MISURE DI SICUREZZA

AM.I.CO. DI CONCA & C. SAS
VIALE GUGLIEMO MARCONI 161
09131 CAGLIARI
P.IVA 02682410929

SOMMARIO

1. ANALISI DEI RISCHI

Si è provveduto ad analizzare, coerentemente con quanto indicato nell' art.32 del nuovo regolamento europeo 679/2016, i principali eventi potenzialmente dannosi per la sicurezza dei dati.
L'analisi dei rischi ha l'obiettivo finale di individuare un insieme di misure di protezione, commisurate alle reali necessità di sicurezza, da adottare nell'ambito del perimetro d'intervento, ovvero, dell'area di analisi. Le necessità di sicurezza vengono valutate in relazione alle minacce cui è sottoposto il sistema informativo oggetto dell'analisi. La conoscenza di tali minacce è essenziale nell'iter metodologico per l'individuazione e la progettazione delle misure di protezione che possono concretizzarsi in meccanismi di natura logica, di natura fisica.

Metodologicamente si è proceduto ad individuare i principali eventi potenzialmente dannosi per la sicurezza dei dati, e valutate le possibili conseguenze e la gravità in relazione al contesto fisico-ambientale di riferimento e agli strumenti elettronici utilizzati.

Sono individuati ed elencati gli eventi che possono generare danni e che comportano, quindi, rischi per la sicurezza dei dati personali effettuando una suddivisione per rischi gravanti su:
- operatori presenti,
- strumenti utilizzati, sia di tipo elettronico sia di tipo non elettronico,
- contesto fisico ed ambientale nel quale attualmente operiamo.

Per ogni categoria di rischio si è stimata la probabilità che esso si manifesti (Alta, Media, Bassa) e identificate le possibili conseguenze (gravità) per la sicurezza dei dati derivabili dal verificarsi dello stesso (Alto, Medio e Basso).

		Gravità (GR)		
		Basso	***Medio***	***Alto***
Probabilità (PR)	***Alta***	3	6	9
	Media	2	4	6
	Bassa	1	2	3

Dal prodotto "impatto" x "probabilità" viene ricavato una matrice da cui ricavare un Indice di Rischio (IR) per mezzo del quale si potranno distinguere rischi:
- rischi ad alta priorità (IR=9);
- rischi a media priorità (4≤IR≤6);
- rischi a bassa priorità (3≤IR≤1).

La metodologia applicata implica che per i rischi con alta priorità siano definite ed attuate misure di protezione ulteriori rispetto a quelle previste nelle normali operazioni di trattamento dati.

Eventi	Impatto sulla sicurezza dei dati				Rif. misure d'azione
	Descrizione	PR	GR	IR	
Comportamenti operatori					
Sottrazione di credenziali di autenticazione	Fa riferimento al caso in cui le credenziali di autenticazione siano acquisite e utilizzate indebitamente da terzi. Ciò consente l'accesso non autorizzato ai dati e espone a rischi ulteriori (come il danneggiamento), se si aggiungono altri eventi.	B	B	1	MIS01
Carenza di consapevolezza, disattenzione o incuria	Fa riferimento al caso in cui, a causa di un utilizzo disattento degli strumenti, i dati vengano alterati o corrotti in modo irrecuperabile, ovvero vengano cancellati.	B	B	1	MIS01
Comportamenti sleali o fraudolenti	Fa riferimento alla possibilità di sfruttare, nell'ottica di un comportamento sleale o fraudolento, eventuali debolezze - scoperte in modo fortuito e non - nel sistema di sicurezza dei programmi o della rete. Questo può portare non solo all'accesso non autorizzato ai dati, ma anche ad un danneggiamento dei dati stessi.	B	B	1	MIS02
Errore materiale	Fa riferimento al caso in cui, a causa di un errore commesso in modo inconsapevole durante l'utilizzo di software o di apparecchiature elettroniche, i dati vengano danneggiati, corrotti o cancellati.	B	B	1	MIS02
Eventi relativi agli strumenti					
Azione di virus informatici o di programmi suscettibili di recare danno	Fa riferimento all'effetto di virus informatici programmati per cancellare i dati a cui l'utente ha accesso e comunque danneggiarli, ovvero per causare la paralisi di servizi informatici che possono risultare in una indisponibilità temporanea dei dati. L'azione di questi agenti dannosi è generalmente innescata dallo scaricamento di programmi eseguibili di varia natura che vengono diffusi per posta elettronica sotto forma di allegati, oppure provengono da siti che, ingannando l'utente, lo inducono a salvare questi file sulla propria postazione.	B	B	1	MIS03
Spamming o tecniche di sabotaggio	Fa riferimento ad azioni di sabotaggio compiute da terzi tramite programmi appositi che, sfruttando difetti del software utilizzato per la gestione della posta elettronica o altri servizi informatici, saturano il servizio stesso di richieste fino alla paralisi parziale o totale. Questa azione risulta nella indisponibilità temporanea dei dati gestiti dal servizio che viene attaccato.	B	B	1	MIS03
Malfunzionamento, indisponibilità o degrado degli strumenti	Fa riferimento alla possibilità, insita in ogni software, di rivelare difetti di funzionamento inizialmente non presenti o non evidenti. Tale possibilità esiste sempre in quanto ogni software dipende da altri prodotti software (primo fra tutti il sistema operativo) e hardware (le apparecchiature di rete) che possono dover essere sostituiti o aggiornati nel tempo con altri di caratteristiche differenti. Il risultato di tale evento può essere l'indisponibilità temporanea o addirittura persistente di dati nel caso più grave, in cui cioè non sia più possibile ristabilire la situazione originaria.	B	B	1	MIS03
Accessi esterni non autorizzati	Fa riferimento al caso in cui dall'esterno vi siano intrusioni via rete, avvenute senza furto di credenziali e non dovute a semplice comportamento sleale, ma semplicemente dovute allo sfruttamento di difetti del software, per effettuare accessi non autorizzati ai dati.	M	M	4	MIS03
Intercettazione di informazioni di rete	Fa riferimento a un'operazione volontaria che si basa sull'analisi e sul filtraggio dei pacchetti dati in transito sulla rete, generalmente con l'ausilio di software apposito. Il rischio è di accesso non autorizzato ai dati.	M	M	4	MIS03
Elementi relativi al contesto					
Accessi non autorizzati a locali/reparti ad accesso ristretto	Fa riferimento alla possibilità di accedere fisicamente a locali o reparti il cui accesso sia limitato ai soli impiegati della struttura. Il rischio è quello di accesso non autorizzato ai dati	B	B	1	MIS04
Sottrazione di strumenti contenenti dati	Fa riferimento al rischio di furto di una intera postazione di lavoro o di un server, con relativa perdita dei dati in esso contenuti. Il rischio correlato è quello di accesso non autorizzato ai dati, nonché di perdita degli stessi.	B	B	1	MIS05
Eventi distruttivi, naturali o artificiali, nonché dolosi, accidentali o	Include tutti gli eventi di effetto distruttivo sui supporti fisici contenenti i dati o sulle apparecchiature, indipendentemente dalla loro natura, qualora non siano già inclusi nelle casistiche precedenti. Il rischio risultante sui dati è quello di Danneggiamento, indisponibilità temporanea o perdita parziale o totale.	B	B	1	MIS05
Guasto ai sistemi complementari	Si riferisce a tutti quegli eventi che, avendo impatto sui sistemi esterni e complementari agli strumenti informatici, ne inficiano la funzionalità. Ciò include impianto elettrico, climatizzazione, ecc. Il rischio correlato è quello di danneggiamento dei dati, e di indisponibilità temporanea.	B	B	1	MIS05

Errori umani nella gestione della sicurezza fisica	Si riferisce a ogni evento causato da errore umano nella gestione della sicurezza sugli ambienti fisici. In questa categoria ricadono porte o serrature lasciate erroneamente aperte, protezioni fisiche male installate, eccetera. Il rischio correlato va da quello di accesso non autorizzato ai dati nei casi meno gravi, fino a quello di perdita dei dati per i casi più gravi.	B	B	1	MIS05

2. ANALISI DELLE MISURE

Coerentemente con quanto previsto dall'Art. 32 del Nuovo Regolamento Europeo 679/2016, ed in base all'analisi dei rischi effettuata, all'interno si è provveduto a mettere in atto idonee misure a contrastare i rischi individuati.

2.1. Trattamenti automatizzati

I dati personali oggetto di trattamento devono essere custoditi e controllati durante tutto il loro ciclo di vita, dalla raccolta alla distruzione ed in qualunque altra operazione.
Tali principi di "custodia" e "controllo" sono impostati in relazione alla natura dei dati, ma anche in funzione delle caratteristiche del trattamento, ossia delle modalità con cui esso viene svolto. Il fine della custodia e del controllo è la riduzione di specifici rischi che incombono sui dati, mediante l'adozione di idonee misure di sicurezza. Pertanto, il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate le misure Idonee.
Il suddetto condominio non dispone di una propria struttura IT ma opera attraverso lo studio AM.I.CO. DI CONCA & C. SAS di cui il Sig. Conca Davide e stato eletto nostro amministratore. Le voci sotto elencare sono riportate in base a quanto riferito dallo studio che gestisce le nostre informazioni

2.2. Identificazione ed autenticazione

Si è stabilito l'adozione di un meccanismo di identificazione ed autenticazione degli utenti che accedono ai dati proprio al fine di garantire che l'identità dichiarata da un utente al momento in cui accede ad un sistema venga verificata e conseguentemente autenticata.
A tal fine ogni utente è riconosciuto dal sistema sulla base di un codice identificativo personale univoco (user id) a cui è associato una password.
Relativamente alla user id vengono adottate le seguenti misure:

- assegnazione agli utenti di una user id univoca che non può essere attribuita a soggetti diversi neppure in tempi diversi;
- disattivazione delle user id in caso di mancato utilizzo dell'utenza per un periodo superiore a sei mesi;
- disattivazione delle user id attribuite agli utenti a cui è stata revocata l'autorizzazione di accesso ai dati.

Inoltre, viene assegnata ad ogni utente una password per la cui gestione sono state previste specifiche disposizioni che prendono in considerazione tutti gli aspetti che ne caratterizzano l'efficacia:

- cambio obbligatorio della password di default alla prima connessione;
- lunghezza di almeno 8 caratteri con l'utilizzo di caratteri alfanumerici e speciali;
- cambio almeno ogni 90 giorni o immediatamente nei casi in cui sia compromessa.

Infine, va evidenziato che il personale incaricato del trattamento dei dati è stato idoneamente informato e istruito sulle accortezze da seguire per evitare che terzi possano venire in possesso della propria password, per la cui disamina si rimanda alla consultazione "Istruzioni Operative per gli Incaricati".

2.3. Controllo accesso logico

L'accesso ai dati è regolamentato attraverso l'attribuzione di un profilo ad ogni utente. Generalmente si tratta di profili precostituiti, anteriormente al trattamento, in base all'Unità Organizzativa di appartenenza dell'utente ed alla relativa mansione. E' stato disposto che tali profili vengano revisionati dal Responsabile della società di manutenzione IT per verificarne l'adeguatezza.

2.4. Riutilizzo supporti

All’interno delle "Istruzioni Operative per gli Incaricati" è stato disposto che i dati registrati su supporti di memoria rimovibili vengano cancellati in modo che le informazioni precedentemente contenute non siano tecnicamente recuperabili. Nel caso in cui non fosse possibile la cancellazione completa del supporto, è stata disposta la distruzione dello stesso.

2.5. Antivirus

Per la prevenzione dei rischi derivanti dall’introduzione di programmi contenenti virus sono state adottate misure di natura tecnica ed organizzativa. Tra quelle di natura tecnica, è presente all’interno dello Studio, un sistema antivirus aziendale con funzionalità automatiche di aggiornamento sia sul server che sulle singole postazioni di lavoro. Relativamente alle misure organizzative, il responsabile, ha emanato specifiche istruzioni, volte a garantire il corretto utilizzo degli strumenti elettronici da parte degli utenti ("Istruzioni Operative per gli Incaricati").

2.6. Protezione delle applicazioni

Il nuovo Regolamento Europeo dispone che gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire le vulnerabilità di strumenti elettronici e correggerne i difetti (c.d. patch), siano effettuati almeno annualmente e, in caso di dati sensibili e giudiziari, almeno semestralmente. AM.I.CO. DI CONCA & C. SAS ha disposto che le patch correttive volte a prevenire la vulnerabilità di strumenti elettronici ed a correggerne i difetti siano installate almeno semestralmente.

2.7. Back up e ripristino dei dati

Secondo quanto disposto da AM.I.CO. DI CONCA & C. SAS, i dati devono essere tutelati dalla possibilità che vengano distrutti in parte o completamente, e ciò richiede, oltre ad appropriate misure di sicurezza, che i dati siano periodicamente copiati in supporti o sistemi di riserva da utilizzare in caso di necessità per il loro ripristino. Le copie di back-up devono essere custodite in maniera idonea a fronteggiare l’emergenza (provandone quindi preventivamente il funzionamento) e in maniera da consentire il rispetto dei tempi di ripristino programmati. Al riguardo, presso AM.I.CO. DI CONCA & C. SAS, viene effettuato un back-up automatico su CLoud.

2.8. Sicurezza della rete e della trasmissione dei dati

I dati personali sensibili o giudiziari sono protetti contro l’accesso abusivo mediante l’utilizzo di idonei strumenti elettronici. Al fine di proteggere i dati personali da accessi non autorizzati, AM.I.CO. DI CONCA & C. SAS ha adottato sistemi di protezione perimetrale (firewall Hardware e Software).

2.9. Sicurezza fisica locali I.T.

L’accesso ai locali situati all’interno delle sedi è consentito soltanto al personale autorizzato. All’interno dei locali sono presenti:

- impianti di climatizzazione;
- porta blindata.

3. TRATTAMENTI CARTACEI

Vengono illustrate di seguito le misure di sicurezza adottate per la protezione dei locali che ospitano le informazioni in formato cartaceo.

3.1. CONTROLLO ACCESSO ALLA DOCUMENTAZIONE CARTACEA

Per quanto riguarda l’accesso alla documentazione cartacea, va evidenziato che la stessa è sempre sotto il controllo del personale incaricato al trattamento dei dati. Al riguardo il personale ha ricevuto specifiche istruzioni scritte circa le modalità di conservazione ed utilizzo della documentazione cartacea (cfr. "Istruzioni operative per gli Incaricati del trattamento").

4. SCHEDE TECNICHE

Scheda n°	1	Compilata da	Conca Davide	Data compilazione	Thu Nov 20 2025
Misura	MIS01				
Descrizione sintetica	Password sui sistemi informatici				
Elementi descrittivi	Password dei sistemi informatici rispettanti i criteri dettati dalla legge				

Scheda n°	2	Compilata da	Conca Davide	Data compilazione	Thu Nov 20 2025
Misura	MIS02				
Descrizione sintetica	Backup				
Elementi descrittivi	Cloud				

Scheda n°	3	Compilata da	Conca Davide	Data compilazione	Thu Nov 20 2025
Misura	MIS03				
Descrizione sintetica	Software Antivirus, Antispam e firewall				
Elementi descrittivi	Beet defender				

Scheda n°	4	Compilata da	Conca Davide	Data compilazione	Thu Nov 20 2025
Misura	MIS04				
Descrizione sintetica	Sistema di antifurto e antintrusione, video sorveglianza				
Elementi descrittivi	Porta blindata				

Scheda n°	5	Compilata da	Conca Davide	Data compilazione	Thu Nov 20 2025
Misura	MIS05				
Descrizione sintetica	Manutenzione programmatica dei sistemi, personale qualificato				
Elementi descrittivi	A chiamata				

5. FORMAZIONE DEGLI INCARICATI DEL TRATTAMENTO

Il nuovo Regolamento Europeo sul trattamento dei dati prevede un programma di formazione ed aggiornamento indirizzato ai dipendenti dell'organizzazione che operano sui dati personali.

AM.I.CO. DI CONCA & C. SAS ha prodotto una documentazione esaustiva al fine di effettuare una formazione indirizzata alle figure che svolgono attività significative ai fini della gestione degli adempimenti privacy.