



## VALUTAZIONE ARCHIVI INFORMATICI

Azienda/Organizzazione **ISTITUTO COMPRENSIVO STATALE FALCOMATA' -  
ARCHI**

<b>SEDE LEGALE</b>	ISTITUTO COMPRENSIVO STATALE FALCOMATA' - ARCHI Via Montello 7, 89122 - Reggio Calabria
--------------------	---

Data revisione: 01/09/2022

## 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 ≤ LR ≤ 3)
Medio - basso	(4 ≤ LR ≤ 6)
Rilevante	(8 ≤ LR ≤ 12)
Alto	(15 ≤ LR ≤ 25)

## RISULTATI

<b>Nome</b>	<b>ARCHIVIO INFORMATICO - ISTITUTO COMPRENSIVO STATALE FALCOMATA' - ARCHI</b>
<b>Tipo Struttura</b>	Interna
<b>Sede</b>	ISTITUTO COMPRENSIVO STATALE FALCOMATA' - ARCHI Via Montello 7, 89125 - Reggio Calabria
<b>Personale con diritti di accesso</b>	<p>CORRADO SERAFINA (DIRIGENTE)  NERI VALERIA (DSGA)  BOMBARDIERE PASQUALE (ASS.AMM.)  CUTRUPI FRANCESCA, (ASS.AMM.)  MALARA GIUSEPPE (ASS.AMM.)  MARRA ERNESTA (ASS.AMM.)  NAPOLI ADRIANA (ASS.AMM.)  SPINELLA ANGELA CARMELA (ASS.AMM.)  ZIRILLI CARMELA STEFANIA (ASS.AMM.)  TOSCANO CARMEN (1° COLLABORATORE DS)  ARCONTE MARIA FILIPPA (2° COLLABORATORE DS)  ALBANO ROSARIA CARMELA (COORD. DID. PLESSO)  CAPPELLACCIO PATRIZIA (COORD. DID. PLESSO)  CALARCO MILENA (COORD. DID. PLESSO)  LA FACE FRANCESCA (COORD. DID. PLESSO)  MARRA ANTONIETTA ROSA (COORD. DID. PLESSO)  MUSOLINO ROSSANA (COORD. DID. PLESSO)  PANSERA MARIA (COORD. DID. PLESSO)  SORGONA' GEMMA LUCIA (COORD. DID. PLESSO)  CARIDI BARBARA (REFERENTE REGISTRO ELETTRONICO)  COTRONEO CATERINA GIOVANNA (ANIMATORE DIGITALE)  DI STEFANO ERNESTA TERESA (FUNZIONE STRUMENTALE)  LO SCHIAVO RITA (FUNZIONE STRUMENTALE)  MALASPINA MAURIZIO (FUNZIONE STRUMENTALE)  QUATTRONE GIOVANNI (FUNZIONE STRUMENTALE)  ZANGARI FRANCESCA (FUNZIONE STRUMENTALE)  SETTIMIO SAVERIO MARIA (AMMINISTRATORE DI SISTEMA)</p>

Note	Personale con diritto di accesso: DOCENTI CON NOMINA DI INCARICO DI CUI SI ALLEGA ELENCO AL REGISTRO
Software utilizzati	Software Gestionale - File Excel Server Cloud Certificati Utilizzati: Axios Cloud - Sidi Miur

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
Probabile	Gravissime	Alto

PERICOLO		
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)		
RISCHI		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> </ul>		
VALUTAZIONE RISCHIO		
Probabilità	Conseguenza	Livello di rischio
Probabile	Gravissime	Alto

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
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
Probabile	Limitate	Rilevante

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
Probabile	Limitate	Rilevante

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
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	Gravissime	Rilevante

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
Probabile	Gravi	Rilevante

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
<ul style="list-style-type: none"> <li>• Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati</li> <li>• Dispositivi antincendio</li> <li>• E' applicata una gestione della password degli utenti</li> <li>• E' applicata una procedura per la gestione degli accessi</li> <li>• E' eseguita la DPIA</li> <li>• E' presenta una politica per la sicurezza e la protezione dei dati</li> <li>• Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati</li> <li>• Esistono procedure per l'individuazione del custode delle password</li> <li>• Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi</li> <li>• Le password sono costituite da almeno otto caratteri alfanumerici</li> <li>• Le password sono modificate al primo utilizzo</li> <li>• Le password sono modificate ogni 3 mesi</li> <li>• Le procedure sono riesaminate con cadenza predefinita</li> <li>• L'impianto elettrico è certificato ed a norma</li> <li>• Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee</li> <li>• Sistemi di allarme e di sorveglianza anti-intrusione</li> <li>• Sono applicate regole per la gestione delle password.</li> <li>• Sono definiti i ruoli e le responsabilità</li> <li>• Sono definiti i termini di conservazione e le condizioni di impiego dei dati.</li> <li>• Sono gestiti i back up</li> </ul>

- 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