DPA.000.24 – ALLEGATO III

CONTROLLI NORMA UNI CEI EN ISO/IEC 27017:2021

Misure tecniche e organizzative per garantire la sicurezza dei dati (in vigore dal 26/03/2026)

Il presente allegato contiene la descrizione delle misure tecniche e organizzative messe in atto dal/dai Fornitore/i del trattamento per garantire un adeguato livello di sicurezza, tenuto conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche.

NR	CONTROLLO	I NOSTRI CONTROLLI	STRUMENTI E FUNZIONALITÀ A DISPOSIZIONE DEL CLIENTE
5.1.1	Policies for information security	**Politiche del Sistema di Gestione della Sicurezza delle Informazioni:** Datalite ha definito la propria Politica di sicurezza delle Informazioni aggiornata periodicamente e pubblicata sul proprio sito web.	https://datalite.it/
6.1.1	Information security roles and responsibili ties	**Ruoli e responsabilità:** All'interno dell'ambito di responsabilità di Datalite come fornitore di soluzioni SaaS/PaaS, Datalite ha definito le figure, i ruoli, le competenze e le responsabilità connesse ai processi, secondo i principi di segregation of duties, least privilege e dual control. **Segregation of Duties (SoD)** - Nell'ambito dei processi operativi dei servizi, una sequenza di procedure viene svolta da diverse persone, mai una sola, a garanzia che il controllo dell'intero processo non sia affidato ad un singolo individuo. **Least privilege** - I permessi di accesso a locali, apparati, dati, funzionalità, ecc. sono concessi, al personale addetto ai servizi, secondo il principio del "least privilege" ossia nella misura necessaria affinché tali risorse possano svolgere i compiti loro assegnati, ma non oltre. **Dual control** - Le procedure più critiche dal punto di vista della sicurezza prevedono il concorso di almeno due persone.	Indirizzo mail dedicato all'assistenza supporto@datalite.it
6.1.3	Contact with authorities	**Contatti con le autorità:** Datalite è in contatto costante con le autorità competenti la materia di sicurezza delle informazioni e protezione dei dati. GARANTE PRIVACY ACN	Datalite ha nominato un DPO raggiungibile tramite mail: privacy@datalite.it
7.2.2	Information security awareness, education and training	**Formazione del personale:** il personale di Datalite e i sub-appaltatori addetti al servizio hanno adeguata competenza ed esperienza, e viene loro fornito o richiesto un addestramento specifico a fronte di ogni importante aggiornamento dei sistemi. **Consapevolezza (Awareness):** periodicamente, il personale di Datalite viene sensibilizzato sulle tematiche di sicurezza, sul cybercrime in generale e sulle best practice da adottare, mediante specifici corsi di formazione. Ai sub-appaltatori viene richiesto quale requisito essenziale per poter collaborare con Datalite. **Non Disclosure Agreement (NDA):** ai nuovi assunti e ai sub-appaltatori viene richiesto di sottoscrivere un accordo di confidenzialità al fine di tutelare il know-how aziendale e le informazioni trattate nell'ambito della collaborazione.	

8.1.1	Inventory of assets	**Inventario Asset:** all'interno di Datalite è presente un inventario aggiornato degli asset, al cui interno è censita l'infrastruttura fisica e virtuale e la loro collocazione. Datalite testa e censisce l'hardware e il software autorizzato all'inserimento nell'infrastruttura aggiornato l'inventario al termine delle nuove installazioni. Ogni asset è classificato per tipologia di informazioni trattate e caratteristiche tecniche, nonché relativi responsabili.	
8.2.2	Labelling of information	**Etichettatura delle informazioni:** Datalite adotta un sistema per etichettare le informazioni in base alla classificazione definita nelle proprie procedure.	I Prodotti SaaS offerti da Datalite non prevedono per il Cliente la possibilità di classificare o etichettare le informazioni e le risorse associate.
9.1.2	Access to networks and network services	**Controlli di accesso:** il personale di Datalite che accede alle risorse è stato autorizzato. Prima di accedere ai sistemi interni, viene chiesto al personale che ne ha diritto di identificarsi e di autenticarsi (tramite nome utente, password). Il personale Datalite può accedere, previa autenticazione, alle sole risorse per cui è stato autorizzato.	
9.2.1	User registration and deregistrati on	Alla fornitura di un servizio, Datalite crea le utenze necessarie all'utilizzo del servizio SaaS, le cui password sono modificabili in autonomia dall'utente.	
9.2.2	User access provisioning	Ogni Prodotto SaaS di Datalite prevede la gestione degli accessi.	
9.2.3	Manageme nt of privileged access rights	**Gestione dei privilegi di accesso:** i Prodotti SaaS di Datalite gestisce l'accesso per i Clienti tramite il sistema proprietario del prodotto che si basa su username e password e facoltativamente OTP	
9.2.4	Manageme nt of secret authenticati on information of users	**Password policy** - Coerentemente con le policy di sicurezza di Datalite e nel rispetto della normativa vigente, è applicata una politica sicura di gestione delle password.	Al Cliente vengono fornite istruzioni dirette o tramite il manuale di prodotto.
9.4.4	Use of privileged utility programs	**Utilizzo di programmi di utilità privilegiati:** in conformità alle policy della norma ISO 27001, Datalite ha definito una politica di uso dei programmi di utilità privilegiata, autorizzato gli utenti abilitati, definendo e censendo i programmi autorizzati.	
10.1.1	Policy on the use of cryptograph ic controls	**Canale sicuro SSL** - I flussi di dati da/verso i sistemi, sono protetti da canale sicuro SSL, mediante opportuna configurazione sui server, tale da assicurare: autenticazione del server e la cifratura della sessione. Questo vale sia per i flussi originati in modo interattivo (web browsing) sia per quelli generati in modo automatico (es. utilizzo di API di servizi terzi).	

10.1.2	Key manageme nt	Le chiavi crittografiche eventualmente utilizzate da Datalite sono conservate all'interno del Cloud. **Policy:** Datalite ha definito internamente una politica per l'uso della crittografia.	
11.2.7	Secure disposal or reuse of equipment	Alla conclusione del contratto di un Prodotto SaaS, Datalite provvede alla cancellazione e rimozione definitiva dei dati del Cliente come da accordi contrattuali e comunicandolo al cliente a mezzo pec.	
12.1.2	Change manageme nt	I cambiamenti resi necessari dalle circostanze tecniche e di gestione vengono gestiti in modo controllato per permettere di verificarne i risultati e di mantenere traccia delle attività svolte.	Per le attività impattanti sul servizio Datalite informa i propri clienti mediante comunicazioni mail preventive.
12.1.3	Capacity manageme nt	Al fine di garantire la corretta erogazione del servizio, Datalite monitora costantemente il proprio Cloud e tutte le risorse di cui dispone, analizzando le capacità e adottando gli opportuni accorgimenti per lo sfruttamento ottimale delle stesse e per assicurare la normale fruizione dei Prodotti SaaS/PaaS.	
12.3.1	Information backup	Backup delle informazioni: la struttura dei backup, i controlli, la verifica, i test, sono a carico di Datalite che garantisce al Cliente la conservazione di un backup: - Degli ultimi 30 giorni - Di un backup al mese per 12 mesi Inoltre, le componenti funzionali all'erogazione dei servizi di Datalite, la gestione degli utenti e le altre componenti architetturali seguono le procedure di backup definite a livello aziendale e vengono periodicamente verificate e testate. I sistemi di backup prevedono sistemi di notifica in caso di problemi.	Il Cliente non dispone dei backup eseguiti da Datalite, ma ne può richiedere copia ad Datalite in qualsiasi momento.
12.4.1	Event logging	Log applicazioni: la soluzione SaaS, erogata da Datalite, dispone di un proprio Log	
12.4.3	Administrat or and operator logs	Log applicazioni: la soluzione SaaS, erogata da Datalite, dispone di un proprio Log attivabile	
12.4.4	Clock syncronizati on	Sincronizzazione – Datalite utilizza il sistema NTP per sincronizzare gli orologi dei propri asset fisici e virtuali e mantenere coerenza degli eventi. La fonte per la sincronizzazione dell'orologio è 2.debian.pool.ntp.org	
12.6.1	Administrat or and operator logs	Processo di Vulnerability Management – Il perimetro Datalite, composto dal Cloud e i prodotti SaaS, viene regolarmente scansionato da strumenti automatici e da professionisti qualificati del settore al fine di identificare ogni possibile vulnerabilità anche solo potenziale. Le criticità individuate vengono segnalate al responsabile competente, dando il via al ciclo di risoluzione della problematica che può concludersi con un nuovo rilascio oppure con una mitigazione. Per verificarne l'efficacia, si esegue infine una nuova scansione per avere la certezza del rientro della vulnerabilità.	Il Cliente può segnalare eventuali Vulnerabilità riscontrate tramite mail all'indirizzo teamsoc@datalite.it

13.1.3	Segregation in network	Datalite, in conformità con gli standard di sicurezza internazionali, garantisce la segregazione dell'accesso dei Clienti rispetto agli accessi interni degli operatori di Datalite. Inoltre, Datalite assicura un'efficace separazione degli ambienti in configurazione multi- tenant, a tutela della riservatezza e dell'integrità dei dati di ciascun Cliente.	
14.1.1	Information security requirement s analysis and specification	Datalite informa i propri Clienti mediante il presente documento e mediante il contratto.	Datalite ha nominato un DPO raggiungibile tramite mail: privacy@datalite.it
14.2.1	Secure developme nt policy	Datalite adotta le Linee Guida AGID e la metodologia OWASP come riferimenti fondamentali per lo sviluppo dei propri prodotti, garantendo così standard elevati di qualità e sicurezza.	
15.1.1	Secure developme nt policy	Il Cloud Datalite è locato in Italia presso un'infrastruttura di cloud computing avanzata che fornisce servizi scalabili, sicuri e distribuiti a livello nazionale, e ridondati per garantirne la disponibilità (Provider IaaS: Zucchetti S.p.A.)	
15.1.2	Addressing security within supplier agreements	Le soluzioni SaaS di Datalite prevedono l'accettazione delle condizioni contrattuali al cui interno sono specificate le responsabilità di Datalite e del Cliente.	
15.1.3	Information and communica tion technology supply chain	Il Cloud Datalite è locato in Italia presso un'infrastruttura di cloud computing avanzata che fornisce servizi scalabili, sicuri e distribuiti a livello nazionale, e ridondati per garantirne la disponibilità.	
16.1.1	Responsibili ties and procedures	Le soluzioni SaaS di Datalite prevedono l'accettazione delle condizioni contrattuali al cui interno sono specificate le responsabilità di Datalite e del Cliente.	Il Cliente può segnalare eventuali Incidenti di Sicurezza tramite mail all'indirizzo teamsoc@datalite.it In caso di Data Breach, Il Cliente può contattare il DPO designato da Datalite scrivendo una e-mail all'indirizzo privacy@datalite.it
16.1.2	Reporting information security events	Datalite mette a disposizione un indirizzo mail, oltra al numero telefonico, tramite cui aprire segnalazioni per qualsiasi problematica o richiesta.	Il Cliente può segnalare eventi di sicurezza tramite mail all'indirizzo teamsoc@datalite.it
16.1.7	Collection of evidence	Datalite collaborerà con il Cliente per rispondere ad eventuali richieste di evidenze e/o prove da parte delle autorità fornendo all'occorrenza log o altre tipologie di evidenze come specificato nelle condizioni generali del servizio.	

18.1.1	Identification of applicable legislation and contractual requirements	Legge Italiana, Diritto d'autore, GDPR e Codice Privacy e Provvedimenti del Garante, Norme ISO 9001 | 27001 | 27017 | 27018 I NIS2	
18.1.2	Intellectual property rights	La proprietà intellettuale dei prodotti SaaS è soggetta al diritto d'autore italiano ed è di Datalite Srl, Zucchetti Spa	Il Cliente può segnalare eventi reclami sulla proprietà intellettuale tramite mail all'indirizzo supporto@datalite.it
18.1.3	Protection of records	Datalite fornisce indicazioni sulla protezione dei dati tramite informativa privacy e nomina a Responsabile del trattamento firmata nella fase di definizione contrattuale.	Allegato I, II alle condizioni generali e nomina apposita.
18.1.5	Regulation of cryptograph ic controls	Canale sicuro SSL - I flussi di dati da/verso i sistemi, sono protetti da canale sicuro SSL, mediante opportuna configurazione sui server, tale da assicurare: autenticazione del server e la cifratura della sessione. Questo vale sia per i flussi originati in modo interattivo (web browsing) sia per quelli generati in modo automatico (es. utilizzo di API di servizi terzi).	
18.2.1	Independen t review of information security	Datalite sottopone i propri sistemi e relativi sistemi di gestione ad audit periodici effettuati da Enti di Certificazione. Queste informazioni possono essere richieste dal Cliente in casi di necessità.	
CLD 6.3.1	Shared roles and responsibili ties within a cloud computing environmen t	Datalite è responsabile della sicurezza del Cloud e dei prodotti SaaS.	
CLD 8.1.5	Removal of cloud service customer assets Control	Alla conclusione del contratto di un Prodotto SaaS, Datalite provvede alla cancellazione e rimozione definitiva dei dati del Cliente come da accordi contrattuali e comunicandolo al cliente a mezzo PEC. Datalite gestisce con un processo definito la cancellazione periodica dei file temporanei dei propri sistemi cloud.	
CLD 9.5.1	Segregation in virtual computing environmen ts	Datalite, in conformità con gli standard di sicurezza internazionali, garantisce la segregazione dell'accesso dei Clienti rispetto agli accessi interni degli operatori di Datalite. Inoltre, Datalite assicura un'efficace separazione degli ambienti in configurazione multi- tenant, a tutela della riservatezza e dell'integrità dei dati di ciascun Cliente.	
CLD 9.5.2	Virtual machine hardening	Datalite, in conformità agli standard internazionali di sicurezza, adotta procedure collaudate per la configurazione di ogni nuovo ambiente, fisico o virtuale, o nuovo servizio.	
CLD 12.1.5	Administrat or's operational security	Datalite programma le attività critiche sui propri sistemi, comunicando preventivamente tramite mail ai propri clienti.	

CLD 12.4.5	Monitoring of Cloud Services	Datalite monitora i propri servizi informando i clienti su eventi rilevanti che possano compromettere o possano aver compromesso il servizio.	All'interno del Servizio SaaS è presente una sezione di avvisi con cui Datalite comunica eventuali disservizi agli utilizzatori
CLD 13.1.4	Alignment of security manageme nt for virtual and physical networks	Datalite ha definito le politiche di configurazione delle reti fisiche e virtuali.	

DPA.000.24 - ALLEGATO III

CONTROLLI NORMA UNI CEI EN ISO/IEC 27017:2021

Misure tecniche e organizzative per garantire la sicurezza dei dati (in vigore dal 26/03/2026)

NR	CONTROLLO	I NOSTRI CONTROLLI	STRUMENTI E FUNZIONALITÀ A DISPOSIZIONE DEL CLIENTE
5.1.1	Policies for information security	Politiche del Sistema di Gestione della Sicurezza delle Informazioni: Datalite ha definito la propria Politica di sicurezza delle Informazioni aggiornata periodicamente e pubblicata sul proprio sito web	https://datalite.it/
6.1.1	Information security roles and responsibilities	Datalite ha nominato un DPO raggiungibile tramite mail privacy@datalite.it	Mail DPO privacy@datalite.it
7.2.2	Information security awareness, education and training	Formazione del personale: il personale di Datalite e i sub-appaltatori addetti al servizio hanno adeguata competenza ed esperienza, e viene loro fornito o richiesto un addestramento specifico a fronte di ogni importante aggiornamento dei sistemi. Consapevolezza (Awareness): periodicamente, il personale di Datalite viene sensibilizzato sulle tematiche di sicurezza, sul cybercrime in generale e sulle best practice da adottare, mediante specifici corsi di formazione. Ai sub-appaltatori viene richiesto quale requisito essenziale per poter collaborare con Datalite. Non Disclosure Agreement (NDA): ai nuovi assunti e ai sub-appaltatori viene richiesto di sottoscrivere un accordo di confidenzialità al fine di tutelare il know-how aziendale e le informazioni trattate nell'ambito della collaborazione.	
9.2	User access management	Alla fornitura di un servizio, Datalite crea le utenze necessarie all'utilizzo del servizio SaaS, le cui password sono modificabili in autonomia dall'utente.	
9.2.1	User registration and de-registration	Alla fornitura di un servizio, Datalite crea le utenze necessarie all'utilizzo del servizio SaaS, le cui password sono modificabili in autonomia dall'utente.	
9.4.2	Secure log-on procedures	L'accesso al servizio avviene tramite credenziali di accesso o sistema di autenticazione con OTP	
10.1.1	Policy on the use of cryptographic controls	Canale sicuro SSL - I flussi di dati da/verso i sistemi, sono protetti da canale sicuro SSL, mediante opportuna configurazione sui server, tale da assicurare: autenticazione del server e la cifratura della sessione. Questo vale sia per i flussi originati in modo interattivo (web browsing) sia per quelli generati in modo automatico (es. utilizzo di API di servizi terzi).	
11.2.7	Secure disposal or re-use of equipment	Alla conclusione del contratto di un Prodotto SaaS, Datalite provvede alla cancellazione e rimozione definitiva dei dati del Cliente come da accordi contrattuali e comunicandolo al cliente a mezzo PEC. Datalite gestisce con un processo definito la cancellazione periodica dei file temporanei dei propri sistemi cloud.	

12.1.4	Separation of development, testing and operational environments	Eventuali test necessari, effettuati da Datalite avvengono esclusivamente nel perimetro Datalite, in appositi sistemi dedicati per garantire la protezione dei dati personali e delle informazioni.	
12.3.1	Information backup	Backup delle informazioni: la struttura dei backup, i controlli, la verifica, i test, sono a carico di Datalite che garantisce al Cliente la conservazione di un backup: o Degli ultimi 30 giorni o Di un backup al mese per 12 mesi Inoltre, le componenti funzionali all'erogazione dei servizi di Datalite, la gestione degli utenti e le altre componenti architetturali seguono le procedure di backup definite a livello aziendale e vengono periodicamente verificate e testate. I sistemi di backup prevedono sistemi di notifica in caso di problemi.	
12.4.1	Event logging	Log applicazioni: la soluzione SaaS, erogata da Datalite, dispone di un proprio Log	
12.4.2	Protection of log information	Datalite attua tutte le misure di sicurezza necessarie per la protezione delle informazioni di Log contenenti dati personali.	
13.2.1	Information transfer policies and procedures	Datalite ha definito una politica di trasferimento delle informazioni tramite canali di comunicazione sicuri.	
16.1	Management of information security incidents and improvements	Datalite coopererà con il Cliente nel caso di segnalazioni di incidenti di sicurezza delle informazioni, implementando controlli e apportando con rapidità i miglioramenti necessari affinché non riaccadano.	Il Cliente è responsabile dei dati personali contenuti nei prodotti SaaS
16.1.1	Responsibilities and procedures	Datalite ha definito le procedure per la gestione degli incidenti di sicurezza, con eventuale registrazione del Data Breach e relativa notifica al Garante e agli interessati (se previsto). A seguito di ogni incidente Datalite adotta procedure di miglioramento atte a evitare incidenti successivi.	
18.2.1	Independent review of information security	Datalite è certificata secondo lo schema della norma ISO UNI CEI EN ISO/IEC 27001:2022 con l'estensione dei controlli delle norme ISO UNI CEI EN ISO/IEC 27017 e 27018 ed è sottoposta periodicamente ad Audit di verifica da parte dell'Ente di Certificazione	
A.2.1	Obligation to co-operate regarding PII principals' rights	Datalite rende disponibile ai propri clienti l'informativa privacy e relativo modello di esercizio dei diritti dell'interessato. Ha inoltre nominato un DPO contattabile all'indirizzo_ privacy@datalite.it	
A.3.1	Public cloud PII processor's purpose	Datalite utilizza i dati personali di cui è Responsabile del trattamento per le esclusive finalità necessarie all'erogazione del servizio	Nomina Responsabile trattamento
A.3.2	Public cloud PII processor's commercial use	Datalite utilizza i dati personali di cui è Responsabile del trattamento per le esclusive finalità necessarie all'erogazione del servizio	Nomina Responsabile trattamento
A.5.1	Secure erasure of temporary files	I file temporanei presenti nei sistemi di Datalite sono cancellati tempestivamente come definito nelle policy interne.	
A.6.1	PII disclosure notification	Nel caso di richieste da parte delle autorità di informazioni personali contenute del Cloud, se non configura reato, Datalite comunicherà al Cliente l'avvenuta comunicazione e la relativa autorità e motivazione.	

A.6.2	Recording of PII disclosures	Datalite si è strutturata in modo da registrare tempestivamente eventuali Data Breach e provvedere alla corretta gestione.	Datalite, non ha registrato Data Breach.
A.8.1	Disclosure of sub-contracted PII processing	Datalite può utilizzare sub responsabili del trattamento per svolgere le proprie attività. Datalite conserva un registro, con relative nomine, di tutti i sub responsabili che possono essere richiesti dal Cliente in qualsiasi momento.	Nomina Responsabile Trattamento
A.10.1	Notification of a data breach involving PII	In caso di Data Breach Datalite informa tempestivamente il Cliente di quanto avvenuto e di tutti i dettagli della violazione nonché delle contromisure adottare per contenere i danni.	
A.10.2	Notification of a data breach involving PII	Datalite conserva tutta la documentazione interna (comprensiva di politiche, procedure, istruzioni, manuali, ecc.) in conformità alla normativa vigente.	
A.10.3	PII return, transfer and disposal	Alla conclusione del contratto di un Prodotto SaaS, Datalite provvede alla cancellazione e rimozione definitiva dei dati del Cliente come da accordi contrattuali e comunicandolo al cliente a mezzo _pec____. Datalite gestisce con un processo definito la cancellazione periodica dei file temporanei dei propri sistemi cloud.	
A.11.1	Confidentiality or non-disclosure agreements	Non Disclosure Agreement (NDA): Datalite sottoscrive con tutti i propri addetti (dipendenti o collaboratori) un accordo di riservatezza al fine di tutelare anche i dati personali trattati nell'ambito della collaborazione.	
A.11.2	Restriction of the creation of hardcopy material	Datalite ha definito una politica per ridurre l'utilizzo di materiale cartaceo.	
A.11.3	Control and logging of data restoration	Datalite mantiene un registro dei ripristini dati.	
A.11.4	Protecting data on storage media leaving the premises	Datalite ha definito una politica di sicurezza per il trasporto e/o trasferimento di dispositivi fisici contenenti informazioni personali che prevede tra le altre misure di sicurezza la cifratura dei dati.	
A.11.5	Use of unencrypted portable storage media and devices	Datalite ha definito una politica di sicurezza per il trasporto e/o trasferimento di dispositivi fisici contenenti informazioni personali che prevede tra le altre misure di sicurezza la cifratura dei dati.	
A.11.6	Encryption of PII transmitted over public data-transmission networks	Canale sicuro SSL - I flussi di dati da/verso i sistemi, sono protetti da canale sicuro SSL, mediante opportuna configurazione sui server, tale da assicurare: autenticazione del server e la cifratura della sessione. Questo vale sia per i flussi originati in modo interattivo (web browsing) sia per quelli generati in modo automatico (es. utilizzo di API di servizi terzi).	
A.11.7	Secure disposal of hardcopy materials	Datalite ha definito una policy interna per la distruzione della documentazione cartacea tramite appositi distruggi documenti.	
A.11.8	Unique use of user IDs	Datalite ha definito una politica di accesso alle informazioni che prevede un ID utente distinto per ogni addetto.	

A.11.9	Records of authorized users	Datalite mantiene un registro degli accessi dettagliati per risorsa e tipologia di informazioni.	
A.11.10	User ID management	Datalite ha definito apposita policy interna per non assegnare utenti disattivi o scaduti ad altri individui.	
A.11.11	Contract measures	Datalite sottoscrive la Nomina a Responsabile del Trattamento dei Dati Personali fornita dal Cliente.	Nomina Responsabile del Trattamento
A.11.12	Sub-contracted PII processing	Datalite predispone apposite nomine per Sub Responsabili del Trattamento dei Dati Personali e mantiene un registro aggiornato.	
A.11.13	Access to data on pre-used data storage space	Nel Cloud di Datalite sono previste procedure per la cancellazione delle informazioni non più utilizzate prima che sia allocato nuovamente lo spazio.	
A.12.1	Geographical location of PII	Il Cloud di Datalite e di eventuali Partner è situato in Italia o in altro paese dell'Unione Europea.	Italia
A.12.2	Intended destination of PII	Le reti del perimetro di Datalite sono sottoposte periodicamente a test di sicurezza, tra cui Vulnerability Assessment.	

Procedura di anonimizzazione database clienti

Datalite Srl ha predisposto una misura di sicurezza aggiuntiva sui server SQL applicata nei casi in cui sia necessario, per motivi di assistenza tecnica o per attività di sviluppo software commissionata dal cliente, prendere in carico un database del cliente o parte di esso.

Ogni volta che viene ripristinato un database di un cliente il sistema, automaticamente, provvede ad anonimizzare i dati di clienti e fornitori presenti al suo interno. In particolare, l'anonimizzazione consiste nell' aggiornare in maniera irreversibile tutti quei dati che permetterebbero di risalire alle anagrafiche dei clienti e fornitori: ragione sociale, indirizzi, recapiti, partita iva o codice fiscale, etc.

DPA.000.24 - ALLEGATO III

CONTROLLI NORMA UNI CEI EN ISO/IEC 27017:2021

Misure tecniche e organizzative per garantire la sicurezza dei dati (in vigore dal 26/03/2026)

Misure tecniche e organizzative del datacenter di ZUCCHETTI SPA

DATA CENTER ZUCCHETTI LODI: CONTINUITÀ E HIGH PERFORMANCE

Concepito per far fronte alle esigenze di continuità di servizio, il Business Data Center Zucchetti è stato progettato e realizzato adottando le più moderne tecnologie che garantiscono il più elevato Livello di Servizio agli utenti, 24 ore su 24, 7 giorni su 7. La localizzazione del Business Data Center è in Lodi, dove la società ha la propria sede primaria, con oltre 1000 addetti dedicati allo sviluppo delle soluzioni e alla loro assistenza al fine di garantire un pieno supporto sistemistico e applicativo. Per offrire il massimo livello di sicurezza fisica, oltre che logica e applicativa, il Business Data Center Zucchetti è situato nell'ex caveaux bancario all'interno del complesso Bipielle City di Lodi, progetto dell'architetto Renzo Piano, che oltre ad essere uno straordinario esempio di architettura moderna, offre soluzioni tecnologiche d'avanguardia anche in termini di robustezza ed affidabilità.

Nella realtà data center di LODI si identificano 2 centri di erogazione e 1 centro di backup:

- il sito primario o "Caveaux" ove sono localizzati gli elementi principali di erogazione dei servizi;
- il polo secondario, ove sono concentrati in una logica di disaster recovery le piattaforme di erogazione;
- il polo "Backup", ove sono ospitate le infrastrutture di backup e conservati i nastri.

DATA CENTER DISTRIBUITI

Sito di SIZIANO

Il complesso di Siziano, che occupa circa 42.000m2, è certificato ANSI/TIA-942 LEVEL: RATING 4 "FAULT TOLERANT" e si prefigura come il più grande e avanzato data center italiano; è collegato con il Data Center Zucchetti attraverso una connettività garantita e ridondata. Al Cliente viene fornita la massima disponibilità e qualità di servizio, rispondendo ai requisiti ed agli standard internazionali in tema di sicurezza, fisica e logica, ed affidabilità. Tutti gli impianti e le infrastrutture sono realizzati in ottica di Business Continuity (alimentazione elettrica, condizionamento, anti-incendio, sicurezza perimetrale, network IP) e sono soggetti a monitoraggio e sorveglianza continua H24 mediante sistemi automatizzati e presidio di personale specializzato. Nel corso della progettazione del data center è stata tenuta in grande considerazione l'efficienza energetica tramite l'utilizzo di tecnologie avanzate per la climatizzazione.

Il data center è stato progettato e costruito con l'attenzione alla mitigazione dei rischi ambientali:

- costruzione di nuova realizzazione rispondente alle norme tecniche NTC d.m. 14/01/2008 (norme tecniche di costruzione con criteri anti sismici);
- realizzazione di un doppio tetto resistente a venti fino a 280 km/h.;
- struttura metallica protetta da vernice intumescente;
- le mura perimetrali dell'area tecnica rispondono ai requisiti REI120;
- la protezione da eventuali esondazioni è garantita da un muro di cinta alto 3 mt impermeabilizzato fino ad una altezza di1,5 mt e da una sopraelevazione rispetto l'urbanizzazione primaria di 1 mt;
- vasca di laminazione atta a compensare eventuali accumuli di acqua piovana;

- raffreddamento delle sale dati tramite aria (nel DC non sono presenti tubazioni d'acqua).

L'accesso fisico/logico ai rack, agli apparati e ai server sarà autorizzato solamente al personale tecnico di Zucchetti così come l'installazione, l'implementazione e la gestione del servizio.

Locali

Il data center di Siziano è composto da 4 data hall. Ogni hall può ospitare fino a 1056 rack. La connettività verso il DC è garantita da 100 coppie di fibre con percorsi differenziati in modalità multi-carrier. In ogni data hall i rack sono suddivisi in isole (T-SCIF Thermal Separate Compartment in Facility) protette da una struttura a "cage". La struttura del T-SCIF garantisce la totale compartimentazione tra l'aria calda e quella fredda, garantendo che il calore emesso dalle apparecchiature non entri in contatto con i corridoi freddi all'interno del data center.

Tutto il cablaggio strutturato (rame, fibra ed elettrico) è distribuito su canaline aeree dedicate.

I rack sono installati direttamente sul pavimento, garantendo una elevata capacità di carico, che superano i limiti meccanici dei rack stessi.

Alimentazione

Il campus a regime potrà sostenere consumi fino a 40 Mw ed è alimentato da una linea ridondata in alta tensione da 132 kV. Tutto il carico è protetto da un sistema UPS tri-ridondante in grado di assicurare il 100% di disponibilità (uptime). Questo è reso possibile dall'architettura del sistema elettrico, ingegnerizzato secondo quanto richiesto per l'ottenimento della certificazione Tier IV Gold (modalità "system + system" (2N+1)). Un impianto "system + system" è basato su due impianti elettrici separati, ognuno dei quali può sostenere, in ogni momento, il carico dell'intera Facility. Ogni sistema è dotato di un suo UPS (Uninterruptible Power Systems), System Bypass Modules, PDU (Power Distribution Units), RPP (Remote Power Panels) e altri componenti adeguati al livello di tiering. Questi sistemi sono totalmente indipendenti uno dall'altro in modo da consentire tutte le attività di manutenzione, aggiornamenti e troubleshooting sia come attività pianificata che su specifica esigenza senza creare nessun impatto all'attività dei Clienti. Nel data center ogni sistema di alimentazione elettrica è identificato da un colore differente consentendo ai manutentori di sapere in modo univoco e ben identificabile su quale sistema di alimentazione si sta lavorando. Tutti i rack dei clienti sono dotati di una doppia alimentazione, entrambe derivanti da due sistemi di alimentazione totalmente separati. Tutti i collegamenti (cablaggio strutturato, fibre ottiche, collegamenti elettrici) sono posati in apposite canaline aeree dedicate. Il data center offre elevati livelli di efficienza, come confermato dal parametro che misura l'efficienza energetica dei data center, pari a una media annuale P.U.E. (Power Usage Effectiveness) minore di 1,4 (valore stimato in sede di progetto).

Condizionamento

L'impianto di raffreddamento si basa su un set modulare di AHU (Air Handling Unit) che sfruttano il principio del raffrescamento evaporativo indiretto tramite scambiatori aria-aria opportunamente raffreddati da sistemi ad acqua posti all'esterno del data center. L'infrastruttura in acciaio, che sostiene il sistema T-SCIF, ha anche la funzione di volano termico, permettendo alla Facility di raggiungere livelli di resilienza superiori ai più elevati standard di settore. Nel DC possono essere ospitati rack ad alta densità (fino a 40KW) totalmente raffrescati ad aria.

Sicurezza

Il data center presenta i seguenti sistemi di sicurezza:

- controllo degli accessi con badge;
- sistema di rilevamento anti-intrusione e presidio con agenti di vigilanza 24hx7x365;
- telecamere a circuito chiuso con archiviazione digitale delle riprese nel rispetto delle attuali normative in termini di privacy;
- sistemi di rilevamento anti-fumo, anti-incendio e anti-allagamento;
- monitoraggio delle performance e delle regolazioni dei parametri ambientali (assorbimento energetico, regolazione temperatura e umidità, regolazione flusso dell'aria, etc.) monitorato 24x7 dal Network Operation Center (NOC) onsite.

Sistemi di sicurezza networking (Firewall, IPS, Antiddos)

Tutti i flussi dati tra il networking del data center ed il mondo internet, nonché i collegamenti VPN con l'esterno vengono mediati da sistemi di firewall. Tali sistemi di firewall permettono il transito soltanto ai flussi dati necessari al funzionamento del servizio ed esplicitamente autorizzati. Il servizio è gestito tramite sistemi ridondati al 100% prodotti da primari produttori HW internazionali. La sicurezza logica è garantita sia a livello perimetrale che tra i sistemi di front-end e il back-end. Sono applicate policy globali per l'inspection dei pacchetti applicando class map standard. I sistemi di firewall perimetrale ed i sistemi AntiDDos proteggono i Data Center Zucchetti dalle minacce provenienti dal mondo Internet. Utilizzando le migliori tecnologie presenti sul mercato sono in grado di garantire, in ogni momento, la massima fruibilità e protezione per i servizi esposti sul web. Il servizio è ridondato in ogni suo componente, assicurando così una continua disponibilità dei sistemi. Il data center è protetto inoltre da sistemi di Intrusion Prevention System (IPS) e IDS in grado di analizzare tutto il traffico in entrata individuando immediatamente i tentativi di attacco in corso. Il traffico di rete, su segmenti significativi della piattaforma, passa attraverso sistemi che ispezionano ogni pacchetto del traffico in transito e si comportano in modo trasparente nei confronti del traffico legittimo.

Linee di comunicazione

La comunicazione tra il sito di Siziano ed il "Business Data Center" di Lodi è garantita con un doppio collegamento punto-punto in logica L2 . Tale configurazione permette con canali ridondati a 10 Gb cad. e distribuiti sui 2 siti di Lodi di garantire la massima sicurezza e la riservatezza degli ambienti ospitati, estendendo le reti di Lodi verso il sito remoto.

Certificazioni

Zucchetti ritiene la sicurezza un elemento prioritario e irrinunciabile per l'azienda e per i propri clienti; per questo ha organizzato i propri sistemi di gestione in modo da seguire rigidi criteri di sicurezza. L'organizzazione di un sistema di gestione impone la creazione di ruoli, flussi di attività e procedure definite a presidio dei processi aziendali. Lo scopo primario di Zucchetti è il perseguimento della soddisfazione del proprio cliente in merito ai prodotti e servizi forniti, nonché il miglioramento continuo delle prestazioni aziendali, assicurando ai propri clienti il mantenimento e il miglioramento nel tempo della qualità dei propri beni e servizi. Al fine di garantire la sicurezza delle informazioni, che transitano all'interno dell'azienda, sia il Data Center Zucchetti situato in Lodi che il Data Center di Siziano hanno conseguito importanti certificazioni quali:

- la certificazione ISO 9001, volta a migliorare la gestione organizzativa di un'impresa, mediante l'impiego di risorse, procedure ed istruzioni ispirate ai principi di semplificazione, efficienza ed efficacia;
- la certificazione ISO 27001, volta ad assicurare il rispetto di determinati standard di sicurezza nella gestione dei dati e delle informazioni aziendali, preservandone l'integrità, la riservatezza e la disponibilità.

Il Data Center di Lodi, inoltre, è conforme allo standard BS10012 che prevede procedure e tecnologie predisposte appositamente a tutela dei dati personali dei clienti in conformità al Reg UE 2016/679.