Sistema di Gestione Integrato per la Qualità e Sicurezza delle Informazioni

Politica di qualità e sicurezza delle informazioni

Versione	1.0
Stato	Attivo
Classificazione	Confidenziale - Interno
Redatta da	CSC Arcas
Approvata da	Amministratore unico
Data di emissione	19/01/2026
Data di revisione	

Controllo delle modifiche

Qualsiasi richiesta di modifica al presente documento deve essere inoltrata, specificando dettagli e motivazioni al Cybersecurity Steering Committee all'indirizzo email: csc@arcassecurity.it

Storia

Autore	Data	Versione	Note
CSC Arcas	19/01/2026	1.0	

Periodo di revisione

Il periodo di revisione per questo documento è di dodici mesi dalla data di emissione e ogni dodici mesi successivi.Potrebbe essere soggetto a revisioni e modifiche ad hoc come dettato dalle esigenze aziendali o dai requisiti legali e normativi.

Sommario

1 Finalità e contesto dell'organizzazione

Arcas S.R.L. è una società italiana di cybersecurity fondata nel 2013, con sede a Verona, un organico di 11 collaboratori e un fatturato nell'ordine di €2,7 milioni. L'azienda opera su due pilastri strategici complementari:

- servizi di consulenza specialistica in cybersecurity, penetration testing, risk assessment, formazione e GRC (GDPR/NIS2);
- rivendita, installazione e supporto di soluzioni tecnologiche per la sicurezza informatica, attraverso partnership quasi-esclusive con vendor nazionali e internazionali.

Il campo di applicazione del Sistema di Gestione Integrato (SGI) è: "*Servizi di consulenza in cybersecurity e conformità normativa; rivendita, installazione e supporto di soluzioni per la sicurezza informatica*".

La presente Politica è stata definita tenendo conto dei fattori interni ed esterni che influenzano la capacità di Arcas di raggiungere i propri obiettivi strategici, così come analizzati nel documento ***Analisi del Contesto Organizzativo***. In particolare:

- Sul piano esterno: il contesto normativo in evoluzione (GDPR, NIS2), la crescente domanda di servizi di conformità nei settori bancario, industriale, utilities e GDO, e un mercato del lavoro specialistico caratterizzato da forte competizione per i talenti cybersecurity.
- Sul piano interno: un modello operativo cloud-first basato su Google Workspace, infrastruttura gestionale su datacenter Aruba, team tecnico con competenze distintive e un approccio Agile alla delivery dei servizi.

La Politica si applica a tutte le attività, i processi, le risorse e le informazioni gestite da Arcas nell'ambito del proprio campo di applicazione.

1.1 Rilevanza del cambiamento climatico rispetto al contesto organizzativo

In conformità a quanto richiesto dall'Amendment 1:2024 alle norme ISO 9001:2015 e ISO/IEC 27001:2022, Arcas ha valutato la rilevanza del cambiamento climatico rispetto al proprio contesto organizzativo, considerando due dimensioni distinte.

1.1.1 Impatto di Arcas sul clima

Sul piano dell'impatto di Arcas sul clima, il modello operativo cloud-first — fondato su Google Workspace per le operazioni quotidiane e su Aruba Datacenter per i sistemi gestionali Fluentis — comporta l'assenza di infrastrutture IT fisiche proprie.

Questo elimina strutturalmente i consumi energetici diretti legati a raffreddamento e alimentazione di data center interni, delegando la gestione energetica a provider che operano su scala e con standard di efficienza — incluso l'utilizzo di energie rinnovabili — superiori a quelli raggiungibili da un'organizzazione delle dimensioni di Arcas.

L'impatto climatico diretto legato all'infrastruttura IT è pertanto minimizzato strutturalmente dal modello operativo adottato.

1.1.2 Rischio climatico per Arcas

Sul piano del rischio climatico per Arcas, il cambiamento climatico è identificato come fattore non rilevante sotto il profilo del rischio operativo diretto: i provider esterni (Google, Aruba) dispongono di architetture ridondanti e geograficamente distribuite che riducono a livelli trascurabili l'esposizione a eventi climatici localizzati; inoltre, il modello cloud-first consente ad Arcas di operare integralmente da remoto, rendendo la sede di coworking un punto di accesso comodo ma non critico, la cui eventuale indisponibilità non pregiudica la continuità operativa dell'organizzazione.

1.1.3 Valutazione del rischio climatico per Arcas

Arcas ha pertanto determinato che il cambiamento climatico non costituisce un fattore di rischio rilevante per la propria continuità operativa.

Questa valutazione viene riesaminata annualmente nell'ambito del processo di riesame del contesto (SGI-ORG01).

2 Indirizzo strategico

La Direzione riconosce che la qualità dei servizi erogati e la sicurezza delle informazioni trattate — proprie e dei propri clienti — costituiscono un vantaggio competitivo fondamentale e un obbligo verso tutte le parti interessate.

La Direzione si impegna a:

- integrare la gestione della qualità e della sicurezza delle informazioni nei processi di business, assicurando coerenza tra gli obiettivi del SGI e la strategia aziendale;
- fornire le risorse necessarie — umane, tecnologiche e finanziarie — per il funzionamento efficace e il miglioramento continuo del SGI;
- assicurare che ruoli, responsabilità e autorità relativi al SGI siano chiaramente definiti, comunicati e compresi all'interno dell'organizzazione;
- promuovere una cultura aziendale orientata alla qualità, alla protezione delle informazioni e alla conformità normativa, a tutti i livelli dell'organizzazione;
- mantenere una visione integrata della gestione qualità (ISO 9001:2015) e della sicurezza delle informazioni (ISO/IEC 27001:2022), evitando approcci compartimentati.

Il Cyber Security Committee (CSC), composto dall'Amministratore Unico e dal Chief Technical Officer, costituisce il presidio interno per le decisioni strategiche relative alla sicurezza delle informazioni.

3 Quadro di riferimento per gli obiettivi

Arcas definisce obiettivi integrati per la qualità e la sicurezza delle informazioni che sono misurabili, coerenti con la presente Politica e monitorati attraverso i KPI definiti nel documento ***Analisi del Contesto Organizzativo***.

Gli obiettivi sono organizzati nelle seguenti aree:

Area	Obiettivo Strategico	Riferimento KPI
Soddisfazione del Cliente	Erogare servizi di consulenza e soluzioni tecnologiche che soddisfino o superino le aspettative dei clienti nei settori bancario, industriale, utilities e GDO	NPS / tasso reclami
Sicurezza delle Informazioni	Garantire riservatezza, integrità e disponibilità delle informazioni trattate, con disponibilità target dei sistemi Google Workspace > 99,9% e Fluentis >99,5% e zero incidenti critici non gestiti	Uptime sistemi / n° incidenti
Conformità Normativa	Raggiungere la conformità NIS2 entro Q3 2026, mantenere la compliance GDPR e conseguire la doppia certificazione ISO 9001 + ISO/IEC 27001 entro Q2 2026	Stato audit / non conformità
Efficienza Operativa	Standardizzare i processi di delivery dei servizi core (pentest, assessment, GRC), implementare il knowledge management strutturato e automatizzare le attività amministrative a basso valore	Lead time / costo per progetto
Continuità Operativa	Formalizzare il Business Continuity Plan entro Q3 2026 con test annuale di disaster recovery, e qualificare il 100% dei fornitori critici ICT entro Q3 2026	Esito test BCP / fornitori qualificati
Persone e Competenze	Sviluppare percorsi di crescita per tutti i collaboratori, documentare le metodologie proprietarie e ridurre il rischio di perdita di know-how in un mercato caratterizzato da forte war for talent	Turnover / ore formazione

Gli obiettivi sono riesaminati almeno annualmente in occasione del Riesame della Direzione, oppure in anticipo qualora eventi significativi — nuove normative, cambiamenti organizzativi, incidenti rilevanti — ne richiedano l'aggiornamento.

4 Impegno al soddisfacimento dei requisiti

Arcas si impegna formalmente a identificare, comprendere e rispettare tutti i requisiti applicabili alla propria attività, integrando tale impegno nei processi operativi del SGI.

4.1 Requisiti cogenti

Arcas opera nel rispetto delle seguenti normative principali, il cui elenco aggiornato è mantenuto nel ***Registro dei requisiti legali e regolamentari***:

- Regolamento (UE) 2016/679 (GDPR) — protezione dei dati personali di dipendenti, clienti e soggetti terzi trattati nell'ambito dei servizi erogati;
- Direttiva (UE) 2022/2555 (NIS2) — sicurezza delle reti e dei sistemi informativi per i soggetti nei settori critici, con recepimento nazionale atteso entro 2026;
- D.Lgs. 81/2008 — tutela della salute e della sicurezza nei luoghi di lavoro;
- CCNL applicabile al settore di riferimento — gestione del rapporto di lavoro con i dipendenti.

4.2 Requisiti delle norme di riferimento

Il SGI è progettato per soddisfare i requisiti di:

- ISO 9001:2015 e relativo Amendment 1:2024 (Climate action changes) — Sistema di Gestione per la Qualità;
- ISO/IEC 27001:2022 e relativo Amendment 1:2024 (Climate action changes) — Sistema di Gestione per la Sicurezza delle Informazioni.

4.3 Requisiti contrattuali e delle parti interessate

Arcas si impegna a identificare e rispettare i requisiti specifici dei propri clienti (accordi contrattuali, NDA, requisiti di sicurezza dei dati) e a tenere conto delle aspettative delle altre parti interessate rilevanti, tra cui fornitori critici, partner tecnologici e autorità di vigilanza.

5 Impegno al miglioramento continuo

Arcas si impegna a migliorare costantemente l'efficacia, l'idoneità e l'adeguatezza del proprio Sistema di Gestione Integrato attraverso un approccio sistematico e proattivo.

Il miglioramento continuo si concretizza attraverso:

- la gestione dei rischi e delle opportunità, identificando in modo sistematico gli eventi che potrebbero influenzare il raggiungimento degli obiettivi del SGI e definendo azioni proporzionate al loro impatto potenziale;
- il monitoraggio dei KPI definiti nell'***Analisi del Contesto*** e degli indicatori di processo, con revisione periodica degli scostamenti e delle cause;
- la gestione delle non conformità e delle azioni correttive, garantendo l'eliminazione delle cause radice e la verifica dell'efficacia degli interventi;
- il Riesame della Direzione, condotto almeno annualmente dall'Amministratore Unico con il coinvolgimento dei responsabili di funzione, per valutare le prestazioni del SGI e definire le priorità di miglioramento;
- l'audit interno, condotto con periodicità almeno annuale, per verificare la conformità e l'efficacia del SGI rispetto ai requisiti delle norme di riferimento;

- la valorizzazione del contributo di tutti i collaboratori, incoraggiando la segnalazione di problemi e opportunità di miglioramento.

6 Comunicazione e disponibilità

La presente Politica costituisce un'informazione documentata del SGI.
La sua gestione segue le seguenti modalità:

Attività	Modalità	Responsabile
Mantenimento e aggiornamento	La Politica è revisionata almeno annualmente o al verificarsi di modifiche significative al contesto, all'organizzazione o ai requisiti applicabili	Responsabile SGI
Comunicazione interna	Condivisa con tutti i collaboratori al momento dell'assunzione e ad ogni revisione, tramite Google Workspace (Drive condiviso SGI).	Responsabile SGI / Responsabili di Funzione
Approvazione	Ogni versione è approvata e firmata dall'Amministratore Unico prima della diffusione	Amministratore Unico
Disponibilità esterna	La Politica può essere resa disponibile a clienti, partner e organismi di certificazione su richiesta, nella versione approvata in vigore	Responsabile SGI
Archiviazione	Le versioni precedenti sono archiviate nel repository documentale SGI su Google Drive con accesso controllato, per un periodo minimo di 5 anni	Office Assistant

Dichiarazione di Approvazione

La presente Politica Integrata per la Qualità e la Sicurezza delle Informazioni è approvata e adottata da Arcas S.R.L. con decorrenza dalla data di firma indicata di seguito. Essa è vincolante per tutti i collaboratori, a prescindere dalla tipologia contrattuale, e per tutti i soggetti che operano a qualunque titolo per conto di Arcas nell'ambito del campo di applicazione del SGI.

Michele Mantovani
Amministratore Unico