Sistema gestionale
Trattamento Dati Personali

VALUTAZIONE ARCHIVI INFORMATICI

Azienda/Organizzazione **Liceo Statale "M.L.King"- Favara Ente Pubblico**

SEDE LEGALE	plesso centrale Via P.Nenni 136, 92026 Favara - AG

Data revisione: 19/11/2021

GDPR

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:

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	$(1 \leq LR \leq 3)$
Medio - basso	$(4 \leq LR \leq 6)$
Rilevante	$(8 \leq LR \leq 12)$
Alto	$(15 \leq LR \leq 25)$

RISULTATI

Nome	**sistema informatico scolastico area amministrativa**
Tipo Struttura	Interna
Sede	plesso centrale (Favara)
Personale con diritti di accesso	Scrivano Valerio, c.f. SCRVLR72A13G812T Messana Antonio, c.f. MSSNTN69B12D514O Assistenti Amministrativi .
Note	
Software utilizzati	• Pacchetto Office • programmi gestionali • S.O. Windows varie edizioni • SO Antivirus

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		
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**
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
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**
Poco probabile	Marginali	Medio-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		
Probabilità	**Conseguenza**	**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 procedura per la gestione degli accessi • E' eseguita la DPIA • E' applicata una gestione della password degli utenti • 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 costituite da almeno otto caratteri alfanumerici • Le password sono modificate al primo utilizzo • Le password sono modificate ogni 3 mesi • Viene eseguita una regolare formazione del personale • Viene eseguita opportuna manutenzione • Sono utilizzati software antivirus e anti intrusione • Sono stabiliti programmi di formazione e sensibilizzazione • Sono gestiti i back up • Sono definiti i ruoli e le responsabilità • Sono applicate regole per la gestione delle password. • Registrazione e deregistrazione degli utenti • Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee • Le procedure sono riesaminate con cadenza predefinita

Nome	**sistema informatico scolastico area didattica**
Tipo Struttura	Interna
Sede	plesso centrale (Favara)
Personale con diritti di accesso	Scrivano Valerio, c.f. SCRVLR72A13G812T Messana Antonio, c.f. MSSNTN69B12D514O Corpo Docente .
Note	
Software utilizzati	• gestionale registro elettronico • Pacchetto Office • S.O. Windows varie edizioni • SO Antivirus

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		
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**
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
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
Poco probabile	Marginali	Medio-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

Probabilità	Conseguenza	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 • 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 password sono costituite da almeno otto caratteri alfanumerici • Le password sono modificate al primo utilizzo • Le password sono modificate ogni 3 mesi • L'impianto elettrico è certificato ed a norma • Le procedure sono riesaminate con cadenza predefinita • Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee • Registrazione e deregistrazione degli utenti • Viene eseguita una regolare formazione del personale • Viene eseguita opportuna manutenzione • Viene effettuata la registrazione ed il controllo degli accessi • Sono stabiliti programmi di formazione e sensibilizzazione

- Sono utilizzati software antivirus e anti intrusione
- Sono gestiti i back up
- Sono definiti i ruoli e le responsabilità
- Sono applicate regole per la gestione delle password.

LA DIRIGENTE SCOLASTICA
Prof.ssa [illegible]