
# VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

*ai sensi del GDPR 2016/679 e normativa nazionale in vigore*

**Azienda/Organizzazione** **I.C. "S.G. BOSCO" - Barrafranca Ente Pubblico**

| | |
|---|---|
| **TITOLARE** | Dott.ssa Nadia Rizzo |
| **SEDE** | I.C. "S.G. DON BOSCO" -Scuola Primaria<br>Via Mazzini 62, 94012<br>Barrafranca - EN |

Data revisione: 24/01/2022

# 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:

a. 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;
b. 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;
c. 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:

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 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.

# ALGORITMO VALUTAZIONE

## 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 X 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 interessati 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

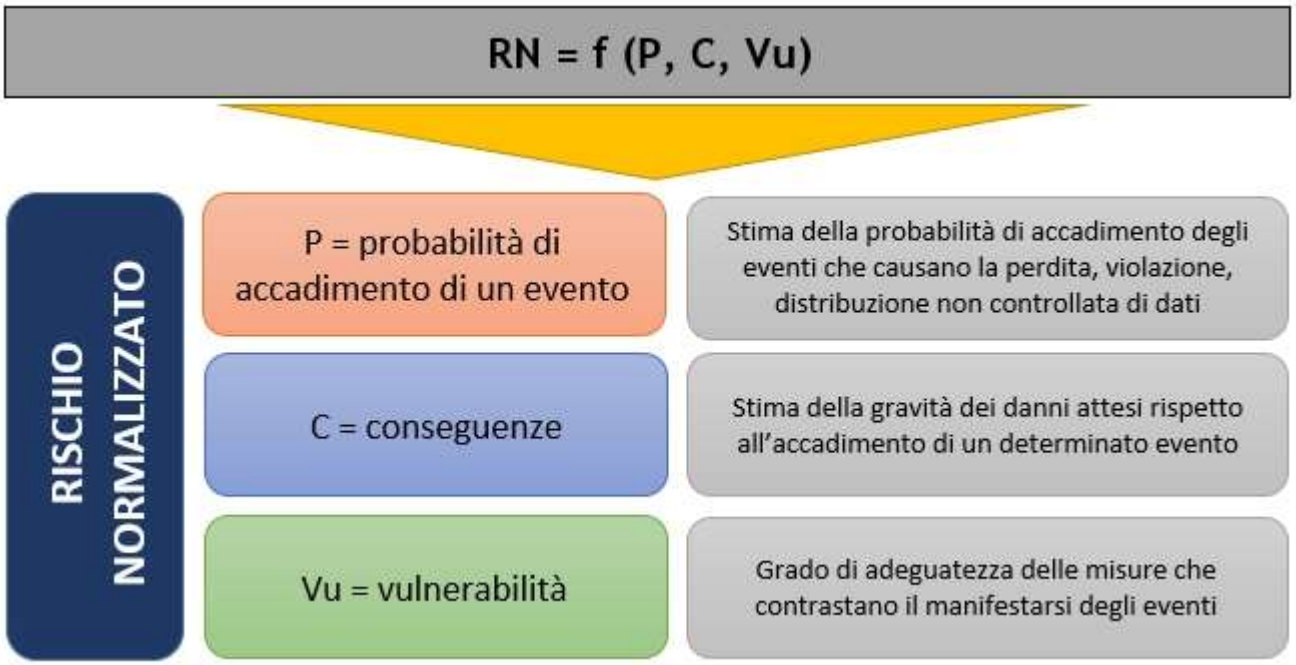
Ai sensi dell'art. 35 del GDPR, vengono individuate tutte le attività di trattamento che in prima analisi presentano un livello di rischio alto e/o prevendono due o più criteri di obbligo DPIA.
Nel caso in cui, quindi, l'indice di rischio si colloca nel range 15 ÷ 25, l'attività necessita di una valutazione 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*** ≤ 2 | 3 ≤ ***RN*** ≤ 4 | 6 ≤ ***RN*** ≤ 9 | 12 ≤ ***RN*** ≤ 16 |
| | 0,5 | 0,5 < ***RN*** ≤ *1* | 1,5 ≤ ***RN*** ≤ 2 | 3 < ***RN*** ≤ 5 | 6 ≤ ***RN*** ≤ 8 |
| | 0,25 | 0,25 ≤ ***RN*** ≤ 0,5 | 0,75 ≤ ***RN*** ≤ 1 | 1,5 ≤ ***RN*** < 3 | 3 ≤ ***RN*** ≤ 4 |
| | | 1 ≤ ***Ri*** ≤ 2 | 3 ≤ ***Ri*** ≤ 4 | 6 ≤ ***Ri*** ≤ 9 | 12 ≤ ***Ri*** ≤ 16 |
| | | Ri | | | |

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

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

## RISULTATI DPIA

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

- Scuole - registro titolare trattamento - Titolare del trattamento
- Scuole - registro responsabile trattamento - Responsabile del trattamento

## Scuole - registro titolare trattamento - Titolare del trattamento

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

| **Personale coinvolto** | |
|---|---|
| **Titolare del trattamento** | Rizzo Nadia |
| **Persone autorizzate** | Assistenti Amministrativi .<br>• Blocco<br>• Cancellazione<br>• Comunicazione<br>• Conservazione<br>• Consultazione<br>• Diffusione<br>• Distribuzione<br>• Elaborazione<br>• Interconnessione<br>• Modifica<br>• Organizzazione<br>• Raccolta<br>• Raffronto<br>• utilizzo programmi gestionali<br><br>Corso Maria Teresa, c.f. CRSMTR62L47F065O<br>• Blocco<br>• Cancellazione<br>• Comunicazione<br>• Conservazione<br>• Consultazione<br>• Diffusione<br>• Distribuzione<br>• Elaborazione<br>• Interconnessione<br>• Modifica<br>• Organizzazione<br>• Raccolta<br>• Raffronto<br>• utilizzo programmi gestionali<br><br>Corpo Docente .<br>• Blocco |

| | |
|---|---|
| | • Cancellazione<br>• Comunicazione<br>• Conservazione<br>• Consultazione<br>• Diffusione<br>• Distribuzione<br>• Elaborazione<br>• Interconnessione<br>• Modifica<br>• Organizzazione<br>• Raccolta<br>• Raffronto<br>• utilizzo registro elettronico<br><br>Faraci Angelo, c.f. FRCNGL71E23C342Y<br>• Amministrazione del sistema |
| **Partners - Responsabili esterni** | ARGO SOFTWARE S.r.l., p.iva 00838520880, nella persona di LO PRESTI LORENZO<br>• Conservazione<br><br>CODEBASE Soc. coop. A.r.l., p.iva 018495500853, nella persona di Cocca Andrea<br>• Conservazione<br><br>Lo Brutto Riccardo, c.f. LBRRCR59A13B429M<br>• Adempimenti specifici del DPO |
| **Altro** | |

| **Processo di trattamento** | |
|---|---|
| **Descrizione** | Trattamento di dati personali dei dipendenti: Docenti, Dirigenti, Tecnici ed Amministrativi. alunni e loro familiari |
| **Fonte dei dati personali** | Raccolti direttamente |
| **Base giuridica per il trattamento per dati comuni (art. 6 GDPR)** | Consenso<br>Contratto<br>Legge |
| **Base giuridica per il trattamento per dati particolari (art. 9 GDPR)** | Consenso<br>Contratto<br>Legge |
| **Finalità del trattamento** | Adempimenti connessi al versamento delle quote di iscrizione a sindacati<br>Attività extra curriculari<br>Gestione programmi gestionali, registro elettronico, archiviazione digitale<br>Pubblicazione foto e video di dipendenti<br>Pubblicazione foto e video di minori<br>Pubblicazione foto e/o video sul sito web e/o annuario scolastico<br>Igiene e sicurezza del lavoro<br>Programmazione delle attività (pianificazione e monitoraggio del lavoro)<br>Reclutamento, selezione, valutazione e monitoraggio del personale: test attitudinali<br>Istituzione ed assistenza scolastica<br>Verifica dell'idoneità al servizio<br>Contratto di assunzione<br>Relazioni con il pubblico<br>Adempimenti istituzionali obbligatori inerenti gli istituti scolastici |
| **Tipo di dati personali** | Dati sul comportamento (creazione di profili di utenti, |

| | |
|---|---|
| | consumatori, contribuenti, ecc.; profili della personalità e dei tratti caratteriali)<br>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>Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare)<br>Codice fiscale ed altri numeri di identificazione personale (carte sanitarie)<br>Adesione a sindacati o organizzazioni a carattere sindacale<br>Convinzioni filosofiche o di altro genere, adesioni ad organizzazioni a carattere filosofico<br>Convinzioni religiose, adesioni ad organizzazioni a carattere religioso<br>Origini razziali o etniche<br>Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.)<br>Giudiziari<br>Particolari (sensibili)<br>Personali |
| **Categorie di interessati** | Dipendenti<br>Collaboratori<br>Familiari dell'interessato<br>Docenti<br>Alunni |
| **Categorie di destinatari** | Soggetti che svolgono attività di archiviazione della documentazione<br>Rappresentante dei lavoratori per la sicurezza<br>Organismi paritetici in materia di lavoro<br>Organizzazioni sindacali e patronati<br>Familiari dell'interessato<br>Datore di lavoro<br>Clienti ed utenti<br>Responsabili interni<br>Associazioni ed enti locali |
| **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 del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi. |
| **Trasferimento dati (paesi terzi)** | No |
| **Autorizzazione del Garante** | Non presente |

| **Modalità di elaborazione dati: Mista - elettronica e cartacea** | |
|---|---|
| **Strumenti** | Software gestionale |
| **Strutture informatiche di archiviazione** | |
| **sistema informatico scolastico area amministrativa** | Struttura interna |
| Sede di riferimento | I.C. "S.G. DON BOSCO" -Scuola Primaria |
| Personale con diritti di accesso | Faraci Angelo, c.f. FRCNGL71E23C342Y<br>Corso Maria Teresa, c.f. CRSMTR62L47F065O |

| | |
|---|---|
| | Assistenti Amministrativi . |
| Software utilizzati | - Pacchetto Office<br>- programmi gestionali<br>- S.O. Windows varie edizioni<br>- SO Antivirus |
| **sistema informatico scolastico area didattica** | Struttura interna |
| Sede di riferimento | I.C. "S.G. DON BOSCO" -Scuola Primaria |
| Personale con diritti di accesso | Faraci Angelo, c.f. FRCNGL71E23C342Y<br>Corpo Docente . |
| Software utilizzati | - Pacchetto Office<br>- gestionale registro elettronico<br>- S.O. Windows varie edizioni<br>- SO Antivirus |
| **Strutture informatiche di backup** | |
| **sistema informatico scolastico area amministrativa** | Struttura interna |
| Sede di riferimento | I.C. "S.G. DON BOSCO" -Scuola Primaria |
| Frequenza di backup | 1 Giorni |
| Tempo di storicizzazione | 15 Giorni |
| Personale con diritti di accesso | Faraci Angelo, c.f. FRCNGL71E23C342Y<br>Corso Maria Teresa, c.f. CRSMTR62L47F065O<br>Assistenti Amministrativi . |
| Note | |
| Software utilizzati | - Pacchetto Office<br>- programmi gestionali<br>- S.O. Windows varie edizioni<br>- SO Antivirus |
| **sistema informatico scolastico area didattica** | Struttura interna |
| Sede di riferimento | I.C. "S.G. DON BOSCO" -Scuola Primaria |
| Frequenza di backup | 1 Giorni |
| Tempo di storicizzazione | 15 Giorni |
| Personale con diritti di accesso | Faraci Angelo, c.f. FRCNGL71E23C342Y<br>Corpo Docente . |
| Note | |
| Software utilizzati | - Pacchetto Office<br>- gestionale registro elettronico<br>- S.O. Windows varie edizioni<br>- SO Antivirus |

| 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<br>- Dispositivi antincendio<br>- E' applicata una gestione della password degli utenti<br>- E' applicata una procedura per la gestione degli accessi<br>- E' eseguita la DPIA<br>- E' presente una politica per la sicurezza e la protezione dei dati<br>- Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può |

assicurare la disponibilità dei dati
- 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
- Le credenziali sono disattivate in caso di perdita della qualità
- Le credenziali sono disattivate se inutilizzate per sei mesi
- Le password sono costituite da almeno otto caratteri alfanumerici
- Le password sono modificate al primo utilizzo
- Le password sono modificate ogni 3 mesi
- Le procedure sono riesaminate con cadenza predefinita
- 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 regole per la gestione delle password.
- 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 presenti istruzioni per la custodia e l'uso dei supporti rimovibili
- Sono stabiliti programmi di formazione e sensibilizzazione
- Sono utilizzati software antivirus e anti intrusione
- Viene effettuata la registrazione ed il controllo degli accessi
- 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 |
| 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' applicata una procedura per la gestione degli accessi | • 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>• 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 |
| E' presente una politica per la sicurezza e la protezione dei dati | • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)<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 |
| Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati | • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) | 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 | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, | Adeguate |

| | | |
|---|---|---|
| autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili | ecc.) | |
| 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 |
| Le credenziali sono disattivate in caso di perdita della qualità | • 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 |
| Le credenziali sono disattivate se inutilizzate per sei mesi | • 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 |
| Le password sono costituite da almeno otto caratteri alfanumerici | • 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 |
| Le password sono modificate al primo utilizzo | • Compromissione informazioni (intercettazioni, rivelazione | Adeguate |

| | | |
|---|---|---|
| | informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | |
| Le password sono modificate ogni 3 mesi | • 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.) | Parzialmente adeguate |
| Le procedure sono riesaminate con cadenza predefinita | • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| L'impianto elettrico è certificato ed a norma | • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>• Agenti fisici (incendio, allagamento, attacchi esterni) | Adeguate |
| 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) | Adeguate |

| | | |
|---|---|---|
| | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)<br>• Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) | |
| Sono applicate regole per la gestione delle password. | • 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 |
| 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) | Parzialmente adeguate |
| Sono presenti istruzioni per la custodia e l'uso dei supporti rimovibili | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)<br>• Agenti fisici (incendio, | Adeguate |

| | | |
|---|---|---|
| | allagamento, attacchi esterni) | |
| 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 effettuata la registrazione ed il controllo degli accessi | • 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 |

## VALUTAZIONE DEI RISCHI

| **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 | 0,5 | 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 | 0,5 | 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 | 0,5 | Basso |

| **PERICOLO** |
|---|
| Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) |
| **RISCHI** |

- Perdita
- Distruzione non autorizzata
- Modifica non autorizzata
- Divulgazione non autorizzata
- 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 | 0,5 | Basso |

| PERICOLO |
|---|
| Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) |
| **RISCHI** |

- Perdita
- Distruzione non autorizzata
- Modifica non autorizzata
- Divulgazione non autorizzata
- 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 | 0,5 | Basso |

| PERICOLO |
|---|
| Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) |
| **RISCHI** |

- Perdita
- Distruzione non autorizzata
- Modifica non autorizzata

| VALUTAZIONE RISCHIO INTRINSECO | | |
|---|---|---|
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Marginali | Basso |
| **VALUTAZIONE RISCHIO NORMALIZZATO** | | |

| *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 | 0,5 | Basso |

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

## Scuole - registro responsabile trattamento - Responsabile del trattamento

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

| **Personale coinvolto** | |
|---|---|
| **Responsabile del trattamento** | Corso Maria Teresa |
| **Persone autorizzate** | Assistenti Amministrativi .<br>• Blocco<br>• Cancellazione<br>• Comunicazione<br>• Conservazione<br>• Consultazione<br>• Diffusione<br>• Distribuzione<br>• Elaborazione<br>• Interconnessione<br>• Modifica<br>• Organizzazione<br>• Raccolta<br>• Raffronto<br>• utilizzo programmi gestionali<br><br>Corso Maria Teresa, c.f. CRSMTR62L47F065O<br><br>Corpo Docente .<br><br>Faraci Angelo, c.f. FRCNGL71E23C342Y<br>• Amministrazione del sistema |
| **Partners - Responsabili esterni** | ARGO SOFTWARE S.r.l., p.iva 00838520880, nella persona di LO PRESTI LORENZO<br>• Conservazione<br><br>CODEBASE Soc. coop. A.r.l., p.iva 018495500853, nella persona di Cocca Andrea<br>• Conservazione<br><br>Lo Brutto Riccardo, c.f. LBRRCR59A13B429M<br>• Adempimenti specifici del DPO |
| **Altro** | |

| **Processo di trattamento** | |
|---|---|
| **Descrizione** | Trattamento di dati personali dei dipendenti: Docenti, Dirigenti, |

| | |
|---|---|
| | Tecnici ed Amministrativi. alunni e loro familiari. |
| **Fonte dei dati personali** | Raccolti direttamente |
| **Base giuridica per il trattamento per dati comuni (art. 6 GDPR)** | Consenso<br>Contratto<br>Legge |
| **Base giuridica per il trattamento per dati particolari (art. 9 GDPR)** | Consenso<br>Contratto<br>Legge |
| **Finalità del trattamento** | Programmazione delle attività (pianificazione e monitoraggio del lavoro)<br>Adempimenti connessi al versamento delle quote di iscrizione a sindacati<br>Attività extra curriculari<br>Igiene e sicurezza del lavoro<br>Attività di previdenza<br>Istituzione ed assistenza scolastica<br>Verifica dell'idoneità al servizio<br>Contratto di assunzione<br>Relazioni con il pubblico<br>Trattamento giuridico ed economico del personale<br>Adempimenti istituzionali obbligatori inerenti gli istituti scolastici<br>Adempimento di obblighi fiscali o contabili<br>Gestione del personale |
| **Tipo di dati personali** | Dati sul comportamento (creazione di profili di utenti, consumatori, contribuenti, ecc.; profili della personalità e dei tratti caratteriali)<br>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>Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare)<br>Codice fiscale ed altri numeri di identificazione personale (carte sanitarie)<br>Adesione a sindacati o organizzazioni a carattere sindacale<br>Convinzioni filosofiche o di altro genere, adesioni ad organizzazioni a carattere filosofico<br>Convinzioni religiose, adesioni ad organizzazioni a carattere religioso<br>Origini razziali o etniche<br>Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.)<br>Giudiziari<br>Particolari (sensibili)<br>Personali |
| **Categorie di interessati** | Dipendenti<br>Collaboratori<br>Familiari dell'interessato<br>Docenti<br>Alunni |
| **Categorie di destinatari** | Soggetti che svolgono attività di archiviazione della documentazione<br>Rappresentante dei lavoratori per la sicurezza<br>Organismi paritetici in materia di lavoro<br>Organizzazioni sindacali e patronati<br>Familiari dell'interessato |

| | |
|---|---|
| | Datore di lavoro<br>Clienti ed utenti<br>Responsabili interni<br>Associazioni ed enti locali |
| **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 del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi. |
| **Trasferimento dati (paesi terzi)** | No |
| **Autorizzazione del Garante** | Non presente |

| **Modalità di elaborazione dati: Mista - elettronica e cartacea** | |
|---|---|
| **Strumenti** | Software gestionale |
| **Strutture informatiche di archiviazione** | |
| **sistema informatico scolastico area amministrativa** | Struttura interna |
| Sede di riferimento | I.C. "S.G. DON BOSCO" -Scuola Primaria |
| Personale con diritti di accesso | Faraci Angelo, c.f. FRCNGL71E23C342Y<br>Corso Maria Teresa, c.f. CRSMTR62L47F065O<br>Assistenti Amministrativi . |
| Software utilizzati | - Pacchetto Office<br>- programmi gestionali<br>- S.O. Windows varie edizioni<br>- SO Antivirus |
| **sistema informatico scolastico area didattica** | Struttura interna |
| Sede di riferimento | I.C. "S.G. DON BOSCO" -Scuola Primaria |
| Personale con diritti di accesso | Faraci Angelo, c.f. FRCNGL71E23C342Y<br>Corpo Docente . |
| Software utilizzati | - Pacchetto Office<br>- gestionale registro elettronico<br>- S.O. Windows varie edizioni<br>- SO Antivirus |
| **Strutture informatiche di backup** | |
| **sistema informatico scolastico area amministrativa** | Struttura interna |
| Sede di riferimento | I.C. "S.G. DON BOSCO" -Scuola Primaria |
| Frequenza di backup | 1 Giorni |
| Tempo di storicizzazione | 15 Giorni |
| Personale con diritti di accesso | Faraci Angelo, c.f. FRCNGL71E23C342Y<br>Corso Maria Teresa, c.f. CRSMTR62L47F065O<br>Assistenti Amministrativi . |
| Note | |
| Software utilizzati | - Pacchetto Office<br>- programmi gestionali<br>- S.O. Windows varie edizioni<br>- SO Antivirus |
| **sistema informatico scolastico area didattica** | Struttura interna |
| Sede di riferimento | I.C. "S.G. DON BOSCO" -Scuola Primaria |
| Frequenza di backup | 1 Giorni |
| Tempo di storicizzazione | 15 Giorni |

| | |
|---|---|
| Personale con diritti di accesso | Faraci Angelo, c.f. FRCNGL71E23C342Y<br>Corpo Docente . |
| Note | |
| Software utilizzati | - Pacchetto Office<br>- gestionale registro elettronico<br>- S.O. Windows varie edizioni<br>- SO Antivirus |

| 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
- E' applicata una gestione della password degli utenti
- E' applicata una procedura per la gestione degli accessi
- E' eseguita la DPIA
- E' presente una politica per la sicurezza e la protezione dei dati
- E' prevista la distruzione dei supporti rimovibili non utilizzati
- Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati
- 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
- Le credenziali sono disattivate in caso di perdita della qualità
- Le credenziali sono disattivate se inutilizzate per sei mesi
- Le password sono costituite da almeno otto caratteri alfanumerici
- Le password sono modificate al primo utilizzo
- Le password sono modificate ogni 3 mesi
- Le procedure sono riesaminate con cadenza predefinita
- 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 regole per la gestione delle password.
- 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 presenti istruzioni per la custodia e l'uso dei supporti rimovibili
- Sono stabiliti programmi di formazione e sensibilizzazione
- Sono utilizzati software antivirus e anti intrusione
- Viene effettuata la registrazione ed il controllo degli accessi
- 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 |
| 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' applicata una procedura per la gestione degli accessi | • 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>• 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 |
| E' presente una politica per | • Eventi naturali (terremoti, | Adeguate |

| | | |
|---|---|---|
| la sicurezza e la protezione dei dati | eruzioni vulcaniche, ecc.)<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.) | |
| E' prevista la distruzione dei supporti rimovibili non utilizzati | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati | • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) | 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 |
| Le credenziali sono disattivate in caso di perdita della qualità | • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)<br>• Compromissione informazioni (intercettazioni, rivelazione | Adeguate |

| | | |
|---|---|---|
| | informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | |
| Le credenziali sono disattivate se inutilizzate per sei mesi | • 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 |
| Le password sono costituite da almeno otto caratteri alfanumerici | • 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 |
| Le password sono modificate al primo utilizzo | • 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 |
| Le password sono modificate ogni 3 mesi | • 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.) | Parzialmente adeguate |
| Le procedure sono riesaminate con cadenza | • Problemi tecnici (Anomalie e malfunzionamento software, | Adeguate |

| | | |
|---|---|---|
| predefinita | problemi hardware o componenti servizio IT)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | |
| L'impianto elettrico è certificato ed a norma | • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>• Agenti fisici (incendio, allagamento, attacchi esterni) | Adeguate |
| 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 regole per la gestione delle password. | • 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 |
| Sono definiti i ruoli e le responsabilità | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, | Adeguate |

| | | |
|---|---|---|
| | ecc.) | |
| 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) | Parzialmente adeguate |
| Sono presenti istruzioni per la custodia e l'uso dei supporti rimovibili | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, 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 effettuata la registrazione ed il controllo degli accessi | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in | Adeguate |

| | | |
|---|---|---|
| | messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | |
| 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 |

## VALUTAZIONE DEI RISCHI

| **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 | 0,5 | 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 | 0,5 | 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 | 0,5 | 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 | 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 | 0,5 | 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 | 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 | 0,5 | 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 | 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 | 0,5 | Basso |

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