VALUTAZIONE ARCHIVI INFORMATICI

Azienda/Organizzazione

ORDINE DEI GEOLOGI DELLA CALABRIA

Ordine dei Geologi della Calabria

SEDE LEGALE	Sede Operativa Via Federico Bisceglia 4, 88100 Catanzaro - Cz

Data revisione: 25/01/2022

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 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 Aziendale
Tipo Struttura	Interna
Sede	Sede Operativa (Catanzaro)
Personale con diritti di accesso	Mazzarella Angela Giuseppina, c.f. MZZNLG66C59A155D Valente Valentina, c.f. VLNVNT81M51C352H
Note	
Software utilizzati	

PERICOLO		
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	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	Limitate	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**
Poco probabile	Limitate	Medio-basso

PERICOLO
Agenti fisici (incendio, allagamento, attacchi esterni)
RISCHI
• Perdita

• Distruzione non autorizzata

VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	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**
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	Limitate	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 • 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 password sono costituite da almeno otto caratteri alfanumerici • 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 definiti i termini di conservazione e le condizioni di impiego dei dati. • Sono eseguiti gli aggiornamenti di sicurezza del sistema operativo • Sono gestiti i back up • Sono utilizzati software antivirus e anti intrusione • Viene eseguita opportuna manutenzione • Viene eseguita una regolare formazione del personale

- Configurata la modalità di blocco automatico quando ci si allontani dalla postazione di lavoro

Nome	**PC Aziendali**
Tipo Struttura	Interna
Sede	Sede Operativa (Catanzaro)
Personale con diritti di accesso	Mazzarella Angela Giuseppina, c.f. MZZNLG66C59A155D Valente Valentina, c.f. VLNVNT81M51C352H
Note	
Software utilizzati	• Contabilità • Gestionale

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	Limitate	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	Limitate	Medio-basso

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Improbabile	Limitate	Accettabile

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati
- Dispositivi antincendio
- 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 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 eseguiti gli aggiornamenti di sicurezza del sistema operativo
- Sono gestiti i back up
- Sono utilizzati software antivirus e anti intrusione
- Viene eseguita opportuna manutenzione
- Viene eseguita una regolare formazione del personale

Nome	**NAS INTERNO**
Tipo Struttura	Interna
Sede	Sede Operativa (Catanzaro)
Personale con diritti di accesso	Mazzarella Angela Giuseppina, c.f. MZZNLG66C59A155D Valente Valentina, c.f. VLNVNT81M51C352H
Note	Backup effettuati ogni giorno . Previsti anche backup settimanali e mensili.
Software utilizzati	

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**
Poco 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**
Improbabile	Gravi	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	Gravi	Rilevante

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
• Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati • Dispositivi antincendio • 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 eseguiti gli aggiornamenti di sicurezza del sistema operativo • Sono gestiti i back up • Sono utilizzati software antivirus e anti intrusione • Viene eseguita opportuna manutenzione • Viene eseguita una regolare formazione del personale • E' applicata una gestione della password degli utenti