utente potrebbe avere la possibilità di accedere direttamente ai propri dati attraverso un'area riservata del portale.
 - Fornitura dei dati: Google e le App di terze parti verificate dovrebbero fornire i dati richiesti in un formato strutturato e comunemente utilizzato, consentendo all'utente di trasmetterli facilmente ad altri servizi.
 - Trasferimento diretto: in alcuni casi, Google e le App di terze parti verificate potrebbero essere in grado di trasferire direttamente i dati a un altro titolare del trattamento, su richiesta dell'utente.

Valutazione : Accettabile

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

Diritto di rettifica

Il diritto di rettifica permette agli utenti di correggere eventuali dati personali inesatti o incompleti che li riguardano. Per esercitare questo diritto, l'utente può seguire le seguenti modalità:

- Identificazione: Come per l'accesso ai dati, l'utente dovrà prima verificare la propria identità.
- Richiesta formale: L'utente dovrà presentare una richiesta formale, indicando chiaramente quali dati sono errati o incompleti e quale è la versione corretta.
- Tempi di risposta: Gemini e le App di terze parti verificate sono tenuti a rispondere alla richiesta entro un termine ragionevole e a procedere alla rettifica dei dati nel minor tempo possibile.
- Prova della rettifica: L'utente dovrebbe ricevere conferma della rettifica effettuata.

Diritto alla cancellazione (diritto all'oblio)

Il diritto alla cancellazione, comunemente noto come "diritto all'oblio", permette agli utenti di richiedere la cancellazione dei propri dati personali quando non sono più necessari rispetto alle finalità per cui sono stati raccolti o trattati.

- Condizioni: L'utente può esercitare questo diritto quando:
 - I dati non sono più necessari rispetto alle finalità per cui sono stati raccolti.
 - L'utente revoca il consenso su cui si basa il trattamento.
 - L'utente si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento.
 - I dati sono stati trattati illecitamente.
- Richiesta formale: La richiesta di cancellazione deve essere presentata in forma scritta e deve specificare i motivi della richiesta.
- Eccezioni: Gemini e le App di terze parti verificate possono negare la richiesta di cancellazione se la conservazione dei dati è necessaria, ad esempio, per adempiere a un obbligo legale, per motivi di interesse pubblico o per la difesa in giudizio.
- Tempi di risposta: Anche in questo caso, Gemini e le App di terze parti verificate hanno l'obbligo di rispondere alla richiesta entro un termine ragionevole e di procedere alla cancellazione dei dati nel minor tempo possibile, tenendo conto delle eventuali eccezioni.

Modalità pratiche per esercitare i diritti

Google, e le App di terze parti verificate dovrebbero mettere a disposizione degli utenti diversi canali per presentare le loro richieste, come:

- Area riservata del portale: Un'area dedicata dove l'utente può accedere alle proprie informazioni e presentare le richieste direttamente online.
- Modulo online: Un modulo dedicato che l'utente può compilare e inviare elettronicamente.
- Indirizzo email dedicato: Un indirizzo email specifico a cui inviare le richieste.
- Servizio clienti: La possibilità di contattare il servizio clienti telefonicamente o tramite chat.

Informazioni che l'utente dovrebbe ricevere

In risposta alla richiesta, Google e le App di terze parti verificate dovrebbero fornire all'utente:

- Conferma della ricezione: Una conferma scritta della ricezione della richiesta.
- Informazioni sull'esito: Una comunicazione sull'esito della richiesta, indicando se la richiesta è stata accolta o meno e, in caso negativo, i motivi del rifiuto.
- Diritto di reclamo: L'informazione sul diritto di presentare reclamo all'autorità di controllo (Garante per la protezione dei dati personali).

Misure di sicurezza

È fondamentale che Google e le App di terze parti verificate adottino misure di sicurezza adeguate per proteggere i dati personali degli utenti durante il processo di gestione delle richieste.

Valutazione : Accettabile

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

Diritto di limitazione del trattamento

Il diritto di limitazione del trattamento consente all'interessato di richiedere che il trattamento dei suoi dati personali sia limitato a determinate circostanze. Ad esempio, quando l'interessato contesta l'esattezza dei dati, quando il trattamento è illecito o quando i dati sono necessari all'interessato per la constatazione, l'esercizio o la difesa di un diritto in sede giudiziaria.

Modalità per esercitare il diritto di limitazione:

- Richiesta formale: L'interessato deve presentare una richiesta formale a Google e alle App di terze parti verificate specificando il motivo della limitazione.
- Verifica dell'identità: Come per gli altri diritti, è necessaria la verifica dell'identità dell'interessato.
- Tempi di risposta: Google e le App di terze parti verificate hanno l'obbligo di rispondere alla richiesta entro un termine ragionevole e di comunicare all'interessato l'accoglimento o il rifiuto della richiesta, motivando quest'ultimo.

Diritto di opposizione

Il diritto di opposizione permette all'interessato di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei suoi dati personali effettuato per il perseguimento di un legittimo interesse del titolare del trattamento o di un terzo, compresa la profilazione.

Modalità per esercitare il diritto di opposizione:

- Richiesta formale: L'interessato deve presentare una richiesta formale a Google e alle App di terze parti verificate, specificando i motivi della sua opposizione.
- Verifica dell'identità: Come per gli altri diritti, è necessaria la verifica dell'identità dell'interessato.

- Tempi di risposta: Google e le App di terze parti verificate hanno l'obbligo di valutare la richiesta e di comunicare all'interessato l'esito entro un termine ragionevole.

Modalità pratiche per esercitare i diritti di limitazione e opposizione

Le modalità pratiche per esercitare questi diritti sono simili a quelle descritte per i diritti di accesso, rettifica e cancellazione:

- Area riservata del portale: Un'area dedicata dove l'utente può accedere alle proprie informazioni e presentare le richieste online.
- Modulo online: Un modulo dedicato che l'utente può compilare e inviare elettronicamente.
- Indirizzo email dedicato: Un indirizzo email specifico a cui inviare le richieste.
- Servizio clienti: La possibilità di contattare il servizio clienti telefonicamente o tramite chat.

Informazioni che l'utente dovrebbe ricevere

In risposta alla richiesta, Google e le App di terze parti verificate dovrebbero fornire all'interessato:

- Conferma della ricezione: Una conferma scritta della ricezione della richiesta.
- Informazioni sull'esito: Una comunicazione sull'esito della richiesta, indicando se la richiesta è stata accolta o meno e, in caso negativo, i motivi del rifiuto.
- Diritto di reclamo: L'informazione sul diritto di presentare reclamo all'autorità di controllo (Garante per la protezione dei dati personali).

Valutazione : Accettabile

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

Obblighi generali di Google e di App di terze parti verificate come responsabili del trattamento

In linea di massima, come responsabile del trattamento, Google e le App di terze parti verificate hanno l'obbligo di:

- Trattare i dati esclusivamente su istruzioni del titolare del trattamento (in questo caso, l'istituzione educativa) e nel rispetto delle finalità indicate.
- Assicurare la riservatezza e l'integrità dei dati.
- Adottare misure tecniche e organizzative adeguate a garantire la sicurezza dei dati.
- Collaborare con il titolare del trattamento per rispondere alle richieste degli interessati.
- Informare immediatamente il titolare in caso di violazione dei dati.
- Tenere un registro delle attività di trattamento.

Dove trovare i dettagli degli obblighi di Google e delle App di terze parti verificate

Per avere una visione completa e precisa degli obblighi specifici di Google in relazione a Gemini for Education, è necessario consultare:

- Contratto di servizio: Il contratto stipulato tra Google e le App di terze parti verificate e l'istituzione educativa è il documento fondamentale che definisce i diritti e gli obblighi di entrambe le parti.
- Contratti di sotto-trattamento: se Google e le App di terze parti si avvalgono di terzi per il trattamento dei dati, i relativi contratti dovranno prevedere clausole che garantiscano il rispetto delle norme sulla protezione dei dati.
- Politiche sulla privacy di Google e App di terze parti: Le politiche sulla privacy di Google e App di terze parti verificate forniscono informazioni generali sulle modalità di trattamento dei dati e sui diritti degli utenti.
- Codici di condotta: Google e le App di terze parti verificate potrebbero aderire a codici di condotta specifici per il settore dell'istruzione o della tecnologia, che impongono ulteriori obblighi.
- Certificazioni: Certificazioni come ISO 27001 possono attestare l'adozione di misure di sicurezza adeguate per la protezione dei dati.

Valutazione : Accettabile

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

- Infrastruttura Cloud: Google utilizza una vasta infrastruttura cloud distribuita in diverse regioni del mondo, incluso il territorio europeo. Ciò significa che i dati degli utenti di Gemini Education potrebbero essere replicati e trattati in diversi data center europei. Le App di terze parti verificate utilizzano i principali fornitori di servizi cloud (ad esempio, AWS per Canva e Kahoot).
- Regolamentazione Europea: Essendo aziende che operano all'interno dell'Unione Europea, Google e App di terze parti verificate sono soggette al Regolamento Generale sulla Protezione dei Dati (GDPR), che impone rigorosi standard per la protezione dei dati personali.
- Principio di minimizzazione: Google e le App di terze parti verificate sono tenute ad applicare il principio di minimizzazione dei dati, il che significa che i dati vengono conservati solo per il tempo necessario e nell'ambito delle finalità per cui sono stati raccolti.
- Trasferimenti Internazionali: Anche se i dati sono principalmente trattati all'interno dell'UE, potrebbero esserci alcuni casi in cui i dati vengono trasferiti verso paesi terzi (fuori dall'UE). In questi casi, Google e le App di terze parti verificate devono garantire che siano adottate misure adeguate per proteggere i dati, come le clausole contrattuali standard (SCC).

Valutazione : Accettabile

Rischi

Misure esistenti o pianificate

Crittografia

A riposo: I dati vengono crittografati quando sono memorizzati sui server di Google e delle App di terze parti verificate, rendendoli illeggibili a chiunque non disponga della chiave di decrittazione.

In transito: Le comunicazioni tra i dispositivi degli utenti e i server di Google e delle App di terze parti verificate sono crittografate utilizzando protocolli SSL/TLS per proteggere i dati da intercettazioni non autorizzate.

Valutazione : Accettabile

Controllo degli accessi

Autenticazione a più fattori: Google e le App di terze parti verificate richiedono spesso l'autenticazione a più fattori per accedere ai servizi, aggiungendo un ulteriore livello di sicurezza.

Autorizzazioni granulari: Gli accessi ai dati sono limitati ai soli utenti autorizzati e solo per le operazioni necessarie.

Valutazione : Accettabile

Monitoraggio e rilevamento delle minacce

Sistemi di rilevamento delle intrusioni: Google e le App di terze parti verificate utilizzano sistemi sofisticati per rilevare e bloccare eventuali intrusioni o attività sospette.

Analisi delle minacce: Gli esperti di sicurezza di Google e le App di terze parti verificate monitorano costantemente le minacce emergenti e aggiornano continuamente i sistemi di difesa.

Valutazione : Accettabile

Backup e ripristino

Backup regolari: Vengono effettuati backup regolari dei dati per garantire la possibilità di ripristino in caso di perdita o danneggiamento.

Test di ripristino: I sistemi di backup vengono testati periodicamente per verificarne l'efficacia.

Valutazione : Accettabile

Aggiornamenti di sicurezza continui

Patch e aggiornamenti: Google e le App di terze parti verificate rilasciano regolarmente patch e aggiornamenti per correggere vulnerabilità e migliorare la sicurezza dei suoi sistemi.

Valutazione : Accettabile

Misure applicate ai device utilizzati

- Utilizzare password forti e uniche per ogni servizio.
- Mantenere aggiornato il software del dispositivo.
- Essere diffidente nei confronti di email e messaggi sospetti.

Valutazione : Accettabile



Rischi

Accesso illegittimo ai dati

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

Diffusione di informazioni private, Danno alla reputazione, Danni economici da frodi, Costi legali, Danni psicologici da ansia e stress, Danni all'istituzione Scolastica da sanzioni, Danno da discontinuità del servizio e alla reputazione del fornitore

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Errore umano per disattenzione, Malintenzionati, Attacchi informatici con phishing, malware, ransomware, SQL injection, DDoS

Quali sono le fonti di rischio?

Uso di dispositivi personali compromessi, perdita dei dispositivi, furto dei dispositivi, perdita o furto credenziali di accesso

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi, Aggiornamenti di sicurezza continui, misure applicate ai device utilizzati, Backup e ripristino, Divieto esplicito di inserire dati personali sensibili nei *prompt*, Crittografia, Monitoraggio e rilevamento delle minacce, **Formazione Obbligatoria** annuale per docenti e personale sull'uso responsabile e sui rischi, supervisione umana, i servizi sono configurati per non consentire l'uso dei dati per l'addestramento.

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

Limitata, la tipologia e la quantità dei dati trattati, anche in relazione agli impatti potenziali e alle misure di sicurezza implementate rende la gravità del rischio limitato

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

Limitata, Il rischio di potenziali minacce rimane comunque basso proprio in relazione all'ambiente nel quale viene utilizzato il servizio

Valutazione : Accettabile

Rischi

Modifiche indesiderate dei dati

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

Costi legali, Danni psicologici da ansia e stress, Danno alla reputazione, Danni economici da frodi

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

Errore umano per disattenzione, Attacchi informatici con phishing, malware, ransomware, SQL injection, DDoS

Quali sono le fonti di rischio?

Uso di dispositivi personali compromessi, perdita o furto credenziali di accesso, furto dei dispositivi

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

Crittografia, Controllo degli accessi, Backup e ripristino

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

Limitata. La gravità del rischio resta limitata in funzione della tipologia e quantità di dati trattati

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

Limitata. La probabilità del rischio resta limitata in funzione della tipologia e quantità di dati trattati, nonché alle misure di sicurezza implementate.

Valutazione : Accettabile

Rischi

Perdita di dati

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

Danni psicologici da ansia e stress, Danno alla reputazione, Diffusione di informazioni private

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

Errore umano per disattenzione, Attacchi informatici con phishing, malware, ransomware, SQL injection, DDoS

Quali sono le fonti di rischio?

Firmato digitalmente da SAVINI ANNA ARGELLI

Uso di dispositivi personali compromessi, furto dei dispositivi, perdita o furto credenziali di accesso

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

Crittografia, Controllo degli accessi, Backup e ripristino

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

Limitata. La tipologia e la quantità di dati trattati determina una stima del rischio derivante dalla perdita limitato, anche in funzione degli impatti e delle misure pianificate

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

Limitata. La tipologia e la quantità di dati trattati determina una probabilità del rischio derivante dalla perdita limitato, anche in funzione delle possibili minacce e delle misure pianificate

Valutazione : Accettabile

Rischi

Panoramica dei rischi

Impatti potenziali

Diffusione di informazioni ...
Danno alla reputazione
Danni economici da frodi
Costi legali
Danni psicologici da ansia ...
Danni all'istituzione Sco...
Danno da discontinuità del ...

Minaccia

Errore umano per disattenzi...
Malintenzionati
Attacchi informatici con ph...

Fonti

Uso di dispositivi personal...
perdita dei dispositivi
furto dei dispositivi
perdita o furto credenziali...

Misure

Controllo degli accessi
Aggiornamenti di sicurezza ...
misure applicate ai device ...
Backup e ripristino
Crittografia
Monitoraggio e rilevamento ...

Accesso illegittimo ai dati

Gravità : Limitata

Probabilità : Limitata

Modifiche indesiderate dei dati

Gravità : Limitata

Probabilità : Limitata

Perdita di dati

Gravità : Limitata

Probabilità : Limitata