Politica del Sistema di Gestione Integrato

Redatto da: _____ Data 03/11/2022
(firma)
Maurizio Pallotti, Settore Qualità
(nome, cognome, qualifica)

Verificato da: _____ Data 14/11/2022
(firma)
Massimo Ortensi, Settore Sistemi
(nome, cognome, qualifica)

Approvato da: Comitato Sicurezza Data 30/11/2022
(nome, cognome, qualifica)

Versione : 2.1

Distribuzione : Distribuibile

Classificazione di sicurezza : Normale

Il documento è da ritenersi "IN LAVORAZIONE" se provvisto della sola firma: *Redatto da*
Il documento è da ritenersi "VERIFICATO ED EMESSO IN BOZZA" se provvisto anche della firma: *Verificato da*
Il documento è da ritenersi "DISTRIBUIBILE" se provvisto anche della firma: *Approvato da*

Indice

0 Storia Dei Cambiamenti

DATA	Versione	MOTIVO DEL CAMBIAMENTO
18/05/2017	1.0	Prima stesura
12/06/2018	1.1	Descrizione azienda (cap. 7.1) Obiettivi 2018 (cap. 7.4)
11/03/2019	1.2	Estensioni di certificazione 27017 e 27018 Obiettivi 2019 (cap. 7.4)
27/09/2019	1.3	Obiettivi 2019 aggiornamenti (cap. 7.4)
28/01/2020	1.4	Obiettivi 2020 aggiornamenti (cap. 7.4)
18/01/2021	1.5	Obiettivi 2021 aggiornamenti (cap. 7.4)
15/06/2021	1.6	Adeguamento per certificazione ISO 14001:2015 Aggiornamento Obiettivi generali e Obiettivi 2021 (cap. 7.4)
11/11/2021	2	Aggiornamento ragione sociale, Adeguamento per estensione certificazione ISO/IEC 27701:2019
30/11/2022	2.1	Aggiornamento Obiettivi generali e Obiettivi 2022 e 2023 (cap. 7.4), aggiornamento per ISO 37001.

1 Scopo del documento

Il presente documento ha lo scopo di definire la Politica del Sistema di Gestione Integrato aziendale al fine di comunicare l'impegno di UNIMATICA-RGI nel perseguire i principi di Qualità, di Sicurezza, di rispetto dell'Ambiente nonché di prevenzione della Corruzione.
Il rispetto di tali principi è fondamentale per implementare e governare l'insieme delle misure organizzative, logiche e fisiche, necessarie a garantire la qualità del servizio/prodotto fornito, il suo continuo miglioramento, la soddisfazione del cliente, la protezione del patrimonio informativo dell'azienda, la sostenibilità ed il rispetto dell'ambiente e la prevenzione della corruzione.

2 Lista di distribuzione

Portale aziendale.

3 Riferimenti

Il seguente documento è redatto in conformità ai requisiti della norma ISO 9001:2015, della norma ISO/IEC 27001:2013, comprese le estensioni di certificazione ISO/IEC 27017:2015, ISO/IEC 27018:2019 e ISO/IEC 27701:2019, nonché delle norme ISO 14001:2015 e ISO 37001:2016.

4 Responsabilità

La presente Politica è stata formulata in accordo e su indicazioni della Direzione Unimatica-RGI e redatta dal RSGQ, congiuntamente con il RSGSI, il RSGA e la Funzione di conformità.
La Politica è relativa al sistema di gestione integrato, per quanto riguarda gli aspetti di Qualità, di Sicurezza delle informazioni, di rispetto dell'ambiente e di prevenzione della corruzione e sarà riesaminata annualmente secondo i piani stabiliti direttamente dalla Direzione stessa.
I responsabili dell'attuazione della presente politica sono:

- La Direzione di Unimatica-RGI che stabilisce gli obiettivi, i criteri e i livelli di accettabilità del rischio, fornisce le risorse necessarie per garantire la corretta applicazione della qualità e della sicurezza delle informazioni, assicura lo svolgimento di audit interni e garantisce il pieno supporto nell'attuazione della presente politica, affidando alle diverse funzioni compiti di implementazione, gestione e monitoraggio dell'efficacia ed efficienza del sistema. All'interno di ogni funzione è stabilita la definizione degli opportuni ruoli e responsabilità per la gestione della qualità e della sicurezza dell'informazione e la gestione del servizio.
- Il RSGQ, il RSGSI e il RSGA che, rispettivamente per quanto riguarda Qualità – Sicurezza Informatica - Ambiente, facilitano l'attuazione della presente politica attraverso norme e procedure appropriate.
- La funzione di conformità per la prevenzione della Corruzione alla quale sono assegnate le responsabilità e l'autorità per supervisionare la progettazione e l'attuazione da parte dell'Organizzazione del sistema di gestione per la prevenzione della corruzione.
- Tutto il personale di Unimatica, a cui sono assegnati precisi ruoli e responsabilità Il personale deve avere un'adeguata competenza per svolgere i compiti richiesti, perciò deve essere informato e formato adeguatamente riguardo agli obiettivi dell'azienda in tema di qualità e sicurezza. Sono definite e mantenute registrazioni sull'istruzione, formazione, abilità, esperienze e qualifiche. Tutto il personale ha la responsabilità di reagire tempestivamente agli incidenti contro la sicurezza e/o non conformità del servizio e a segnalare alla Direzione qualsiasi punto debole individuato nel sistema.
- Clienti e Fornitori, coinvolti nella gestione dei sistemi implementati che rientrano nei perimetri di applicazione del Sistema di Gestione Integrato, sono tenuti al rispetto della Politica Integrata Unimatica-RGI per concorrere al mantenimento della qualità, della sicurezza delle informazioni trattate e del rispetto dell'ambiente.

5 Riesame

Il riesame della presente politica viene effettuato periodicamente dalla Direzione al fine di valutare l'efficienza e l'efficacia dei sistemi di gestione impostati ed al fine di garantire l'adozione delle azioni atte a consentirne il miglioramento continuo secondo i requisiti minimi definiti dalle rispettive norme. Il Riesame è effettuato almeno una volta all'anno ed al presentarsi delle situazioni per le quali viene richiesta una modifica relativa agli obiettivi aziendali che possono avere impatto anche sulla sicurezza delle informazioni, sulla qualità del servizio/prodotto e sull'ambiente.

6 Violazioni della politica

La Politica aziendale Unimatica-RGI deve essere osservata da tutti gli attori coinvolti nel pieno rispetto del Codice Etico, della Politica anticorruzione e del Modello Organizzativo e Gestionale di Unimatica-RGI, redatto in conformità al D.lgs. 231/01.

7 Politica del Sistema di Gestione aziendale

La presente Politica costituisce uno strumento fondamentale per sensibilizzare l'intera organizzazione sui principi aziendali di qualità, di sicurezza, di rispetto dell'ambiente e di prevenzione della corruzione e viene applicata a tutti gli ambiti specificati nel perimetro di certificazione, nonché a tutto il personale Unimatica-RGI, ai clienti e ai fornitori che siano in qualche modo coinvolti nei processi e/o nel trattamento di informazioni che rientrano nel campo di applicazione del Sistema di Gestione Integrato, in qualsiasi forma tali informazioni si presentino (cartaceo, elettronico, trasmesse oralmente).

La Politica aziendale integrata è stata sviluppata sulla base degli standard internazionali che forniscono i requisiti di un Sistema di Gestione della Sicurezza dell'Informazione ISO/IEC 27001:2017, della qualità ISO 9001:2015, dell'ambiente ISO 14001:2015 e della prevenzione della corruzione ISO 37001:2016.
Unimatica-RGI è infatti certificata per le seguenti norme:

- **ISO 9001:2015** - Sistema per la Qualità;
- **ISO/IEC 27001:2013** - Sicurezza delle Informazioni;
- **ISO/IEC 27017:2015** - Sicurezza delle Informazioni per i Servizi Cloud;
- **ISO/IEC 27018:2019** - Protezione delle Informazioni di identificazione personali (PII) nei servizi di public cloud per i cloud provider;
- **ISO/IEC 27701:2019** – Protezione delle informazioni sulla privacy (PIMS);
- **ISO 14001:2015** – Sistema di Gestione Ambientale;
- **ISO 37001:2016** – Sistema di Gestione Anticorruzione.

I principi strategici ai quali la Direzione di Unimatica-RGI si ispira per raggiungere i propri obiettivi sono così sintetizzabili:

- La Focalizzazione sul Cliente, ponendo al centro della propria filosofia la soddisfazione dei Clienti, sia per i prodotti che per i servizi;
- La leadership, impegnandosi a mantenere attivo e migliorare con periodici riesami il Sistema di Gestione per la Qualità;
- La pianificazione del sistema, definendo periodicamente, in occasione del riesame del sistema da parte della direzione, obiettivi chiari, quantificabili e misurabili per valutare la funzionalità del Sistema di Gestione;

- La partecipazione attiva delle persone, coinvolgendole e sensibilizzandole, a tutti i livelli, sui concetti di qualità, sicurezza e rispetto dell'ambiente e incoraggiando ogni iniziativa volta al perseguimento delle stesse;
- La formazione del personale, promuovendo la qualificazione e la formazione continua delle risorse umane;
- Il controllo dei Fornitori, privilegiando, quando possibile, la scelta di Fornitori in linea con la filosofia aziendale e che garantiscano il massimo rispetto possibile dell'ambiente e collaborando con loro nel perseguimento della miglior qualità di prodotti e servizi;
- L'approccio per processi, semplificando e snellendo al contempo la struttura dei processi operativi, mediante procedure e istruzioni semplici, al fine di eliminare le eventuali sovrastrutture peggiorative ai fini della qualità dei risultati e della sicurezza;
- Il miglioramento, verificando i risultati ottenuti e rilanciando nel tempo verso il raggiungimento di livelli di eccellenza;
- Il processo decisionale basato sulle evidenze e sulla valutazione del rischio;
- La gestione delle relazioni interne ed esterne;
- Il mantenimento della riservatezza, integrità e disponibilità delle informazioni.

Nel dettaglio gli ambiti di applicazione identificati sono:

- Politica;
- Organizzazione;
- Gestione degli information asset;
- Gestione delle risorse umane;
- Gestione dei fornitori;
- Sicurezza fisica ed ambientale;
- Gestione operativa delle risorse informatiche;
- Controllo accessi;
- Acquisizione, Sviluppo e Manutenzione del Sistema Informativo;
- Progettazione, sviluppo, controllo, riesame, produzione ed erogazione del servizio/prodotto;
- Soddisfazione del Cliente;
- Gestione degli incidenti di sicurezza;
- Gestione della continuità operativa;
- Gestione degli aspetti ambientali;
- Gestione delle emergenze ambientali;
- Gestione e controllo anti-corruzione;
- Conformità.

Lo scopo delle misure di sicurezza identificate dal Sistema di Gestione Integrato è quello di "contrastare", "prevenire", "dissuadere", "rilevare", "attenuare", "ripristinare" o "correggere" le minacce che possono incombere sui sistemi informativi aziendali e sull'ambiente circostante. Tali misure di sicurezza dovranno essere attuate secondo le modalità descritte all'interno di specifiche procedure operative e/o istruzioni operative.

7.1 Mission Aziendale

Unimatica-RGI (già Unimatica) è una S.p.A. nata nel 2000 dalla partnership tra il gruppo Logital S.p.A. e l'Università di Bologna. Nel 2009 l'azionariato di Unimatica S.p.A. si è ulteriormente esteso ed arricchito grazie all'ingresso in qualità di azionista del Gruppo Intesa Sanpaolo, che ha acquistato il 25% delle azioni della società tramite Infogroup S.p.A. A partire dal 2010 Unimatica ha acquisito anche la partecipazione di un nuovo socio, il Gruppo RGI, leader in Italia ed in Europa nei servizi IT per il settore Assicurativo che da luglio 2022 detiene il 100% del capitale della società.

La missione della società è di sviluppare applicazioni informatiche e servizi per l'amministrazione digitale, basati sulla sicurezza della firma digitale e la dematerializzazione, con archiviazione e conservazione a norma dei documenti. Le applicazioni ed i servizi di Unimatica-RGI sono tutti in tecnologia web sicura grazie all'uso appropriato della firma digitale e delle metodologie più avanzate di autenticazione e sicurezza delle transazioni in rete.
Unimatica-RGI è società leader in Italia per i servizi di conservazione e di amministrazione digitale nelle pubbliche amministrazioni, nelle banche e nelle aziende private.
I servizi di Unimatica-RGI per i processi e le organizzazioni "paperless", utilizzano certificati di firma qualificata con validità giuridico-legale (rilasciati e rinnovati dalle diverse Certification Authority nazionali) e soluzioni di firma grafometrica.

7.2 Processi strategici

Il processo primario che fornisce margine di contribuzione al fatturato di Unimatica-RGI è lo sviluppo e delivery dei Servizi/Prodotti. Tale processo è suddiviso in sottoprocessi:

- Definizione e riesame dei requisiti e del contratto
- Progettazione, sviluppo, controllo, riesame, produzione ed erogazione del servizio/prodotto, supportato dalle linee guida per lo sviluppo sicuro;
- Gestione della documentazione;
- Procedure di Business Continuity;
- Soddisfazione del cliente

I processi secondari a supporto di quello primario sono:

- Gestione degli acquisti
- Gestione del personale
- Gestione dei fornitori
- Gestione delle emergenze ambientali
- Controllo e gestione anti-corruzione
- Processo degli audit interni

7.3 Risorse da salvaguardare

Le risorse che Unimatica-RGI si impegna a salvaguardare sono tutte quelle che sottendono ai processi strategici e che sono elencate nell'asset inventory aziendale. Le categorie principali sono:

- dati/documenti/informazioni
- asset fisici
- asset logici
- servizi/prodotti

- personale e competenze

oltre che il rispetto e la salvaguardia dell'ambiente.
Maggiori dettagli sono riportati nel DOC001 - Principi e Regole di Sicurezza per la protezione del patrimonio informativo.
Relativamente all'ambito del delivery di servizi ed in conformità alla norma ISO IEC 27001:2013 viene condotta con frequenza annuale l'analisi dei rischi che incombono sugli asset aziendali. L'analisi tiene in considerazione gli obiettivi strategici espressi nella presente politica, gli incidenti occorsi, i cambiamenti di business e di tecnologia avvenuti nel corso di tale periodo.

7.4 Obiettivi di Unimatica-RGI

L'obiettivo di Unimatica-RGI è di garantire un adeguato livello di qualità e di sicurezza dei dati e delle informazioni trattate durante la gestione dei processi di fornitura di servizi/prodotti, identificando, valutando e trattando i rischi ai quali i servizi/prodotti stessi sono soggetti.
Con la presente politica Unimatica-RGI intende formalizzare i seguenti obiettivi generali nell'ambito della Qualità, della Sicurezza delle Informazioni e nel rispetto dell'ambiente:

- Fornire con regolarità prodotti e servizi che soddisfino i requisiti del cliente e quelli cogenti applicabili
- Facilitare le opportunità per accrescere la soddisfazione del cliente
- Affrontare rischi ed opportunità associati al proprio contesto ed ai propri obiettivi
- Dimostrare la conformità ai requisiti specificati dal Sistema di Gestione
- Preservare al meglio l'immagine dell'azienda quale fornitore affidabile e competente
- Proteggere il proprio patrimonio informativo in modo che:
  - Le informazioni siano protette da accessi non autorizzati tramite opportune politiche di accesso basate sui requisiti per l'accesso relativi alla sicurezza e all'attività dell'azienda (profilazione e uso delle password)
  - Le informazioni non vengano divulgate a personale non autorizzato a seguito di azioni deliberate, per incuria o per atti corruttivi
  - L'integrità delle informazioni sia protetta e salvaguardata da modifiche non autorizzate
  - Tutte le risorse di supporto alle informazioni siano protette adeguatamente
- Assicurare la continuità del business aziendale affinché le informazioni siano a disposizione degli utenti autorizzati quando ne hanno bisogno tramite:
  - Predisposizione di sistemi di backup delle informazioni, gestiti e monitorati
  - Redazione di piani per la continuità dell'attività aziendale e di piani e obiettivi per la sicurezza, opportunamente aggiornati, controllati e migliorati
- Minimizzare i danni derivanti da attività esterne o interne, accidentale o intenzionale mediante:
  - Controlli opportuni dell'accesso alle informazioni o agli asset dell'Organizzazione da parte di terzi
  - Mantenimento della sicurezza dell'informazione e del software scambiato all'interno dell'Organizzazione o con qualunque parte esterna
  - Procedure per le necessarie autorizzazioni a esportare informazioni critiche, apparati e/o software
  - Procedure per la sicurezza degli apparati all'esterno dell'Organizzazione che stabiliscano le modalità di assegnazione degli accessi
- Rispondere e reagire tempestivamente ad eventi che possano ridurre la sicurezza delle informazioni mediante:
  - Redazione di procedure per la comunicazione tempestiva e per la gestione degli incidenti in caso di minaccia alla sicurezza dell'informazione, con definizione delle responsabilità e delle azioni correttive da intraprendere

- Comunicazioni tempestive a chi di dovere relativamente a violazioni della sicurezza delle informazioni
- Rispondere pienamente alle indicazioni della normativa vigente e cogente
- Aumentare, nella propria organizzazione, il livello di sensibilità e la competenza sui temi di sicurezza attraverso:
  - Comunicazioni aggiornate e adeguata formazione al personale circa l'attuazione del SGI
  - Programmi formativi di dettaglio sulla qualità e la sicurezza delle informazioni per tutto il personale interno e per tutto il personale esterno che opera per periodi prolungati all'interno dell'organizzazione
- Assicurare la massima attenzione al rispetto dell'ambiente tramite:
  - Controllo e riduzione dei consumi di energia elettrica ed acqua;
  - Controllo e riduzione della produzione di rifiuti associati alle sue attività (ad es. RAEE, carta e cartoni, ecc.)
  - Corretta gestione delle emergenze ambientali e rapporti con le autorità competenti.
- Massimizzare il rendimento del capitale
- Fornire opportunità di miglioramento continuo
- Mantenere la conformità con i requisiti legali e contrattuali in materia di protezione dei dati personali
- Diffondere in azienda una cultura della sicurezza delle informazioni, considerata necessaria per la tipologia di servizi offerti dall'azienda e dei dati trattati

Il dettaglio degli obiettivi definiti per il 2023 é definito nell'apposito documento del SGI "Piano Obiettivi 2023.xslx".
Fra questi si riportano di seguito gli obiettivi che Unimatica-RGI ritiene più significativi per il 2023:

- Consolidare e ampliare l'offerta aziendale di "Servizi web collaborativi".
  Incrementare i Servizi web di audio-video-collaborazione proposti da Unimatica-RGI per la collaborazione remota fra utenti di pubbliche amministrazioni, cittadini, aziende private, professionisti per sessioni di lavoro comprendenti il riconoscimento e l'autenticazione della controparte, la condivisione dei documenti, la firma digitale degli stessi, il pagamento contestuale degli importi, la conservazione a norma dei documenti trattati, la registrazione della sessione.
- Rafforzare la già esistente struttura organizzativa aziendale che opera a supporto degli Enti nell'ambito dei progetti e dei servizi sostenuti dagli investimenti del PNRR.
- Ottenere la certificazione UNI/PDR 125:2022 relativa alla Parità di Genere per contribuire concretamente al processo verso l'uguaglianza fra donne ed uomini.
- Incrementare la sicurezza dei propri data center innalzandola al livello TIER4.

7.5 Dichiarazione della Direzione e Ambito

La Dichiarazione della Direzione e l'ambito di certificazione sono contenuti nel documento DOC050 - Ambiti e Perimetri dei Sistemi di Gestione.

7.6 Leadership e commitment

La Direzione si impegna a predisporre le risorse necessarie alla gestione dei sistemi, in linea con la politica e gli obiettivi aziendali, garantendo a tutto il personale massima disponibilità per l'attuazione della presente politica e affidando alle diverse figure presenti in azienda compiti di implementazione, gestione e monitoraggio dell'efficienza del sistema. Sono state individuate le

figure dei responsabili e sono stati loro assegnati gli opportuni ruoli nella gestione dei sistemi. Sono pianificati periodicamente, e ogni volta sia necessario, incontri di confronto e condivisione attraverso lo strumento dei comitati e dei riesami che vedono coinvolti i responsabili delle varie funzioni aziendali.

7.7 Analisi dei rischi e degli impatti ambientali

La Direzione di Unimatica-RGI ha istituito ed attua un approccio basato sulla valutazione quantitativa e qualitativa dei rischi inerenti la pianificazione del sistema di gestione e dei suoi obiettivi, al fine di raggiungerli, riducendo o tenendo sotto controllo gli effetti indesiderati. Vengono inoltre analizzati i rischi associati alle risorse esistenti in azienda. Tale metodo consente di determinare valori oggettivi che permettono di definire le contromisure che devono essere adottate per abbattere e rendere accettabile il valore del rischio residuo associato al bene. In aggiunta, la metodologia adottata è pienamente rispondete ai requisiti stabiliti dalla ISO IEC 27005:2011, dalla ISO 31000:2018 e pertanto in linea con quanto prevede la norma stessa.
In tal senso vengono adottati strumenti informatici e metodi deterministici che permettono, oltre che implementare e gestire l'inventario degli asset aziendali, di misurare l'efficacia dell'applicazione delle azioni e soprattutto la replicabilità della valutazione al fine di mantenere il processo di miglioramento.
Tali strumenti, con l'ausilio anche delle funzionalità messe a disposizione dal prodotto di risk management utilizzato, permettono di mantenere sempre aggiornata la lista dei beni e il controllo sulle minacce e vulnerabilità che su di essi incombono. Applicando di conseguenza il processo di analisi e gestione dei rischi è possibile avere in qualsiasi momento lo stato di sicurezza implementato sulle risorse aziendali e sull'ambiente circostante.
La metodologia e l'analisi dei rischi vengono riesaminate ad intervalli di tempo definiti, per garantire la sicurezza delle informazioni dell'azienda e fornire opportunità di miglioramento.

7.8 Sistema di Gestione per la Privacy (PIMS)

Al fine di perseguire gli obiettivi di compliance ai requisiti del GDPR, Unimatica-RGI ha adottato un sistema di gestione per la privacy conforme allo standard ISO 27701 (ISO/IEC 27701). Il Sistema di gestione per la Privacy è stato integrato nel più generale sistema di gestione aziendale ed è stato pianificato in modo da considerare aspetti di Governance, di Sistema di Controllo Interno ed aspetti di Risk Management. Unimatica-RGI si impegna ad adeguare e a migliorare continuamente il proprio Sistema di Gestione per la Privacy e a sensibilizzare e formare i propri stakeholders in merito alla sua corretta applicazione. Tutti coloro che trattano dati per conto di Unimatica-RGI sono da formati e sensibilizzati in conformità all'articolo 29 del GDPR sulla corretta applicazione della presente politica e delle politiche operative da questa richiamate. Tutti i fornitori che trattano dati personali per conto di Unimatica-RGI sono nominati responsabili del trattamento in conformità all'articolo 28 del GDPR.

8 Documentazione

Le registrazioni dei sistemi di gestione descritte nelle procedure e nelle politiche adottate da Unimatica-RGI sono tenute sotto controllo secondo quanto previsto dalla procedura "PRO011 Gestione documentazione".