# DOCUMENTO DI VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

Ai sensi del Regolamento UE GDPR 679/2016 Art. 35

# ISTITUTO ISTRUZIONE SUPERIORE SCIENTIFICO E TECNICO

| | |
|---|---|
| **EMISSIONE** | 08/11/2021 |
| **SEDE LEGALE E** | VIA DEI TIGLI, snc - ORVIETO (TR) 05018 |
| **SEDE OPERATIVA** | ISTITUTO ISTRUZIONE SUPERIORE SCIENTIFICO E TECNICO - LICEO - ORVIETO (TR) 05018<br>ISTITUTO ISTRUZIONE SUPERIORE SCIENTIFICO E TECNICO - GEOMETRI - ORVIETO (TR) 05018 |
| **PARTITA IVA** | 90017210551 |

| | |
|---|---|
| **TITOLARE TRATTAMENTO DATI** | Dott.ssa MONICHINI LORELLA |
| **DPO** | Avv. MARTINI LUCA |

| DATA | REDAZIONE | VERIFICA | APPROVAZIONE |
|---|---|---|---|
| 08/11/2021 | Avv. MARTINI LUCA | Avv. MARTINI LUCA | Dott.ssa MONICHINI LORELLA |

## SOMMARIO

**ISTITUTO ISTRUZIONE SUPERIORE SCIENTIFICO E TECNICO**

**ANAGRAFICA AZIENDALE**

| | |
|---|---|
| Azienda: | **ISTITUTO ISTRUZIONE SUPERIORE SCIENTIFICO E TECNICO** |
| Sede Legale: | **VIA DEI TIGLI, snc - ORVIETO (TR) 05018** |
| Sede Operativa in esame: | **ISTITUTO ISTRUZIONE SUPERIORE SCIENTIFICO E TECNICO - LICEO - ORVIETO (TR) 05018**<br>**ISTITUTO ISTRUZIONE SUPERIORE SCIENTIFICO E TECNICO - GEOMETRI - ORVIETO (TR) 05018** |
| C.F. | **90017210551** |
| Titolare Trattamento Dati: | **Dott.ssa MONICHINI LORELLA** |
| DPO: | **Avv. MARTINI LUCA** |
| Attività svolta: | **ENTE PUBBLICO** |

# VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

La DPIA, acronimo di Data Protection Impact Assessment, è una valutazione preliminare, eseguita dal titolare del trattamento dei dati personali, relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati.

In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento; è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35 del Regolamento 2016/679).

**OBBLIGO DPIA**
Ai sensi dell'articolo 35, paragrafo 3 del Regolamento 2016/679 la valutazione è stata effettuata nei casi in cui un trattamento può presentare rischi elevati, ossia quando:

una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

**CRITERI DA CONSIDERARE PER OBBLIGO DPIA**
Nel percorso di analisi sono stati presi in considerazione i seguenti 9 criteri:

- Valutazione o assegnazione di un punteggio
- Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
- Monitoraggio sistematico
- Dati sensibili o aventi carattere altamente personale
- Trattamento di dati su larga scala
- Creazione di corrispondenze o combinazione di insieme di dati
- Dati relativi ad interessati vulnerabili
- Uso innovativo o applicazione di nuove soluzioni tecnologiche
- Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Nel caso in cui un'attività di trattamento dati soddisfa due o più criteri viene eseguita la valutazione d'impatto sulla protezione dei dati.

**REVISIONE**
Secondo le buone prassi, la valutazione d'impatto sulla protezione dei dati viene riesaminata continuamente e rivalutata con regolarità.

## 1° STEP: identificazione dei trattamenti

Il primo step consiste nel censire tutte le attività di trattamento di dati personali specificandone:

- dati identificativi (Sede, struttura, funzioni),
- finalità,
- tipologia di dati personali trattati,
- categorie di interessati,
- destinatari,
- modalità di elaborazione dati (cartacea, elettronica, mista),
- termine cancellazione dati,
- eventuale trasferimento paesi terzi,
- misure di sicurezza.

## 2° STEP: valutazione del rischio e individuazione criteri per DPIA

Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. L'entità dei rischi viene ricavata assegnando un opportuno valore alla probabilità di accadimento (P) ed alle conseguenze di tale evento (C). Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

$$LR = P \times C$$

LR = livello di rischio
P = probabilità di accadimento
C = conseguenze

Alla probabilità di accadimento dell'evento P è associato un indice numerico rappresentato nella seguente tabella:

| PROBABILITA' DELL'EVENTO | |
|---|---|
| **1** | **Improbabile** |
| **2** | **Poco probabile** |
| **3** | **Probabile** |
| **4** | **M. Probabile** |
| **5** | **Quasi certo** |

Alle conseguenze (C) è associato un indice numerico rappresentato nella seguente tabella:

| CONSEGUENZE | |
|---|---|
| **1** | **Trascurabili** |
| **2** | **Marginali** |
| **3** | **Limitate** |
| **4** | **Gravi** |
| **5** | **Gravissime** |

## MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di probabilità e conseguenze è rappresentata in figura seguente:

| | | | | | | |
|---|---|---|---|---|---|---|
| **Probabilità** | **5** | **5** | **10** | **15** | **20** | **25** |
| | **4** | **4** | **8** | **12** | **16** | **20** |
| | **3** | **3** | **6** | **9** | **12** | **15** |
| | **2** | **2** | **4** | **6** | **8** | **10** |
| | **1** | **1** | **2** | **3** | **4** | **5** |
| | | **1** | **2** | **3** | **4** | **5** |
| | | **Conseguenze** | | | | |

| Entità Rischio | Valori di riferimento |
|---|---|
| **Accettabile** | ***(1 ≤ LR ≤ 3)*** |
| **Medio - basso** | ***(4 ≤ LR ≤ 6)*** |
| **Rilevante** | ***(8 ≤ LR ≤ 12)*** |
| **Alto** | ***(15 ≤ LR ≤ 25)*** |

Si ricava, così, per ogni attività di trattamento un Livello di Rischio (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati).

In questo step viene anche ricercata la presenza di criteri di obbligo DPIA:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico
4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli intere**ssati di esercitare un diritto o di avvalersi di un** servizio o di un contratto

Se vi è presenza di almeno due criteri e/o il Livello di Rischio risulta ALTO, l'attività richiede la DPIA.

### 3 STEP: DPIA – valutazione del rischio normalizzato

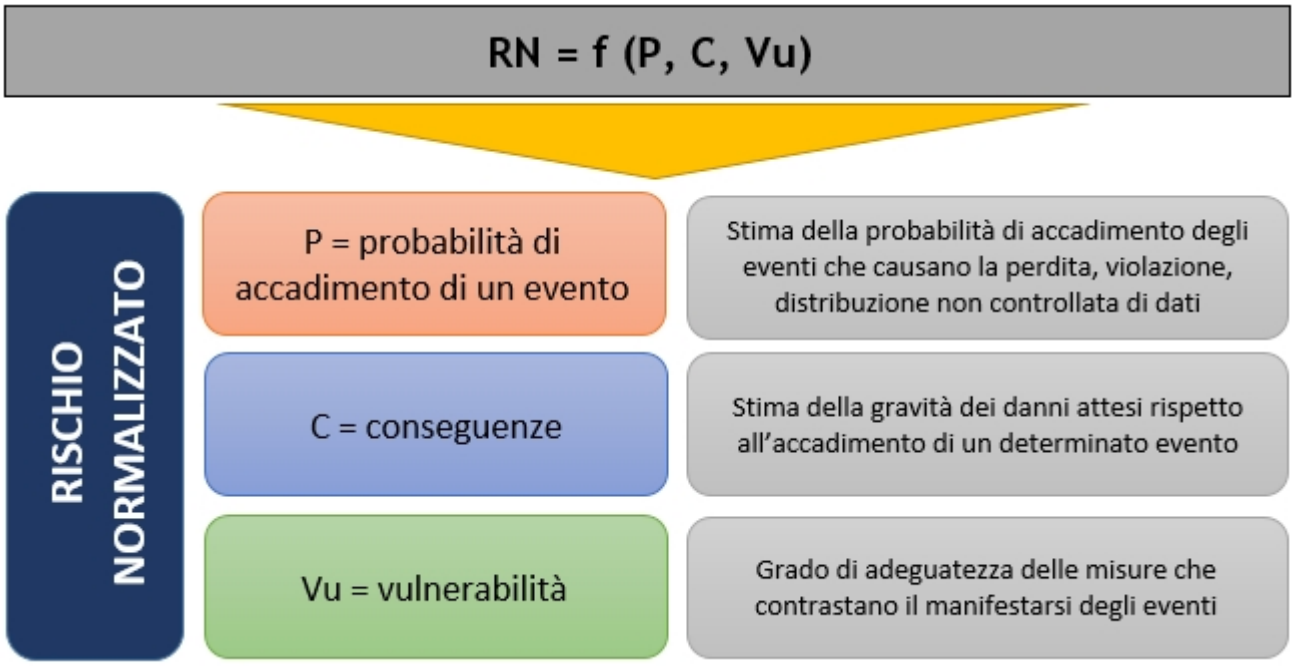
Ai sensi dell'art. 35 del GDPR, vengono individuate tutte le attività di trattamento che in prima analisi presentano un livello di rischio alto e/o prevendono due o più criteri di obbligo DPIA.
Nel caso in cui, quindi, l'indice di rischio si colloca nel range 15 ÷ 25, l'attività necessita di una valutazione di impatto mediante un'analisi approfondita di alcuni aspetti.
La DPIA si basa su un'analisi dei rischi più dettagliata cercando di dare un peso ai possibili controlli applicabili, ricavando, così, un indice di rischio "normalizzato" rispetto al contesto aziendale.

Il rischio viene calcolato in funzione dei 3 fattori seguenti:

$$RN = f(P, C, Vu)$$

Dove:

P = probabilità
C = conseguenze generate dall'evento
V = vulnerabilità rispetto al grado di adeguatezza delle misure




In prima battuta viene ricavato il rischio intrinseco Ri come prodotto della probabilità P e delle conseguenze C, in base agli indici numerici assegnati ad entrambi i fattori.

Alla probabilità P è associato un indice numerico rappresentato nella seguente tabella:

| Probabilità | |
|---|---|
| 1 | **Improbabile** |
| 2 | **Poco probabile** |
| 3 | **Probabile** |
| 4 | **Quasi certo** |

Alle conseguenze (C) è associato un indice numerico rappresentato nella seguente tabella:

| CONSEGUENZE | |
|---|---|
| 1 | **Trascurabili** |
| 2 | **Marginali** |
| 3 | **Limitate** |
| 4 | **Gravi** |

Rispetto al 1 STEP, la matrice ha un range ridotto, essendo una matrice 4 x 4:

| | | | | | |
|---|---|---|---|---|---|
| **PROBABILITÀ** | **4** | **4** | **8** | **12** | **16** |
| | **3** | **3** | **6** | **9** | **12** |
| | **2** | **2** | **4** | **6** | **8** |
| | **1** | **1** | **2** | **3** | **4** |
| | | **1** | **2** | **3** | **4** |
| | | **CONSEGUENZE** | | | |

| **RISCHIO INTRINSECO** | |
|---|---|
| **Ri = P x C** | **Valori di riferimento** |
| **Molto basso** | ***(1 ≤ Ri ≤ 2)*** |
| **Basso** | ***(3 ≤ Ri ≤ 4)*** |
| **Rilevante** | ***(6 ≤ Ri ≤ 9)*** |
| **Alto** | ***(12 ≤ Ri ≤ 16)*** |

Il rischio intrinseco viene ricavato prendendo in considerazione tutti i possibili Pericoli e Rischi.
Di seguito la suddivisione delle aree di pericolo con i rischi generati.

| PERICOLO | RISCHI |
|---|---|
| Agenti fisici (incendio, allagamento, attacchi esterni) | • Perdita<br>• Distruzione non autorizzata |
| Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) | • Perdita<br>• Distruzione non autorizzata |
| Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) | • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato |
| Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) | • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato |
| Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) | • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato |
| Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato |

Per ricavare il Rischio Normalizzato RN, viene introdotto il fattore Vulnerabilità Vu che fornisce un'indicazione circa l'adeguatezza delle misure di sicurezza attuate per ogni rischio.

Alla Vulnerabilità (Vu) è associato un indice numerico rappresentato nella seguente tabella:

| VULNERABILITA' | | Valore |
|---|---|---|
| 1 | Adeguate | 0,25 |
| 2 | Parzialmente adeguate | 0,5 |
| 3 | Inadeguate | 1 |

Per ogni rischio vengono indicate le misure di sicurezza adottate, per ognuna delle quali viene definito il grado di adeguatezza, assegnando uno dei possibili valori:

- 0,25;
- 0,5;
- 1.

Per ricavare il valore del rischio normalizzato RN viene moltiplicato il Rischio Intrinseco Ri con il valore peggiore assegnato alle misure di sicurezza relativamente a quel rischio.

| | | | | | |
|---|---|---|---|---|---|
| Vu | 1 | $1 < RN \leq 2$ | $3 \leq RN \leq 4$ | $6 \leq RN \leq 9$ | $12 \leq RN \leq 16$ |
| | 0,5 | $0,5 < RN \leq 1$ | $1,5 \leq RN \leq 2$ | $3 < RN \leq 5$ | $6 \leq RN \leq 8$ |
| | 0,25 | $0,25 \leq RN \leq 0,5$ | $0,75 \leq RN \leq 1$ | $1,5 \leq RN < 3$ | $3 \leq RN \leq 4$ |
| | | $1 \leq Ri \leq 2$ | $3 \leq Ri \leq 4$ | $6 \leq Ri \leq 9$ | $12 \leq Ri \leq 16$ |
| | | Ri | | | |

| RISCHIO NORMALIZZATO | |
|---|---|
| RN = Ri x Vu | Valori di riferimento |
| Molto basso | $0,25 \leq RN \leq 1$ |
| Basso | $1 < RN < 3$ |
| Rilevante | $3 \leq RN \leq 9$ |
| Alto | $12 \leq RN \leq 16$ |

**Se, a valle dell'analisi DPIA, l'attività ricade comunque in fascia ALTA, il Titolare attiva l'iter di consultazione del Garante.**

Di seguito, viene riportata l'analisi di tutte le attività di trattamento per cui si è resa necessaria la valutazione di impatto sulla protezione dei dati.

## Elenco attività sottoposte a DPIA

- Trattamento di dati personali dei dipendenti e degli Alunni - Segreteria Scolastica Istituto Istruzione Superiore Scientifico e Tecnico - Liceo
- Gestione Amministrativa - Segreteria Scolastica Istituto Istruzione Superiore Scientifico e Tecnico - Liceo
- Gestione Server interno alla Scuola - Segreteria Scolastica Istituto Istruzione Superiore Scientifico e Tecnico - Liceo
- Attività svolte all'interno della Scuola - Istituto Istruzione Superiore Scientifico e Tecnico - Liceo
- Attività svolte all'interno della Scuola - Istituto Istruzione Superiore Scientifico e Tecnico - Geometri

ISTITUTO ISTRUZIONE SUPERIORE SCIENTIFICO E TECNICO

# VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI PER L' ISTITUTO ISTRUZIONE SUPERIORE SCIENTIFICO E TECNICO - SEDE DEL LICEO SCENTIFICO

## TRATTAMENTO DI DATI PERSONALI DEI DIPENDENTI E DEGLI ALUNNI

| | |
|---|---|
| **Struttura** | • Amministrazione<br>• Sede legale<br>• Sede operativa |

| **Personale coinvolto** | |
|---|---|
| **Titolare del trattamento** | Dott.ssa Monichini Lorella |
| **Persone autorizzate** | Direttore dei servizi generali e amministrativi (Persona Autorizzata)<br>• Conservazione<br>• Comunicazione<br>• Consultazione<br>• Raccolta<br><br>Assistente Amministrativo (Persona Autorizzata)<br>• Consultazione<br>• Conservazione<br>• Comunicazione<br>• Raccolta |
| **Partners** | |
| **Altro** | |

| **Processo di trattamento** | |
|---|---|
| **Descrizione** | Trattamento di dati tecnici, amministrativi e personali dei dipendenti e degli Alunni |
| **Fonte dei dati personali** | Raccolti direttamente |
| **Base giuridica per il trattamento per dati comuni (art. 6 GDPR)** | Consenso<br>Legge<br>Contratto |
| **Base giuridica per il trattamento per dati particolari (art. 9 GDPR)** | Consenso<br>Legge |
| **Finalità del trattamento** | Contratto di assunzione<br>Istituzione ed assistenza scolastica<br>Finalità didattiche |
| **Tipo di dati personali** | Curriculum di studi e accademico, pubblicazioni, articoli, monografie, relazioni, materiale audiovisivo, titoli di studio, ecc.<br>Lavoro (occupazione attuale e precedente, informazioni sul reclutamento, sul tirocinio o sulla formazione professionale, informazioni sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione, curriculum vitae<br>Codice fiscale ed altri numeri di identificazione personale (carte sanitarie)<br>Particolari (sensibili)<br>Personali |
| **Categorie di interessati** | Docenti<br>Familiari dell'interessato<br>Collaboratori<br>Dipendenti<br>Studenti |
| **Categorie di destinatari** | Familiari dell'interessato<br>Clienti ed utenti |

| | |
|---|---|
| | Associazioni ed enti locali<br>Responsabili interni<br>Persone autorizzate |
| **Informativa** | Si |
| **Profilazione** | Non necessario |
| **Dati particolari** | Si |
| **Consenso minori** | Si |
| **Frequenza trattamento** | Giornaliera |
| **Termine cancellazione dati** | I dati saranno trattati per tutto il tempo necessario allo svolgimento delle attività d'istruzione. |
| **Trasferimento dati (paesi terzi)** | Non presente |

| **Modalità di elaborazione dati: Mista - elettronica e cartacea** | |
|---|---|
| **Strumenti** | Software gestionale<br>PC interno alla Struttura |
| **Archiviazione** | Mobile da Archivio<br>Armadio chiuso a chiave |
| **Strutture informatiche di archiviazione** | |
| **Server Interno della Scuola** | Struttura interna |
| Sede di riferimento | Sede Liceo Scientifico |
| Personale con diritti di accesso | |
| Note | |
| Software utilizzati | |
| **Strutture informatiche di backup** | |
| **Server Interno della Scuola** | Struttura interna |
| Sede di riferimento | Sede Liceo Scientifico |
| Frequenza di backup | 2 giorni |
| Tempo di storicizzazione | 21 giorni |
| Personale con diritti di accesso | |
| Note | |
| Software utilizzati | |

| **VALUTAZIONE DEL LIVELLO DI RISCHIO** | | |
|---|---|---|
| **PROBABILITÀ** | **CONSEGUENZE** | **LIVELLO DI RISCHIO** |
| **Poco probabile** | **Grave** | **Rilevante** |

**MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE**

- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati
- Dispositivi antincendio
- Documenti chiusi a chiave in apposito locale/armadio
- E' applicata una gestione della password degli utenti
- E' eseguita la DPIA
- I dati sono crittografati
- I documenti vengono firmati digitalmente
- I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili
- Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi
- L'impianto elettrico è certificato ed a norma
- Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee
- Registrazione e deregistrazione degli utenti
- Sistemi di allarme e di sorveglianza anti-intrusione
- Sono applicate procedure di disaster recovery che garantiscono il ripristino dell'accesso ai dati in tempi ridotti
- Sono definiti i ruoli e le responsabilità
- Sono definiti i termini di conservazione e le condizioni di impiego dei dati.

- Sono gestiti i back up
- Sono stabiliti programmi di formazione e sensibilizzazione
- Sono utilizzati software antivirus e anti intrusione
- Viene eseguita opportuna manutenzione
- Viene eseguita una regolare formazione del personale

## VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

| MISURE DI SICUREZZA | PERICOLI ASSOCIATI | LIVELLO DI ADEGUATEZZA |
|---|---|---|
| Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Dispositivi antincendio | • Agenti fisici (incendio, allagamento, attacchi esterni) | Adeguate |
| Documenti chiusi a chiave in apposito locale/armadio | | Adeguate |
| E' applicata una gestione della password degli utenti | • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)<br>• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| E' eseguita la DPIA | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| I dati sono crittografati | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| I documenti vengono firmati digitalmente | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi | • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>• Agenti fisici (incendio, allagamento, attacchi esterni) | Adeguate |
| L'impianto elettrico è certificato ed a norma | • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) | Adeguate |

| | | |
|---|---|---|
| | • Agenti fisici (incendio, allagamento, attacchi esterni) | |
| Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Registrazione e deregistrazione degli utenti | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)<br>• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) | Adeguate |
| Sistemi di allarme e di sorveglianza anti-intrusione | • Agenti fisici (incendio, allagamento, attacchi esterni)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)<br>• Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) | Adeguate |
| Sono applicate procedure di disaster recovery che garantiscono il ripristino dell'accesso ai dati in tempi ridotti | • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) | Adeguate |
| Sono definiti i ruoli e le responsabilità | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Sono definiti i termini di conservazione e le condizioni di impiego dei dati. | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)<br>• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) | Adeguate |
| Sono gestiti i back up | • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)<br>• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)<br>• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>• Agenti fisici (incendio, allagamento, attacchi esterni) | Adeguate |
| Sono stabiliti programmi di formazione e sensibilizzazione | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Sono utilizzati software antivirus e anti intrusione | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |

| | | |
|---|---|---|
| Viene eseguita opportuna manutenzione | • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) | Adeguate |
| Viene eseguita una regolare formazione del personale | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |

| PERICOLO | | |
|---|---|---|
| **Agenti fisici (incendio, allagamento, attacchi esterni)** | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Marginali | Basso |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*** | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Basso | 0,25 | Molto basso |

| PERICOLO | | |
|---|---|---|
| **Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)** | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Marginali | Basso |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*** | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Basso | 0,25 | Molto basso |

| PERICOLO | | |
|---|---|---|
| **Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)** | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*** | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,25 | Basso |

| PERICOLO | | |
|---|---|---|
| **Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)** | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*** | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,25 | Basso |

| PERICOLO | | |
|---|---|---|
| **Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)** | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Gravi | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*** | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,25 | Basso |

| PERICOLO | | |
|---|---|---|
| **Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)** | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Gravi | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*** | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,25 | Basso |

**A valle della DPIA l'attività risulta a rischio Basso**

| | |
|---|---|
| **Struttura** | • Sede legale<br>• Sede operativa<br>• Amministrazione |

| **Personale coinvolto** | |
|---|---|
| **Titolare del trattamento** | Dott.ssa Monichini Lorella |
| **Persone autorizzate** | Direttore dei servizi generali e amministrativi (Persona Autorizzata)<br>• Conservazione<br>• Comunicazione<br>• Consultazione<br>• Raccolta<br><br>Assistente Amministrativo (Persona Autorizzata)<br>• Consultazione<br>• Conservazione<br>• Comunicazione<br>• Raccolta |
| **Partners** | |
| **Altro** | |

| **Processo di trattamento** | |
|---|---|
| **Descrizione** | Attività di Gestione Amministrativa |
| **Fonte dei dati personali** | Forniti da terzi |
| **Base giuridica per il trattamento per dati comuni (art. 6 GDPR)** | Contratto<br>Legge |
| **Base giuridica per il trattamento per dati particolari (art. 9 GDPR)** | |
| **Finalità del trattamento** | Gestione del personale<br>Pagamento Progetti Scolastici<br>Gestione fornitori<br>Adempimento di obblighi di legge connessi a rapporti commerciali |
| **Tipo di dati personali** | Codice fiscale ed altri numeri di identificazione personale<br>Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.)<br>Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro) |
| **Categorie di interessati** | Fornitori<br>Consulenti e liberi professionisti, anche in forma associata<br>Dipendenti |
| **Categorie di destinatari** | Persone autorizzate<br>Provveditorato<br>Banche e istituti di credito<br>Responsabili esterni<br>Autorità di vigilanza e controllo |
| **Informativa** | Si |
| **Consenso** | Non necessario |
| **Profilazione** | Non necessario |
| **Dati particolari** | Non presenti |
| **Frequenza trattamento** | Mensile |
| **Termine cancellazione dati** | I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere. |
| **Trasferimento dati (paesi terzi)** | No |

| | |
|---|---|
| **Autorizzazione del Garante** | Non presente |

| **Modalità di elaborazione dati: Mista - elettronica e cartacea** | |
|---|---|
| **Strumenti** | PC interno alla Struttura |
| **Archiviazione** | Mobile da Archivio |
| **Strutture informatiche di archiviazione** | |
| **Server Interno della Scuola** | Struttura interna |
| Sede di riferimento | Sede Liceo Scientifico |
| Personale con diritti di accesso | |
| Software utilizzati | |
| **Strutture informatiche di backup** | |
| **Server Interno della Scuola** | Struttura interna |
| Sede di riferimento | Sede Liceo Scientifico |
| Frequenza di backup | 2 giorni |
| Tempo di storicizzazione | 21 giorni |
| Personale con diritti di accesso | |
| Note | |
| Software utilizzati | |

| **VALUTAZIONE DEL LIVELLO DI RISCHIO** | | |
|---|---|---|
| **PROBABILITÀ** | **CONSEGUENZE** | **LIVELLO DI RISCHIO** |
| **Poco probabile** | **Marginali** | **Medio-basso** |

**MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE**

- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati
- Dispositivi antincendio
- Documenti chiusi a chiave in apposito locale/armadio
- E' applicata una gestione della password degli utenti
- E' eseguita la DPIA
- I dati sono crittografati
- I documenti vengono firmati digitalmente
- I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili
- Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi
- L'impianto elettrico è certificato ed a norma
- Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee
- Registrazione e deregistrazione degli utenti
- Sistemi di allarme e di sorveglianza anti-intrusione
- Sono applicate procedure di disaster recovery che garantiscono il ripristino dell'accesso ai dati in tempi ridotti
- Sono definiti i ruoli e le responsabilità
- Sono definiti i termini di conservazione e le condizioni di impiego dei dati.
- Sono gestiti i back up
- Sono stabiliti programmi di formazione e sensibilizzazione
- Sono utilizzati software antivirus e anti intrusione
- Viene eseguita opportuna manutenzione
- Viene eseguita una regolare formazione del personale

## VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

| MISURE DI SICUREZZA | PERICOLI ASSOCIATI | LIVELLO DI ADEGUATEZZA |
|---|---|---|
| Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Dispositivi antincendio | • Agenti fisici (incendio, allagamento, attacchi esterni) | Adeguate |
| Documenti chiusi a chiave in apposito locale/armadio | | Adeguate |
| E' applicata una gestione della password degli utenti | • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)<br>• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| E' eseguita la DPIA | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| I dati sono crittografati | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| I documenti vengono firmati digitalmente | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi | • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>• Agenti fisici (incendio, allagamento, attacchi esterni) | Adeguate |
| L'impianto elettrico è certificato ed a norma | • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) | Adeguate |

| | | |
|---|---|---|
| | • Agenti fisici (incendio, allagamento, attacchi esterni) | |
| Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Registrazione e deregistrazione degli utenti | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)<br>• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) | Adeguate |
| Sistemi di allarme e di sorveglianza anti-intrusione | • Agenti fisici (incendio, allagamento, attacchi esterni)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)<br>• Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) | Adeguate |
| Sono applicate procedure di disaster recovery che garantiscono il ripristino dell'accesso ai dati in tempi ridotti | • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) | Adeguate |
| Sono definiti i ruoli e le responsabilità | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Sono definiti i termini di conservazione e le condizioni di impiego dei dati. | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)<br>• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) | Adeguate |
| Sono gestiti i back up | • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)<br>• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)<br>• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>• Agenti fisici (incendio, allagamento, attacchi esterni) | Adeguate |
| Sono stabiliti programmi di formazione e sensibilizzazione | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Sono utilizzati software antivirus e anti intrusione | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |

| | | |
|---|---|---|
| Viene eseguita opportuna manutenzione | • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) | Adeguate |
| Viene eseguita una regolare formazione del personale | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |

| PERICOLO | | |
|---|---|---|
| **Agenti fisici (incendio, allagamento, attacchi esterni)** | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Marginali | Basso |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*** | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Basso | 0,25 | Molto basso |

| PERICOLO | | |
|---|---|---|
| **Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)** | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Marginali | Basso |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*** | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Basso | 0,25 | Molto basso |

| PERICOLO | | |
|---|---|---|
| **Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)** | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Marginali | Basso |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*** | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Basso | 0,25 | Molto basso |

| PERICOLO | | |
|---|---|---|
| **Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)** | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*** | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,25 | Basso |

| PERICOLO | | |
|---|---|---|
| **Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)** | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*** | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,25 | Basso |

| PERICOLO | | |
|---|---|---|
| **Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)** | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*** | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,25 | Basso |

**A valle della DPIA l'attività risulta a rischio Basso**

# ISTITUTO ISTRUZIONE SUPERIORE SCIENTIFICO E TECNICO
# GESTIONE SERVER INTERNO ALLA SCUOLA

| | |
|---|---|
| **Struttura** | • Amministrazione<br>• Sede legale<br>• Sede operativa |

| **Personale coinvolto** | |
|---|---|
| **Titolare del trattamento** | Dott.ssa Monichini Lorella |
| **Persone autorizzate** | |
| **Partners - Responsabili esterni** | |
| **Altro** | |

| **Processo di trattamento** | |
|---|---|
| **Descrizione** | Gestione strutture di rete e pc interni alla scuola |
| **Fonte dei dati personali** | Raccolti direttamente |
| **Base giuridica per il trattamento per dati comuni (art. 6 GDPR)** | Consenso<br>Legge |
| **Base giuridica per il trattamento per dati particolari (art. 9 GDPR)** | Consenso |
| **Finalità del trattamento** | Finalità didattiche<br>Finalità istituzionale della scuola, relative all'istruzione e formazione degli alunni<br>Gestione del personale<br>Servizi internet |
| **Tipo di dati personali** | Dati relativi alla famiglia e a situazioni personali<br>Personali<br>Particolari (sensibili)<br>Nominativi Alunni |
| **Categorie di interessati** | Dipendenti<br>Docenti<br>Alunni |
| **Categorie di destinatari** | Persone autorizzate<br>Familiari dell'interessato<br>Enti locali |
| **Informativa** | Non necessaria |
| **Profilazione** | Non necessario |
| **Dati particolari** | Non presenti |
| **Consenso minori** | Non necessario |
| **Frequenza trattamento** | Giornaliera |
| **Termine cancellazione dati** | I dati saranno trattati per tutto il tempo necessario allo svolgimento delle attività d'istruzione. |
| **Trasferimento dati (paesi terzi)** | No |
| **Autorizzazione del Garante** | Non presente |

| **Modalità di elaborazione dati: Mista - elettronica e cartacea** | |
|---|---|
| **Strumenti** | PC interno alla Struttura |
| **Strutture informatiche di archiviazione** | |
| **Server Interno della Scuola** | Struttura interna |
| Sede di riferimento | Sede Liceo Scientifico |
| Personale con diritti di accesso | |
| Software utilizzati | |
| **Strutture informatiche di backup** | |
| **Server Interno della Scuola** | Struttura interna |
| Sede di riferimento | Sede Liceo Scientifico |
| Frequenza di backup | 2 giorni |

| | |
|---|---|
| Tempo di storicizzazione | 21 giorni |
| Personale con diritti di accesso | |
| Note | |
| Software utilizzati | |

| VALUTAZIONE DEL LIVELLO DI RISCHIO | | |
|---|---|---|
| **PROBABILITÀ** | **CONSEGUENZE** | **LIVELLO DI RISCHIO** |
| Poco probabile | Limitate | Medio-basso |

**MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE**

- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati
- Dispositivi antincendio
- Documenti chiusi a chiave in apposito locale/armadio
- E' applicata una gestione della password degli utenti
- E' eseguita la DPIA
- I dati sono crittografati
- I documenti vengono firmati digitalmente
- I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili
- Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi
- L'impianto elettrico è certificato ed a norma
- Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee
- Registrazione e deregistrazione degli utenti
- Sistemi di allarme e di sorveglianza anti-intrusione
- Sono applicate procedure di disaster recovery che garantiscono il ripristino dell'accesso ai dati in tempi ridotti
- Sono definiti i ruoli e le responsabilità
- Sono definiti i termini di conservazione e le condizioni di impiego dei dati.
- Sono gestiti i back up
- Sono stabiliti programmi di formazione e sensibilizzazione
- Sono utilizzati software antivirus e anti intrusione
- Viene eseguita opportuna manutenzione
- Viene eseguita una regolare formazione del personale

## VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

| MISURE DI SICUREZZA | PERICOLI ASSOCIATI | LIVELLO DI ADEGUATEZZA |
|---|---|---|
| Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Dispositivi antincendio | • Agenti fisici (incendio, allagamento, attacchi esterni) | Adeguate |
| Documenti chiusi a chiave in apposito locale/armadio | | Adeguate |
| E' applicata una gestione della password degli utenti | • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)<br>• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| E' eseguita la DPIA | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| I dati sono crittografati | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| I documenti vengono firmati digitalmente | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi | • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>• Agenti fisici (incendio, allagamento, attacchi esterni) | Adeguate |
| L'impianto elettrico è certificato ed a norma | • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) | Adeguate |

| | | |
|---|---|---|
| | • Agenti fisici (incendio, allagamento, attacchi esterni) | |
| Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Registrazione e deregistrazione degli utenti | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)<br>• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) | Adeguate |
| Sistemi di allarme e di sorveglianza anti-intrusione | • Agenti fisici (incendio, allagamento, attacchi esterni)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)<br>• Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) | Adeguate |
| Sono applicate procedure di disaster recovery che garantiscono il ripristino dell'accesso ai dati in tempi ridotti | • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) | Adeguate |
| Sono definiti i ruoli e le responsabilità | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Sono definiti i termini di conservazione e le condizioni di impiego dei dati. | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)<br>• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) | Adeguate |
| Sono gestiti i back up | • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)<br>• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)<br>• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>• Agenti fisici (incendio, allagamento, attacchi esterni) | Adeguate |
| Sono stabiliti programmi di formazione e sensibilizzazione | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Sono utilizzati software antivirus e anti intrusione | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |

| | | |
|---|---|---|
| Viene eseguita opportuna manutenzione | • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) | Adeguate |
| Viene eseguita una regolare formazione del personale | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |

| PERICOLO | | |
|---|---|---|
| Agenti fisici (incendio, allagamento, attacchi esterni) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi* | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,25 | Basso |

| PERICOLO | | |
|---|---|---|
| Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi* | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,25 | Basso |

| PERICOLO | | |
|---|---|---|
| Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi* | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,25 | Basso |

| PERICOLO | | |
|---|---|---|
| Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi* | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,25 | Basso |

| PERICOLO | | |
|---|---|---|
| Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi* | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,25 | Basso |

| PERICOLO | | |
|---|---|---|
| Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi* | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,25 | Basso |

**A valle della DPIA l'attività risulta a rischio Basso**

| | |
|---|---|
| **Struttura** | • Amministrazione<br>• Sede legale<br>• Sede operativa |

| **Personale coinvolto** | |
|---|---|
| **Titolare del trattamento** | Dott.ssa Monichini Lorella |
| **Persone autorizzate** | Docente (Persona Autorizzata)<br>• Comunicazione<br>• Conservazione<br>• Consultazione<br>• Raccolta<br><br>Collaboratore Scolastico (Persona Autorizzata)<br>• Comunicazione<br>• Conservazione<br>• Consultazione<br>• Raccolta |
| **Partners** | |
| **Altro** | |

| **Processo di trattamento** | |
|---|---|
| **Descrizione** | Trattamento di dati personali degli Alunni |
| **Fonte dei dati personali** | Raccolti direttamente |
| **Base giuridica per il trattamento per dati comuni (art. 6 GDPR)** | Consenso<br>Legge<br>Contratto |
| **Base giuridica per il trattamento per dati particolari (art. 9 GDPR)** | Consenso<br>Legge |
| **Finalità del trattamento** | Istituzione ed assistenza scolastica<br>Finalità didattiche |
| **Tipo di dati personali** | Particolari (sensibili)<br>Personali<br>Nominativo Alunni |
| **Categorie di interessati** | Familiari dell'interessato<br>Studenti |
| **Categorie di destinatari** | Familiari dell'interessato<br>Persone autorizzate |
| **Informativa** | Si |
| **Profilazione** | Non necessario |
| **Dati particolari** | Si |
| **Consenso minori** | Si |
| **Frequenza trattamento** | Giornaliera |
| **Termine cancellazione dati** | I dati saranno trattati per tutto il tempo necessario allo svolgimento delle attività d'istruzione. |
| **Trasferimento dati (paesi terzi)** | Non presente |

| **Modalità di elaborazione dati: Mista - elettronica e cartacea** | |
|---|---|
| **Strumenti** | PC interno alla Struttura |
| **Strutture informatiche di archiviazione** | |
| **Server Interno della Scuola** | Struttura interna |
| Sede di riferimento | Sede Liceo Scientifico |
| Personale con diritti di accesso | |
| Software utilizzati | |

| Strutture informatiche di backup | |
|---|---|
| **Server Interno della Scuola** | Struttura interna |
| Sede di riferimento | Sede Liceo Scientifico |
| Frequenza di backup | 2 giorni |
| Tempo di storicizzazione | 21 giorni |
| Personale con diritti di accesso | |
| Note | |
| Software utilizzati | |

| VALUTAZIONE DEL LIVELLO DI RISCHIO | | |
|---|---|---|
| **PROBABILITÀ** | **CONSEGUENZE** | **LIVELLO DI RISCHIO** |
| **Poco probabile** | **Grave** | **Rilevante** |

**MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE**

- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati
- Dispositivi antincendio
- Documenti chiusi a chiave in apposito locale/armadio
- E' applicata una gestione della password degli utenti
- E' eseguita la DPIA
- I dati sono crittografati
- I documenti vengono firmati digitalmente
- I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili
- Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi
- L'impianto elettrico è certificato ed a norma
- Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee
- Registrazione e deregistrazione degli utenti
- Sistemi di allarme e di sorveglianza anti-intrusione
- Sono applicate procedure di disaster recovery che garantiscono il ripristino dell'accesso ai dati in tempi ridotti
- Sono definiti i ruoli e le responsabilità
- Sono definiti i termini di conservazione e le condizioni di impiego dei dati.
- Sono gestiti i back up
- Sono stabiliti programmi di formazione e sensibilizzazione
- Sono utilizzati software antivirus e anti intrusione
- Viene eseguita opportuna manutenzione
- Viene eseguita una regolare formazione del personale

## VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

| MISURE DI SICUREZZA | PERICOLI ASSOCIATI | LIVELLO DI ADEGUATEZZA |
|---|---|---|
| Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Dispositivi antincendio | • Agenti fisici (incendio, allagamento, attacchi esterni) | Adeguate |
| Documenti chiusi a chiave in apposito locale/armadio | | Adeguate |
| E' applicata una gestione della password degli utenti | • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)<br>• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| E' eseguita la DPIA | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| I dati sono crittografati | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| I documenti vengono firmati digitalmente | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi | • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>• Agenti fisici (incendio, allagamento, attacchi esterni) | Adeguate |
| L'impianto elettrico è certificato ed a norma | • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) | Adeguate |

| | | |
|---|---|---|
| | • Agenti fisici (incendio, allagamento, attacchi esterni) | |
| Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Registrazione e deregistrazione degli utenti | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)<br>• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) | Adeguate |
| Sistemi di allarme e di sorveglianza anti-intrusione | • Agenti fisici (incendio, allagamento, attacchi esterni)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)<br>• Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) | Adeguate |
| Sono applicate procedure di disaster recovery che garantiscono il ripristino dell'accesso ai dati in tempi ridotti | • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) | Adeguate |
| Sono definiti i ruoli e le responsabilità | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Sono definiti i termini di conservazione e le condizioni di impiego dei dati. | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)<br>• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) | Adeguate |
| Sono gestiti i back up | • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)<br>• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)<br>• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>• Agenti fisici (incendio, allagamento, attacchi esterni) | Adeguate |
| Sono stabiliti programmi di formazione e sensibilizzazione | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Sono utilizzati software antivirus e anti intrusione | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |

| | | |
|---|---|---|
| Viene eseguita opportuna manutenzione | • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) | Adeguate |
| Viene eseguita una regolare formazione del personale | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |

| PERICOLO | | |
|---|---|---|
| **Agenti fisici (incendio, allagamento, attacchi esterni)** | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Marginali | Basso |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*** | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Basso | 0,25 | Molto basso |

| PERICOLO | | |
|---|---|---|
| **Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)** | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Marginali | Basso |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*** | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Basso | 0,25 | Molto basso |

| PERICOLO | | |
|---|---|---|
| **Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)** | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*** | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,25 | Basso |

| PERICOLO | | |
|---|---|---|
| **Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)** | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*** | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,25 | Basso |

| PERICOLO | | |
|---|---|---|
| **Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)** | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Gravi | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*** | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,25 | Basso |

| PERICOLO | | |
|---|---|---|
| **Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)** | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*** | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,25 | Basso |

**A valle della DPIA l'attività risulta a rischio Basso**

## ATTIVITÀ SVOLTA ALL'INTERNO DELLA SCUOLA

| | |
|---|---|
| **Struttura** | • Sede operativa |

| **Personale coinvolto** | |
|---|---|
| **Titolare del trattamento** | Dott.ssa Monichini Lorella |
| **Persone autorizzate** | Docente (Persona Autorizzata)<br>• Comunicazione<br>• Conservazione<br>• Consultazione<br>• Raccolta<br><br>Collaboratore Scolastico (Persona Autorizzata)<br>• Comunicazione<br>• Conservazione<br>• Consultazione<br>• Raccolta |
| **Partners** | |
| **Altro** | |

| **Processo di trattamento** | |
|---|---|
| **Descrizione** | Trattamento di dati personali degli Alunni |
| **Fonte dei dati personali** | Raccolti direttamente |
| **Base giuridica per il trattamento per dati comuni (art. 6 GDPR)** | Consenso<br>Legge<br>Contratto |
| **Base giuridica per il trattamento per dati particolari (art. 9 GDPR)** | Consenso<br>Legge |
| **Finalità del trattamento** | Istituzione ed assistenza scolastica<br>Finalità didattiche |
| **Tipo di dati personali** | Particolari (sensibili)<br>Personali<br>Nominativo Alunni |
| **Categorie di interessati** | Familiari dell'interessato<br>Studenti |
| **Categorie di destinatari** | Familiari dell'interessato<br>Persone autorizzate |
| **Informativa** | Si |
| **Profilazione** | Non necessario |
| **Dati particolari** | Si |
| **Consenso minori** | Si |
| **Frequenza trattamento** | Giornaliera |
| **Termine cancellazione dati** | I dati saranno trattati per tutto il tempo necessario allo svolgimento delle attività d'istruzione. |
| **Trasferimento dati (paesi terzi)** | Non presente |

| **Modalità di elaborazione dati: Mista - elettronica e cartacea** | |
|---|---|
| **Strumenti** | Software gestionale<br>PC interno alla Struttura |

| | |
|---|---|
| **Archiviazione** | Mobile da Archivio<br>Armadio chiuso a chiave |
| **Strutture informatiche di archiviazione** | |
| **Server Interno della Scuola** | Struttura interna |
| Sede di riferimento | Sede Liceo Scientifico |
| Personale con diritti di accesso | |
| Note | |
| Software utilizzati | |
| **Strutture informatiche di backup** | |
| **Server Interno della Scuola** | Struttura interna |
| Sede di riferimento | Sede Liceo Scientifico |
| Frequenza di backup | 2 giorni |
| Tempo di storicizzazione | 21 giorni |
| Personale con diritti di accesso | |
| Note | |
| Software utilizzati | |

| **VALUTAZIONE DEL LIVELLO DI RISCHIO** | | |
|---|---|---|
| **PROBABILITÀ** | **CONSEGUENZE** | **LIVELLO DI RISCHIO** |
| **Poco probabile** | **Grave** | **Rilevante** |

**MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE**

- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati
- Dispositivi antincendio
- Documenti chiusi a chiave in apposito locale/armadio
- E' applicata una gestione della password degli utenti
- E' eseguita la DPIA
- I dati sono crittografati
- I documenti vengono firmati digitalmente
- I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili
- Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi
- L'impianto elettrico è certificato ed a norma
- Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee
- Registrazione e deregistrazione degli utenti
- Sistemi di allarme e di sorveglianza anti-intrusione
- Sono applicate procedure di disaster recovery che garantiscono il ripristino dell'accesso ai dati in tempi ridotti
- Sono definiti i ruoli e le responsabilità
- Sono definiti i termini di conservazione e le condizioni di impiego dei dati.
- Sono gestiti i back up
- Sono stabiliti programmi di formazione e sensibilizzazione
- Sono utilizzati software antivirus e anti intrusione
- Viene eseguita opportuna manutenzione
- Viene eseguita una regolare formazione del personale

# ISTITUTO ISTRUZIONE SUPERIORE SCIENTIFICO E TECNICO
# VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

| MISURE DI SICUREZZA | PERICOLI ASSOCIATI | LIVELLO DI ADEGUATEZZA |
|---|---|---|
| Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Dispositivi antincendio | • Agenti fisici (incendio, allagamento, attacchi esterni) | Adeguate |
| Documenti chiusi a chiave in apposito locale/armadio | | Adeguate |
| E' applicata una gestione della password degli utenti | • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)<br>• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| E' eseguita la DPIA | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| I dati sono crittografati | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| I documenti vengono firmati digitalmente | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi | • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>• Agenti fisici (incendio, allagamento, attacchi esterni) | Adeguate |
| L'impianto elettrico è certificato ed a norma | • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) | Adeguate |

| | | |
|---|---|---|
| | • Agenti fisici (incendio, allagamento, attacchi esterni) | |
| Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Registrazione e deregistrazione degli utenti | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)<br>• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) | Adeguate |
| Sistemi di allarme e di sorveglianza anti-intrusione | • Agenti fisici (incendio, allagamento, attacchi esterni)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)<br>• Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) | Adeguate |
| Sono applicate procedure di disaster recovery che garantiscono il ripristino dell'accesso ai dati in tempi ridotti | • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) | Adeguate |
| Sono definiti i ruoli e le responsabilità | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Sono definiti i termini di conservazione e le condizioni di impiego dei dati. | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)<br>• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) | Adeguate |
| Sono gestiti i back up | • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)<br>• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)<br>• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>• Agenti fisici (incendio, allagamento, attacchi esterni) | Adeguate |
| Sono stabiliti programmi di formazione e sensibilizzazione | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Sono utilizzati software antivirus e anti intrusione | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |

| | | |
|---|---|---|
| Viene eseguita opportuna manutenzione | • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) | Adeguate |
| Viene eseguita una regolare formazione del personale | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |

| PERICOLO | | |
|---|---|---|
| **Agenti fisici (incendio, allagamento, attacchi esterni)** | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Marginali | Basso |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*** | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Basso | 0,25 | Molto basso |

| PERICOLO | | |
|---|---|---|
| **Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)** | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Marginali | Basso |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*** | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Basso | 0,25 | Molto basso |

| PERICOLO | | |
|---|---|---|
| **Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)** | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*** | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,25 | Basso |

| PERICOLO | | |
|---|---|---|
| **Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)** | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*** | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,25 | Basso |

| PERICOLO | | |
|---|---|---|
| **Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)** | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Gravi | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*** | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,25 | Basso |

| PERICOLO | | |
|---|---|---|
| **Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)** | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Limitate | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*** | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,25 | Basso |

**A valle della DPIA l'attività risulta a rischio Basso**

# CONCLUSIONI

In conclusione si può constatare che le attività a rischio rilevante sono dovute al server interno alla Scuola sita nella struttura di Orvieto sede del Liceo Scientifico e alle criticità riscontrate nelle misure di sicurezza all'interno del sistema informatico.

Per ovviare ad eventuali criticità che si dovessero presentare, si raccomanda l'utilizzo di un protocollo sulla sicurezza informatica da predisporre a cura dei soggetti utilizzatori e/o responsabili individuati dalla Dirigente Scolastica ed allegare al presente documento.

Per quanto riguarda i soggetti autorizzati, sono state individuati dal Dirigente Scolastica tre Persone Autorizzate per Struttura, che fanno capo ai diversi Gruppi Omogenei al suo interno (es. Collaboratori Scolastici e Docenti).

Inoltre, in qualità di soggetti autorizzati, sono state nominate dal Dirigente Scolastico tutte le Persone presenti nella Segreteria didattica della sede del Liceo Scientifico.
Si allega alla presente DPIA l'elenco aggiornato per l'a.s. 2021/2022 dei dipendenti divisi per mansione.

I soggetti autorizzati individuati dalla Dirigente Scolastica, a seguito di adeguata formazione, dovranno effettuare idonea attività informativa nei confronti di tutti i soggetti facenti parte dei seguenti gruppi omogenei: Docenti, Collaboratori Scolastici e Personale di segreteria.

Resta inteso che, in caso di criticità o cambiamenti sostanziali nell'organizzazione interna dell'Istituto Scolastico, si raccomanda l'immediata comunicazione al DPO per le valutazioni del singolo caso concreto e la necessaria attività di risoluzione della problematica riscontrata.

**ISTITUTO ISTRUZIONE SUPERIORE SCIENTIFICO E TECNICO**

**VERBALE DI REDAZIONE SULL'ESITO DELLA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI**

In data odierna il Titolare del Trattamento Dati della **ISTITUTO ISTRUZIONE SUPERIORE SCIENTIFICO E TECNICO** ed in collaborazione con il del DPO, procede alla redazione del documento di valutazione di impatto sulla protezione dei dati in data 08.11.2021.

I lavoratori assunti presso l'**ISTITUTO ISTRUZIONE SUPERIORE SCIENTIFICO E TECNICO** sono stati informati e formati in relazione ai rischi relativa alla perdita di dati e alle misure di protezione adottate per proteggerli nel rispetto del Regolamento Europeo 2016/679.

Data _____

| | |
|---|---|
| Titolare del Trattamento Dati<br><br>Dott.ssa MONICHINI LORELLA | _____ |
| Data Protection Officer<br><br>Avv. MARTINI LUCA | _____ |