*Ministero dell'Istruzione e del Merito*
**ISTITUTO COMPRENSIVO DI CASTELLAMONTE**
VIA TRABUCCO 15 - 10081 CASTELLAMONTE (TO)
Codice Fiscale 92522690012 - Telefono 0124 515498

# Valutazione del rischio per attività digitali Google Workspace

La valutazione dei rischi qui svolta è stata redatta in conformità con le indicazioni fornite dall'ENISA (European Union Agency for Network and Information Security) nell'elaborato "Handbook on Security of Personal Data Processing".

## 1. Definizione dell'operazione di trattamento e del suo contesto

### 1. Descrizione del trattamento dei dati personali

Il trattamento dei dati è eseguito per lo svolgimento delle attività didattiche digitali e informatiche nonché per l'iscrizione dell'alunno/a e del personale scolastico alla piattaforma digitale di Google Workspace for Education nonché per la fruizione dei servizi da essa erogati in ambito esclusivamente scolastico per fini didattici, amministrativi ed istituzionali.

### 2. Quali sono le tipologie di dati personali trattati

Dati anagrafici, dati di contatto, credenziali di accesso alle piattaforme (che vengono consegnate dalla scuola per il primo accesso e che poi devono essere modificate), indirizzo ip di collegamento, dati audio, video e immagini, domande e risposte a domande, commenti (anche vocali), informazioni scritte tramite chat e informazioni potenzialmente contenute nel materiale didattico.

### 3. Qual è la finalità del trattamento

Il trattamento dei dati personali è finalizzato allo svolgimento di attività didattiche digitali e informatiche (compresa l'iscrizione dell'alunno/a e del personale scolastico alla piattaforma Google Workspace for Education e alla fruizione dei servizi da essa erogati in ambito esclusivamente scolastico) anche per lo svolgimento di attività di Didattica digitale integrata nonché per incrementare la dematerializzazione delle risorse, esplorare nuove modalità di comunicazione, educare a un uso consapevole e responsabile di internet e fornire una adeguata alfabetizzazione informatica di base.

### 4. Quali sono gli strumenti utilizzati per il trattamento dei dati personali

Il trattamento avviene attraverso una piattaforma Google Workspace for Education a cui si accede tramite qualsiasi tipo di device (smartphone, tablet, PC) mediante un collegamento alla rete internet e con le credenziali assegnate individualmente dalla Scuola.

### 5. Quali sono le categorie di soggetti interessate

Alunni, genitori / tutori, personale scolastico.

### 6. Chi sono i destinatari dei dati

Viene a conoscenza dei dati Google Ireland Limited in qualità di azienda fornitrice della piattaforma che è stata designata dalla scuola responsabile del trattamento dei dati.

### 7. Dove avviene il trattamento dei dati personali

*Ministero dell'Istruzione e del Merito*
**ISTITUTO COMPRENSIVO DI CASTELLAMONTE**
VIA TRABUCCO 15 - 10081 CASTELLAMONTE (TO)
Codice Fiscale 92522690012 - Telefono 0124 515498

I dati personali possono essere trasferiti verso Paesi terzi rispetto all'Unione Europea, in quanto il Titolare utilizza i servizi della "Google Workspace for Education" offerti da Google Ireland Limited, che si avvale, per la versione gratuita, di server ubicati anche in Stati extra UE. Tuttavia, qualora ciò dovesse rendersi necessario, Google garantisce che l'eventuale trasferimento avverrà in conformità ai requisiti prescritti dalla normativa europea e quindi in presenza di condizioni tali da assicurare un livello di protezione dei Dati Personali conforme a quello richiesto dal GDPR (come, ad esempio, in forza di clausole contrattuali standard, decisioni di adeguatezza, etc.).

***

NOMINA RESPONSABILE DEL TRATTAMENTO AI SENSI DELL'art.28 DEL GDPR - CONTRATTO (ONLINE) GOOGLE WORKSPACE FOR EDUCATION https://workspace.google.com/intl/it/terms/education_terms.html

INFORMATIVA sulla PRIVACY DI GOOGLE WORKSPACE PER L'ISTRUZIONE, GDPR artt. 13-14, https://workspace.google.com/terms/education_privacy.html

CERTIFICAZIONE AgID Workspace Scheda di Workspace tipologia SaaS ID Scheda: SA-690 https://catalogocloud.agid.gov.it/service/690

WHITE PAPER "GOOGLE CLOUD E IL GDPR" GUIDA DI RIFERIMENTO RAPIDO AL GDPR DI GOOGLE CLOUD GUIDA ALL'IMPLEMENTAZIONE DELLA PROTEZIONE DEI DATI IN Workspace https://cloud.google.com/privacy/gdpr

DATA PROCESSSING ADDENDUM https://cloud.google.com/terms/data-processing-addendum/ (si veda punto 10 dove Google dichiara di rispettare la normativa europea sul trasferimento dei dati)

FAQ PRIVACY DI GOOGLE PER LA PIATTAFORMA GOOGLE WORKESPACE: https://support.google.com/googlecloud/answer/6056650

## 2: Comprensione e valutazione dell'impatto

| LIVELLO DI IMPATTO | DESCRIZIONE |
|---|---|
| Basso | Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.). |
| Medio | Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.). |
| Alto | Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fon- |

*Ministero dell'Istruzione e del Merito*
**ISTITUTO COMPRENSIVO DI CASTELLAMONTE**
VIA TRABUCCO 15 - 10081 CASTELLAMONTE (TO)
Codice Fiscale 92522690012 - Telefono 0124 515498

| | |
|---|---|
| | di, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.). |
| Molto alto | Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.). |

*Ministero dell'Istruzione e del Merito*
**ISTITUTO COMPRENSIVO DI CASTELLAMONTE**
VIA TRABUCCO 15 - 10081 CASTELLAMONTE (TO)
Codice Fiscale 92522690012 - Telefono 0124 515498

## Valutazione

| N. | VALUTAZIONE |
|---|---|
| I.1.<br>**Perdita di riservatezza** | Nell'ambito dell'operazione di trattamento specifica, l'impatto della perdita di riservatezza è considerato come **MEDIO**, in quanto in ragione della tipologia di dati trattati per le attività didattiche digitali (anche attraverso gli strumenti informatici utilizzati) non si prospettano impatti rilevanti sui diritti e le libertà degli interessati derivanti da una divulgazione non autorizzata. Di norma vengono trattati dati comuni relativi alle attività didattiche. |
| I.2.<br>**Perdita di integrità** | L'impatto derivante dalla perdita di integrità può parimenti essere considerato come di valore **MEDIO**, in quanto la modifica non autorizzata di questi dati potrebbe ostacolare la corretta gestione e l'utilizzo degli strumenti informatici per le attività didattiche con ulteriori complicazioni per gli interessati sino alla non fruizione del servizio e lo svolgimento, momentaneo, delle attività stesse. Detti inconvenienti posso, tuttavia, essere superati attraverso l'intervento del soggetto designato amministratore della piattaforma o del tecnico informatico della scuola. |
| I.3.<br>**Perdita di disponibilità** | L'impatto derivante dalla perdita di disponibilità può essere considerato **MEDIO**, dal momento che l'indisponibilità dei dati può determinare inconvenienti che comunque possono essere superati senza grosse difficoltà in quanto i dati sono inseriti e utilizzati per lo svolgimento delle attività didattiche digitali quotidiane e una eventuale loro perdita può essere agevolmente ovviata reinserendo i documenti di lavoro quotidiani o, nel caso, ad esempio, di perdita credenziali tramite un immediato ripristino delle stesse. |

Essendo il risultato complessivo della valutazione dell'impatto il più alto identificato, l'impatto complessivo valutato risulta essere **MEDIO**.

Oltre alle ipotesi formulate nell'ambito del presente scenario pratico potrebbero verificarsi casi in cui l'impatto complessivo potrebbe essere superiore a quello appena sopra calcolato. Un esempio di tali ipotesi è quando vi sono particolari dati di alunni con condizioni di disabilità.

## 3. Definizione di possibili minacce e valutazione della loro probabilità

Le domande a seguire sono relative a quattro diverse aree di valutazione che interessano gli ambienti di elaborazione e trattamento dei dati, vale a dire:

*Ministero dell'Istruzione e del Merito*
**ISTITUTO COMPRENSIVO DI CASTELLAMONTE**
VIA TRABUCCO 15 - 10081 CASTELLAMONTE (TO)
Codice Fiscale 92522690012 - Telefono 0124 515498

- Risorse di rete e tecniche (hardware e software)
- Processi / procedure relativi all'operazione di trattamento dei dati
- Diverse parti e persone coinvolte nell'operazione di trattamento
- Settore di operatività e scala del trattamento

Qui vi sono una serie di domande relative alla valutazione della probabilità di occorrenza di una minaccia di cui occorre valutare se la probabilità di accadimento è:

**BASSA:** è improbabile che la minaccia si materializzi;

**MEDIA**: c'è una ragionevole possibilità che la minaccia si materializzi;

**ALTA**: la minaccia potrebbe materializzarsi.

A. RISORSE DI RETE E TECNICHE

1 **Qualche parte del trattamento dei dati personali viene eseguita tramite Internet?**
Quando il trattamento dei dati personali viene eseguito in tutto o in parte tramite Internet, aumentano le possibili minacce da parte di aggressori esterni online (ad esempio Denial of Service, SQL injection, attacchi Man-in-the-Middle), soprattutto quando il servizio è disponibile (e, quindi, rintracciabile / noto) a tutti gli utenti di Internet.
**SI** (per lo svolgimento delle attività didattiche digitali vengono utilizzati degli strumenti informatici e piattaforme alle quali si accede tramite il collegamento alla rete internet e per questo i collegamenti e l'utilizzo a tali sistemi è regolamentato dalla scuola. Si segnala inoltre che la scuola ha due reti internet separate: una per la didattica e una per la segreteria /amministrazione).

2 **È possibile fornire l'accesso a un sistema interno di trattamento dei dati personali tramite Internet (ad esempio per determinati utenti o gruppi di utenti)?**
Quando l'accesso a un sistema di elaborazione interna dei dati viene fornito tramite Internet, la probabilità di minacce esterne aumenta (ad esempio a causa di aggressori esterni online). Allo stesso tempo aumenta anche la probabilità di abuso (accidentale o intenzionale) dei dati da parte degli utenti (ad esempio divulgazione accidentale di dati personali quando si lavora in spazi pubblici). Un'attenzione particolare dovrebbe essere prestata ai casi in cui è consentita la gestione / amministrazione remota del sistema IT.
**SI** (la piattaforma e gli strumenti utilizzati per le attività didattiche sono dei sistemi di elaborazione interna di dati e tutti i dati salvati all'interno di tali applicativi rimangono al suo interno e conservati in cloud dal fornitore. Alla piattaforma vi si accede tramite la rete internet. Si segnala altresì che per accedere alla piattaforma la scuola fornisce specifiche credenziali e accessi differenti in base a ruoli e compiti definiti incarico ai vari utenti).

3 **Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno?**
La connessione a sistemi IT esterni può introdurre ulteriori minacce dovute alle minacce (e ai potenziali difetti di sicurezza) inerenti a tali sistemi. Lo stesso vale anche per i sistemi interni, tenendo conto che, se non opportunamente configurati, tali connessioni possono consentire l'accesso (ai dati personali) a

*Ministero dell'Istruzione e del Merito*
**ISTITUTO COMPRENSIVO DI CASTELLAMONTE**
VIA TRABUCCO 15 - 10081 CASTELLAMONTE (TO)
Codice Fiscale 92522690012 - Telefono 0124 515498

più persone all'interno dell'organizzazione (che in linea di principio non sono autorizzate a tale accesso).
**NO** (piattaforma non è interconnessa ad altri sistemi o servizi IT).

4 **Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?**
Sebbene l'attenzione sia stata posta su sistemi e servizi elettronici, l'ambiente fisico (rilevante per questi sistemi e servizi) è un aspetto importante che, se non adeguatamente salvaguardato, può seriamente compromettere la sicurezza (ad esempio consentendo alle parti non autorizzate di accedere fisicamente all'IT, apparecchiature e componenti di rete, o non riuscendo a fornire protezione della sala computer in caso di disastro fisico).
**NO** (possono accedere alla piattaforma solo i soggetti autorizzati e dotati di password; inoltre tutti gli utenti devono rispettare i regolamenti e le norme di sicurezza imposte dalla Scuola sia per l'uso delle piattaforma che per la rete. Inoltre vi sono utenze differenti, con accesso a specifiche informazioni, in base al ruolo e al compito rivestito).

5 **Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le migliori prassi?**
Componenti hardware e software mal progettate, implementate e / o mantenute possono comportare gravi rischi per la sicurezza delle informazioni. A tal fine, le buone o le migliori pratiche accrescono l'esperienza di eventi precedenti e possono essere considerate come linee guida pratiche su come evitare esposizione (ai rischi) e raggiungere determinati livelli di resilienza.
**NO** (tutti i sistemi e anche la piattaforma devono essere implementati secondo le raccomandazioni del GDPR e il fornitore dei servizi deve garantire alla scuola l'adesione alle attuali norme in materia di trattamento dei dati. Tutti gli strumenti cloud utilizzati dalla scuola sono certificati e presenti nell'AgID Cloud Martekplace).

**VALUTAZIONE DELLA PROBABILITA' DI ACCADIMENTO DI UNA MINACCIA: MEDIA**

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

| | | | |
|---|---|---|---|
| 6 | **I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?** | Quando i ruoli e le responsabilità non sono chiaramente definiti, l'accesso (e l'ulteriore trattamento) dei dati personali può essere incontrollato, con conseguente uso non autorizzato delle risorse e compromissione della sicurezza complessiva del sistema. | **NO** (i ruoli e le autorizzazioni sono chiari e definiti nessuno può entrare nel sistema e negli applicativi utilizzati se non autorizzato dalla scuola e può visualizzare determinati dati solamente in base ai permessi assegnati per lo svolgimento dei compiti e del ruolo assegnato. Inoltre è stato designato anche un Amministratore della Piattaforma di |

*Ministero dell'Istruzione e del Merito*
**ISTITUTO COMPRENSIVO DI CASTELLAMONTE**
VIA TRABUCCO 15 - 10081 CASTELLAMONTE (TO)
Codice Fiscale 92522690012 - Telefono 0124 515498

| | | | |
|---|---|---|---|
| | | | Google e la Scuola ha altresì incaricato un Amministratore di sistema dell'intera rete). |
| 7 | **L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?** | Quando un uso accettabile delle risorse non è chiaramente obbligatorio, potrebbero sorgere minacce alla sicurezza a causa di incomprensioni o di un uso improprio, intenzionale del sistema. La chiara definizione delle politiche per le risorse di rete, di sistema e fisiche può ridurre i rischi potenziali. | **NO** (la scuola ha predisposto regole e istruzioni sia per il personale che per le famiglie e gli studenti). |
| 8 | **I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?** | I dipendenti che utilizzano i loro dispositivi personali all'interno dell'organizzazione potrebbero aumentare il rischio di perdita di dati o accesso non autorizzato al sistema informativo. Inoltre, poiché i dispositivi non sono controllati a livello centrale, possono introdurre nel sistema bug o virus aggiuntivi. | **SI** (la piattaforma e gli applicativi usati per le attività didattiche digitali possono essere utilizzati anche per svolgere attività da casa, come compiti, e quindi anche con i propri device ma gli stessi vengono implementati, controllati e regolamentati dalla scuola. Il personale e le famiglie che utilizzano i propri pc devo garantire che i medesimi siano dotati di sistemi antivirus e anti malware). |
| 9 | **I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?** | L'elaborazione di dati personali al di fuori dei locali dell'organizzazione può offrire molta flessibilità, ma allo stesso tempo introduce rischi aggiuntivi, sia legati alla trasmissione di informazioni attraverso canali di rete potenzialmente insicuri (es. Reti Wi-Fi aperte), sia uso non autorizzato di queste informazioni. | **SI** (la piattaforma di Google Workspace for Education consente l'utilizzo di uno spazio cloud ed il personale e gli alunni, nei limiti consentiti dalla scuola, e nel caso in cui sia necessario per lo svolgimento dell'attività didattica, possono utilizzarlo. Tutto il materiale condiviso però non può essere divulgato e usato per altri fini. Infine periodicamente la scuola controlla gli account ed elimina quelli degli alunni e del |

*Ministero dell'Istruzione e del Merito*
**ISTITUTO COMPRENSIVO DI CASTELLAMONTE**
VIA TRABUCCO 15 - 10081 CASTELLAMONTE (TO)
Codice Fiscale 92522690012 - Telefono 0124 515498

| | | | |
|---|---|---|---|
| | | | personale non più in servizio e iscritto). |
| 10 | **Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?** | La mancanza di adeguati meccanismi di registrazione e monitoraggio può aumentare l'abuso intenzionale o accidentale di processi/ procedure e risorse, con conseguente abuso di dati personali. | **NO** (tutte le operazioni compiute all'interno della piattaforma di Google Workspace for Education possono essere tracciate per fini di sicurezza.<br>Gli accessi degli utenti sono perciò monitorati e ciò è garantito dall'univocità delle credenziali assegnate ad ogni utente utilizzatore). |

**VALUTAZIONE DELLA PROBABILITA' DI ACCADIMENTO DI UNA MINACCIA: <u>MEDIA</u>**

C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI

| | | | |
|---|---|---|---|
| 11 | **Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?** | Quando l'accesso (e l'ulteriore trattamento) dei dati personali è aperto a un gran numero di dipendenti, le possibilità di abuso a causa del fattore umano incrementano. Definire chiaramente chi ha realmente bisogno di accedere ai dati e limitare l'accesso solo a quelle persone può contribuire alla sicurezza dei dati personali. | **NO** (tutti i dipendenti, gli studenti e gli utenti sono monitorati, per soli fini di sicurezza, e definiti. Tutti gli accessi sono limitati e gestiti dalla scuola in persona dell'amministratore della piattaforma). |
| 12 | **Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?** | Quando l'elaborazione viene eseguita da contraenti esterni, l'organizzazione può perdere parzialmente il controllo su questi dati. Inoltre, possono essere introdotte ulteriori minacce alla sicurezza a causa delle minacce intrinseche a questi appaltatori. È importante che l'organizzazione selezioni gli appaltatori che possono offrire un massimo livello di sicurezza e definire chiaramente quale parte del | **SI** (dal soggetto fornitore della piattaforma, Google Ireland Limited, che è stato designato dalla scuola responsabile del trattamento). |

*Ministero dell'Istruzione e del Merito*
**ISTITUTO COMPRENSIVO DI CASTELLAMONTE**
VIA TRABUCCO 15 - 10081 CASTELLAMONTE (TO)
Codice Fiscale 92522690012 - Telefono 0124 515498

| | | | |
|---|---|---|---|
| | | processo è loro assegnata, mantenendo il più possibile un alto livello di controllo. | |
| 13 | **Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?** | Quando i dipendenti non sono chiaramente informati sui loro obblighi, le minacce derivanti da un uso improprio accidentale (ad es. divulgazione o distruzione) di dati aumentano in modo significativo. | **NO** (la scuola ha definito specifiche istruzioni per il trattamento dei dati. Tutto il personale scolastico è stato inoltre autorizzato al trattamento dei dati, istruito e formato attraverso specifici corsi formativi). |
| 14 | **Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?** | Quando i dipendenti non sono consapevoli della necessità di applicare le misure di sicurezza, possono causare accidentalmente ulteriori minacce al sistema. La formazione può contribuire notevolmente a sensibilizzare i dipendenti sia sui loro obblighi di protezione dei dati, sia sull'applicazione di specifiche misure di sicurezza. | **NO** (il personale è stato formato e istruito. Inoltre la scuola ha anche regolamentato lo svolgimento delle attività didattiche e digitali con appositi regolamenti). |
| 15 | **Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?** | Molte violazioni dei dati personali si verificano a causa della mancanza di misure di protezione fisica, come serrature e sistemi di distruzione sicura. I file cartacei sono solitamente parte dell'input o dell'output di un sistema informativo, possono contenere dati personali e devono anche essere protetti da divulgazione e riutilizzo non autorizzati. | **NO** (il personale è stato formato e istruito e al termine del progetto didattico devono essere eliminati i dati condivisi). |

**VALUTAZIONE DELLA PROBABILITA' DI ACCADIMENTO DI UNA MINACCIA: MEDIA**

*Ministero dell'Istruzione e del Merito*
**ISTITUTO COMPRENSIVO DI CASTELLAMONTE**
VIA TRABUCCO 15 - 10081 CASTELLAMONTE (TO)
Codice Fiscale 92522690012 - Telefono 0124 515498

D. SETTORE DI OPERATIVITA' E SCALA DI TRATTAMENTO

| | | | |
|---|---|---|---|
| 16 | **Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?** | Quando gli attacchi alla sicurezza si sono già verificati in uno specifico settore dell'organizzazione del Titolare del trattamento, questa è un'indicazione che l'organizzazione probabilmente dovrebbe prendere ulteriori misure per evitare un evento simile. | **NO** (il settore dell'istruzione non è esposto a particolari attacchi informatici) |
| 17 | **La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?** | Se l'organizzazione è già stata attaccata o ci sono indicazioni che questo potrebbe essere stato il caso, è necessario prendere ulteriori misure per prevenire eventi simili in futuro. | **NO** |
| 18 | **Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?** | Bug di sicurezza / vulnerabilità possono essere sfruttati per eseguire attacchi (cyber o fisici) a sistemi e servizi. Si dovrebbero prendere in considerazione bollettini sulla sicurezza contenenti informazioni importanti relative alle vulnerabilità della sicurezza che potrebbero influire sui sistemi e sui servizi menzionati sopra. | **SI'** (l'istituzione scolastica ha avuto una segnalazione di vulnerabilità da parte della società MONITORA PA) |
| 19 | **Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?** | Il tipo e il volume dei dati personali (scala) possono rendere l'operazione di trattamento dei dati di interesse per gli aggressori (a causa del valore intrinseco di questi dati). | **NO** (l'istituzione scolastica, in genere, non effettua trattamenti di dati personali su larga scala). |
| 20 | **Esistono *best practice* di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?** | Le misure di sicurezza specifiche del settore sono solitamente adattate ai bisogni (e ai rischi) del particolare settore. La mancanza di conformità con le migliori pratiche pertinenti potrebbe essere un indicatore di scarsa gestione della sicurezza. | **NO** (la scuola segue le best practice suggerite dal Ministero dell'istruzione e dall'AGID). |

*Ministero dell'Istruzione e del Merito*
**ISTITUTO COMPRENSIVO DI CASTELLAMONTE**
VIA TRABUCCO 15 - 10081 CASTELLAMONTE (TO)
Codice Fiscale 92522690012 - Telefono 0124 515498

**VALUTAZIONE DELLA PROBABILITA' DI ACCADIMENTO DI UNA MINACCIA: BASSA**

## 4: Valutazione del rischio

Utilizzando le tabelle 4 e 5 si determina la probabilità di occorrenza delle minacce per ciascuna area di valutazione e di conseguenza calcolare il suo valore finale.

Dopo aver valutato l'impatto dell'operazione di trattamento dei dati personali e la probabilità di accadimento della minaccia rilevante, la valutazione finale del rischio è possibile (Tabella 6).

| AREA DI VALUTAZIONE | PROBABILITA' | |
|---|---|---|
| | LIVELLO | PUNTEGGIO |
| RETE E RISORSE TECNICHE | Basso | 1 |
| | Medio | 2 |
| | Alto | 3 |
| PROCESSI / PROCEDURE RELATIVI AL TRATTAMENTO DEI DATI PERSONALI | Basso | 1 |
| | Medio | 2 |
| | Alto | 3 |
| PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI | Basso | 1 |
| | Medio | 2 |
| | Alto | 3 |
| SETTORE DI OPERATIVITA' E SCALA DI TRATTAMENTO | Basso | 1 |
| | Medio | 2 |
| | Alto | 3 |

Tabella 4: Valutazione della probabilità di occorrenza delle minacce per area

| Somma globale della probabilità di occorrenza di una minaccia | LIVELLO DI PROBABILITÀ DELLE MINACCE |
|---|---|
| 4 - 5 | Basso |
| 6 - 8 | Medio |
| 9 -12 | Alto |

Tabella 5: Valutazione della probabilità di occorrenza di una minaccia

*Ministero dell'Istruzione e del Merito*
**ISTITUTO COMPRENSIVO DI CASTELLAMONTE**
VIA TRABUCCO 15 - 10081 CASTELLAMONTE (TO)
Codice Fiscale 92522690012 - Telefono 0124 515498

**IMPACT LEVEL**

| **THREAT OCCURRENCE PROBABILITY** | Low | Medium | High / Very High |
|---|---|---|---|
| Low | | | |
| Medium | | | |
| High | | | |

*Legend*

*Low Risk* *Medium Risk* *High Risk*

# Il rischio finale calcolato è: MEDIO