VALUTAZIONE ARCHIVI INFORMATICI

Azienda/Organizzazione	**COOPERATIVA SOCIALE SEMI DI SENAPE**

SEDE LEGALE	SEDE OPERATIVA 1 PIAZZA DON ANGELO CAMPORA 72/B, 15121 ALESSANDRIA - AL

Data revisione: 15/04/2019

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	ARCHIVIO VIRTUALE
Tipo Struttura	Esterna
Azienda	MEGADROPBOX
Personale con diritti di accesso	BRAMERI TRISTANA, c.f. BRMTST82E65A182R BRIANNI ELISA, c.f. BRNLSE82M61A182S VOLPI GIULIA, c.f. VLPGLI78H67A182Q
Note	
Software utilizzati	• OFFICE • WINDOWS

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		
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)		
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

- Adozione di cifratura e anonimizzazione dei dati su stato di salute e vita sessuale
- 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
- I dati sono crittografati
- 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
- Sono applicate procedure di disaster recovery che garantiscono il ripristino dell'accesso ai dati in tempi ridotti
- 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 stabiliti programmi di formazione e sensibilizzazione
- Sono utilizzati software antivirus e anti intrusione
- E' presenta una politica per la sicurezza e la protezione dei dati
- Esistono procedure per l'individuazione del custode delle password

Nome	**HD INTERNO AL PC**
Tipo Struttura	Interna
Sede	SEDE OPERATIVA 1 (ALESSANDRIA)
Personale con diritti di accesso	BRAMERI TRISTANA, c.f. BRMTST82E65A182R BRIANNI ELISA, c.f. BRNLSE82M61A182S VOLPI GIULIA, c.f. VLPGLI78H67A182Q
Note	
Software utilizzati	• SOFTWARE GESTIONALE • WINDOWS • OFFICE

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**
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
• Dispositivi antincendio • E' applicata una gestione della password degli utenti • E' applicata una procedura per la gestione degli accessi • E' presenta una politica per la sicurezza e la protezione dei dati • I dati sono crittografati • 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

- 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 gestiti i back up
- Sono definiti i ruoli e le responsabilità
- Viene eseguita opportuna manutenzione
- Viene eseguita una regolare formazione del personale
- Sono utilizzati software antivirus e anti intrusione