Misure di Sicurezza delle Informazioni

Per Installazioni SaaS e On Premise

Q-Web srl | PMI INNOVATIVA
Via G. Dall'Armi, 27/1 - 30027 San Donà di Piave (VE)
+39 0421 307703 | info@qweb.eu | **www.qweb.eu**
Reg.Impr. di VE/C.F e P.iva 03222120275

ISO 9001:2015 – CERT. nº 82664
ISO 27001:2022 – CERT. nº 82665
ISO 27018:2016 – CERT. nº 82666
ISO 27017:2019 – CERT. nº 82667

Sommario

1. Introduzione **3**
2. Compliance e Certificazioni sulla Sicurezza delle Informazioni **4**
3. Competenze del personale **5**
4. Gestione dei Rischi e Opportunità **5**
5. Gestione dei Cambiamenti e delle Capacità **6**
6. Sicurezza Logica **6**
6.1. Archiviazione sicura delle Informazioni 6
6.2. Trasmissione sicura delle informazioni 6
6.3. Sicurezza della Rete 7
7. Sicurezza Fisica **7**
8. Sicurezza dei Fornitori di Servizi Cloud IaaS di Q-Web **8**
9. Sicurezza degli Applicativi e Sviluppo Sicuro **8**
10. Gestione delle Vulnerabilità **11**
11. Gestione degli Incidenti di Sicurezza **12**
12. Gestione dei Log **13**
13. Gestione delle Emergenze **13**
14. Service Level Agreement (SLA) **14**
15. Protezione dei dati personali **15**
16. Contatti Q-Web **17**

Q-Web srl | PMI INNOVATIVA
Via G. Dall'Armi, 27/1 - 30027 San Donà di Piave (VE)
+39 0421 307703 | info@qweb.eu | **www.qweb.eu**
Reg.Impr. di VE/C.F e P.iva 03222120275

CSQA
ISO 9001:2015 – CERT. nº 82664
ISO 27001:2022 – CERT. nº 82665
ISO 27018:2016 – CERT. nº 82666
ISO 27017:2019 – CERT. nº 82667

1. Introduzione

Q-Web Srl opera dal 2000 a fianco delle Aziende e della Pubblica Amministrazione, realizzando le migliori soluzioni di siti web, e-commerce, APP mobile, software web based e strategie di web marketing puntando su una forte specializzazione nella "Web Technology".
Grazie alla profonda conoscenza del mercato e alle numerose esperienze maturate con oltre 300 clienti e 800 progetti realizzati, l'azienda è in grado di prendersi cura dei clienti, elaborando la migliore strategia di comunicazione e di marketing per raggiungere obiettivi concreti e misurabili.

Q-Web Srl propone servizi e prodotti in linea con i suoi valori:

IDEE INNOVATIVE

Viviamo un'epoca in cui l'Innovazione è il principale "fattore di successo" di un'Impresa.
Q-Web realizza Siti Web graficamente attraenti e comunicativi, orientati al design, e sviluppa software e APP con tecnologie innovative per soluzioni personalizzate per ogni cliente.

UN TEAM SPECIALIZZATO

Il Team di QWEB è costituito da: Account Manager, Analisti Capoprogetto, Grafici e Web designer, Programmatori, CopyWriter, Social Media e Seo Specialist, continuamente allineati ed aggiornati sulle nuove tecnologie e sulle principali piattaforme.

ATTENZIONE AL CLIENTE

QWEB offre ai Clienti un servizio di consulenza e assistenza puntuale e tempestivo assicurando garanzia di funzionamento dei prodotti nel tempo. Il servizio di Help desk fornisce risposte e supporto in tempo reale, per soddisfare il Cliente e guadagnarsi la sua fedeltà nel tempo.

L'offerta per le Aziende è presentata all'interno di un catalogo disponibile all'interno del sito web https://www.qweb.eu/

L'offerta per la Pubblica Amministrazione è presentata attraverso il portale FacilePA disponibile all'interno del sito web https://www.facilepa.it/

Il documento presenta le misure per la sicurezza delle informazioni e la protezione dei dati personali messe in campo da Q-Web e dai fornitori dei servizi cloud dove pertinente.

Q-Web srl | PMI INNOVATIVA
Via G. Dall'Armi, 27/1 - 30027 San Donà di Piave (VE)
+39 0421 307703 | info@qweb.eu | **www.qweb.eu**
Reg.Impr. di VE/C.F e P.iva 03222120275

CSQA
ISO 9001:2015 – CERT. n° 82664
ISO 27001:2022 – CERT. n° 82665
ISO 27018:2016 – CERT. n° 82666
ISO 27017:2019 – CERT. n° 82667

2. Compliance e Certificazioni sulla Sicurezza delle Informazioni

Data la natura delle proprie attività, Q-Web considera la qualità e la sicurezza delle informazioni, inclusi i dati personali, un fattore irrinunciabile per la protezione del proprio patrimonio informativo e di quello affidatole dai clienti. Per questo motivo l'azienda ha sviluppato un Sistema di Gestione Integrato per Qualità e la Sicurezza delle Informazioni (SGQSI) definito secondo regole e criteri previsti dalle best practice e dagli standard internazionali di riferimento in conformità alle indicazioni delle seguenti norme internazionali:

- **ISO 9001** - "Quality Management System"
- **ISO/IEC 27001** - "Information Security Management System"
- **ISO/IEC 27017** – "Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services".
- **ISO/IEC 27018** - "Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors"

Il campo di applicazione è "**Progettazione, sviluppo, commercializzazione, manutenzione e assistenza di applicazioni software web e mobile oriented erogate in modalità SaaS e On Premise**".

Q-Web è sottoposta a valutazione di conformità da parte di CSQA, un ente di controllo di terza parte indipendente accreditato da Accredia, l'ente unico nazionale di accreditamento designato dal Governo italiano. I certificati emessi da CSQA sono riconosciuti a livello internazionale.

A livello normativo Q-Web è perfettamente allineata a tutte le leggi nazionali ed europee in merito alla sicurezza delle informazioni e protezione dei dati personali. Potrete trovare maggiori informazioni sulle compliance e sulle certificazioni di Q-Web nella pagina dedicata del sito web aziendale https://www.qweb.eu/it/chi-siamo/certificazioni/certificazioni.

Q-Web srl | PMI INNOVATIVA
Via G. Dall'Armi, 27/1 - 30027 San Donà di Piave (VE)
+39 0421 307703 | info@qweb.eu | **www.qweb.eu**
Reg.Impr. di VE/C.F e P.iva 03222120275

CSQA
ISO 9001:2015 – CERT. n° 82664
ISO 27001:2022 – CERT. n° 82665
ISO 27018:2016 – CERT. n° 82666
ISO 27017:2019 – CERT. n° 82667

3. Competenze del personale

Q-Web comunica regolarmente con il proprio personale circa gli obblighi esistenti relativi alla sicurezza delle informazioni, inclusi i dati dei clienti e sulla protezione dei dati personali. In dettaglio l'azienda si avvale dei seguenti canali di comunicazione:

- Attività di formazione annuali
- Attività di formazione all'atto dell'assunzione di nuovi dipendenti
- Attività di aggiornamento annuali per le figure di responsabilità
- Survey interne per misurare il livello di competenza/consapevolezza
- Email interne
- Cartellonistica

4. Gestione dei Rischi e Opportunità

La direzione di Q-Web ha sviluppato un piano aziendale strategico che include l'identificazione dei rischi e opportunità sulla sicurezza delle informazioni e l'implementazione di specifici trattamenti per mitigarli o perseguirli. Per quanto riguarda l'identificazione dei rischi e delle opportunità ogni anno vengono effettuate sessioni interne di valutazione da parte dei responsabili di area, valutazioni esterne da parte di società terze indipendenti o direttamente dai clienti per le loro infrastrutture in hosting.

L'analisi del rischio e delle opportunità viene condotta prendendo in esame gli scenari di rischi e opportunità per le informazioni relativamente a integrità, disponibilità e riservatezza, nel seguente modo:

- Elencando gli scenari di rischio e opportunità;
- Valutando per ognuno di essi:
    - il potenziale impatto negativo o positivo;
    - la probabilità di accadimento;
- Calcolando in questo modo il valore del rischio o opportunità.

Il valore del rischio o opportunità viene confrontato con i criteri di accettazione stabiliti dalla direzione di Q-Web e se necessario vengono identificate le contromisure da attuare per gestirlo.

Q-Web srl | PMI INNOVATIVA
Via G. Dall'Armi, 27/1 - 30027 San Donà di Piave (VE)
+39 0421 307703 | info@qweb.eu | **www.qweb.eu**
Reg.Impr. di VE/C.F e P.iva 03222120275

CSQA
ISO 9001:2015 – CERT. n° 82664
ISO 27001:2022 – CERT. n° 82665
ISO 27018:2016 – CERT. n° 82666
ISO 27017:2019 – CERT. n° 82667

5. Gestione dei Cambiamenti e delle Capacità

Le procedure di gestione dei cambiamenti di Q-Web assicurano che cambiamenti concordati agli applicativi e all'infrastruttura minimizzino gli impatti e gli incidenti rispetto i prodotti e i servizi erogati. Le politiche per la gestione sicura del cambiamento coinvolgono tutti i sistemi in gestione, come ad esempio: hardware, apparati di comunicazione e software, sistemi software, la documentazione e le procedure legate alla gestione, supporto e manutenzione degli ambienti di produzione. Ogni proposta di cambiamento è sempre progettata e verificata tra le parti per mezzo di specifici documenti di analisi tecnica e commerciale.

Le procedure di gestione della capacità di Q-Web assicurano la comprensione di tutti gli aspetti relativi alle prestazioni e capacità attuali dell'organizzazione e quelle future al fine di anticiparle e veicolarle secondo esigenze aziendali.

Il processo per la gestione delle capacità include i seguenti elementi:

- Comprensione della domanda di servizi attuale e previsione dei bisogni futuri;
- Capacità di influenzare la domanda di servizi e risorse;
- Comprensione degli obiettivi di Qualità e Sicurezza delle Informazioni;

Le risorse cloud di calcolo e di storage sono scalabili e possono essere ridimensionate in modo affidabile e flessibile a seconda della specifica esigenza.

6. Sicurezza Logica

6.1. Archiviazione sicura delle Informazioni

I dati gestiti da Q-Web in archiviazione sono sempre criptati con chiavi di cifratura sicure. Dietro specifico accordo contrattuale viene offerta la possibilità di utilizzare chiavi di proprietà dei clienti.

6.2. Trasmissione sicura delle informazioni

I dati trasmessi in entrata e in uscita dai sistemi gestiti da Q-Web vengono criptati attraverso protocolli sicuri quali ad esempio HTTPS, FTPS, VPN secondo specifica esigenza. Eventuali

Q-Web srl | PMI INNOVATIVA
Via G. Dall'Armi, 27/1 - 30027 San Donà di Piave (VE)
+39 0421 307703 | info@qweb.eu | **www.qweb.eu**
Reg.Impr. di VE/C.F e P.iva 03222120275

CSQA
ISO 9001:2015 – CERT. nº 82664
ISO 27001:2022 – CERT. nº 82665
ISO 27018:2016 – CERT. nº 82666
ISO 27017:2019 – CERT. nº 82667

eccezioni dovranno essere segnalate dal cliente fin dalle fasi iniziali del progetto e saranno soggette a proposte di riconversione sicura da parte di Q-Web.

6.3. Sicurezza della Rete

Le infrastrutture su cui poggiano gli applicativi gestiti da Q-Web sono progettate secondo elevati standard di sicurezza:

- Sistemi di configurazione iniziale automatici permettono di limitare rischi di errate implementazioni;
- Soluzioni di Firewall per la protezione del traffico in ingresso e in uscita;
- Sistemi di protezione per tentativi di attacco DDoS;
- Sistemi di monitoraggio, di log management e aggiornamento/applicazione di patch di sicurezza.

L'infrastruttura cloud, formata dai componenti hardware e software, le reti e le strutture che eseguono i servizi è tutelata dai fornitori cloud stessi per cui Q-Web ha sottoscritto specifici accordi contrattuali vincolanti in termini di sicurezza delle informazioni e protezione dei dati personali.

7. Sicurezza Fisica

I locali di Q-Web, con attenzione alle aree sicure contenenti dati di tipo riservato anche di tipo personale sono difesi dalle seguenti misure di sicurezza fisiche: accessi chiusi a chiave, muri, videosorveglianza, personale di sicurezza e altri dispositivi elettronici. Apposite procedure regolano le visite occasionali o regolari del personale esterno all'azienda. Il sistema di monitoraggio è sotto il presidio di Q-Web che controlla e garantisce gli accessi.

Q-Web è attenta anche ai fenomeni naturali come terremoti, alluvioni, eventi metereologici o incendi che possono causare rischi per la salute dei lavoratori e l'indisponibilità delle strutture; per questo effettua regolarmente sessioni di formazione al personale, prove di evacuazione e interventi migliorativi e del controllo funzionamento degli impianti speciali di sicurezza.

Q-Web srl | PMI INNOVATIVA
Via G. Dall'Armi, 27/1 - 30027 San Donà di Piave (VE)
+39 0421 307703 | info@qweb.eu | **www.qweb.eu**
Reg.Impr. di VE/C.F e P.iva 03222120275

CSQA
ISO 9001:2015 – CERT. n° 82664
ISO 27001:2022 – CERT. n° 82665
ISO 27018:2016 – CERT. n° 82666
ISO 27017:2019 – CERT. n° 82667

8. Sicurezza dei Fornitori di Servizi Cloud IaaS di Q-Web

I fornitori cloud di Q-Web che permettono la fornitura di servizi SaaS controllano rigorosamente l'accesso ai data center, anche nel caso di dipendenti interni. Le terze parti hanno accesso ai data center solo se espressamente autorizzati secondo specifiche policies di accesso. Prima di creare un data center i fornitori dedicano molto tempo all'analisi delle minacce potenziali e alla progettazione, implementazione e test dei controlli per verificare che sistemi, tecnologia e persone siano in grado di reagire ai rischi. Prima di scegliere una sede, sono eseguiti valutazioni ambientali e geografiche. Le posizioni dei data center sono attentamente selezionate per mitigare i rischi ambientali, come alluvioni, condizioni meteorologiche estreme e attività sismica. Le zone di disponibilità sono costruite per essere indipendenti e fisicamente separate l'una dall'altra.

Q-Web garantisce che i servizi IT e i sistemi operativi utilizzati vengono regolarmente aggiornati secondo i criteri e le tempistiche indicate dal produttore. I servizi IT di cui si avvale Q-Web utilizzano come meccanismo di sincronizzazione orario i server NTP di ServerPlan e più precisamente ntp.serverplan.com.

9. Sicurezza degli Applicativi e Sviluppo Sicuro

Q-Web propone applicativi proprietari e software di terze parti (es. CMS) integrandole ove necessario con funzionalità custom nel rispetto del copyright delle case produttrici.

Per tutti gli aspetti legati alla sicurezza degli applicativi di terze parti utilizzati si rimanda alla documentazione specifica di volta in volta pertinente rispetto a quanto presente all'interno degli accordi tra le parti e condiviso dal commerciale di riferimento.

Q-Web, nello sviluppare le modifiche agli applicativi, ne salvaguarda le caratteristiche di sicurezza intrinseche nel rispetto degli standard di sicurezza richiesti dai requisiti cogenti e contrattuali e più in generale seguendo le linee guida di sviluppo indicate dai produttori.

Q-Web srl | PMI INNOVATIVA
Via G. Dall'Armi, 27/1 - 30027 San Donà di Piave (VE)
+39 0421 307703 | info@qweb.eu | **www.qweb.eu**
Reg.Impr. di VE/C.F e P.iva 03222120275

CSQA
ISO 9001:2015 – CERT. nº 82664
ISO 27001:2022 – CERT. nº 82665
ISO 27018:2016 – CERT. nº 82666
ISO 27017:2019 – CERT. nº 82667

Per le attività di programmazione Q-Web si basa sull'approccio OWASP (Open Web Application Security Project), volto a diminuire il rischio di introdurre possibili vulnerabilità raggruppabili in 10 macro-categorie:

- *A01:2021-Broken Access Control moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than any other category.*

- *A02:2021-Cryptographic Failures shifts up one position to #2, previously known as Sensitive Data Exposure, which was broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise.*

- *A03:2021-Injection slides down to the third position. 94% of the applications were tested for some form of injection, and the 33 CWEs mapped into this category have the second most occurrences in applications. Cross-site Scripting is now part of this category in this edition.*

- *A04:2021-Insecure Design is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to "move left" as an industry, it calls for more use of threat modeling, secure design patterns and principles, and reference architectures.*

- *A05:2021-Security Misconfiguration moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration. With more shifts into highly configurable software, it's not surprising to see this category move up. The former category for XML External Entities (XXE) is now part of this category.*

- *A06:2021-Vulnerable and Outdated Components was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis. This category moves up from #9 in 2017 and is a known issue that we struggle to test and assess risk. It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores.*

Q-Web srl | PMI INNOVATIVA
Via G. Dall'Armi, 27/1 - 30027 San Donà di Piave (VE)
+39 0421 307703 | info@qweb.eu | **www.qweb.eu**
Reg.Impr. di VE/C.F e P.iva 03222120275

CSQA
ISO 9001:2015 – CERT. n° 82664
ISO 27001:2022 – CERT. n° 82665
ISO 27018:2016 – CERT. n° 82666
ISO 27017:2019 – CERT. n° 82667

- *A07:2021-Identification and Authentication Failures was previously Broken Authentication and is sliding down from the second position, and now includes CWEs that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of standardized frameworks seems to be helping.*

- *A08:2021-Software and Data Integrity Failures is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. Insecure Deserialization from 2017 is now a part of this larger category.*

- *A09:2021-Security Logging and Monitoring Failures was previously Insufficient Logging & Monitoring and is added from the industry survey (#3), moving up from #10 previously. This category is expanded to include more types of failures, is challenging to test for, and isn't well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.*

- *A10:2021-Server-Side Request Forgery is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it's not illustrated in the data at this time.*

In dettaglio, Q-Web adotta metodologie per lo sviluppo di applicazioni web e mobile per clienti PMI e Pubblica Amministrazione e richiamate da ACN - Agenzia per la cybersicurezza nazionale.

Gli ambienti di sviluppo sono sempre separati dagli ambienti di test e di produzione ove si potrebbero annidare dati riservati aziendali tra cui dati personali. Nel caso fosse necessario utilizzare fin dalle prime fasi di sviluppo dati similari ai dati reali sono predisposte in accordo con i clienti specifiche procedure di anonimizzazione.

Q-Web ha implementato automatismi collegati alla propria pipeline di sviluppo e rilascio che permettono di ispezionare continuamente la qualità e la sicurezza del codice in tutte le fasi di sviluppo e rilascio attraverso code reviewing e tool di verifica del software.

Q-Web srl | PMI INNOVATIVA
Via G. Dall'Armi, 27/1 - 30027 San Donà di Piave (VE)
+39 0421 307703 | info@qweb.eu | **www.qweb.eu**
Reg.Impr. di VE/C.F e P.iva 03222120275

CSQA
ISO 9001:2015 – CERT. n° 82664
ISO 27001:2022 – CERT. n° 82665
ISO 27018:2016 – CERT. n° 82666
ISO 27017:2019 – CERT. n° 82667

Ogni funzionalità concordata prima di essere rilasciata in ambiente di produzione deve passare positivamente diverse verifiche interne ed esterne. La procedura standard adoperata da Q-Web consiste in una fase preliminare di controllo da parte dello sviluppatore al termine della realizzazione, eventualmente supportato da tool di scan. La seconda fase di verifica consiste nel controllo da parte della Direzione / Ufficio Commerciale rispetto la rispondenza logica, funzionale e di layout di quanto sviluppato. L'ultima fase consiste in una ulteriore sessione di verifica logica/funzionale e di layout da parte del cliente stesso, il quale se ritiene sia tutto ok certifica il via libera al rilascio in produzione in una finestra temporale concordata. Ogni fase della presente procedura può essere modificata secondo esigenza dietro accordo specifico tra Q-Web e il Cliente.

10. Gestione delle Vulnerabilità

In Q-Web è operativo un processo continuo di identificazione, valutazione e rientro delle vulnerabilità dei sistemi informativi e delle applicazioni. Il processo di gestione delle vulnerabilità prevede le seguenti macro-attività principali:

- Stilare un inventario degli asset IT della società, classificati in base al livello di criticità, inclusi server, infrastrutture di rete, postazioni di lavoro, stampanti e applicazioni;
- Rilevare le vulnerabilità esistenti, segnalate dai fornitori o verificate internamente/esternamente dai clienti utilizzando scanner di rete, scanner delle vulnerabilità e software per i test di penetrazione automatizzati stabilendo di volta in volta livelli di rischio appropriati. Q-Web utilizza tool per effettuare scansioni di Vulnerabilità del codice sviluppato consigliati da OWASP;
- Valutazione tecnica della vulnerabilità rilevata rispetto a criteri di gravità, numero di sistemi impattati, disponibilità di upgrade, fix di sicurezza;
- Comunicazione ai clienti della vulnerabilità e di come Q-Web intende andare a mettere in sicurezza gli applicativi a tutte le parti interessate;
- Applicazione di patch di sicurezza e test successivi secondo logica di rilascio sicuro;
- Comunicazione di applicazione patch avvenuta con successo e registrazione misure correttive nella knowledge base in Confluence.

Q-Web srl | PMI INNOVATIVA
Via G. Dall'Armi, 27/1 - 30027 San Donà di Piave (VE)
+39 0421 307703 | info@qweb.eu | **www.qweb.eu**
Reg.Impr. di VE/C.F e P.iva 03222120275

CSQA
ISO 9001:2015 – CERT. n° 82664
ISO 27001:2022 – CERT. n° 82665
ISO 27018:2016 – CERT. n° 82666
ISO 27017:2019 – CERT. n° 82667

Il Cliente può procedere in autonomia a test di assessment di vulnerabilità non invasivi nei confronti degli applicativi offerti in modalità SaaS da Q-Web esclusivamente dopo averlo notificato con un preavviso di almeno 10 giorni lavorativi. Il Cliente non può procedere in autonomia a Penetration Test se non attraverso uno specifico accordo scritto sottoscritto tra le parti e solo dopo aver tutelato l'infrastruttura ove poggiano gli applicativi erogati da possibili incidenti di sicurezza correlati. Il Cliente risponderà di eventuali danni diretti e indiretti causati da tali attività.

11. Gestione degli Incidenti di Sicurezza

Q-Web ha istituito un processo per la pianificazione, preparazione e gestione dell'organizzazione nell'eventualità di un incidente relativo alla sicurezza delle informazioni. Il processo di gestione degli incidenti relativi alla sicurezza delle informazioni comprende un insieme dettagliato di attività volte a prevenire, scoprire e mitigare l'impatto di un evento che possa compromettere la disponibilità, l'integrità, la riservatezza delle informazioni.

Figure adeguatamente formate in Q-Web si occupano di valutare quali eventi si possono concretamente definire come Incidenti sulla Sicurezza delle Informazioni e gestirli nella loro totalità fino alla piena risoluzione e verbalizzazione finale. In caso di Incidenti a elevato impatto, tramite logiche interne di escalation, si attivano misure di gestione delle emergenze descritte all'interno del paragrafo successivo. In caso di data breach si attivano le specifiche procedure di notifica tra le parti secondo le modalità pattuite.

La segnalazione di possibili incidenti relativi alla sicurezza delle informazioni può giungere da fonti differenti: dai partner, da un sistema di monitoraggio anti intrusione, da un dipendente o dai clienti stessi. In caso di presunto o accertato incidente per cui non sia stata data ancora nessuna comunicazione, Q-Web richiede a tutti i suoi clienti di darne una immediata notifica attraverso i canali di ticketing concordati tra le parti.

Q-Web srl | PMI INNOVATIVA
Via G. Dall'Armi, 27/1 - 30027 San Donà di Piave (VE)
+39 0421 307703 | info@qweb.eu | **www.qweb.eu**
Reg.Impr. di VE/C.F e P.iva 03222120275

CSQA
ISO 9001:2015 – CERT. nº 82664
ISO 27001:2022 – CERT. nº 82665
ISO 27018:2016 – CERT. nº 82666
ISO 27017:2019 – CERT. nº 82667

12. Gestione dei Log

Q-Web ritiene che sia cruciale per la salvaguardia delle informazioni trattate per conto dei suoi clienti porre il focus non solo sulle attività di prevenzione e gestione dei problemi di sicurezza ma anche sul sistema di log management posto in essere per comprendere gli eventi negativi dopo che questi si sono verificati. I log, sono asset fondamentali per far fronte efficacemente alle necessità di data protection, alla continuità di servizio e per garantire la compliance aziendale rispetto le normative in vigore in ambito nazionale e internazionale.

I sistemi di log implementati da Q-Web includono sempre le informazioni sul chi e quando ha fatto una determinata operazione e sono mantenuti inalterabili.

Nel rispetto del provvedimento del 27 novembre 2008 del Garante per la Privacy italiano, Q-Web mantiene secondo gli stessi principi anche i log degli amministratori di sistema.

13. Gestione delle Emergenze

Se un Incidente sulla sicurezza delle informazioni ha impatti rilevanti in termini di riservatezza, disponibilità e integrità delle informazioni vengono attivati tramite escalation specifici processi di gestione delle emergenze. Il processo di gestione delle emergenze è un processo basato su tecniche di continuità operativa, disaster recovery e di pubbliche relazioni nei confronti di clienti, fornitori, autorità, altre parti interessate e mezzi di informazione.

Q-Web anche in fase di crisi mette in campo tutte le misure e le procedure volte a garantire la continuità delle operazioni relative alla sicurezza delle informazioni. In termini operativi Q-Web si occupa:

- della disponibilità delle informazioni con opportune ridondanze;
- della continuità dei processi di sicurezza delle informazioni, tra cui: controllo degli accessi, controllo degli archivi fisici e dei sistemi informatici, monitoraggio, gestione degli incidenti;
- della gestione completa dei backup i quali sono ridondati, criptati e ne è verificato periodicamente il restore.

Q-Web srl | PMI INNOVATIVA
Via G. Dall'Armi, 27/1 - 30027 San Donà di Piave (VE)
+39 0421 307703 | info@qweb.eu | **www.qweb.eu**
Reg.Impr. di VE/C.F e P.iva 03222120275

CSQA
ISO 9001:2015 – CERT. n° 82664
ISO 27001:2022 – CERT. n° 82665
ISO 27018:2016 – CERT. n° 82666
ISO 27017:2019 – CERT. n° 82667

Per eventuali ulteriori informazioni si rimanda ai canali di contatto con il commerciale di riferimento.

14. Service Level Agreement (SLA)

Nella tabella seguente sono indicati gli standard minimi di servizio che Q-Web si impegna a mantenere per tutta la durata deIIa fornitura:

PARAMETRO	TARGET MINIMO SLA
Disponibilità del servizio di hosting su base annuale (sito accessibile sulla rete internet)	99,9%
Backup e messa in sicurezza dati/documenti	24 ore
Tempo di recupero dati	24 ore

Q-Web srl | PMI INNOVATIVA
Via G. Dall'Armi, 27/1 - 30027 San Donà di Piave (VE)
+39 0421 307703 | info@qweb.eu | **www.qweb.eu**
Reg.Impr. di VE/C.F e P.iva 03222120275

CSQA
ISO 9001:2015 – CERT. n° 82664
ISO 27001:2022 – CERT. n° 82665
ISO 27018:2016 – CERT. n° 82666
ISO 27017:2019 – CERT. n° 82667

Copertura oraria dei servizi di manutenzione e assist enza	Dal **lunedì al venerdì**, dalle **8:30** alle **13:00** e dalle **14:00** alle **17:30**. Intervento su ticket riconducibile ad interventi di manutenzione ordinaria e sistemistica per risolvere: 1. **ANOMALIA BLOCCANTE**, ovvero un'anomalia che renda impossibile l'utilizzo del sito web del Committente e dei servizi collegati 2. **ANOMALIA NON BLOCCANTE**, ovvero un'anomalia che, pur causando un'interruzione/riduzione della continuità/qualità di un servizio, non impedisca l'utilizzo dell'applicativo del Committente e dei servizi collegati. La presa in carico delle anomalie occorse in orario **lunedì - venerdì** dalle **8:30** alle **13:00** e dalle **14:00** alle **17:30** deve avvenire **entro 2 ore dalla segnalazione** e in caso di: 1. **ANOMALIA BLOCCANTE**, la risoluzione deve avvenire **entro 6 ore** dalla presa in carico; 2. **ANOMALIA NON BLOCCANTE**, la risoluzione deve avvenire **entro 24 ore** dalla presa in carico. Intervento su ticket riconducibile a richieste estemporanee di interventi di assistenza, funzionali alle esigenze operative e che non richieda sviluppi applicativi: · **presa in carico entro 12 ore lavorative** dalla segnalazione; · valutazione e pianificazione dell'intervento **entro 18 ore** dalla presa in carico.

15. Protezione dei dati personali

Per Q-Web è fondamentale definire fin da subito il perimetro dei dati personali trattati all'interno dei sistemi forniti. Attenzione verrà posta alle situazioni dove si potrebbero annidate dati personali particolari e giudiziari secondo la definizione degli Articoli 9 e 10 del Regolamento UE 2016/679. Tali elementi devono essere valutati attentamente in fase di prevendita.

Q-Web srl | PMI INNOVATIVA
Via G. Dall'Armi, 27/1 - 30027 San Donà di Piave (VE)
+39 0421 307703 | info@qweb.eu | **www.qweb.eu**
Reg.Impr. di VE/C.F e P.iva 03222120275

CSQA
ISO 9001:2015 – CERT. n° 82664
ISO 27001:2022 – CERT. n° 82665
ISO 27018:2016 – CERT. n° 82666
ISO 27017:2019 – CERT. n° 82667

I Clienti di Q-Web risultano Titolari del Trattamento dei dati personali trattati e Q-Web Responsabile del Trattamento. Tra i due soggetti, ai sensi dell'Art. 28 paragrafo 3 del GDPR, è necessaria la stipula di un atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Q-Web ha predisposto un template di nomina responsabile del trattamento che sarà inoltrato dal commerciale di riferimento al momento della stipula del contratto. Eventuali modelli di accordo alternativi devono essere validati dalle parti.

Ai sensi dell'Art. 28 paragrafo 2 il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

Q-Web condivide la lista dei subfornitori pertinenti e concordati tra le parti. Con tali subfornitori, Q-Web ha sottoscritto a sua volta specifici accordi di data processing agreement. Eventuali trattamenti Extra-UE trattamenti sono effettuati nel rispetto delle leggi dell'UE.

Q-Web, in riferimento ai servizi di consulenza erogati, in seguito a periodiche valutazioni d'impatto sulla protezione dei dati e per mezzo del suo sistema di gestione per la sicurezza delle informazioni ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018, mette in atto di volta in volta il set di misure di sicurezza adeguate per garantire ai propri clienti il mantenimento dei principi di riservatezza, integrità, disponibilità delle informazioni e la protezione dei dati personali. Eventuali misure di sicurezza aggiuntive devono essere valutate attentamente in fase di prevendita. Inoltre, Q-Web dietro approfondita valutazione e specifici accordi contrattuali garantisce la conformità dei sistemi rispetto ai diritti dell'interessato di cui al capo III del regolamento UE 2016/679.

Q-Web si impegna a non utilizzare, modificare o rivelare a nessuno, a meno che non indicato dal cliente, i dati relativi ai suoi clienti. Q-Web si impegna a non accedere agli account dei propri clienti, inclusi i dati relativi al cliente, se non per motivi di manutenzione del servizio, per anticipare o rispondere a problematiche tecniche o relative all'assistenza, su richiesta del cliente in connessione a un problema di supporto o quando richiesto dalla legge. Ove quindi sorgesse la

Q-Web srl | PMI INNOVATIVA
Via G. Dall'Armi, 27/1 - 30027 San Donà di Piave (VE)
+39 0421 307703 | info@qweb.eu | **www.qweb.eu**
Reg.Impr. di VE/C.F e P.iva 03222120275

CSQA
ISO 9001:2015 – CERT. nº 82664
ISO 27001:2022 – CERT. nº 82665
ISO 27018:2016 – CERT. nº 82666
ISO 27017:2019 – CERT. nº 82667

necessità, l'accesso da parte del personale di Q-Web avverrà tramite credenziali che rispettano le policies minime di sicurezza e secondo specifico profilo di autorizzazione.

In caso di violazione dei dati personali (di seguito "Data Breach"), Q-Web, ai sensi dell'Art. 28 paragrafo 3 lettera f) e ai sensi dell'Art. 33 paragrafo 2 del GDPR, al fine di assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli 33, 34 notificherà la violazione al Titolare del Trattamento entro i termini di legge o viceversa i termini concordati all'interno dei contratti pattuiti o in un altro documento alternativo definito tra le parti rispetto il momento in cui si è venuti a conoscenza della violazione. In parallelo, Q-Web opererà ad adottare tempestivamente tutte le azioni correttive necessarie ad impedire ulteriori violazioni e a minimizzare gli effetti negativi.

16. Contatti Q-Web

Per qualsiasi necessità in ambito Sicurezza delle Informazioni e Protezione dei dati personali in QWeb sono attivi e disponibili i seguenti punti di contatto:

- **Email**: amministrazione@qweb.eu
- **Tel**: +39 0421 307703
- **Tel**: +39 0421 1896112

Nonché i punti di contatto già a disposizione del commerciale di Q-Web di riferimento.

Q-Web srl | PMI INNOVATIVA
Via G. Dall'Armi, 27/1 - 30027 San Donà di Piave (VE)
+39 0421 307703 | info@qweb.eu | **www.qweb.eu**
Reg.Impr. di VE/C.F e P.iva 03222120275

ISO 9001:2015 – CERT. nº 82664
ISO 27001:2022 – CERT. nº 82665
ISO 27018:2016 – CERT. nº 82666
ISO 27017:2019 – CERT. nº 82667