

	Politica	Sicurezza delle informazioni
	Modello – Codice - Revisione	S – DS4211 - Rev. 6
	Classificazione	Pubblico

POLITICA SICUREZZA DELLE INFORMAZIONI

Rev.	data	Parti revisionate	Emesso	Verificato	Approvato
5	02/05/2024	Revisione per adeguamento ISO IEC 27001:2022	RSGSI	EPS	DIR
6	30/01/2026	Modifica riferimenti a policy interne	RSGSI	EPS	DIR

	Politica	Sicurezza delle informazioni
	Modello – Codice - Revisione	S – DS4211 - Rev. 6
	Classificazione	Pubblico

Sommario

1. Introduzione	3
1.1. Scopo del documento.....	3
1.2. Ambito del Sistema di Gestione della Sicurezza delle Informazioni	3
1.3. Riferimenti	4
1.4. Definizioni e acronimi	4
1.5. Dichiarazione d'intenti.....	4
2. Principi, obiettivi e requisiti.....	5
2.1. Principi guida	5
2.2. Obiettivi e requisiti per la sicurezza delle informazioni	5

	Politica	Sicurezza delle informazioni
	Modello – Codice - Revisione	S – DS4211 - Rev. 6
	Classificazione	Pubblico

1. Introduzione

1.1. Scopo del documento

Lo scopo del presente documento è quello di definire le linee di indirizzo in materia di sicurezza delle informazioni, approvate dalla Direzione di QUA.D.R.A. S.r.l., nella figura dall'Amministratore Unico, al fine di poterle comunicare in maniera ottimale al suo interno e alle parti esterne interessate.

Il processo di gestione della sicurezza delle informazioni è basato sullo standard ISO/IEC27001:2022

1.2. Ambito del Sistema di Gestione della Sicurezza delle Informazioni

QUA.D.R.A. S.r.l. (di seguito anche "QUADRA" o "Organizzazione") è una azienda italiana con sede legale presso lo studio del proprio commercialista a Orsago (TV) e sede operativa a San Vendemiano. QUADRA progetta, realizza, distribuisce e mantiene software dedicati al settore della raccolta e smaltimento rifiuti.

Il campo di applicazione del Sistema di Gestione della Sicurezza delle Informazioni definito da QUADRA è:

"Sviluppo, Implementazione, Gestione e controllo di dati e sistemi informativi per il settore ambientale erogati in modalità Application Service Provider e Software as a Service"

Rientrano nel perimetro del SGSI:

- Le attività svolte all'interno della sede QUA.D.R.A. SRL effettuate dal proprio personale;
- Le attività di sviluppo software svolte sia dal proprio personale che affidate in outsourcing;
- Le attività di hosting dei dati e la connettività affidate in outsourcing;
- La trasmissione dei dati in ambiente Internet.

Restano invece esclusi dal perimetro:

- La gestione dei dati effettuata direttamente dal cliente tramite il proprio personale operante presso le sedi del cliente stesso;
- Le verifica di integrità dei dati inseriti e/o forniti dal cliente;
- La garanzia di riservatezza, integrità e disponibilità causata da:
 - Forza maggiore (a titolo esemplificativo eventi dipendenti da fatti naturali e di terzi di grave entità, come catastrofi naturali, guerre, rivolte della popolazione, etc.);
 - Manomissione di apparati hardware e/o sistemi software ad opera del cliente o da parte di personale non autorizzato da QUA.D.R.A. SRL
 - Errato utilizzo del sistema da parte del cliente;
 - Malfunzionamento dei sistemi hardware e software sotto la cura e la responsabilità del cliente;
 - Interruzione del servizio di connessione Internet fornito da operatori di telecomunicazioni;
 - Mancato adempimento da parte del cliente di disposizioni e prescrizioni in materia di tutela dei dati personali, sicurezza sui luoghi di lavoro, prevenzione

	Politica	Sicurezza delle informazioni
	Modello – Codice - Revisione	S – DS4211 - Rev. 6
	Classificazione	Pubblico

incidenti o in generale il mancato rispetto di normative tempo per tempo applicabili e non rispettate.

La presente politica sarà mantenuta aggiornata con cadenza almeno annuale in modo tale da riflettere costantemente la situazione aziendale.

1.3. Riferimenti

La presente politica è redatta in conformità con:

- ISO/IEC 27001:2022
- ISO/IEC 27017:2015
- ISO/IEC 27018:2019

La documentazione interna di dettaglio (procedure, valutazione dei rischi, organigramma nominativo) è gestita nell'ambito del SGSI aziendale e disponibile su richiesta delle parti interessate aventi titolo:

- DS4212;
- DVRI001;
- DS5512.

1.4. Definizioni e acronimi

SGSI	<i>Sistema di Gestione della Sicurezza delle Informazioni</i>
DIR	<i>Direzione</i>
RSGSI	<i>Responsabile del Sistema di Gestione della Sicurezza delle Informazioni</i>

Per le ulteriori definizioni dei termini specialistici si fa riferimento al Glossario SGSI adottato dall'organizzazione.

Per le definizioni dei ruoli citati si deve fare riferimento all'Organigramma nominativo (DS5512).

1.5. Dichiarazione d'intenti

L'Organizzazione tiene in massimo conto la "sicurezza delle informazioni" in quanto ritiene che le "informazioni" siano un bene e un valore da proteggere e salvaguardare dalle minacce a cui possono essere esposte, così come le altre risorse relative al proprio business.

È volontà dell'Organizzazione assicurare la continuità del business, valutare e risolvere le vulnerabilità, minimizzare i danni per eventuali minacce, massimizzare il ritorno sugli investimenti fatti, favorire nuove opportunità di business.

L'Organizzazione ritiene, inoltre, un impegno essenziale il rispetto degli obblighi contrattuali relativi alla sicurezza ed il rispetto delle prescrizioni legali applicabili, dei regolamenti e degli accordi sottoscritti volontariamente.

Ha pertanto deciso di attuare e mantenere efficiente ed aggiornato un SGSI con l'obiettivo di:

- stabilire, attraverso il SGSI, gli indirizzi generali ed i principi di azione concernenti la gestione dei rischi strategici dell'organizzazione per la sicurezza delle informazioni, in modo che detti indirizzi e principi siano adeguati alle caratteristiche dell'organizzazione, alla sua localizzazione, a beni e tecnologia adottata;

	Politica	Sicurezza delle informazioni
	Modello – Codice - Revisione	S – DS4211 - Rev. 6
	Classificazione	Pubblico

- coinvolgere e sensibilizzare il management, i fornitori, i clienti, e tutte le parti terze riguardo la sicurezza delle informazioni;
- stabilire obiettivi che devono essere condivisi e perseguiti.

2. Principi, obiettivi e requisiti

2.1. Principi guida

Tutte le misure per la sicurezza delle informazioni adottate devono essere sempre progettate, implementate e gestite tenendo in considerazione i principi generali riconosciuti ed adottati da QUADRA e di seguito enunciati.

Il SGSI di QUADRA garantisce la riservatezza, integrità e disponibilità di tutte le informazioni trattate in linea con i vincoli contrattuali, di legge e di immagine dell'Organizzazione stessa.

I requisiti per la sicurezza delle informazioni sono parte degli obiettivi aziendali di QUADRA.

Il processo di gestione del rischio dell'organizzazione fornisce il contesto per identificare, valutare e controllare i rischi connessi alla sicurezza delle informazioni attraverso l'implementazione ed il mantenimento del SGSI.

Le modalità con cui vengono controllati tali rischi sono documentate nella valutazione del rischio e nel piano di trattamento del rischio, entrambi parte integrante del SGSI¹.

In particolare, sono fondamentali per tale politica la gestione dei backup di dati e processi, la capacità di evitare malware ed attacchi, il controllo degli accessi di utenti amministrativi e tradizionali ai sistemi e la gestione degli incidenti relativi alla sicurezza delle informazioni.

La continuità operativa del business è assicurata da un piano di Business Continuity e di Disaster Recovery supportato dalla logica Cloud.

Tutto il personale QUADRA coinvolto nell'ambito di applicazione si deve conformare con la presente politica e con il SGSI che implementa tale politica, e riceve opportuna formazione.

Il SGSI è soggetto a revisioni e miglioramenti continui, discussi ed approvati dalla Direzione. L'Organizzazione garantisce che tale politica viene revisionata al fine di rispondere a qualsiasi cambiamento nella valutazione del rischio o nel piano del trattamento del rischio in sede di "Riesame della Direzione" annuale o straordinario.

La politica e le procedure per la sicurezza delle informazioni fanno parte del SGSI che è stato progettato in conformità con quanto specificato nella norma ISO/IEC 27001:2022.

2.2. Obiettivi e requisiti per la sicurezza delle informazioni

In coerenza con le finalità della propria politica, QUADRA ha definito i seguenti obiettivi:

- Obiettivo 1)** assicurare che le informazioni siano accessibili solo a coloro che sono autorizzati ad averne accesso (confidenzialità);
- Obiettivo 2)** salvaguardare l'accuratezza e la completezza delle informazioni e dei metodi di processo (integrità);

¹ Si veda: DS2112 e DVRI001

	Politica	Sicurezza delle informazioni
	Modello – Codice - Revisione	S – DS4211 - Rev. 6
	Classificazione	Pubblico

- Obiettivo 3)** assicurare che gli utenti autorizzati abbiano accesso alle informazioni e alle risorse connesse quando necessario (disponibilità);
- Obiettivo 4)** assicurare la protezione dei dati e della privacy delle informazioni personali;
- Obiettivo 5)** salvaguardare le registrazioni aziendali;
- Obiettivo 6)** rispettare la proprietà dei diritti intellettuali;
- Obiettivo 7)** *rispettare la normativa applicabile, monitorando costantemente le fonti normative e legislative rilevanti per la propria attività anche attraverso un sistema informatizzato;*
- Obiettivo 8)** attuare la formazione e la sensibilizzazione alla sicurezza;
- Obiettivo 9)** garantire la continuità del business;
- Obiettivo 10)** minimizzare le conseguenze della violazione della politica di sicurezza;
- Obiettivo 11)** attuare una politica di scrivania pulita e schermo pulito al fine di minimizzare i rischi di uso non corretto delle informazioni.

La politica e gli obiettivi del SGSI e della Sicurezza delle Informazioni sono riesaminati e ridefiniti annualmente, tenendo conto, quando pertinente, anche dell'evoluzione tecnica e legislativa secondo specifiche procedure tese ad assicurare il corretto rispetto della presente politica.

La Direzione provvede ad effettuare l'aggiornamento della Politica per la Sicurezza delle Informazioni ogni qual volta si rende necessario l'adeguamento in relazione alle mutate variazioni di contesto e/o legislative.

La Direzione
Corrado Altinier