



## VALUTAZIONE ARCHIVI INFORMATICI

Azienda/Organizzazione

**ISTITUTO COMPRENSIVO STATALE "FILIPPO  
SURICO" AP**

**SEDE LEGALE**

MATHER CHRISTI  
VIA DELLE SPINELLE -, 74011  
CASTELLANETA - TARANTO

Data revisione: 28/04/2023

## VALUTAZIONE ARCHIVI INFORMATICI

Di seguito, è riportata la valutazione degli archivi informatici in dotazione all'organizzazione. 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:

P r o b a b i l i t à	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	$(1 \leq LR \leq 3)$
Medio - basso	$(4 \leq LR \leq 6)$
Rilevante	$(8 \leq LR \leq 12)$
Alto	$(15 \leq LR \leq 25)$

## RISULTATI

<b>Nome</b>	Server Segreteria I.C. FILIPPO SURICO
<b>Tipo Struttura</b>	Interna
<b>Sede</b>	PLESSO PASCOLI (CATELLANETA)
<b>Personale con diritti di accesso</b>	RUSSO Anna Santa, c.f. RSSNSN62R43L049T CALABRESE LUCA, c.f. CLBLCU78L27C136Q
<b>Note</b>	
<b>Software utilizzati</b>	<ul style="list-style-type: none"> <li>Axios - Software per la segreteria didattica</li> <li>Antivirus Kaspersky - Antivirus</li> <li>Titanium Backup - Software per il backup dati Server</li> <li>Axios - Software in Cloud per gestione alunni</li> <li>Axios - Software in Cloud per la Segreteria</li> </ul>

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
<ul style="list-style-type: none"> <li>Perdita</li> <li>Distruzione non autorizzata</li> </ul>		
VALUTAZIONE RISCHIO		
Probabilità	Conseguenza	Livello di rischio
Poco probabile	Marginali	Medio-basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
<ul style="list-style-type: none"> <li>Perdita</li> <li>Distruzione non autorizzata</li> <li>Modifica non autorizzata</li> <li>Divulgazione non autorizzata</li> <li>Accesso dati non autorizzato</li> </ul>		
VALUTAZIONE RISCHIO		
Probabilità	Conseguenza	Livello di rischio
Poco probabile	Marginali	Medio-basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
<ul style="list-style-type: none"> <li>Perdita</li> <li>Distruzione non autorizzata</li> <li>Modifica non autorizzata</li> </ul>		
VALUTAZIONE RISCHIO		
Probabilità	Conseguenza	Livello di rischio
Poco probabile	Marginali	Medio-basso

**MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE**

- E' applicata una gestione della password degli utenti
- E' presente una politica per la sicurezza e la protezione dei dati
- 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
- Le password sono modificate ogni 3 mesi
- Sono gestiti i back up
- Viene eseguita opportuna manutenzione

Nome	Postazione DS Prof. Luca Calabrese
Tipo Struttura	Interna
Sede	PLESSO PASCOLI (CATELLANETA)
Personale con diritti di accesso	CALABRESE LUCA, c.f. CLBLCU78L27C136Q
Note	
Software utilizzati	<ul style="list-style-type: none"> <li>• Axios - Software per la segreteria didattica</li> <li>• Antivirus Kaspersky - Antivirus</li> <li>• Titanium Backup - Software per il backup dati Server</li> <li>• Axios - Software in Cloud per gestione alunni</li> <li>• Axios - Software in Cloud per la Segreteria</li> </ul>

**PERICOLO**

Agenti fisici (incendio, allagamento, attacchi esterni)

**RISCHI**

- Perdita
- Distruzione non autorizzata

**VALUTAZIONE RISCHIO**

Probabilità	Conseguenza	Livello di rischio
Poco probabile	Marginali	Medio-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**

Probabilità	Conseguenza	Livello di rischio
Poco probabile	Marginali	Medio-basso

**PERICOLO**

Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)

RISCHI		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> </ul>		
VALUTAZIONE RISCHIO		
Probabilità	Conseguenza	Livello di rischio
Poco probabile	Marginali	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
<ul style="list-style-type: none"> <li>• E' applicata una gestione della password degli utenti</li> <li>• E' presente una politica per la sicurezza e la protezione dei dati</li> <li>• 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</li> <li>• Le password sono modificate ogni 3 mesi</li> <li>• Sono gestiti i back up</li> <li>• Viene eseguita opportuna manutenzione</li> </ul>

Nome	PC Postazione DSGA Sig.ra Russo Anna Santa
Tipo Struttura	Interna
Sede	PLESSO PASCOLI (CATELLANETA)
Personale con diritti di accesso	RUSSO Anna Santa, c.f. RSSNSN62R43L049T
Note	
Software utilizzati	<ul style="list-style-type: none"> <li>• Axios - Software per la segreteria didattica</li> <li>• Antivirus Kaspersky - Antivirus</li> <li>• Titanium Backup - Software per il backup dati Server</li> <li>• Axios - Software in Cloud per gestione alunni</li> <li>• Axios - Software in Cloud per la Segreteria</li> </ul>

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> </ul>		
VALUTAZIONE RISCHIO		
Probabilità	Conseguenza	Livello di rischio
Poco probabile	Marginali	Medio-basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> <li>• Divulgazione non autorizzata</li> </ul>		

<ul style="list-style-type: none"> <li>• Accesso dati non autorizzato</li> </ul>		
<b>VALUTAZIONE RISCHIO</b>		
<b>Probabilità</b>	<b>Conseguenza</b>	<b>Livello di rischio</b>
Poco probabile	Marginali	Medio-basso

<b>PERICOLO</b>		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
<b>RISCHI</b>		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> </ul>		
<b>VALUTAZIONE RISCHIO</b>		
<b>Probabilità</b>	<b>Conseguenza</b>	<b>Livello di rischio</b>
Poco probabile	Marginali	Medio-basso

<b>MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE</b>
<ul style="list-style-type: none"> <li>• E' applicata una gestione della password degli utenti</li> <li>• E' presente una politica per la sicurezza e la protezione dei dati</li> <li>• 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</li> <li>• Le password sono modificate ogni 3 mesi</li> <li>• Sono gestiti i back up</li> <li>• Viene eseguita opportuna manutenzione</li> </ul>

<b>Nome</b>	PC Postazione Assistente Amministrativo Matarrese Angela
Tipo Struttura	Interna
Sede	PLESSO PASCOLI (CATELLANETA)
Personale con diritti di accesso	MATARRESE ANGELA, c.f. MTRNGL83P48H096I
Note	
Software utilizzati	<ul style="list-style-type: none"> <li>• Axios - Software per la segreteria didattica</li> <li>• Antivirus Kaspersky - Antivirus</li> <li>• Titanium Backup - Software per il backup dati Server</li> <li>• Axios - Software in Cloud per gestione alunni</li> <li>• Axios - Software in Cloud per la Segreteria</li> </ul>

<b>PERICOLO</b>		
Agenti fisici (incendio, allagamento, attacchi esterni)		
<b>RISCHI</b>		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> </ul>		
<b>VALUTAZIONE RISCHIO</b>		
<b>Probabilità</b>	<b>Conseguenza</b>	<b>Livello di rischio</b>
Poco probabile	Marginali	Medio-basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> <li>• Divulgazione non autorizzata</li> <li>• Accesso dati non autorizzato</li> </ul>		
VALUTAZIONE RISCHIO		
Probabilità	Conseguenza	Livello di rischio
Poco probabile	Marginali	Medio-basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> </ul>		
VALUTAZIONE RISCHIO		
Probabilità	Conseguenza	Livello di rischio
Poco probabile	Marginali	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
<ul style="list-style-type: none"> <li>• E' applicata una gestione della password degli utenti</li> <li>• E' presente una politica per la sicurezza e la protezione dei dati</li> <li>• 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</li> <li>• Le password sono modificate ogni 3 mesi</li> <li>• Sono gestiti i back up</li> <li>• Viene eseguita opportuna manutenzione</li> </ul>

Nome	PC Postazione Assistente Amministrativo Rocci Antonella
Tipo Struttura	Interna
Sede	PLESSO PASCOLI (CATELLANETA)
Personale con diritti di accesso	ROCCI ANTONIA, c.f. RCCNTN70T59F784V
Note	
Software utilizzati	<ul style="list-style-type: none"> <li>• Axios - Software per la segreteria didattica</li> <li>• Antivirus Kaspersky - Antivirus</li> <li>• Titanium Backup - Software per il backup dati Server</li> <li>• Axios - Software in Cloud per gestione alunni</li> <li>• Axios - Software in Cloud per la Segreteria</li> </ul>

PERICOLO
----------

<b>Agenti fisici (incendio, allagamento, attacchi esterni)</b>		
<b>RISCHI</b>		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> </ul>		
<b>VALUTAZIONE RISCHIO</b>		
<b>Probabilità</b>	<b>Conseguenza</b>	<b>Livello di rischio</b>
Poco probabile	Marginali	Medio-basso

<b>PERICOLO</b>		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
<b>RISCHI</b>		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> <li>• Divulgazione non autorizzata</li> <li>• Accesso dati non autorizzato</li> </ul>		
<b>VALUTAZIONE RISCHIO</b>		
<b>Probabilità</b>	<b>Conseguenza</b>	<b>Livello di rischio</b>
Poco probabile	Marginali	Medio-basso

<b>PERICOLO</b>		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
<b>RISCHI</b>		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> </ul>		
<b>VALUTAZIONE RISCHIO</b>		
<b>Probabilità</b>	<b>Conseguenza</b>	<b>Livello di rischio</b>
Poco probabile	Marginali	Medio-basso

<b>MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE</b>	
<ul style="list-style-type: none"> <li>• E' applicata una gestione della password degli utenti</li> <li>• E' presente una politica per la sicurezza e la protezione dei dati</li> <li>• 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</li> <li>• Le password sono modificate ogni 3 mesi</li> <li>• Sono gestiti i back up</li> <li>• Viene eseguita opportuna manutenzione</li> </ul>	

<b>Nome</b>	PC Postazione Assistente Amministrativo Speranza Ester
<b>Tipo Struttura</b>	Interna
<b>Sede</b>	PLESSO PASCOLI (CATELLANETA)
<b>Personale con diritti di accesso</b>	SPERANZA ESTER, c.f. SPRSTR65R57B157B
<b>Note</b>	
<b>Software utilizzati</b>	<ul style="list-style-type: none"> <li>• Axios - Software per la segreteria didattica</li> </ul>

	<ul style="list-style-type: none"> <li>• Antivirus Kaspersky - Antivirus</li> <li>• Titanium Backup - Software per il backup dati Server</li> <li>• Axios - Software in Cloud per gestione alunni</li> <li>• Axios - Software in Cloud per la Segreteria</li> </ul>
--	---

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> </ul>		
VALUTAZIONE RISCHIO		
Probabilità	Conseguenza	Livello di rischio
Poco probabile	Marginali	Medio-basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> <li>• Divulgazione non autorizzata</li> <li>• Accesso dati non autorizzato</li> </ul>		
VALUTAZIONE RISCHIO		
Probabilità	Conseguenza	Livello di rischio
Poco probabile	Marginali	Medio-basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> </ul>		
VALUTAZIONE RISCHIO		
Probabilità	Conseguenza	Livello di rischio
Poco probabile	Marginali	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
<ul style="list-style-type: none"> <li>• E' applicata una gestione della password degli utenti</li> <li>• E' presente una politica per la sicurezza e la protezione dei dati</li> <li>• 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</li> <li>• Le password sono modificate ogni 3 mesi</li> <li>• Sono gestiti i back up</li> <li>• Viene eseguita opportuna manutenzione</li> </ul>

	PC Postazione Assistente Amministrativo Rodia
--	---

<b>Nome</b>	<b>Annamaria</b>
<b>Tipo Struttura</b>	Interna
<b>Sede</b>	PLESSO PASCOLI (CATELLANETA)
<b>Personale con diritti di accesso</b>	RODIA ANNAMARIA, c.f. RDONMR58E71B808Q
<b>Note</b>	
<b>Software utilizzati</b>	<ul style="list-style-type: none"> <li>• Axios - Software per la segreteria didattica</li> <li>• Antivirus Kaspersky - Antivirus</li> <li>• Titanium Backup - Software per il backup dati Server</li> <li>• Axios - Software in Cloud per gestione alunni</li> <li>• Axios - Software in Cloud per la Segreteria</li> </ul>

<b>PERICOLO</b>		
Agenti fisici (incendio, allagamento, attacchi esterni)		
<b>RISCHI</b>		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> </ul>		
<b>VALUTAZIONE RISCHIO</b>		
<b>Probabilità</b>	<b>Conseguenza</b>	<b>Livello di rischio</b>
Poco probabile	Marginali	Medio-basso

<b>PERICOLO</b>		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
<b>RISCHI</b>		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> <li>• Divulgazione non autorizzata</li> <li>• Accesso dati non autorizzato</li> </ul>		
<b>VALUTAZIONE RISCHIO</b>		
<b>Probabilità</b>	<b>Conseguenza</b>	<b>Livello di rischio</b>
Poco probabile	Marginali	Medio-basso

<b>PERICOLO</b>		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
<b>RISCHI</b>		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> </ul>		
<b>VALUTAZIONE RISCHIO</b>		
<b>Probabilità</b>	<b>Conseguenza</b>	<b>Livello di rischio</b>
Poco probabile	Marginali	Medio-basso

<b>MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE</b>		
<ul style="list-style-type: none"> <li>• E' applicata una gestione della password degli utenti</li> <li>• E' presente una politica per la sicurezza e la protezione dei dati</li> </ul>		

- 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
- Le password sono modificate ogni 3 mesi
- Sono gestiti i back up
- Viene eseguita opportuna manutenzione