DILITRUST

Sicurezza in DiliTrust

LA SICUREZZA DEI VOSTRI DATI È LA NOSTRA PRIORITÀ N°1

La sicurezza dei dati è fondamentale per la continuità della tua organizzazione. Il furto o la perdita di dati, il mancato rispetto delle normative come il GDPR o il costo del tempo perso a causa di un'interruzione del servizio può causare danni significativi a qualsiasi azienda.

La sicurezza dei tuoi dati è vitale per te; ma lo è anche per noi.

Che si tratti di protezione contro hacker esterni, violazioni della sicurezza interna, divulgazione di informazioni o errori umani, la sicurezza è essenziale per i nostri clienti ed è parte integrante del nostro servizio. Tutta la nostra organizzazione si concentra su questo obiettivo: offrire il massimo livello di sicurezza possibile.

LA CULTURA DELLA SICUREZZA

DiliTrust è certificata ISO 27001:2017 e ISO 27701:2019. Questa certificazione copre tutti gli aspetti del nostro servizio, compreso il supporto clienti e le Operations. Inoltre, fornisce raccomandazioni circa le corrette pratiche da adottare nella gestione della sicurezza delle informazioni e il suo campo di applicazione è deliberatamente molto ampio.

Tutti i nostri dipendenti vengono formati per adottare comportamenti e procedure conformi alla norma ISO 27001, sia al loro arrivo in azienda che durante il loro percorso di carriera.
La formazione continua assicura che i nostri team siano costantemente aggiornati in materia di sicurezza delle informazioni. Inoltre, tutti i nostri dipendenti firmano un accordo di riservatezza.

Come parte della nostra strategia, sensibilizziamo i nostri clienti sugli standard di sicurezza e su questioni come la gestione delle password e dei tablet.

L'INFRASTRUTTURA

LOCATION DEI SERVER

I nostri server sono certificati secondo i più elevati standard di sicurezza e si trovano in Francia. I dati ospitati non sono condivisi nel cloud e non sono soggetti all'US Cloud Act (e Patriot Act), garantendo ai nostri clienti un controllo costante sui loro dati sensibili.

SICUREZZA FISICA

Un altro aspetto importante della sicurezza dei dati riguarda la sicurezza fisica. L'accesso fisico al data center è controllato da un sistema di badge 24/7, con videosorveglianza e personale in loco.

I locali sono dotati di sistemi di rilevazione fumi e di un impianto a doppia alimentazione con generatori di emergenza con un'autonomia iniziale di 48 ore. Inoltre, i locali sono dotati di due connessioni di rete ridondanti per evitare la dipendenza da un unico provider Internet.

Infine, tutte le strutture sono protette da allagamento, incendi e altri rischi ambientali.

HOSTING ULTRA-SICURO

Per migliorare continuamente la protezione dei dati e garantire la riservatezza di tutte le informazioni, tutti i sistemi e i dati di DiliTrust sono ospitati su server che hanno ottenuto le più alte certificazioni internazionali nel campo della sicurezza informatica.

L'hosting è inoltre certificato secondo la norma ISO/IEC 27001. Questo standard garantisce l'implementazione di un sistema di gestione della sicurezza delle informazioni (ISMS). La ISO 27001 definisce anche le misure di controllo per garantire che i sistemi offerti ai nostri clienti abbiano il massimo livello di sicurezza.

CONTROLLO E SORVEGLIANZA 24/7

I nostri sistemi sono sotto sorveglianza 24 ore su 24, 7 giorni su 7, in particolare per quanto riguarda qualsiasi tentativo di attacco o il verificarsi di un problema tecnico:

- Sorveglianza hardware (RAM, CPU e percentuale di utilizzo di storage), monitoraggio delle prestazioni dell'applicazione;
- Alerts automatici quando vengono rilevate attività sospette;
- Firewall, IDS (Intrusion Detection System), sistema anti-allagamento (DDoS) e protezione contro gli attacchi di forza bruta.

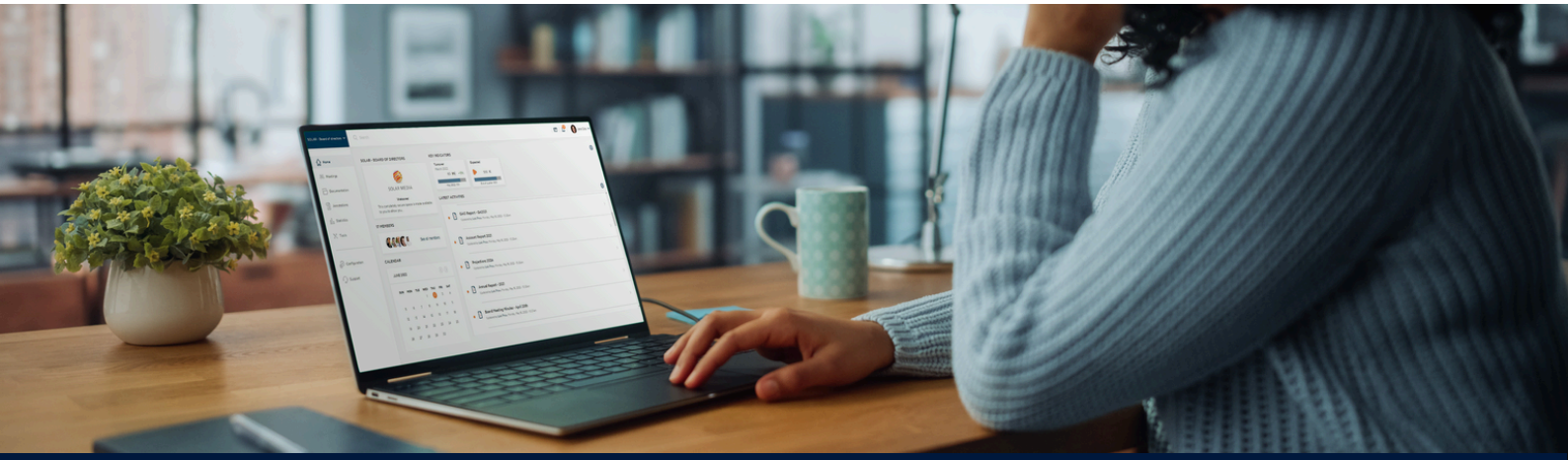
Tutti i server hanno dischi e accesso alla rete ridondante, così come un sistema di backup giornaliero.

BACKUP

I backup dell'intero sistema vengono eseguiti quotidianamente e archiviati in un luogo secondario geograficamente remoto, nelle stesse condizioni di sicurezza dei server di produzione e nello stesso paese (sotto la stessa giurisdizione).

I backup vengono conservati per sette giorni, poi distrutti definitivamente senza possibilità di recupero. Ad esempio: il file di backup del lunedì cancella automaticamente il file del lunedì precedente.

Un secondo sistema operativo è disponibile per qualsiasi situazione di forza maggiore in cui sia necessario riavviare il servizio (durante il tempo di propagazione del DNS).



CRITTOGRAFIA

DATA-AT-REST: AES 256

Tutti i dati At-rest sono crittografati con chiavi di crittografia AES (Advanced Encryption Standard, Rijndael) a 256 bit, ossia il più alto standard di crittografia attuale.

Questo vale sia su server che su dispositivi mobili (per i dati memorizzati localmente).

DATA-IN-MOTION: HTTPS 256 BITS

Il nostro standard per tutto il traffico (data-in-motion) in entrata o in uscita dai nostri server è la crittografia TLS (TLS 1.2 e protocolli superiori) con i più alti livelli di crittografia (chiave a 256 bit). Non è consentito il traffico non criptato.

Vengono utilizzati solo browser moderni e sicuri (IE11, Edge, Firefox, Chrome, Safari) e applicazioni mobili native DiliTrust. L'accesso è negato ai browser obsoleti e non protetti (come IE8).

HARDWARE SECURITY MODULE (HSM)

Un modulo di sicurezza hardware (HSM) è una cassaforte digitale. Si tratta di un processore crittografico dedicato, appositamente progettato per proteggere le chiavi di crittografia durante tutto il loro ciclo di vita.

L'HSM agisce come una base affidabile che protegge l'infrastruttura crittografica delle nostre applicazioni gestendo, elaborando e memorizzando in modo sicuro le chiavi di crittografia all'interno di un server con una sicurezza appositamente migliorata e a prova di manomissione. La tecnologia HSM ci aiuta ad offrire ai nostri clienti il massimo livello di crittografia dei loro dati e il massimo livello di sicurezza attualmente disponibile.

BRING YOUR OWN KEY (BYOK)

Offriamo ai nostri clienti la possibilità di ospitare il proprio HSM (conforme PKCS11) per proteggere la propria chiave di crittografia. Tutti i dati dei nostri clienti saranno criptati con la propria chiave. Queste chiavi sono quindi al sicuro nell'HSM del cliente e non nell'HSM del fornitore.

ALTRE FUNZIONALITÀ

PASSWORD SICURE

Ogni utente è identificato da un nome utente e una password univoci. Tutti gli utenti devono scegliere la propria password sicura. Nessuna password viene inviata via e-mail o visualizzata. Le password sono memorizzate come hash, dopo una crittografia unidirezionale (iniettiva).

La politica di password minima predefinita è la seguente:

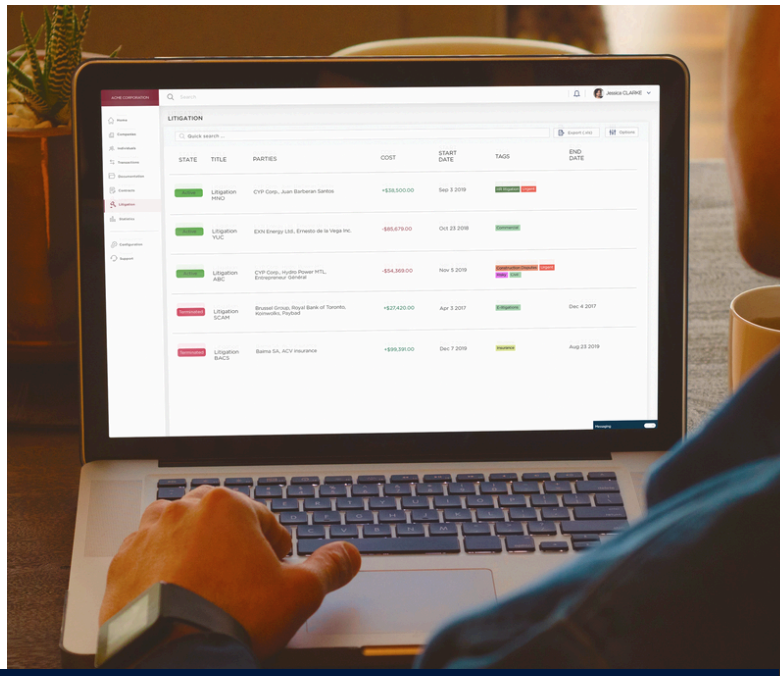
- almeno 3 caratteri di diverso tipo (minuscole, maiuscole, numeri o caratteri speciali).
- un minimo di 10 caratteri.

La procedura per ottenere o recuperare una password prevede l'invio di una e-mail con un unico link di accesso sicuro (che scade dopo 24 ore e dopo il primo utilizzo).

Ogni richiesta fatta ai server viene autenticata per verificare l'identità dell'utente, e se l'utente dispone dei permessi appropriati per eseguire l'azione richiesta. La richiesta viene inoltrata per l'esecuzione se e solo se tutti questi controlli sono stati convalidati con successo.

AUTENTICAZIONE A DUE FATTORI (TFA)

L'autenticazione a due fattori (TFA – Two Factor Authentication) può migliorare ulteriormente la sicurezza dell'utente per accedere all'applicazione. Dopo aver inserito login e password, l'utente riceve via SMS un codice da inserire per completare l'autenticazione. Ogni codice è monouso e corrisponde ad uno specifico tentativo di connessione.



AUDIT

Per garantire il massimo livello di sicurezza, applichiamo tre livelli di controllo: audit interni, audit automatizzati settimanali e audit umani esterni annuali.

Se viene rilevato un security breach, viene corretto il prima possibile. Applichiamo sistematicamente le seguenti raccomandazioni e best practices.

AUDIT INTERNI

DiliTrust applica rigide procedure interne in termini di sicurezza:

- Security by design: i team di sviluppo vengono formati sulle diverse tecniche di intrusione e sul codice sicuro per proteggersi;
- Procedure interne di revisione del codice e test di sicurezza prima del rilascio di ogni nuova feature;
- Test interni di sicurezza e l'utilizzo di diversi tool di security audit, principalmente quelli disponibili attraverso Linux Kali.

AUDIT ESTERNI ESEGUITI DA ESPERTI INDIPENDENTI

Almeno una volta all'anno, viene effettuato un controllo di sicurezza completo da parte di un'azienda esterna indipendente specializzata in sicurezza IT (non-automated human intrusion tests).

Alla fine di ogni test viene generato un security report; le vulnerabilità vengono corrette immediatamente e le raccomandazioni vengono applicate il prima possibile.

AUDIT AUTOMATIZZATI

I nostri sistemi sono protetti da Qualys. Il servizio è soggetto ad un'intensa scansione settimanale di sicurezza a livello di server (configurazione firewall, porte, versioni software aggiornate, configurazione SSL ecc.) così come a livello di applicazione (XSS, iniezione SQL, sessione di hijacking ecc.)

È testato per superare con successo tutti le raccomandazioni per gli audit di vulnerabilità esterna da parte delle seguenti organizzazioni:

- Department of Homeland Security's National Infrastructure Protection Centre (NIPC)
- OWASP Top 10 Most Critical Web Application Security Risks
- SANS/FBI Top 20 Internet Security Vulnerabilities list
- Visa's CISP e AIS
- Mastercard's SDP
- American Express' DSS
- Discover Card's DISC security standards.

DiliTrust è conforme ai criteri di sicurezza prescritti da regolamenti quali:

- Health Insurance Portability & Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley Act (SOA)
- Government Information Security Reform Act (GISRA)
- Canada's Personal Information Protection e Electronic Documents Act.
- General Data Protection Regulation (GDPR)

"La sicurezza è il nostro DNA"

NADIM BAKLOUTI
Chief Technology Officer di DiliTrust

Per maggiori informazioni su DiliTrust, visitate il sito www.dilitrust.com/it

Via Monte di Pietà 19, 20121 Milano – Italia
Tel. : +39 02 30565500 | hello@dilitrust.com

DILITRUST