VALUTAZIONE ARCHIVI INFORMATICI

Organizzazione **Istituto Comprensivo "G. Fanciulli" - Arrone**

SEDE LEGALE	Sede Centrale Via Matteotti 3/A, 05031 Arrone - TR

Data revisione: 07/09/2018

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 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)*

RISULTATI

Nome	Server
Tipo Struttura	Interna
Sede	Sede Centrale (Arrone)
Personale con diritti di accesso	Canolla Fabrizio, c.f. CNLFRZ71P24I921T Ridolfi Agusto, c.f. RDLGST57H29D538U Benedetti Guido, c.f. BNDGDU74C05H282N Trotti Franca, c.f TRTFNC64L52D538N Piazza Maria Lucilla, c.f. PZZMLC63T53L117M
Note	
Software utilizzati	• Nuvola

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Gravi	Rilevante

PERICOLO		
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Probabile	Gravi	Rilevante

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
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**
Probabile	Marginali	Medio-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		
Probabilità	**Conseguenza**	**Livello di rischio**
Probabile	Gravi	Rilevante

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		
Probabilità	**Conseguenza**	**Livello di rischio**
Probabile	Gravi	Rilevante

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' presenta una politica per la sicurezza e la protezione dei dati
- 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
- 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 password sono modificate ogni 3 mesi
- Le password sono costituite da almeno otto caratteri alfanumerici
- L'impianto elettrico è certificato ed a norma

- Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee
- Sistemi di allarme e di sorveglianza anti-intrusione
- Sono definiti i ruoli e le responsabilità
- 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