UQIDO

Sistema di gestione per la sicurezza delle informazioni

Politica della sicurezza delle informazioni

Uqido srl

30/06/2023

Copia Controllata ☒

N. di copia_____

Redatto da	Approvato da	Data
Pierantonio Dainese Pastò	Pier Mattia Avesani	30/06/2023

Note di revisione		
Motivo revisione	**Numero**	**Data**
Prima Emissione	0	30/06/2023

1. Introduzione

Uqido srl, data la natura delle proprie attività, considera la qualità e la sicurezza delle informazioni un fattore irrinunciabile per la protezione del proprio patrimonio informativo ed un fattore di valenza strategica facilmente trasformabile in vantaggio competitivo.

Per questo motivo, la Direzione di Uqido srl ha definito, divulgato e si impegna a mantenere attiva a tutti i livelli della propria organizzazione la presente "politica" per l'implementazione di un Sistema di Gestione integrato della Qualità e della Sicurezza delle Informazioni, comprese le attività svolte tramite "cloud computing".

2. Scopo e Obiettivi

Lo scopo della presente policy è di garantire la qualità dei propri prodotti in accordo con quanto previsto dalla norma **ISO 9001:2015** nonchè la tutela e la protezione da tutte le minacce, interne o esterne, intenzionali o accidentali, delle informazioni nell'ambito delle proprie attività in accordo con le indicazioni fornite dallo standard **ISO/IEC 27001:2013** e dalle linee guida contenute nello standard **ISO/IEC 27002:2013**.

In questo modo Uqido srl vuole garantire un adeguato livello di qualità e di sicurezza dei dati e delle informazioni nell'ambito della progettazione, sviluppo ed erogazione dei servizi aziendali, attraverso l'identificazione, la valutazione ed il trattamento dei rischi ai quali i servizi stessi sono soggetti.

Il Sistema di Gestione integrato Qualità e Sicurezza delle Informazioni definisce un insieme di misure organizzative, tecniche e procedurali a garanzia del soddisfacimento dei sottoelencati requisiti di sicurezza di base delle informazioni:

- ***Riservatezza***, ovvero la proprietà dell'informazione di essere nota solo a chi ne ha i privilegi;
- ***Integrità***, ovvero la proprietà dell'informazione di essere modificata solo ed esclusivamente da chi ne possiede i privilegi;
- ***Disponibilità***, ovvero la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che ne godono i privilegi.

Inoltre, con la presente Politica, Uqido srl intende formalizzare i seguenti **obiettivi** nell'ambito della sicurezza delle informazioni:

- preservare al meglio l'immagine dell'azienda quale fornitore affidabile e competitivo;
- proteggere il proprio patrimonio informativo;
- evitare al meglio ritardi nella delivery;
- adottare le misure atte a garantire la fidelizzazione del personale e la sua professionalizzazione;
- rispondere pienamente alle indicazioni della normativa vigente e cogente;
- aumentare, nel proprio personale, il livello di sensibilità e la competenza sui temi della sicurezza.

3. Campo di applicazione

Questa politica si applica indistintamente a tutte le parti interessate, interne ed esterne all'organizzazione. La sua attuazione è obbligatoria a tutto il personale e deve essere inserita nella regolamentazione degli accordi con qualsiasi soggetto esterno che, a qualsiasi titolo, possa essere coinvolto con il trattamento di informazioni, l'uso del software di gestione, nonché il servizio di "cloud computing", rientranti nel campo di applicazione del Sistema di Gestione della Sicurezza delle Informazioni (**SGSI**), ovvero per tutti i dati provenienti dagli applicativi sviluppati dall'azienda.

Uqido srl consente la comunicazione e la diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali che devono avvenire nel rispetto delle regole e delle norme cogenti, nonché delle regole e dei livelli di sicurezza imposti dalla direzione aziendale, nell'ambito della riduzione dei rischi.

4. Contenuto della Politica

Il SGSI si applica a tutte le attività di analisi, progettazione, sviluppo e manutenzione, ai servizi e ai dati ad esse collegate: tutte le informazioni che vengono create o utilizzate da Uqido srl sono da salvaguardare e debbono essere protette, secondo la classificazione attribuita, dalla loro creazione, durante il loro utilizzo, fino alla loro eliminazione. Le informazioni debbono essere gestite in modo sicuro, accurato e affidabile e debbono essere prontamente disponibili per gli usi consentiti. È qui da intendersi con "utilizzo dell'informazione" qualsiasi forma di trattamento che si avvalga di supporti elettronici, cartacei o consenta, in una qualsiasi forma, la comunicazione verbale.

Relativamente all'ambito della progettazione e sviluppo, tale sistema prevede – in conformità alla norma ISO/IEC 27001:2013 – che il Responsabile per la Sicurezza della Informazioni svolga periodicamente un'analisi dei rischi che tenga in considerazione gli obiettivi strategici espressi nella presente Politica, degli incidenti eventualmente occorsi e dei cambiamenti strategici, di business e tecnologici avvenuti.

L'analisi dei rischi ha lo scopo di valutare il rischio associato ad ogni asset da proteggere rispetto alle minacce individuate. La Direzione condivide con il Responsabile della Sicurezza delle informazioni la metodologia da impiegare per la valutazione del rischio, approvando il relativo documento; nella relazione della metodologia, la Direzione partecipa anche alla definizione delle scale di valore da impiegare per valorizzare i parametri che concorrono alla valutazione del rischio.

In seguito alla elaborazione dell'analisi dei rischi, la Direzione valuta i risultati ottenuti accettando la soglia di rischio accettabile, il trattamento di mitigazione dei rischi oltre tale soglia e il rischio residuo in seguito al trattamento.

Tale analisi sarà ponderata anche rispetto al valore di business dei singoli beni da proteggere e dovrà identificare chiaramente le azioni da intraprendere, classificate secondo una scala di priorità che rispetti gli obiettivi aziendali, il budget a disposizione e la necessità di mantenere la conformità alle norme e alle leggi vigenti. Detta analisi dovrà essere effettuata anche a fronte di eventi che possano modificare il profilo di rischio complessivo del sistema.

5. Responsabilità

Tutto il personale che, a qualsiasi titolo, collabora con l'azienda è responsabile dell'osservanza di questa policy e della segnalazione di anomalie, anche non formalmente codificate, di cui dovesse venire a conoscenza.

Responsabile della Sicurezza delle Informazioni: si occupa della progettazione del Sistema di Gestione per la Sicurezza delle informazioni e, in particolare di:

- emanare tutte le procedure necessarie, ivi inclusa la tipologia di classificazione dei documenti affinché l'organizzazione aziendale possa condurre, in modo sicuro, le proprie attività;
- adottare criteri e metodologie per l'analisi e la gestione del rischio;
- suggerire le misure di sicurezza organizzative, procedurali e tecnologiche a tutela della sicurezza e continuità delle attività di Uqido srl;
- pianificare un percorso formativo, specifico e periodico in materia di sicurezza delle informazioni per il personale;
- controllare periodicamente l'esposizione dei servizi aziendali alle principali minacce;
- verificare gli incidenti di sicurezza e adottare le opportune contromisure;
- promuovere la cultura relativa alla sicurezza delle informazioni.

Tutti i soggetti esterni, che intrattengono rapporti con Uqido srl, devono garantire il rispetto dei requisiti di sicurezza esplicitati nella presente Politica per la Sicurezza, anche attraverso la sottoscrizione di un "**Patto per la Riservatezza**" all'atto del conferimento del conferimento d'incarico (quando questo tipo di vincolo non sia espressamente citato negli accordi).

6. Cloud computing

Per l'implementazione ed erogazione dei servizi in cloud, ai sensi della ISO/IEC 27017 e della ISO/IEC27018 e del Regolamento (UE) 2016/679, la Direzione si impegna ad adottare requisiti di sicurezza e di conformità normativa per garantire anche:

- la protezione dei dati personali degli interessati e che prendano in considerazione i rischi derivanti dal personale interno;
- la gestione sicura del multi-tenancy (condivisione dell'infrastruttura);
- l'accesso agli asset in cloud dei clienti da parte del personale del service provider;
- il controllo degli accessi (in particolare degli amministratori);
- le comunicazioni ai clienti in occasione di cambiamenti dell'infrastruttura;
- la sicurezza dei sistemi di virtualizzazione;
- la protezione e l'accesso dei dati dei clienti in ambiente cloud;
- la gestione del ciclo di vita degli account cloud dei clienti;
- la comunicazione dei data breach;
- le linee guida per la condivisione delle informazioni a supporto delle attività;
- la costante sicurezza sull'ubicazione fisica dei dati nei server in cloud.

Uqido srl in alcuni casi opera in qualità di Cloud Service Provider nei confronti dei propri clienti per offrire servizi in cloud computing in modalità SaaS. Per l'erogazione di detti servizi si avvale di propri fornitori nei confronti dei quali assume il ruolo di Cloud Service

Customer. Inoltre, può erogare servizi in cloud computing in modalità SaaS anche assumendo direttamente il ruolo di Cloud Service Customer nel caso in cui installi direttamente i suoi software su uno spazio cloud gestito e di proprietà del cliente.

Con riferimento ai propri clienti Uqido srl, ai sensi della ISO/IEC 27018 e in accordo con Regolamento (UE) 2016/679, agisce come Titolare ovvero come Responsabile del Trattamento, dichiarando il rispettivo status e i relativi obblighi che ne discendono nei contratti sottoscritti e nelle nomine a responsabile che Uqido srl prevede con i propri fornitori per lo svolgimento delle attività di trattamento.

A tal fine Uqido srl pone cura ed attenzione:

- alla corretta identificazione degli interessati dei dati personali che tratta;
- all'esattezza dei dati personali di cui viene in possesso;
- alla liceità dei trattamenti che esegue su tali dati;
- alla ponderata identificazione, valutazione e gestione di tutti i rischi connessi con i diversi trattamenti eseguiti, con eventuale esecuzione di valutazioni di impatto (DPIA), qualora fosse necessario;
- all'adozione di misure tecniche e organizzative adeguate (processi, strumenti e controlli idonei) per garantire, ed essere in grado di dimostrare, che ogni trattamento è effettuato conformemente alla normativa vigente in materia di protezione dei dati personali;
- all'adozione di criteri e metodi di "privacy by design" e "privacy by default" per la piena conformità ai dettami normativi;
- all'identificazione delle responsabilità e autorità coinvolte nella gestione dei dati personali trattati anche afferenti alle nomine pertinenti di DPO (Data Protection Officer), Delegati e Autorizzati al trattamento, Amministratori di Sistema, Responsabili del trattamento.

7. Riesame

Uqido srl verificherà periodicamente l'efficacia e l'efficienza del Sistema di Gestione per la Sicurezza delle Informazioni, garantendo l'adeguato supporto per l'adozione delle necessarie migliorie al fine di consentire l'attivazione di un processo continuo che controlli il variare delle condizioni o degli obiettivi di business aziendali al fine di garantire il suo corretto adeguamento.