VETTORE MEDICAL

Allegato tecnico sulla sicurezza informatica

Aggiornamento: Ottobre 2023
La versione corrente si trova a: http://sicurezza.vettoremedical.it

Disponibilita` del servizio

Non e` previsto di norma nessun downtime per manutenzioni in orari lavorativi.
La SLA e' del 99,95% su base annuale negli orari 7-21 nei giorni da Lunedi a Sabato.
Sono impiegate le tecniche necessarie ad assicurare la disponibilita` continua del servizio 365 giorni all'anno minimizzando le interruzioni, fermo restando il pre-requisito di buon funzionamento della rete globale e della linea internet propria del cliente.

Monitoraggio

L'infrastruttura IT ed i servizi web sono controllati da sistemi di monitoraggio automatici che consentono la manutenzione preventiva di molte delle piu` comuni anomalie di sistema, e che facilitano la gestione degli incidenti in atto.
Gli interventi di risposta ai guasti di natura tecnico-sistemistica possono essere effettuati sia da personale interno Doctolib, sia da personale incaricato dell'azienda partner "***Laboratori Guglielmo Marconi S.p.A.".***
Il ricorso ad un partner specializzato nel monitoraggio di infrastrutture IT ha l'obiettivo di integrare le risorse interne per garantire un presidio tecnico 365 giorni all'anno e durante tutta la possibile fascia oraria di fruizione dei servizi.

Ridondanza geografica

In caso di guasto ai server, o interruzione di rete o altri incidenti al data-center, le tecnologie di data replication utilizzate permettono il fail-over del sistema verso una struttura completamente separata (in un altra area geografica), in tempi nell'ordine di 10-15 minuti, senza perdita delle ultime operazioni effettuate.
Queste procedure vengono utilizzate e testate regolarmente.

Aggiornamenti del software applicativo

Per la correzione di un difetto al software che venisse eventualmente riscontrato dal cliente, una volta che il problema sia stato corretto internamente dai programmatori, l'aggiornamento al sistema "in produzione" puo` essere eseguito in qualsiasi momento con interruzioni minime di pochi minuti in accordo col cliente.
Le operazioni di aggiornamento applicativo si svolgono con strumenti preposti che minimizzano l'occorrenza di errori operativi al livello di configurazione di sistema.

Salvataggi backup

I salvataggi di backup sono continui, automatici, eseguiti con diversi metodi, e conservati in minimo 3 luoghi diversi (dalla lista dei data-center indicati nell'apposito paragrafo.)

In caso di interruzione del servizio per un guasto tecnico al server o al data-center, il ripristino sull'installazione di fail-over richiede nell'ordine dei 10-15 minuti, ed e' senza alcuna perdita di dati inseriti fino all'istante del guasto.
L'archivio "storico" dei backup invece permette il recupero del database ad una qualsiasi data e ora, con una retention di 3 mesi.

I log delle operazioni di backup sono conservati per il periodo di retention, ed il sistema notifica automaticamente il personale addetto nel caso in cui un job di backup non vada a buon fine.
La verifica del recupero dei salvataggi e' effettuata frequentemente nel contesto delle normali operazioni di gestione del servizio.

Oltre alla disponibilità dei dati salvati e storicizzati, con la stessa metodologia attraverso backup dedicati vengono mantenute tutte le configurazioni di sistema, documentate nelle sue parti, al fine di garantire la ricostruzione dell'intero servizio erogato al cliente.

Disponibilita` dei dati

Per rendere fruibile la disponibilità del dato, sono state implementate funzioni di esportazione automatiche dei dati, da abilitare agli utenti autorizzati dal cliente. Il processo tiene traccia di ogni operazione effettuata.

Collocazione dei server ("Dove sono i dati?")

La rete di Vettore Medical e' attualmente distribuita su data-center gestiti da operatori terzi, in varie nazioni europee, inclusi anche gli operatori cosiddetti "public cloud" (Amazon o similari), il cui elenco -**alla data del documento-** e' sotto riportato.
Ogni data-center e` una struttura specializzata che ospita attrezzature informatiche su larga scala, con la ridondanza di impianti elettrici, comunicazioni e climatizzazione, la presenza di sistemi antincendio e di sorveglianza, ed il presidio tecnico.

Copie estemporanee dei dati, a solo scopo di attivita' di test o di progetto normalmente richieste dal cliente, sono presenti anche presso la sede operativa di Vettore Medical a Bologna i cui locali sono protetti da moderno sistema antifurto.

L'elenco dei provider e' da considerare sempre provvisorio in quanto le strutture utilizzate possono variare per motivi tecnici. La modifica o integrazione di nuovi fornitori verrà comunicata al cliente.

Nota bene: dal 2023 contestualmente alla fusione aziendale in Doctolib e' avviato un piano di lungo termine per confluire tutto l'ambiente IT -produzione e sviluppo- nel cloud di *Amazon Web Services*, con intenzione quindi di eliminare sia l'uso di altri provider diversi da questo sia delle attrezzature pc e server in sede.

Amazon Web Services, Inc. [aws.amazon.com] *CED Localita` varie in UE* *Certificato: ISO 27001*	*Aruba SpA [www.aruba.it]* *CED Localita` Arezzo [IT]* *Certificato: ISO 27001*	*Hetzner Online GmbH* *[www.hetzner.de/en]* *CED Localita` Falkenstein [DE]* *Certificato: ISO 27001*
OVH [www.ovh.net] *CED Localita` Roubaix [FR]* *Certificato: ISO 27001*	*Scaleway ex Online SAS* *[www.online.net]* *CED Localita` Paris [FR] (c/o ILIAD)* *Certificato: ISO 27001*	*Master Internet Sro* *[www.masterdc.com]* *CED Localita` Brno [CZ]* *Certificato: ISO 27001*
Leaseweb Deutschland GmbH *[www.leaseweb.com]* *CED Localita` Frankfurt [DE]* *Certificato: ISO 27001*	*Contabo GmbH [www.contabo.com]* *CED Localita` Munich [DE]* *Certificato: no*	*Velia.net Internetdienste GmbH* *[www.velia.net]* *CED Localita` Strasbourg [FR] (Datadock)* *Certificato: no*
AltusHost B.V. [www.altushost.com] *CED Localita` Zurigo [CH]* *Headquarter situato ad Amsterdam [NL]* *Certificato: ISO 27001*	Netsons Srl [www.netsons.com] *CED Localita` Milano [IT]* *Certificato: ISO 27001*	

Chi ha accesso ai dati

Il personale Doctolib addetto a Vettore Medical ha la possibilita` di diversi livelli di accesso alle informazioni presenti nel gestionale del cliente durante lo svolgimento di mansioni come chiamate di supporto tecnico, inserimento dati per conto del cliente o implementazione di modifiche richieste al prodotto, manutenzione del sistema informatico, ecc.

L'azienda partner "***Laboratori Guglielmo Marconi S.p.A.***" e' certificata ISO 27001, e collabora nel monitoraggio e gestione tecnica da remoto dei sistemi, con il livello di accesso equivalente ai tecnici/sistemisti interni di Doctolib.

Gli accessi al portale web vero e proprio del gestionale del cliente avvengono solo da parte del personale autorizzato dell'Assistenza di Vettore Medical, con controlli di sicurezza aggiuntivi, e tracciati nei log di sistema (vedere anche il paragrafo **Ambiente di hosting multi-tenant**).

Il personale in-loco dei data-center subfornitori, infine, non ha alcun accesso logico ai server ospitati per conto di Doctolib, in nessuna fase delle operazioni, in quanto esso interviene esclusivamente su richiesta per semplici operazioni di montaggio / sostituzione fisica di componenti hardware, ma mai invece per interventi di gestione sistemistica.
Le macchine o i dischi che vengono dismessi, sono preventivamente sottoposti a cancellazione con metodi di sovrascrittura.

Cifratura

Viene impiegata la cifratura dei dati, "in transito" o "a riposo", inclusi i backup, laddove sussista la concreta possibilita` di furto di supporti fisici, o di intercettazione delle comunicazioni, anche all'interno delle LAN aziendali ed anche nelle trasmissioni tra server. Il collegamento in rete dalle postazioni di lavoro del cliente e' cifrato con lo standard del web SSL/TLS.

Controlli di accesso logico-applicativo

L'accesso al software gestionale e` soggetto a verifica delle credenziali utente e password. Il criterio per definire la complessita` delle password e la loro scadenza periodica e` configurabile dal cliente, e presenta per default una impostazione conforme alla normativa. Il codice interno di gestione delle password di accesso del gestionale utilizza le funzioni di ''key derivation''.

Per rafforzare il controllo all'accesso, per ciascun utente del gestionale si puo` sia impostare un blocco da indirizzi rete di origine non riconosciuti, oppure abilitare la modalita' di accesso "a due fattori" col telefono.

E` presente un articolato sistema di autorizzazioni dei livelli di accesso in base alla tipologia e mansioni dell'utente.
Gli accessi alla visualizzazione dei dossier sanitari dei pazienti, ed ogni altra informazione correlata come anche fatture o appuntamenti, vengono registrati sui log con data/ora dell'evento, e conservati indefinitamente.

Conservazione dei log

I log relativi all'uso del software gestionale vengono conservati a tempo indeterminato e gli archivi non sono modificabili.

Sicurezza logica delle postazioni di lavoro e della LAN del Cliente

Rimane a cura del cliente il rispetto delle misure di sicurezza concernenti le stazioni di lavoro presso la propria sede (password del PC, bloccaschermo, antivirus, MFA ecc.).
Non gestendo le postazioni di lavoro e le sicurezze implementate a protezione di esse, anche per le reti LAN/WAN del cliente, Doctolib declina ogni responsabilita` afferente ad esse.

Sicurezza logica del sistema informativo di Vettore Medical

Le verifiche sulla possibile presenza di vulnerabilita' informatiche in tutto il complesso del sistema informativo di Vettore Medical sono effettuati in prima battuta ed anche con strumenti di monitoraggio continuativo dai reparti adibiti interni di Doctolib.
In aggiunta vengono commissionate attivita' di pen-testing indipendenti attualmente con la societa' Advens (www.advens.fr).

I PC ed i laptop aziendali, oltre che i server ove applicabile, sono dotati di antivirus centralizzato / EDR, firewall e/o IDS, ed i relativi software vengono aggiornati regolarmente. I telefoni aziendali sono dotati di sistema MDM.
A tutto il personale viene fornito almeno un laptop aziendale, senza credenziali da "amministratore" nel caso degli utenti non-tecnici. Il lavoro su device propri ("byod") non e' normalmente consentito o incoraggiato salvo necessita' temporanee.

La gestione tecnica del sistema informativo di Vettore Medical e' svolta nel rispetto delle best practice per la sicurezza informatica, che includono, ma non limitatamente, ai principi di "least privilege", "security in depth", e delle tecniche di "hardening" dei sistemi.
Gli accessi di servizio per la gestione tecnica del sistema informativo richiedono alternativamente o la popolare modalita' "a due fattori" oppure la presenza di credenziali crittografiche aggiuntive alla password, di VPN o controlli su origine di rete conosciuta.

Ambiente di hosting multi-tenant

L'infrastruttura hosting prevede la presenza sugli stessi server, di istanze associate a diversi clienti del software gestionale.
La separazione logica tra i servizi erogati a differenti clienti ("tenant") e` imposta dal sistema operativo dei server, ovvero in pratica con utenze e autorizzazioni distinte a livello di processo, di filesystem e di database.

Da questa architettura viene escluso che, a causa di bug di programmazione o impostazioni errate del gestionale, gli utenti appartenenti ad un dato cliente possano uscire dal proprio "tenant" per entrare in uno diverso, oppure che dei dati di clienti diversi possano mischiarsi.
Inoltre in caso di necessita' in base agli accordi specifici e' possibile gestire gli aggiornamenti in modo personalizzato (nel senso di quale versione di Vettore Medical e' installata e la cadenza degli aggiornamenti stessi).

Solo il sistema di accesso per l'Assistenza espone la visibilita' di tutti i clienti ad un'unica utenza, tramite un meccanismo di "single sign-on" del gestionale che deve essere esplicitamente abilitato agli incaricati. Questa modalita' di accesso, inoltre, e' protetta da altri controlli di sicurezza per cui funziona solo su device o reti autorizzate separatamente dall'area Sistemi, e senza che esista alcuna impostazione per aggirare questo controllo.

L'infrastruttura hosting su cui si appoggia Vettore Medical fa uso anche di server virtualizzati in un sistema ''public cloud'' (Amazon o simili). L'utilizzo del provider cloud, prevede che le risorse tecniche di elaborazione sono condivise tra molteplici tenant del provider stesso; e` compito dell'operatore cloud mantenere le caratteristiche tecniche necessarie a garantire l'isolamento logico tra i propri tenant per motivi di sicurezza.

Notifica dei data breach

Doctolib si impegna a notificare tempestivamente il cliente in caso venisse a conoscenza di una fuoriuscita di dati dolosa o accidentale dai propri sistemi informativi, e di notificarne altrettanto l'Autorita` Garante nei casi previsti dalla legge.

Utilizzo dei dati

Doctolib non utilizza i dati di Vettore Medical in alcun altro modo al di fuori delle operazioni tecnologiche occorrenti per l'erogazione e lo sviluppo del servizio.
Non si effettuano ricerche sui dati a scopo commerciale, ne` divulgazione a terzi (se non ove venisse richiesto dall'autorita` giudiziaria nei casi previsti dalla legge.)
Non si effetuano trasferimenti di dati, neanche a scopi di backup, presso strutture situate al di fuori dell'UE. Nei casi in cui e` utilizzato un sistema cloud, le nostre risorse virtuali sono comunque mantenute solo nella parte europea.