

POLITICA INTEGRATA PER LA QUALITA' E LA SICUREZZA DELLE INFORMAZIONI

Chi siamo

Umbria Digitale S.c.a r.l. è una Società consortile in house senza scopo di lucro al servizio della Regione Umbria, dei Comuni, delle Agenzie o organismi pubblici in essa consorziati, svolgendo attività di interesse generale per la gestione e lo sviluppo del settore ICT regionale e attività strumentale nei confronti dei soggetti pubblici soci secondo il modello in house providing.

La società, costituita ai sensi dell'art. 11 della Legge Regionale n° 9/2014, eroga servizi per lo sviluppo e la gestione della rete pubblica regionale per la diffusione della Banda Larga e dei servizi infrastrutturali della Community Network (CN) nonché del Data Center Regionale Unitario (DCRU), operando anche per la produzione di beni e la fornitura di servizi strumentali alle attività degli enti pubblici partecipanti in ambito informatico, telematico e per la sicurezza dell'informazione, curando le attività relative alla gestione del Sistema Informativo Regionale dell'Umbria (SIRU) e alla manutenzione delle reti locali e delle postazioni dei consorziati, configurandosi come centro servizi territoriale.

Il presente documento, organizzato in sezioni, esplicita l'atteggiamento, i propositi, gli impegni e gli obiettivi che la Direzione di Umbria Digitale mette in campo per il perseguimento della Qualità e della Sicurezza delle Informazioni, riconoscendone il fondamento nella ricerca del miglioramento continuo:

- della salvaguardia delle informazioni del cliente;*
- della massima soddisfazione dei propri clienti e delle parti interessate.*

A questo fine Umbria Digitale sviluppa e gestisce un Sistema di Gestione Integrato per la Qualità e la Sicurezza delle informazioni (SGI) che governa l'insieme dei requisiti previsti dalle norme ISO 9001, ISO 27001, ISO 27017 e ISO 27018.

L'organizzazione identifica le proprie attività come processi da pianificare, controllare e migliorare costantemente e attiva al meglio le risorse per la loro realizzazione.

L'organizzazione gestisce i propri processi perché siano univoci:

- gli obiettivi da perseguire e i risultati attesi;*
- le responsabilità connesse e le risorse impiegate.*

I servizi erogati da Umbria Digitale sono pertanto strutturati secondo il seguente schema di processi:

- Progettazione e realizzazione dei servizi (DESIGN)*
- Gest. operativi sistemi IT (IT OPERATION MANAGEMENT)*
- Gest. dei servizi di Service Desk (SERVICE DESK - ACCOGLIENZA)*
- Gest. assistenza applicativa (SERVICE DESK - ASS. APPLICATIVA)*
- Gest. manutenzione software (APPLICATION MANAGEMENT)*
- Assistenza tecnica utenti (TECHNICAL MANAGEMENT)*
- Gestione della domanda (DEMAND MANAGEMENT)*



I nostri valori

Nella gestione delle proprie attività, Umbria Digitale si ispira ai seguenti valori:

- la Società si attiene ai più rigorosi principi di etica professionale nello svolgimento dei servizi ad essa affidati ed in ogni altro settore delle proprie attività;*
- la Società vuole essere un partner leale degli enti soci per le attività ad essa affidate utilizzando le proprie capacità di coordinamento, controllo ed integrazione dei servizi e dei processi e mantenendo gli stessi al livello concordato e programmato di prestazioni;*
- La Società, attraverso i propri standard aziendali, interviene nella conduzione dei progetti di sviluppo e messa in opera di sistemi informatici e nella erogazione dei servizi resi ai clienti con riferimento a puntualità, precisione e nel rispetto dei livelli di servizio contrattualizzati;*
- la Società è a disposizione di utenti e cittadini, tramite la propria struttura di Service Desk, al fine di agevolare l'utilizzazione dei servizi offerti dagli enti soci al fine di migliorare la qualità nella comunicazione tra le parti e l'accesso ai servizi;*
- la Società tutela la sicurezza e la salute nei luoghi di lavoro e ritiene fondamentale nell'espletamento della propria attività, il rispetto dei diritti dei lavoratori. La gestione dei rapporti di lavoro è orientata a garantire pari opportunità e a favorire la crescita professionale di ciascuno.*

Il nostro impegno per la qualità e la sicurezza delle informazioni

L'obiettivo principale di Umbria Digitale è quello di raggiungere la piena soddisfazione dei clienti/soci e degli utenti finali dando prova di essere:

- Affidabile: Rispettando gli impegni e facendo ciò che dichiara affinché gli utenti possano fidarsi di essa;*
- Disponibile: Trattando con gentilezza, rispetto e cordialità gli utenti e i cittadini che si rivolgono a essa;*
- Attenta: Comportandosi con i suoi utenti con professionalità e rispetto dando una consulenza personalizzata con la volontà di aiutarli nell'utilizzo degli strumenti informatici gestiti.*
- Competente: Fornendo personale specializzato e specificamente formato per le attività gestite. La determinazione delle competenze e un monitoraggio continuo delle stesse sono gli strumenti utilizzati per la pianificazione delle esigenze formative per garantire che ogni attività sia affidata a personale adeguatamente preparato.*

L'obiettivo di rispondere alle esigenze delle pertinenti parti interessate è perseguito inoltre:

- prestando attenzione, nello svolgimento dei processi interni, al controllo della qualità al fine di preservarne i requisiti e prevenirne i difetti;*
- agendo in base al principio del risk based thinking per individuare, valutare e attuare le azioni opportune per mitigare i rischi al fine del perseguimento dei risultati attesi.*
- mantenendo una elevata sensibilità ai bisogni, alle aspettative ed alle informazioni di ritorno dagli stessi, con una pronta gestione dei reclami;*

- credendo nel miglioramento continuativo, quale elemento essenziale, per sviluppare ed affermare il successo dell'azienda;
- affermando un'immagine di serietà professionale ed etica;
- mantenendo un sistema integrato di gestione per la Qualità e Sicurezza delle informazioni certificato;
- garantendo la solidità finanziaria e patrimoniale dell'azienda stessa.

Tutti i dipendenti dell'organizzazione sottesa dal SGI sono pertanto tenuti a rispettare le presenti politiche e l'intero SGI, incluse i dettami del Regolamento (Ue) 2016/679 (GDPR) in tema di trattamento dei dati personali delle persone fisiche, adottando tutte le misure tecniche e organizzative tali da garantire un livello di sicurezza adeguato al rischio e attivandosi perché tali misure siano correttamente implementate e oggetto di costante valutazione. Un insieme di regole sono richieste a tutti coloro che, non essendo dipendenti dell'organizzazione si trovano ad operare per conto dell'azienda.

Per perseguire gli obiettivi aziendali, le informazioni trattate devono soddisfare i requisiti di:

- riservatezza: le informazioni devono essere conosciute solo da coloro che ne hanno il relativo diritto, rispettando il principio del minimo privilegio ("necessità di sapere") in base alle mansioni ricoperte ("necessità di operare");*
- integrità: le informazioni devono essere precise e complete, devono rispettare i valori e le aspettative aziendali, e devono essere protette da modifiche e cancellazioni non autorizzate. Per soddisfare tale requisito le informazioni devono essere esatte, aggiornate e leggibili;*
- disponibilità: le informazioni devono essere disponibili quando richiesto dai processi aziendali, in maniera efficace ed efficiente;*
- efficacia: le informazioni devono essere rilevanti e pertinenti al processo aziendale e, allo stesso tempo, devono essere disponibili tempestivamente, senza errori e fornite in modo da poter essere utilizzate dall'utente;*
- efficienza: le informazioni devono essere fornite attraverso l'uso ottimale delle risorse sia dal punto di vista della produttività che della economicità;*

I dati personali devono essere trattati:

- in osservanza dei criteri di riservatezza;*
- in modo lecito e secondo correttezza;*
- per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati;*
- nel pieno rispetto delle misure minime di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.*

La Società predispone ed implementa il proprio Piano di Continuità Operativa ed il Piano di Disaster Recovery. Deve essere sempre assicurata la protezione dei dati e dei sistemi contro le possibili conseguenze dell'attività di software dannoso (c.d. malware). Inoltre, la Società, tenuto conto della

particolare criticità dei ruoli connessi alla gestione del Sistema Informativo, adotta idonee cautele volte a prevenire e ad accertare eventuali utilizzi non in linea con gli obiettivi aziendali.

Enfasi particolare è posta ai servizi contrattualizzati in tecnologia cloud. A tal fine, ai requisiti del sistema di gestione della sicurezza delle informazioni ISO 27001, sono aggiunti i requisiti previsti dalle norme ISO 27017 e ISO 27018.

Valutazione dei rischi e delle opportunità

L'organizzazione pianifica i propri processi con approccio risk-based thinking (RBT) al fine di attuare le azioni più idonee per:

- valutare e trattare rischi associati alle attività ed ai processi;*
- sfruttare e rinforzare le opportunità identificate*

Per poter gestire in modo adeguato il Sistema Informativo, l'organizzazione promuove, a tutti i livelli, un adeguato senso di proattività nella gestione dei rischi ed ha implementato un sistema per la messa in atto delle azioni di mitigazione che consente inoltre la rielaborazione statistica degli incidenti al fine della pronta individuazione e la correzione di eventuali carenze relative a politiche, processi e procedure. Ciò consente di ridurre considerevolmente la frequenza e/o gravità degli eventi dannosi.

La Società con le sue unità organizzative interne assicura l'esecuzione dei processi atti a:

- diffondere il contenuto dei servizi, conoscere i punti di forza e di eventuale debolezza;*
- assicurare agli utenti formazione e accesso alle funzioni secondo criteri di sicurezza aderenti a principi di sana e prudente gestione o comunque alle politiche di gestione del rischio informatico;*
- valorizzare le risorse informatiche, intese come leva per il raggiungimento degli obiettivi della Società;*
- realizzare un sistema di comunicazione dei fabbisogni o delle criticità del Sistema Informativo con l'obiettivo di attivare un processo di miglioramento continuo;*
- attuare controlli finalizzati a valutare la capacità dell'azienda di attenersi alle politiche di sicurezza stabilite;*
- individuare tempestivamente deviazioni (anomalie, malfunzionamenti, differenze) rispetto a quanto conosciuto/approvato/autorizzato;*
- favorire azioni correttive;*
- tracciare qualsiasi deviazione da quanto stabilito.*

Leadership

La Direzione si assume la responsabilità dell'efficacia del proprio SGI, rendendo disponibili tutte le risorse necessarie e assicurandosi che gli obiettivi pianificati siano compatibili con il contesto e gli indirizzi strategici dell'organizzazione, comunicando l'importanza dell'applicazione del Sistema di Gestione Integrato di Umbria Digitale.

Coinvolgimento del personale e degli stakeholders

L'organizzazione è consapevole che il coinvolgimento del personale e di tutti gli stakeholder, unito all'attiva partecipazione di tutti i collaboratori, sono un elemento strategico primario.

Promuove lo sviluppo delle professionalità interne e l'attenta selezione delle collaborazioni esterne al fine di dotarsi di risorse umane competenti e motivate.

L'Azienda adotta tutti gli strumenti a sua disposizione affinché la Politica sia vissuta attivamente e sia testimonianza dell'impegno della Direzione di fronte a tutte le parti interessate.

Il riesame periodico del Sistema di Gestione Integrato, in relazione agli obiettivi definiti nella politica, attuato mediante il riesame da parte della Direzione. La Direzione s'impegna a comunicare ed a far comprendere la presente Politica a tutti i livelli dell'Organizzazione.

Nel ricorso ai servizi esterni, la Società richiede ai fornitori gli stessi criteri di competenza, capacità ed affidabilità richiesti al proprio personale, nello svolgimento dell'incarico affidatogli e la garanzia del pieno rispetto delle vigenti disposizioni di legge, anche quelle in materia di trattamento dei dati e sicurezza delle informazioni.

Miglioramento

L'organizzazione si pone come obiettivo permanente il miglioramento delle prestazioni del proprio SGI. La preliminare valutazione dei rischi e delle opportunità connessi ai processi aziendali, le attività di verifica, interna ed esterna, e il riesame della Direzione sono gli strumenti che l'organizzazione mette in atto per migliorarsi costantemente. Lo strumento scelto per la persecuzione della propria Politica da parte dell'Organizzazione è il Sistema di Gestione Integrato per la Qualità e la Sicurezza delle Informazioni, conforme alle norme UNI EN ISO 9001 e UNI EN ISO 27001 integrate dei requisiti previsti da ISO 27017 e ISO 27018.

Riesami

La presente politica sarà riesaminata ogni qualvolta sarà necessario e comunque almeno una volta all'anno.

Perugia, 18 Novembre 2021

L'Amministratore Unico

Fortunato Bianconi



