kyriba®

Guida alla tecnologia e alla sicurezza di Kyriba

Versione 5.0

Agosto 2021

Sommario

Avvertenza

Kyriba opera in un ambiente dinamico e le nostre offerte tecnologiche sono soggette a modifiche. Le informazioni contenute nel presente documento hanno un mero scopo informativo e non costituiscono un impegno, una promessa o un obbligo giuridico a fornire qualsivoglia materiale, codice o funzionalità. Le tecnologie qui descritte ricadono nella nostra esclusiva discrezione. Kyriba si riserva il diritto di modificare in tutto o in parte e in qualsiasi momento la propria infrastruttura di tecnologie in base alle esigenze dei clienti, alle dinamiche di mercato e ai progressi tecnologici.

1. Pianificazione e registro delle modifiche

Questo documento include le informazioni più recenti sulla linea di prodotti di Kyriba, il suo funzionamento e sulla sua interfaccia con i clienti e i partner. Kyriba opera in un ambiente dinamico, per questo motivo, aggiorna e potenzia costantemente i suoi prodotti e i suoi sistemi. Di conseguenza, alcune informazioni contenute nel presente documento potrebbero nel frattempo essere state modificate, alterate o eliminate a seguito del continuo miglioramento dei sistemi, dei servizi e dell'assistenza offerti da Kyriba. Questo documento viene rivisto con cadenza annuale e ripubblicato dietro controllo di versione. Domande, commenti e repliche vanno indirizzati all'indirizzo Technical-Sales@kyriba.com.

1.1. Registro delle modifiche

Versione	Descrizione della modifica	Data della modifica	Data di pubblicazione
4,0	Aggiornamento annuale	Settembre 2014	Settembre 2014
4,1	Aggiornamento annuale	Luglio 2015	Luglio 2015
4,2	Aggiornamento minore	Ottobre 2015	Ottobre 2015
4,3	Aggiornamento annuale	Gennaio 2016	Gennaio 2016
4,4	Aggiunte alle informazioni sulla sicurezza, alla gestione e al controllo del prodotto Kyriba	Luglio 2016	Luglio 2016
4,5	Rimossa la sezione ridondante sul ripristino di emergenza	Gennaio 2017	Gennaio 2017
4,6	Aggiunta la sezione 3.7 - Centri di controllo di Kyriba e monitoraggio	Agosto 2017	Agosto 2017
4,7	Rimosso un riferimento nella sezione 5.6.1	Gennaio 2018	Gennaio 2018
4,8	Aggiornamento legato ai nuovi data center basati su AWS	Maggio 2018	Luglio 2018
4,9	Aggiornamento legato all'attuale periodo di conservazione dei dati	Dicembre 2019	Dicembre 2019
5,0	Aggiornamento annuale	Agosto 2021	Agosto 2021
5,1	Aggiornamento della grafica di ELM e di alcuni riferimenti	Settembre 2021	Settembre 2021

2. Soluzione di Kyriba per la gestione della liquidità aziendale (ELM)

La piattaforma Enterprise Liquidity Management di Kyriba offre la più completa gamma di funzionalità di gestione della liquidità aziendale per aiutare i team della finanza e i loro partner IT a vedere (tesoreria), trasferire (pagamenti), proteggere (gestione del rischio) e ottimizzare (Working Capital) la cassa e la liquidità.

Queste soluzioni vengono rese possibili da Liquidity Network di Kyriba, un hub di connettività e dati sulla liquidità basato sul cloud che fornisce:

- una connettività di rete che permette una connessione dati robusta e sicura a ERP e a più di 600 banche, con 1.400 varianti di formati di pagamenti e 100.000 fornitori
- un hub di dati sulla liquidità che permette di avere un unico punto di accesso sui flussi di cassa aziendali e sui quali Kyriba fornisce le migliori soluzioni di reportistica per ottenere informazioni operative di altissimo livello

Kyriba vanta un'esperienza e una competenza ineguagliabili nella gestione della liquidità aziendale, portando valore a tutti i membri della community di Kyriba.

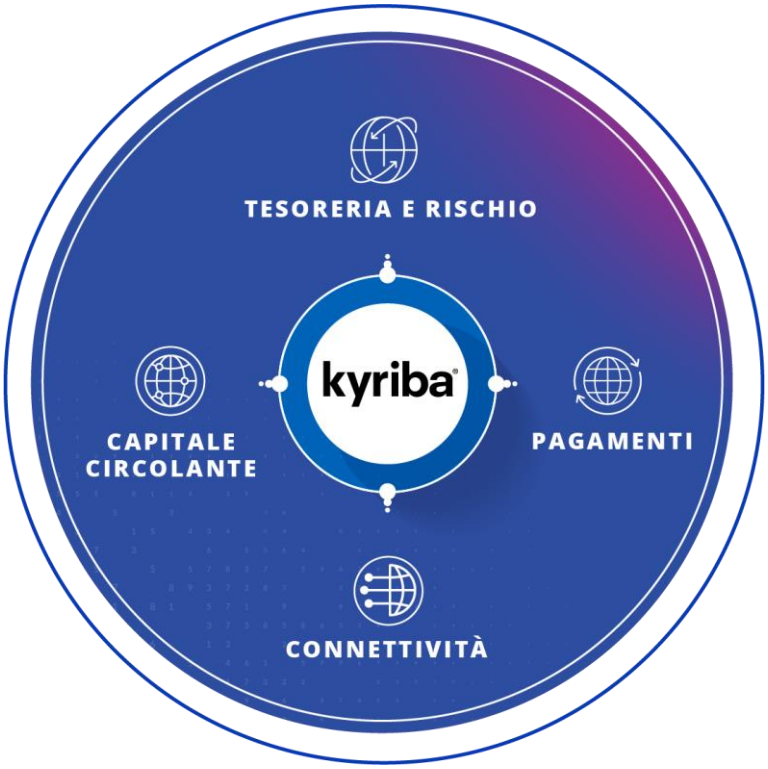

Figura 1: Piattaforma per la gestione della liquidità aziendale di Kyriba

I nostri clienti variano dalle grandi multinazionali blue chip alle imprese di medie dimensioni che intendono sistematizzare i propri processi di tesoreria. CFO e i tesorieri si affidano a Kyriba per godere di:

- una visibilità avanzata in termini di saldi di cassa, previsioni, posizioni, esposizioni
- tempestività e accuratezza dei dati
- un processo decisionale efficace volto all' ottimizzazione della cassa e alla copertura dei rischi
- centralizzazione dei processi di tesoreria e dei controlli interni aziendali
- una maggiore produttività
- un reporting e un'analisi dei dati migliori grazie alla BI
- buone pratiche acclamate e premiate

3. Soluzione SaaS

La soluzione Software-as-a-Service (SaaS) di Kyriba mette a disposizione le innovazioni più recenti con i piu' alti livelli di sicurezza a un prezzo minore di quello richiesto dagli application service provider (ASP) o per le soluzioni on-premise. La nostra soluzione SaaS è progettata e ottimizzata per i browser web e offre vantaggi unici in termini di assistenza, prestazioni, sicurezza, scalabilità, livelli di servizio, integrazione di sistemi e funzionalità del software. Inoltre, il modello SaaS della nostra soluzione permette di eliminare la gestione e i costi generali tipici delle soluzioni on-premise, non essendoci alcuna necessità di acquistare dell'hardware specifico o di gestirne l'installazione, la configurazione, gli aggiornamenti e l'ordinaria manutenzione.

3.1. Piattaforme multiple, sicure e disaster tolerant

La nostra infrastruttura SaaS globale è ospitata sui server di Amazon Web Services (AWS) su più zone e regioni di disponibilità in diversi paesi (Europa, Nord America, Cina). AWS consente a Kyriba di scalare in maniera efficiente quando entrano in gioco esigenze di prestazioni, sicurezza avanzata, disponibilità e pratiche di applicazioni moderne. L'architettura SaaS di Kyriba è configurata per sfruttare i design cloud-native di AWS e offrire ai nostri clienti capacità e possibilità di crescita illimitate. Visita https://aws.amazon.com/compliance/programs/ per ottenere maggiori informazioni sulla sicurezza, la governance e la protezione dei dati. Per i nostri clienti in Cina, la nostra istanza di AWS è gestita da China Sinnet, un partner locale di Amazon.

Inoltre, infrastrutture SaaS di Kyriba sono ospitate in Nord America e in Europa. Nel Nord America, le nostre due strutture si trovano a Phoenix, Arizona e a Edison, New Jersey con ilnostro fornitore Iron Mountain. In entrambi i casi si tratta di data center certificati Tier III da Uptime Institute, conformi SOC 1/SOC 2 Type 2 e certificati ISO/CEI 27001. Questa struttura di hosting geograficamente distribuita consente di ottenere disponibilità e prestazioni elevate con la massima sicurezza. L'infrastruttura SaaS europea è ospitata in due strutture situate in Francia presso il nostro fornitore Equinix. In entrambi i casi si tratta di data center certificati Tier III+ da Uptime Institute e certificati SOC 1/SOC 2 Type 2, ISO 9001 e ISO/CEI 27001.

3.2. Ridondanza

La nostra piattaforma, si caratterizza per una disponibilità del servizio di altissima qualità ed è in grado di resistere ad eventuali guasti del sistema. Inoltre, i sistemi di monitoraggio e di allerta automatici integrati in Kyriba assicurano il mantenimento dei livelli di prestazione indicati negli SLA. Tutti i server vengono costantemente monitorati con una serie di sonde (da 5 a 20 per server) che esaminano, attraverso tecniche di tracciamento distribuito, il comportamento dell'hardware, dell'host virtuale e delle applicazioni in esecuzione sui server stessi.

Quando viene rilevata un'anomalia, una notifica viene automaticamente inviata a un membro del team di Kyriba per permettergli di reagire prontamente all'accaduto sulla base di un set di azioni predefinito e specifico per ciascun tipo di incidente. La reattività e la qualità degli interventi del nostro team sono costantemente analizzati per assicurare che la fornitura dei nostri servizi e l'esperienza del cliente siano sempre di ottimo livello.

Nel nostro SaaS sono integrati meccanismi di failover e clustering per garantire la continuità del servizio anche in caso di guasto al server.

I dati per gli scambi di comunicazioni vengono conservati nel database o nell'array di dischi, e mai nei server front-end connessi a Internet.

In caso di sovra utilizzo delle risorse, viene rapidamente condotta un'analisi più approfondita per determinare se si tratti di un caso eccezionale o se sia richiesta una maggiore potenza di elaborazione. In quest'ultimo caso, è possibile aggiungere al livello corrispondente altri server o altre risorse.

3.3. Disponibilità del sistema

La disponibilità del sistema (System Availability, SA) è data dal rapporto tra il tempo di operatività del sistema e il tempo mensile totale.

$$SA = \frac{\textit{Tempo di operatività del sistema}}{\textit{Tempo mensile totale}}$$

Con:

Tempo mensile totale = Tempo totale (in minuti) a disposizione in un mese di calendario - Tempo di inattività programmata

Tempo di operatività del sistema = Tempo mensile totale – Tempo di inattività programmata

Dove:

- **"Tempo di operatività del sistema"** è la quantità totale di tempo, misurata in minuti, a disposizione in un mese di calendario, durante la quale il cliente può accedere alle funzionalità dei nostri servizi SaaS
- **"Tempo di inattività programmata"** è la quantità totale di tempo, misurata in minuti, a disposizione in un mese, durante la quale il cliente non può accedere alle funzionalità dei servizi SaaS a causa di manutenzioni pianificate del sistema ed effettuate da Kyriba come da tabella sotto.
- **"Tempo di inattività non programmata"** è la quantità totale di tempo, misurata in minuti, a disposizione in un mese civile, durante la quale il cliente non può accedere alle funzionalità dei servizi SaaS per cause diverse da quelle previste per il tempo di inattività programmata, così come definito sopra.

Appuntamenti di inattività programmata:	Scopo dell'inattività programmata:	Durata massima dell'inattività programmata:
Ogni giorno (in orari di chiusura)	Patch e aggiornamenti minori	1 ora
Ogni fine settimana	Manutenzione minore del sistema, del database, delle applicazioni o dell'hardware	4 ore
Una volta per mese	Manutenzione o aggiornamento importante	8 ore

Il contratto con Kyriba va sempre integrato con gli accordi sui livelli del servizio e sui livelli del servizio di disponibilità del sistema, che sono soggetti a variazioni.

3.4. Replicazione e ripristino d'emergenza

L'elevata disponibilità della configurazione di replicazione delle nostre piattaforme garantisce la sicurezza dei dati dei clienti in caso di incidente o emergenza. Le piattaforme sono attive in ciascuna delle nostre infrastrutture nordamericane ed europee, il che significa che su ciascuna di esse è in esecuzione un'istanza dell'applicazione di Kyriba (Figura 2). Ciascun server di produzione di ciascuna piattaforma viene replicato sull'altra piattaforma utilizzando connessioni sicure e dispositivi di replica dedicate. In questa configurazione, i server della piattaforma A vengono replicati su una seconda infrastruttura nella piattaforma B e viceversa.

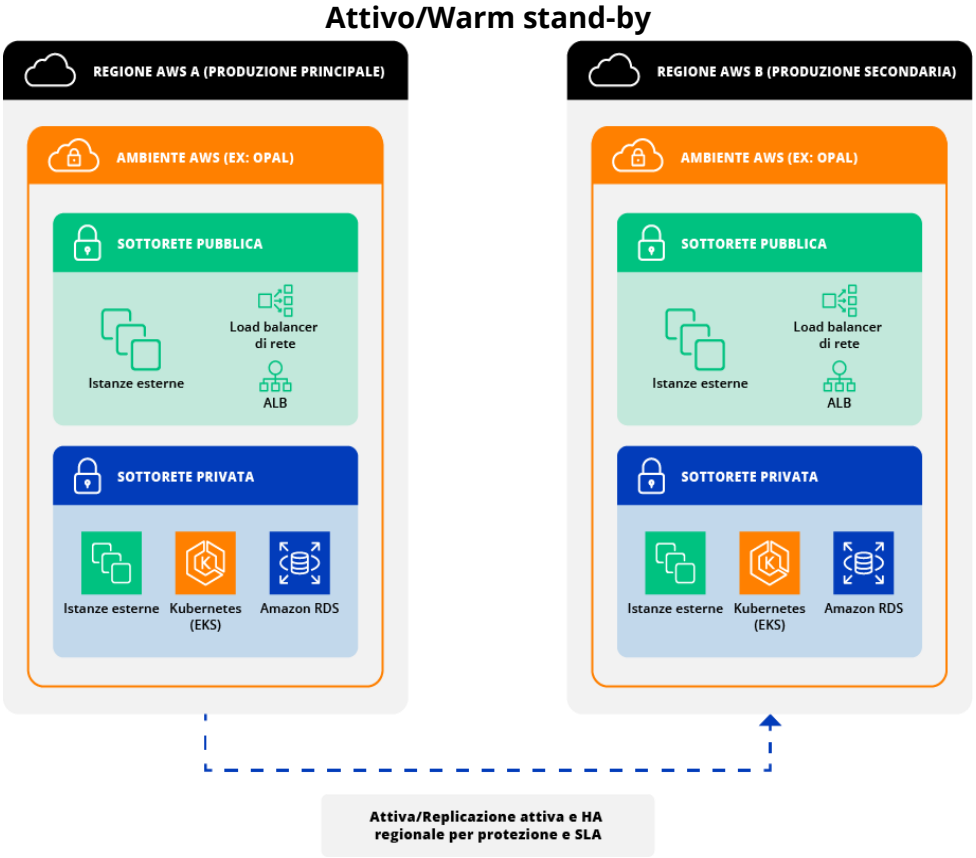

Figura 2: Configurazione di backup attivo/warm stand-by

Poiché la tesoreria deve operare quotidianamente, per garantire ai nostri clienti un'operatività senza interruzioni, abbiamo approntato e testiamo periodicamente (almeno una volta all'anno per ciascuna piattaforma) un piano di ripristino d'emergenza forzato. Il piano e la relativa documentazione vengono inoltre periodicamente rivisti e revisionati secondo le necessità. Il nostro piano di ripristino d'emergenza comprende la repliche di tutti i dati di configurazione e dei dati cliente. In questo modo possiamo tener fede ai nostri impegni in termini di RTO e RPO.

Per misurare la capacità di ridurre al minimo le perdite in termini di tempo e dati si utilizzano due parametri: il Recovery Time Objective (RTO) e il Recovery Point Objective (RPO). L'RTO di Kyriba è di 4 ore, mentre l'RPO è di 2 ore. Per incidente si intende un evento che porta Kyriba a prendere la decisione di dichiarare che si è in presenza di un'emergenza.

Per garantire che l'obiettivo di Kyriba possa essere raggiunto, il monitoraggio delle repliche viene effettuato quotidianamente dal nostro team tecnologico e operativo.

Kyriba ha anche stilato un documento di policy di gestione degli incidenti al fine di reagire prontamente a questi eventi avversi.

Per rimediare agli incidenti critici è attivo un Service Excellence Action Team (SEAT), in grado di reagire prontamente agli eventi con un potenziale impatto sulla sicurezza e sulla disponibilità delle tecnologie di Kyriba.

3.5. Backup e conservazione dei dati

Effettuiamo il backup di tutti i dati e di tutte le applicazioni dei clienti su dispositivi di backup in locale con cadenza giornaliera e settimanale.

I backup sono inoltre replicati su dispositivi in remoto dedicati ai ripristini d'emergenza ospitata sull'altra piattaforma.

Il team di tecnologia e operation verifica giornalmente lo stato dei backup per assicurarsi che siano stati eseguiti con successo e, in caso di necessita', adottare le opportune misure.

Di seguito è descritta la politica di conservazione dei dati di backup seguita da Kyriba:

Backup e conservazione dei dati: Piattaforma di produzione

Tipo di backup programmato	Quando viene effettuato?	Periodo di conservazione dei dati	Descrizione
Backup integrale	Settimanalmente	10 anni	Backup dell'intero server
Incrementale giornaliero	Quotidianamente	30 giornate	Tutti i dati di Kyriba e del cliente

Backup e conservazione dei dati: Piattaforma sandbox

Tipo di backup programmato	Quando viene effettuato?	Periodo di conservazione dei dati	Descrizione
Backup integrale	Settimanalmente	3 mesi	Backup dell'intero server
Incrementale giornaliero	Quotidianamente	15 giornate	Tutti i dati di Kyriba e del cliente

Per garantire la qualità e l'affidabilità della soluzione di backup e per conservare i backup, le cui dimensioni crescono nel tempo, Kyriba usa una soluzione di archiviazione basata sul cloud gestita da AWS.

Per evitare che questo cambiamento possa avere un impatto negativo sugli aspetti legali, contrattuali e legati alla sicurezza della soluzione Kyriba fornita ai clienti, e considerato che Amazon S3/Glacier è progettato per garantire al 99,999999999% la durabilità degli oggetti per un anno, osserviamo diversi principi volti a garantire la sicurezza dei dati:

- i dati del cliente vengono conservati su ciascuna delle piattaforme regionali
- prima di essere caricati su AWS Glacier, i dati vengono criptati Kyriba mantiene il controllo di tutte le chiavi di cifratura
- per caricare i dati su AWS Glacier vengono usati canali criptati
- gli archivi di backup di lungo termine vengono ulteriormente criptati da AWS

3.6. Risposta agli incidenti

Kyriba risponde agli incidenti basandosi sul livello di priorità assegnato loro dal cliente e da Kyriba. Nella tabella sotto sono indicati i tempi di risposta in base alla gravità degli incidenti.

Priorità	Descrizione	Linee guida per la risposta da parte di Kyriba
Priorità 1 *Incidenti critici*	Eventi estremamente gravi. In questa categoria rientrano: • Indisponibilità del servizio • Violazioni della sicurezza (effettive o presunte)	Responsabilità di Kyriba: • Orario principale: risposta in meno di 30 minuti • Orario secondario: risposta in meno di 4 ore • Kyriba assegnerà delle risorse per risolvere il problema o proporre una soluzione per aggirare il problema • Il cliente viene avvisato entro 15 minuti dalla conferma del problema • Ogni 4 ore il cliente riceve aggiornamenti sullo stato del problema e/o tali aggiornamenti vengono pubblicati su un sito alternativo. Il cliente può contattare lo staff di Kyriba, che garantisce tempi di risposta inferiori a 2 ore
Priorità 2 *Incidenti urgenti*	In questa categoria rientrano incidenti quali il peggioramento delle prestazioni dei servizi o l'indisponibilità di funzionalità dei servizi	• Orario principale: risposta in meno di 2 ore • Kyriba farà il possibile per risolvere il problema o proporre una soluzione per aggirarlo entro 2 giorni lavorativi
Priorità 3 *Richieste di informazioni e problemi senza alcun impatto sui servizi*	Tutte le richieste dei clienti, comprese, per esempio, le richieste di informazioni o di istruzioni per operazioni ordinarie	• Orario principale: risposta in meno di 8 ore

3.7. Centri di controllo di Kyriba e monitoraggio

Kyriba si impegna a offrire la massima disponibilità della sua applicazione SaaS. Una componente essenziale di tale disponibilità è fornita tramite i nostri due centri di controllo con sede a San Diego, CA, e a Parigi, Francia. In questi centri di controllo Kyriba utilizza tecnologie all'avanguardia per monitorare proattivamente i sistemi informatici essenziali e la sua infrastruttura di rete. Kyriba inoltre utilizza numerose interfacce personalizzate integrate nell'applicazione che le consentono di monitorare lo stato di salute complessivo dell'applicazione e di risolvere i problemi prima che abbiano un impatto sull'attività dei clienti.

3.8. Architettura del sito SaaS

La nostra architettura SaaS è progettata per offrire il massimo livello di sicurezza e i vantaggi derivanti da tiers logicamente separati sono sfruttati appieno grazie a un'architettura che utilizza due firewall.

Il firewall esterno viene usato per filtrare l'accesso aperto lato Internet, bloccare indirizzi IP pericolosi e controllare i flussi e le comunicazioni con Internet. Il firewall interno separa ciascun livello in una sotto-rete, autorizzando il passaggio da una sotto-rete a un'altra solo per i flussi appropriati. Per esempio, solo il server dell'applicazione può inviare richieste al database, mentre ogni richiesta al database proveniente dai livelli più esterni viene bloccata.

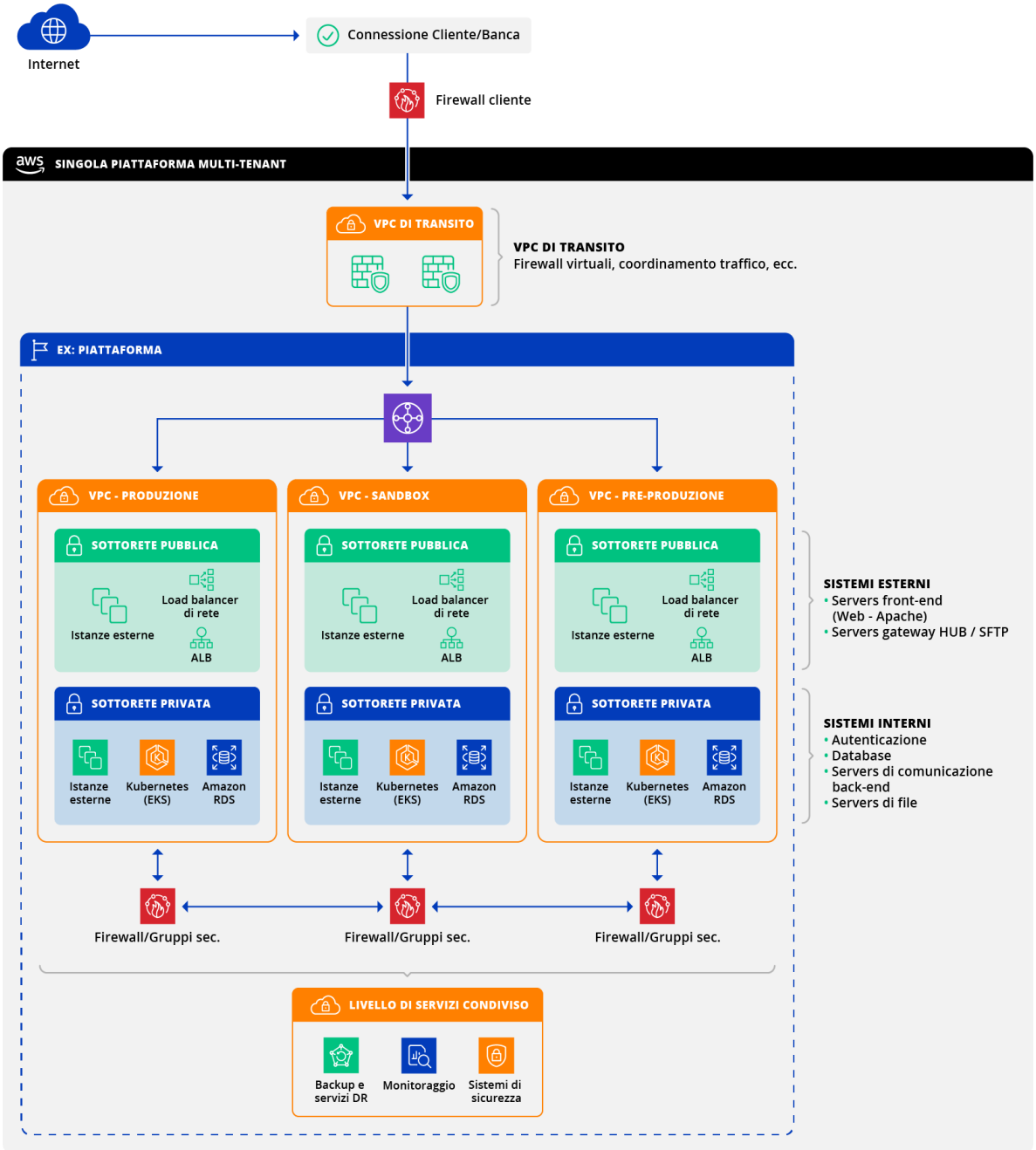

Figura 3: Architettura del sito host di Kyriba

Nel diagramma (Figura 3) dell'architettura del sito host, per semplicità tutti i tiers sono rappresentati da due macchine. La piattaforma di Kyriba è un ambiente completamente virtuale in cui l'utilizzo di ciascun server è attentamente monitorato.

4. Architettura, capacità, scalabilità

L'infrastruttura di Kyriba è totalmente flessibile e in grado di adattarsi alla crescita e alle esigenze di organizzative e ai progetti di tutti i clienti. La piattaforma si adatta rapidamente a un numero sempre crescente di utenti e Kyriba incrementa costantemente la capacità e la potenza della piattaforma di produzione per soddisfare le aspettative legate alle prestazioni e le esigenze di archiviazione. L'espansione della piattaforma viene programmata periodicamente sulla base dell'attività e della crescita dei clienti.

Per raggiungere questo obiettivo, sfruttiamo due aspetti delle nostre fondamenta tecniche: l'architettura multi-livello e il bilanciamento del carico.

4.1. Architettura multi-livello

L'architettura della soluzione di Kyriba è rigorosamente multi-livello. Ciascun livello comunica con gli altri tramite protocolli filtrati da firewall presenti sulla piattaforma di produzione. L'architettura dei server è organizzata in modo da segregare le funzioni all'interno dei livelli nel seguente modo:

Server front-end (server web)

- **Livello di presentazione**, un portale web che fornisce l'accesso a tutte le funzionalità interattive dell'applicazione. Serve tutte le pagine utilizzate per inserire transazioni o mostrare informazioni legate alle attività aziendali e supporta lo scambio dei file legato alle importazioni/esportazioni IT del cliente.

Server back-end (server dell'applicazione)

- **Livello business logic**, dove vengono eseguite tutte le regole dell'azienda.
- **Livello dei dati**, dove sono conservati tutti i dati relativi al livello business logic.
- **Livello di sicurezza**, dove sono conservati i dati sugli utenti e risiedono i diritti di alto livello (LDAP), nonché i certificati e le chiavi pubbliche, archiviati separatamente.
- **Livello di comunicazione**, dove avviene lo scambio di dati (esplicitamente autorizzato e rigorosamente messo in sicurezza attraverso rigide regole dei firewall, filtraggio IP e altri meccanismi di protezione) con banche, fornitori terzi di dati di mercato, ERP e sistemi dei clienti.

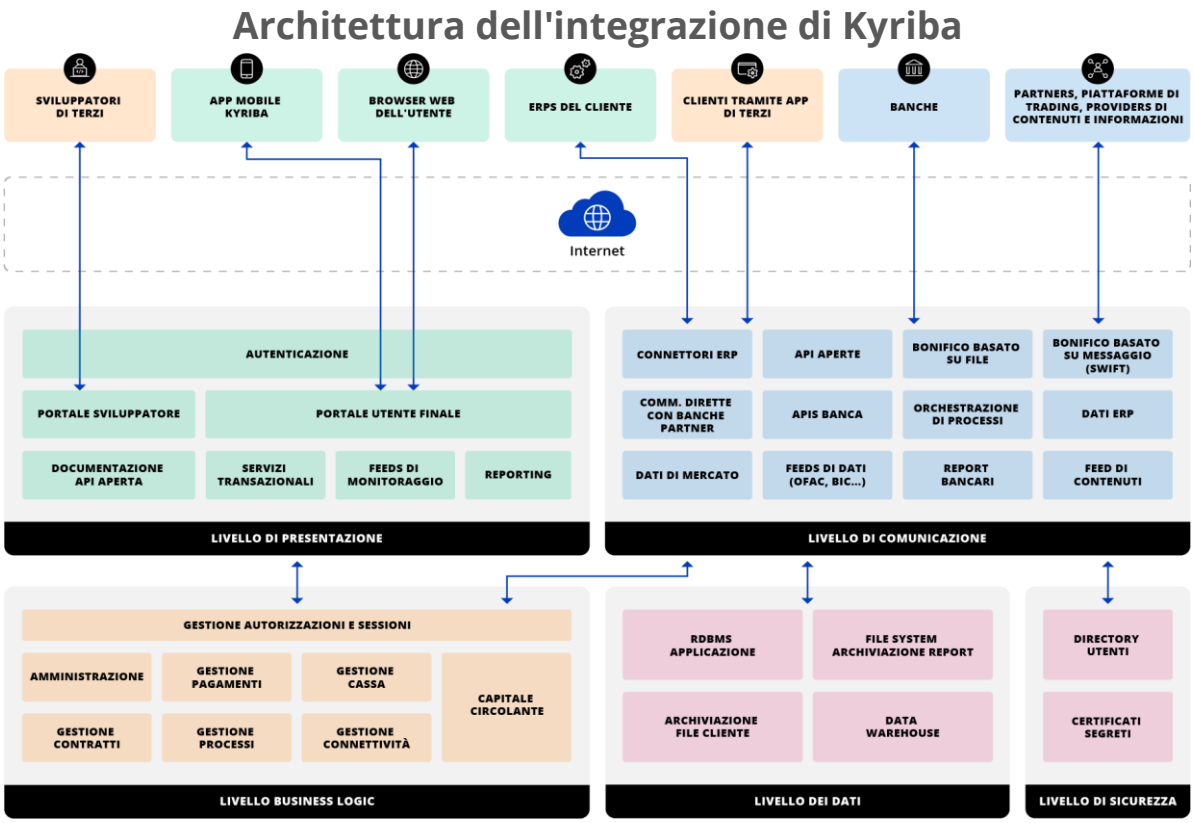

Figura 4: Livelli del prodotto di Kyriba

4.2. Load balancer

Il load balancer è un elemento che permette di distribuire il carico di lavoro tra più server. Inoltre consente di reindirizzare il traffico su un altro server nel caso in cui venisse rilevato un incidente. Per massimizzare la scalabilità del sistema, Kyriba utilizza più load balancer nell'ambito della propria piattaforma e della propria architettura.

4.3. Scalabilità, disponibilità e sicurezza

Grazie a questa architettura, Kyriba è in grado di rilevare gli incidenti e isolare il problema rapidamente e di garantire la disponibilità degli altri livelli. Il livello d'utilizzo di ciascun server è attentamente monitorato. Quando la potenza fornita da un livello diventa insufficiente, grazie alla tecnologia scalabile di AWS è possibile aggiungere server o altre risorse per incrementare automaticamente la potenza di quel livello. Per esempio, se il server dell'applicazione va in sovraccarico, Kyriba può incrementare la potenza del livello dei server delle applicazioni aggiungendovi un server simile.

Tutti gli scambi tra i livelli sono attentamente filtrati e verificati lungo tutto il processo. Alcune componenti possono ricevere richieste solo da determinate componenti individuate con precisione e solo tramite i protocolli appropriati. Il compito del firewall interno è filtrare tutti i flussi e consentire solo gli scambi autorizzati. Ciò fornisce un elevato livello di protezione da qualsiasi tentativo di hackeraggio.

L'elevata disponibilità della piattaforma è gestita livello per livello, il che consente di sfruttare i meccanismi di alta disponibilità degli strumenti implementati da Kyriba (server Apache, server EJB, database Oracle/RDS, LDAP, ecc.). Queste scelte consentono a Kyriba di applicare tecniche quali il clustering, gruppi di autoscaling e meccanismi di failover a ciascun livello separatamente, a seconda della sensibilità e dell'importanza dei servizi coinvolti.

Kyriba utilizza del middleware standard all'interno di un'architettura globale basata su J2EE, con un server EJB a sostenere la business logic. Gli LDAP gestiscono la validazione di tutte le autenticazioni degli utenti al momento dell'accesso e i dati vengono conservati in un robusto database Oracle RDS configurato in modalità HA (alta disponibilità). Inoltre, tutti i livelli con responsabilità tecnologiche precise sono nettamente isolati.

5. Sicurezza

5.1. Sicurezza: il cuore della soluzione

La nostra priorità è operare un'infrastruttura cloud di qualità superiore per offrire la migliore soluzione di gestione della tesoreria sul mercato. Siamo consapevoli del fatto che la sicurezza sia un fattore essenziale per il successo della soluzione e riconosciamo la necessità di adeguarci ai livelli di sicurezza utilizzati dai nostri clienti. Garantire la sicurezza di tutte le componenti della soluzione di Kyriba, dalle macchine fisiche ai dati e al trasferimento dei file, richiede un impegno costante ed è un obiettivo fondamentale per la nostra organizzazione e per le nostre operazioni. Il nostro modello di business e il contenuto dei dati da noi trattati richiedono, da parte nostra, la massima attenzione all'aspetto della sicurezza. Il nostro sistema è stato progettato per consentire l'applicazione, dalla codifica all'implementazione, di modelli di sicurezza di altissima qualità, che sono poi soggetti a verifiche periodiche. La nostra piattaforma viene sottoposta alle verifiche necessarie per accertarne la conformità agli standard ISO/IEC 27001:2013, AICPA SSAE 18/SOC 1 e IAASB ISAE SOC 2.

5.1.1. Valutazione del rischio

Il Management ha reso operativo un sistema di gestione della sicurezza informatica (information security management system, ISMS) per il processo di valutazione del rischio al fine di individuare e gestire i rischi che potrebbero interferire con la capacità di Kyriba di fornire servizi di applicazioni SaaS affidabili ai propri clienti. Tale processo prevede che i dirigenti identifichino i rischi significativi pertinenti alle proprie aree di competenza e che implementino le misure appropriate per far fronte a tali rischi.

Il processo di valutazione del rischio di Kyriba è volto a supportare le decisioni dei dirigenti e a rispondere alle potenziali minacce valutando i rischi e individuando i fattori decisionali importanti. La direzione esecutiva e il gruppo dirigente supervisionano le titolarità e le responsabilità per la gestione del rischio e sono coinvolti nel processo di identificazione dei rischi. In particolare, sono responsabili dell'individuazione degli elementi del rischio aziendale quali minacce, vulnerabilità, misura di salvaguardia e probabilità delle minacce e della determinazione delle azioni da intraprendere.

La direzione è responsabile dell'individuazione dei rischi che minacciano il raggiungimento degli obiettivi. La direzione ha perciò implementato un processo per l'individuazione dei rischi rilevanti afferenti alla sicurezza, alla disponibilità, all'integrità dell'elaborazione e alla riservatezza del sistema. Kyriba ha valutato le interazioni significative tra sé e le parti esterne rilevanti e i rischi che potrebbero interferire con la sua capacità di fornire servizi affidabili ai suoi clienti.

Il nostro processo di individuazione del rischio è di ampio respiro e prevede discussioni a vari livelli e tra varie componenti dell'azienda. La direzione prende in considerazione i rischi che possono sorgere tanto da fattori interni quanto da fattori esterni.

I principali membri della direzione esecutiva e dei team operativi si riuniscono almeno una volta l'anno per individuare e prendere in esame i rischi per il sistema. Oltre a valutare i rischi per l'hardware e per il software che danno corpo ai servizi offerti ai clienti, l'organizzazione si aggiorna continuamente in merito alle varie sfide al suo stato di sicurezza attraverso l'analisi delle tendenze operative emergenti dalle valutazioni di vulnerabilità della rete di produzione e test di penetrazione della rete annuali.

La valutazione del rischio coinvolge i principali soggetti interessati provenienti dai dipartimenti di sviluppo, conformità, sicurezza e operativo. Per coprire i rischi derivanti dai fornitori e agevolare il raggiungimento

degli obiettivi di sicurezza, disponibilità, integrità dell'elaborazione e riservatezza, la direzione effettua una valutazione dei fornitori e/o esamina i report delle verifiche cui si sono sottoposti almeno una volta l'anno.

Nell'ambito del processo, i rischi individuati vengono documentati, analizzati ed esaminati ufficialmente dalla direzione insieme alle relative strategie di mitigazione. Il processo di valutazione dei rischi include una valutazione delle attività di controllo volte alla mitigazione dei rischi derivanti da eventuali interruzioni di attività.

È stato messo in atto un programma di gestione dei fornitori per guidare il personale nell'individuazione, nel monitoraggio e nello sviluppo di strategie di gestione dei fornitori per la selezione di fornitori in grado di soddisfare i requisiti di Kyriba. Prima di elaborare i dati dei clienti, i fornitori vengono valutati nell'ambito di un processo di screening e poi approvati dalla direzione. I requisiti per il fornitore, l'ambito dei servizi, i ruoli, le responsabilità e i livelli di servizio vengono tutti documentati nei contratti di fornitura.

Prima di condividere con terze parti i dati designati come riservati, vengono firmati accordi di riservatezza e protezione.

Oltre a quelle relative alla valutazione dei rischi, la direzione ha individuato e messo in atto le misure necessarie per far fronte a tali rischi. A tal fine, sono stati definiti degli obiettivi di controllo per ciascuna area di rischio significativa. Sono state quindi definite le attività di controllo che permettono di gestire il raggiungimento di quegli obiettivi e che aiutano a mettere in atto correttamente ed efficientemente le azioni associate ai rischi individuati.

Il sistema di gestione del rischio informatico (ISMS) di Kyriba comprende la valutazione e il trattamento del rischio per le aree delle risorse umane, del controllo degli accessi, della sicurezza fisica, dello sviluppo delle applicazioni, del ripristino d'emergenza e molte altre ancora. Profondamente integrati in questo standard sono i concetti del continuo miglioramento, della quantificazione della valutazione del rischio e della metodologia del trattamento nonché la periodica revisione degli obiettivi, dei controlli e delle prestazioni dell'ISMS.

5.2. Politica sulla sicurezza dei dati di Kyriba

Kyriba ha redatto ufficialmente e messo in atto una politica sulla sicurezza dei dati per salvaguardare la sicurezza e la disponibilità della tecnologia di Kyriba, ivi inclusi i dati dei clienti ospitati sui server di Kyriba. È stato individuato un preciso assetto organizzativo che definisce le principali aree di autorità e responsabilità e le linee di responsabilità. Il Chief Information Security Officer (CISO) sovrintende alla sicurezza e alla disponibilità della tecnologia di Kyriba ed è supportato dai team di tecnologia e operazioni, del prodotto e di ingegneria.

Per quanto riguarda la gestione della sicurezza dei dati, Kyriba ha adottato un approccio trasparente e incentrato sulle partnership. Collaboriamo attivamente con i nostri clienti condividendo le nostre pratiche e apprendendo dalle loro, inizialmente tramite le risposte ai questionari sulla sicurezza e a conversazioni faccia a faccia, e poi con aggiornamenti e revisioni annuali. Questo approccio collaborativo ci permette di restare sempre al passo con il panorama della sicurezza e con le sue sfide in perenne evoluzione. Similmente, i nostri rapporti con fidati consulenti della sicurezza e revisori certificati ci consentono di restare aggiornati sulle sfide e sulle soluzioni emerse dall'esperienza di un ampio spettro di organizzazioni. Siamo convinti, e i nostri clienti ce lo confermano, che tutte queste azioni dimostrino il nostro impegno per una gestione sistematica della sicurezza dei dati.

Kyriba effettua verifiche e revisioni delle sue pratiche di sicurezza dei dati diverse volte l'anno. Tra questi controlli sono incluse le verifiche certificate SOC 1 e 2 Type 2 degli standard ISO 27001 e SSAE 18/ISAE 3000. L'importanza di queste verifiche è duplice. Innanzitutto, ci costringono a dimostrare di aver messo in atto i nostri controlli per l'intera durata del periodo di verifica, ossia l'intero anno, e non solo nei momenti in cui si è sotto osservazione. Inoltre si tratta di verifiche esaustive sullo staff, sui processi e sui controlli di Kyriba, non di report forniti da data center di terze parti, da altri fornitori di SaaS o da servizi cloud.

Kyriba è fermamente convinta che la sicurezza dei dati si fondi sulle partnership. Le verifiche di certificazione della sicurezza cui volontariamente ci sottoponiamo dimostrano che con noi i dati sono al sicuro; che ci

impegniamo affinché i nostri clienti sappiano di lavorare con un'organizzazione che conosce le responsabilità della gestione; e che Kyriba dispone dell'infrastruttura necessaria per gestire i dati sensibili che i clienti ci affidano.

In Kyriba, la sicurezza è radicata nella cultura aziendale. Continueremo a investire nel nostro staff, nei nostri sistemi e nei nostri processi per continuare a meritarci la vostra fiducia.

Il Chief Information Security Officer (CISO) è nominato dal CEO e risponde direttamente a lui. Il CISO definisce e sovrintende alla politica globale sulla sicurezza dei dati di Kyriba e aggiorna la politica in base alle necessità. Inoltre ha il potere di ordinare tutte le verifiche necessarie per accertare la conformità ai nostri impegni in merito alle certificazioni della sicurezza.

La politica interna sulla sicurezza dei dati di Kyriba include, tra gli altri, i seguenti contenuti:

- l'identificazione e la documentazione della disponibilità del sistema e dei relativi requisiti di sicurezza degli utenti autorizzati
- la classificazione dei dati secondo la loro criticità e sensibilità, sulla base della quale vengono definiti i requisiti di protezione dei dati, i diritti e le limitazioni di accesso e i requisiti per la conservazione e la distruzione dei dati
- un quadro dettagliato di gestione del rischio che definisce come Kyriba inquadra, valuta, monitora e reagisce ai rischi nel proprio ambiente
- il processo di gestione dei rischi derivanti da fornitori terzi
- la definizione di un programma globale di formazione e sensibilizzazione alla sicurezza
- politiche e procedure per la sicurezza fisica volte a prevenire l'accesso non autorizzato a strutture di Kyriba sicure
- la gestione degli incidenti e politiche e procedure di risposta
- la gestione degli utenti (aggiunta e rimozione degli utenti, modifica dei livelli di accesso degli utenti esistenti)
- l'assegnazione della responsabilità in merito alla disponibilità del sistema e della relativa sicurezza
- l'assegnazione della responsabilità in merito alle modifiche e alla manutenzione del sistema
- la definizione di politiche e procedure volte a garantire la continuità operativa e i ripristini d'emergenza
- i requisiti del ciclo di sviluppo del software, che includono il testing, la valutazione e l'autorizzazione dei componenti del sistema prima della loro implementazione
- l'indicazione di come vanno gestite le lamentele e le richieste circa la disponibilità del sistema e i relativi problemi di sicurezza
- l'individuazione e la mitigazione delle violazioni concernenti la disponibilità del sistema e della relativa sicurezza e degli altri incidenti
- la fornitura di programmi di formazione e di altre risorse a sostegno della disponibilità del sistema e delle relative politiche di sicurezza
- l'indicazione di come gestire le eccezioni e le situazioni non espressamente individuate per ciò che concerne la disponibilità del sistema e le relative politiche di sicurezza
- l'individuazione della normativa applicabile, degli impegni definiti, degli accordi sui livelli di servizio e delle altre obbligazioni contrattuali e la conformità a essi
- le politiche riguardanti la condivisione dei dati con terze parti

- il ripristino e la continuazione del servizio in conformità agli impegni presi con il cliente contrattualmente o in base ad altri accordi
- il monitoraggio della capacità del sistema di tenere fede agli impegni nei confronti dei clienti o ad altri accordi relativi alla disponibilità
- le politiche sulle email aziendali, sulle password e sulla pulizia dello schermo e della scrivania
- le politiche e le procedure riguardanti l'eliminazione e lo smaltimento sicuri dei dati.

Inoltre, la politica di Kyriba richiede periodici contatti con fornitori di sicurezza informatica di primissimo livello nel panorama mondiale affinché conducano dei test standard sulle reti. Infine, il personale dedicato allo sviluppo non può accedere ai dati di produzione dei clienti negli ambienti di produzione, sandbox e di pre-produzione.

5.3. Screening dei dipendenti

Kyriba attua pratiche di assunzione volte ad accertare che i nuovi dipendenti siano qualificati per il loro incarico e le responsabilità che ne derivano. Kyriba sfrutta i servizi di diversi fornitori e società di reclutamento esterne per selezionare i candidati e controllarne i precedenti. Kyriba prende in esame i risultati di tali controlli e li considera parte integrante del processo di assunzione. Kyriba può anche contattare gli ex colleghi del candidato per verificarne le referenze. Prima di essere assunti, i candidati devono anche sostenere un colloquio con l'alta dirigenza. Quando un nuovo dipendente viene assunto, il suo responsabile crea una richiesta elettronica che avvia il processo interno di creazione e configurazione del suo accesso al sistema in base all'incarico e alle responsabilità del dipendente. Il CISO definisce i vari profili professionali cui corrispondono diversi diritti di accesso, a seconda dell'incarico e delle relative responsabilità.

5.4. Sicurezza fisica del SaaS

I siti host presso Iron Mountain ed Equinix sono soggetti a rigide regole:

- i protocolli di sicurezza relativi all'accesso fisico consentono l'accesso a qualsivoglia sistema o dispositivo elettronico solo agli individui autorizzati
- solo il personale autorizzato ha accesso alle aree/stanze dei server o alle console di amministrazione
- tutti i dipendenti devono sempre esibire il proprio badge di identificazione
- i visitatori devono identificarsi ed essere sempre accompagnati
- i server bay sono sempre tenuti sotto chiave
- sono implementati sistemi antincendio a gas inerte ridondanti
- sono implementati sistemi di alimentazione e accessi a Internet ridondanti
- sono implementati dispositivi elettronici per il monitoraggio e la notifica di attività in entrata o in uscita inattese, tra cui firewall, sistemi di rilevamento/prevenzione delle intrusioni (IDS/IPS) e altri dispositivi di sicurezza.

5.5. Comunicazione tramite Internet

Quando si usa la comunicazione tramite Internet vengono utilizzati meccanismi di cifratura a minimo 128-bit (HTTPS), ma che possono arrivare a 256 bit se il browser è in grado di supportarli e nei casi in cui ciò è ammesso dalla legge. Inoltre, la connessione interna tra le nostre piattaforme è messa in sicurezza da una connessione VPN sicura che utilizza lo standard IPsec.

I clienti hanno la possibilità di firmare digitalmente e/o criptare i file che vengono scambiati tramite la piattaforma Kyriba.

5.6. Accesso ai dati da parte di Kyriba

Tutte le informazioni sui nostri siti sono trattate come riservate e la riservatezza dei dati è gestita attraverso un set di regole estremamente rigide. L'accesso al database e ai server della piattaforma è strettamente controllato sulla base di tale set di regole. Inoltre, tutte le attività eseguite sulla piattaforma vengono registrate.

Ai dipendenti dei data center viene consentito l'accesso fisico sulla base di documentate esigenze aziendali e di restrizioni di sicurezza, mentre l'accesso logico ai dati dei clienti di Kyriba è sempre negato. I dipendenti di Kyriba non hanno accesso logico ai dati dei clienti, a meno che non siano i clienti stessi a concederglielo. Dei dispositivi elettronici monitorano e segnalano le attività eseguite dai dipendenti in occasione dei loro accessi al sistema.

5.6.1. Cifratura a livello di applicazione

Inoltre, per rafforzare ulteriormente la riservatezza dei dati, su richiesta del cliente Kyriba ha la possibilità di cifrare al livello dell'applicazione determinati dati (nome, cognome, telefono, indirizzo, nome della società, descrizione del conto corrente, descrizione dell'estratto conto, descrizione del pagamento) nel database utilizzando una cifratura AES-128-bit.

5.7. Cifratura dei dati a riposo

Kyriba si serve della cifratura predefinita di AWS per tutti i dati archiviati. Questo servizio cripta automaticamente tutti i blocchi e i file con una cifratura a 256-bit prima di archiviare i dati su dischi virtuali. Poiché le chiavi di cifratura sono note solo al sistema di archiviazione, i dati conservati su questi dischi NVMe diventano illeggibili qualora i dischi vengano rimossi dal sistema di archiviazione a seguito di una violazione della sicurezza del data center o di normali procedure di servizio. Una tale cifratura del mezzo di archiviazione elimina la necessità di rimuovere i dati alla fine del loro ciclo di vita, poiché in tutti i dischi AWS i dati a riposo vengono criptati. Per maggiori informazioni al riguardo, si prega di consultare https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/data-protection.html.

5.8. Segregazione dei dati

L'isolamento dei dati di ciascun cliente viene attuato basandosi sul concetto di segregazione dei dati, con la creazione di un dominio dati virtuale privato (Virtual Private Data Domain o VPDD) per ciascun cliente. Kyriba utilizza uno specifico meccanismo di segregazione dei dati basato su un identificatore esclusivo di dominio dati. Ciascun cliente di Kyriba possiede un proprio identificatore esclusivo di dominio dati. Questo meccanismo non può essere aggirato da nessun codice di livello funzionale. Ogni richiesta dati afferente ai dati dei clienti è automaticamente soggetta a un filtraggio aggiuntivo basato sull'identificatore esclusivo ed eseguito automaticamente da un livello di accesso ai dati di basso livello all'interno dell'architettura del database. Inoltre, se il cliente ha specificato un determinato livello minimo per l'accesso a quei dati, al fine di impedire accessi non autorizzati la richiesta passa anche attraverso questo filtro automatico secondario. I tentativi di aggirare queste misure di sicurezza generano un errore di sistema. Questi meccanismi si affiancano al normale uso dell'integrità referenziale.

5.9. Gestione delle sessioni

Quando i client si autenticano per accedere a Kyriba, in base al profilo dell'utente viene aperta una sessione per la quale varranno i diritti di accesso assegnati a quell'utente. I diritti d'accesso di base sono configurati nell'LDAP, mentre i dettagli delle autorizzazioni sono archiviati nel database.

Le sessioni vengono organizzate solo dopo l'autenticazione. In questo modo non è possibile prendere il controllo di una sessione dall'esterno o modificare illegittimamente i diritti mentre la sessione è in corso. Quanto all'accesso dei clienti, a ciascun cliente e a ciascuno dei suoi utenti è assegnato un identificatore esclusivo. Kyriba crea l'identificatore esclusivo per il cliente, dopodiché questi crea gli utenti a cui concedere l'accesso. Tutti i dati archiviati nel database di Kyriba sono assegnati all'identificatore esclusivo del cliente. Quando un utente tenta di accedere a dei dati presenti nel database di Kyriba, l'identificatore del cliente viene sistematicamente confrontato

con quello dell'utente per validare il recupero di quei particolari dati. Questo processo consente l'attuazione di una rigida segregazione dell'accesso ai dati da parte degli utenti.

5.10. Autenticazione degli utenti

Kyriba assegna a ciascun cliente un certo numero di token di accesso logico (utenti in contemporanea). Per ciascun cliente ci sarà almeno un amministratore di Kyriba con il compito di assegnare i token agli utenti e abilitato a effettuare modifiche o aggiornamenti all'accesso degli utenti. L'accesso di un nuovo utente e le modifiche all'accesso degli utenti richiedono una formale autorizzazione a monte (ossia al momento della creazione) da parte dello staff di Kyriba.

L'amministratore o gli amministratori di un determinato cliente possiedono tutti i diritti utente di amministrazione, compresi quelli di gestione degli utenti e dei gruppi (aggiunta, modifica, eliminazione) e di configurazione dei diritti di accesso di ciascun utente in base al ruolo. L'amministratore può limitare le funzionalità cui ciascun utente può accedere. Inoltre, l'amministratore può limitare l'accesso ai dati da parte dell'utente ai soli dati di competenza di quest'ultimo.

Esistono diversi modi per autenticare un utente:

5.10.1. Autenticazione standard (ID + password)

Le password degli utenti devono essere composte da un certo numero minimo di caratteri e devono soddisfare determinati requisiti di complessità, definibili dal singolo cliente. Gli utenti vengono costretti a modificare la password periodicamente e automaticamente.

5.10.2. Autenticazione a due fattori

L'autenticazione a due fattori può essere applicata all'autenticazione di utenti con determinati privilegi. La piattaforma può attivare una seconda fase di autenticazione basata su un meccanismo OTP (one time password). La password OTP viene generata all'interno dell'applicazione di Kyriba e può essere trasmessa attraverso diversi mezzi: SMS, Token USB (Yubikey®), Google Authenticator o altre applicazioni TOTP simili.

5.10.3. Single Sign On

SSO è l'acronimo di **S**ingle **S**ign **O**n (autenticazione delegata). Essa consente agli utenti Kyriba di ri-utilizzare un'identità (autenticazione) gestita in un'applicazione di terzi che funge da fornitore dell'identità, mentre Kyriba assume il ruolo di fornitore di servizi che utilizza le identità autenticate dal fornitore d'identità.

Il single sign-on viene supportato tramite il protocollo SAML2. Il cliente può stabilire le proprie regole interne di autenticazione (autenticazione standard, sistema di autenticazione interna a due fattori, ecc.) e può utilizzare per l'autenticazione la propria directory interna (database di ID + password). Kyriba delega l'autenticazione tramite protocollo SAML2, ma i diritti di accesso vengono sempre gestiti all'interno di Kyriba. In questo modo, gli ex dipendenti rimossi dal sistema delle risorse umane del cliente non potranno più accedere a Kyriba anche se i loro diritti d'accesso non sono stati rimossi da Kyriba.

5.11. Controllo funzionale degli accessi

Dalla postazione di lavoro dell'utente finale è possibile richiedere solo le azioni autorizzate per quel profilo utente. Anche qualora l'utente finale sappia come vengono formattate e inviate le richieste dal browser al back-end, potrà accedere solo alle funzionalità autorizzate per il suo profilo. Per ogni richiesta di funzionalità viene eseguito un controllo di validità nel back-end per verificarne l'autorizzazione. Di conseguenza, anche se un utente connesso tentasse di alterare le richieste, potrebbe comunque accedere solo alle funzionalità autorizzate. Nel caso in cui venga richiesto l'accesso ad altre funzionalità, non soltanto l'accesso viene negato, ma viene generato un avviso di sicurezza.

5.12. Possibilità di doppio amministratore

In ottemperanza alle linee guida SOC 1/SOC 2, l'applicazione supporta le funzionalita' di dual administration per consentire che almeno due utenti diversi approvino le stesse modifiche o accettino lo stesso ordine di transazione. I clienti possono impostare un flusso di lavoro più sofisticato con un numero illimitato di passaggi e di fasi di approvazione, con la possibilità di personalizzare le schermate d'immissione per limitare l'immissione o la visualizzazione dei dati ai soli dati necessari affinché un utente possa inviare/completare/approvare una determinata modifica/creazione di dati.

5.13. Trasferimento gestito dei file e gestione della prova

I servizi di Kyriba includono il trasferimento gestito dei file (managed file transfer o MFT) da/verso le banche e i sistemi informatici del cliente. Kyriba gestisce molti protocolli e standard di cifratura, compresi molti standard bancari pre-esistenti.

Nei casi specificati dal cliente, gli utenti possono ricevere la richiesta di creare una prova elettronica o un documento firmato elettronicamente in vista di verifiche interne e/o per il riconoscimento remoto della firma di autorizzazione da parte della banca. Kyriba supporta tutti questi aspetti della creazione, dell'archiviazione, della visualizzazione per verifica e del recupero della prova elettronica. Le prove delle richieste di trasferimento e dello scambio di file sono parte integrante dei servizi di gestione della prova di Kyriba.

5.14. Filtraggio - Traffico su Internet

Kyriba utilizza un firewall esterno per proteggere tutti gli accessi da Internet al server front-end provenienti da utenti non autorizzati. Questo firewall di primo livello protegge tutti i server front-end, bloccando tutto il traffico non autorizzato.

Kyriba ha implementato sistemi di filtraggio e monitoraggio aggiornati con firewall multi-livello integrati per controllare e analizzare il traffico di rete in ingresso e in uscita e un sistema di rilevamento delle intrusioni per individuare e segnalare attività dannose. Consigliamo ai nostri clienti di consentire l'accesso alla rete nell'ambiente di lavoro aziendale solo da punti d'ingresso noti e fidati (LAN aziendale, rete controllata, VPN, ecc.)

5.15. Filtraggio interno

Il flusso delle comunicazioni tra i livelli è filtrato da un firewall interno, che limita il traffico autorizzato per ciascun utente servendosi di protocolli appropriati. Questa configurazione di sicurezza rende difficile violare il sistema, poiché a giungere a destinazione sono solo le richieste pertinenti inviate dalle componenti autorizzate al destinatario appropriato tramite il protocollo e il percorso corretti.

Inoltre, l'organizzazione adottata per i livelli consente di attivare meccanismi di sicurezza all'interno dei singoli livelli. I server front-end inviano richieste ai server EJB. Le componenti EJB inviano richieste al database. La postazione di lavoro dell'utente finale e i server front-end non possono inviare direttamente alcuna richiesta al database. Il server del database è completamente invisibile ai server front-end. I server front-end non contengono alcuna componente in grado di connettersi al database.

Inoltre, i livelli sono separati fisicamente o logicamente. Ciò consente un filtraggio più efficiente tra di essi. Anche se un hacker riuscisse a connettersi a un server front-end, poi non avrebbe modo di connettersi ai server del database.

5.16. Tracciabilità

Un'ampia serie di file di log su tutti i server front-end, i server https/http, i server delle applicazioni back-end e i server di comunicazione con gli hub consente a Kyriba di sapere in forma aggregata quali azioni sono state eseguite su qualsiasi piattaforma Kyriba da ciascun cliente.

Tuttavia, a causa della complessità e della sensibilità dei dati contenuti nei file di log dettagliati, l'accesso e l'esame di tali file vengono eseguiti solo se necessario, in caso di indagini specifiche o di attività di diagnostica e risoluzione di errori. L'accesso ai file di log è sottoposto a esame durante le verifiche SOC 1/SOC 2 per garantire la riservatezza dei dati in essi contenuti.

Inoltre, Kyriba utilizza degli speciali gateway dedicati per controllare e registrare tutte le azioni compiute nell'ambito dell'infrastruttura. Tale soluzione tecnologica è installata nelle nostre piattaforme e controlla i diritti di accesso a esse e registra le sessioni di lavoro. Tali registrazioni possono essere esaminate in caso di necessità (durante una verifica o nel corso di indagini su un incidente inspiegato).

5.17. Sistema di prevenzione delle intrusioni

Per impedire che exploit di vulnerabilità note e ignote della rete e del livello delle applicazioni danneggino o compromettano la piattaforma, Kyriba usa un sistema di prevenzione delle intrusioni (IPS) standard/accettato che monitora le attività di rete e di sistema e genera report e avvisi.

5.18. Gestione degli incidenti

Kyriba ha anche stilato una politica di gestione degli incidenti proprio per reagire prontamente a questi eventi avversi.

Per rimediare agli incidenti critici è attivo uno Special Work Action Team (SWAT), in grado di reagire prontamente agli eventi con un potenziale impatto sulla sicurezza e sulla disponibilità della tecnologia di Kyriba. Una procedura di risposta alle violazioni della sicurezza è stilata e diffusa tra tutti gli individui interessati (dipendenti, appaltatori, lavoratori temporanei, utenti di terze parti).

5.19. Firewall multi-livello

L'architettura della piattaforma SaaS è progettata per garantire il massimo livello di sicurezza. Tutti i server e i firewall vengono periodicamente aggiornati per applicarvi le più recenti patch di sicurezza e in tutti i server sono aperti solo le porte e i servizi necessari. Inoltre, l'architettura è costituita da livelli separati logicamente. Tale separazione è attuata tramite regole di sicurezza avanzate applicate ai firewall, il che offre notevoli vantaggi in termini di sicurezza.

Il firewall esterno viene usato per filtrare l'accesso aperto lato Internet, bloccare indirizzi IP riconosciuti come dannosi o pericolosi e controllare i flussi e le comunicazioni con Internet.

Il firewall interno separa ciascun livello in una sotto-rete o zona di sicurezza. Solo i flussi appropriati vengono autorizzati tra una sotto-rete e l'altra. Per esempio, solo il server dell'applicazione può inviare richieste al database. Ogni richiesta al database proveniente dai livelli più esterni viene bloccata. Questa configurazione di sicurezza rende difficile violare il sistema, poiché solo i livelli autorizzati possono compiere su un determinato livello le azioni autorizzate utilizzando i protocolli autorizzati. In questo modo, i livelli sensibili (database e comunicazione con le banche) sono molto ben isolati e nascosti all'interno dell'infrastruttura.

5.20. Sicurezza di rete

Un'azione può essere eseguita sul server dell'applicazione solo se è attiva una sessione autorizzata e solo se coerente con i diritti associati a quella sessione. Per esempio, se un dipendente malintenzionato cede le sue credenziali di login autorizzate a un individuo non autorizzato, questi potrà eseguire solo le azioni autorizzate per quel profilo.

A tal fine vengono definiti vari profili professionali cui corrispondono diversi diritti di accesso. Il personale del team di sviluppo non ha accesso all'ambiente di produzione. Solo il personale del team tecnologia e operazioni ha accesso all'ambiente di produzione per recuperare dati a fini manutentivi (per es., per controllare le impostazioni di configurazione, analizzare i file di log, ecc.) e per migrare il codice dallo sviluppo alla produzione. Gli accessi all'ambiente di produzione sono registrati e le modifiche sono annotate in un documento di configurazione della piattaforma ed esaminate su base trimestrale. Per accedere alla rete di produzione è richiesta un'autenticazione a più fattori (multifactor authentication, MFA).

La rete di amministrazione è isolata dalla rete operativa e non c'è nessun nodo della rete operativa che ha accesso a tutti gli altri server. Non è possibile accedere alla rete amministrativa da Internet.

Kyriba utilizza antivirus in tutti i livelli della sua infrastruttura. Il primo livello è la postazione di lavoro. Tutte le postazioni di lavoro sono protette da uno dei software antivirus più affidabili presenti sul mercato e ogni due ore viene eseguito un controllo sui client di tutte le postazioni di lavoro per verificare che siano aggiornati. Allo stesso tempo, ogni giorno gli aggiornamenti di sicurezza vengono controllati e implementati in ciascuna postazione di lavoro. Il secondo livello sono i nostri server. Il nostro firewall integra un processo inline e stream-based di prevenzione di infezione da malware che protegge i nostri server dai virus e blocca il malware al livello del gateway prima che possa raggiungere l'host bersaglio. Inoltre, ci protegge da download nascosti e dalle botnet.

Le patch di sicurezza e la manutenzione del sistema operativo vengono aggiornati da meccanismi automatici e un fornitore terzo specializzato in quest'area verifica la presenza di vulnerabilità nelle nuove versioni dell'applicazione di Kyriba.

5.21. Sviluppo sicuro del software

Kyriba ha implementato un programma di sicurezza del software che allinea Kyriba con le pratiche di sviluppo sicuro del software indicate da OWASP e SANS. Tale programma prevede l'analisi del codice statico, condotta sul codebase di Kyriba in modo continuativo e prima di implementare una nuova versione del software con modifiche importanti. Il programma prevede inoltre un'analisi automatica del codice dinamico, la gestione dei pacchetti software di terze parti e un programma di formazione per gli sviluppatori e per il personale della sicurezza di Kyriba sul tema della sicurezza del codice. Kyriba ha ottenuto da Veracode l'attestazione di *Veracode Verified.* Il programma Veracode Verified è un'attestazione di terzi con il quale si accerta che Kyriba utilizza per la propria applicazione un processo di sviluppo sicuro.

5.22. Garanzie e conformità

Test di sicurezza compiuti da terze parti

Ogni anno, Gotham Digital Science esegue un test di penetrazione sulle applicazioni e sulle reti di Kyriba. Le verifiche programmate sono condotte sia in modalità "scatola nera" (non viene fornita alcuna informazione), sia in modalità "scatola bianca" (vengono fornite informazioni e un ID e una password validi). Nell'improbabile caso di effettiva violazione del sistema, ai tecnici della sicurezza non è consentito visualizzare dati riservati. Le raccomandazioni risultanti dai test vengono poi applicate alla piattaforma. La lettera di attestazione dei risultati della verifica può essere fornita ai potenziali clienti a seguito della firma di un accordo di riservatezza, nonché ai clienti di Kyriba già esistenti.

Kyriba inoltre utilizza la soluzione di Tenable per l'esecuzione su base mensile di valutazioni sulle vulnerabilità a livello globale dei sistemi di produzione collegati a Internet.

Validazione dell'efficacia dei controlli di sicurezza

Kyriba effettua verifiche e revisioni delle sue pratiche di sicurezza dei dati diverse volte l'anno. Tra questi controlli sono incluse le verifiche certificate SOC 1 e 2 Type 2 degli standard ISO 27001 e SSAE 18/ISAE 3000. L'importanza di queste verifiche è duplice. Innanzitutto, ci costringono a dimostrare di aver messo in atto i nostri controlli per l'intera durata del periodo di verifica, ossia l'intero anno, e non solo nei momenti in cui si è sotto osservazione. Inoltre si tratta di verifiche esaustive sullo staff, sui processi e sui controlli di Kyriba, non di report forniti da data center di terze parti, da altri fornitori di SaaS o da servizi cloud.

Kyriba è fermamente convinta che la sicurezza dei dati si fondi sulle partnership. Le verifiche di certificazione della sicurezza cui volontariamente ci sottoponiamo dimostrano che con noi i dati sono al sicuro; che ci impegniamo affinché i nostri clienti sappiano di lavorare con un'organizzazione che conosce le responsabilità della gestione; e che Kyriba dispone dell'infrastruttura necessaria per gestire i dati sensibili che i clienti ci affidano.

La nostra piattaforma viene sottoposta alle verifiche necessarie per accertarne la conformità agli standard ISO/IEC 27001:2013 e SSAE 18/SOC 1 e SOC 2.

SSAE 18 e ISAE 3000

Lo standard SSAE 18/ISAE 3402 è definito e regolato dall'American Institute of Certified Public Accountants e dall'International Accounting Standards Board allo scopo di rassicurare i clienti di un'azienda in merito all'efficacia dei controlli nell'ambito dell'organizzazione che presta i servizi. Kyriba si sottopone a verifiche SSAE 18/SOC 1 Type 2 (in precedenza: SAS 70 e SSAE 16) e SOC 2 Type 2 dal 2013. Con l'adozione dello standard SSAE 18, alle aziende sottoposte a verifica si richiede di condurre un'ulteriore attività di due diligence con riguardo a fornitori terzi di sotto-servizi, nel nostro caso le aziende che forniscono un servizio a Kyriba. L'effettiva conduzione di tale attività viene dimostrata dall'esecuzione di esami approfonditi sui fornitori di servizi critici e dall'applicazione delle loro User Control Considerations sui controlli di Kyriba per assicurare la coerenza e la completezza dei controlli tra le diverse organizzazioni.

Ogni anno, Kyriba si sottopone a verifica rispetto agli Statements on Standards for Attestation Engagements (SSAE) n. 18 (SOC 1) per assicurarsi di soddisfarne i requisiti. I nostri processi prevedono punti di controllo rigorosi, eseguiti internamente, secondo necessità, su base giornaliera, settimanale, mensile e trimestrale. Inoltre, gli enti verificatori effettuano sistematicamente visite in presenza negli uffici di Kyriba.

Precedentemente noto come SAS70, SSAE n. 18 (altresì detto SOC 1) è uno standard di attestazione emesso dall'American Institute of Certified Public Accountants (AICPA). In vigore dal 15 giugno 2011, questo standard è pertinente, nelle organizzazioni fornitrici di servizi, ai controlli interni sul reporting finanziario delle entità utilizzatrici. Il report fornisce un'opinione sulla correttezza della descrizione dei controlli, sull'adeguatezza della loro progettazione e sulla loro efficacia operativa, oltre a una descrizione dei test condotti sui controlli e dei risultati. Kyriba dispone della certificazione SOC 1 Type 2.

Lo standard SOC 2 è pertinente, nelle organizzazioni fornitrici di servizi, ai controlli relativi a sicurezza, disponibilità e integrità dell'elaborazione dei sistemi o alla riservatezza dei dati elaborati per conto delle entità utilizzatrici. Il report fornisce un'opinione sulla correttezza della descrizione dei controlli, sull'adeguatezza della loro progettazione e, nel caso del report "Type 2", un'opinione sull'efficacia operativa dei controlli e una descrizione dei test condotti sui controlli e dei risultati. Kyriba attualmente dispone della certificazione SOC 2 Type 2 in relazione a tutti e cinque i principi di affidabilità.

ISO 27001

Lo standard ISO 27001 è un processo di certificazione riconosciuto a livello internazionale che verifica l'implementazione e l'efficacia di 114 controlli di sicurezza informatica specifici, come definiti dall'International Organization for Standardization (ISO). Per ottenere la certificazione ISO 27001, l'organizzazione deve dimostrare di disporre di un sistema di gestione della sicurezza informatica (ISMS) funzionante e di essere in grado di mitigare i rischi grazie all'implementazione di controlli derivanti da processi, politiche o sistemi nei vari dipartimenti e su tutto il personale. L'ISMS è un sistema completo a garanzia della sicurezza informatica e le organizzazioni che hanno raggiunto questo standard hanno dimostrato, come minimo, di disporre di un solido sistema per la gestione della propria sicurezza informatica.

Per il mantenimento della certificazione occorrono due verifiche annuali dei processi e dei controlli dell'ISMS. La prima verifica è denominata Internal Audit e, a dispetto del nome, per essa Kyriba ha scelto di servirsi di un verificatore terzo e certificato. Per la seconda verifica ai fini della certificazione, Kyriba ha scelto di servirsi di Schellman & Company. Il logo della certificazione ISO 27001 è visibile sul sito di Kyriba, mentre la conferma dello stato della certificazione si trova nell'elenco delle certificazioni di Schellman. Kyriba ha iniziato il suo viaggio verso la certificazione ISO 27001 nel 2019, dopo aver acquisito FireApps (ora prodotti Kyriba FX) e, con una ricertificazione, a fine 2020 ne ha ottenuto l'ampliamento dell'ambito, che ora include l'applicazione di Kyriba.

L'ISMS comprende la valutazione e il trattamento del rischio per le aree delle risorse umane, del controllo degli accessi, della sicurezza fisica, dello sviluppo delle applicazioni, del ripristino d'emergenza e molte altre ancora. Profondamente integrati in questo standard sono i concetti del continuo miglioramento, della quantificazione della valutazione del rischio e della metodologia del trattamento nonché la periodica revisione degli obiettivi, dei controlli e delle prestazioni dell'ISMS.

Questionari sulla sicurezza ai clienti

A tutti i clienti forniamo la succitata documentazione di garanzia, di conformità e di reporting (ISO, SOC, SWIFT, ecc.), oltre a questionari sulla sicurezza CAIQ precompilati di Cloud Security Alliance e di SIG Lite.

5.23. Centro di cyberdifesa

Kyriba dispone di un centro di cyberdifesa (Cyber Defense Center o CDC). Il CDC è responsabile della risposta agli incidenti di sicurezza informatica. Lo scopo del Cyber Defense Center e del team di risposta agli incidenti di cybersicurezza (Cyber Security Incident Response Team o CSIRT) è rilevare e reagire agli incidenti di sicurezza informatica, determinarne la portata e il livello di rischio, rispondere in maniera adeguata, comunicare gli esiti e il rischio a tutti i soggetti interessati e ridurre l'impatto e la probabilità del riverificarsi dell'incidente in futuro.

L'organizzazione di Kyriba è esperta e certificata nelle aree della sicurezza informatica coperte da CISSP, CRISC, GIAC e PMP. Il nostro team di sicurezza informatica è esperto conoscitore di vari framework di sicurezza quali ISO, PCI, FedRAMP, DOD e NIST. Al centro delle operazioni del nostro CDC opera Splunk, il nostro sistema di sicurezza informatica e gestione degli eventi (Security Information and Event Management o SIEM).

6. Fondamenta tecniche

6.1. Fondamenta tecniche

Le fondamenta tecniche (TF) sono l'insieme di tecnologie compatibili utilizzate per creare una piattaforma. Attualmente Kyriba supporta, testa e monitora diverse TF, che sono implementate in piattaforme di produzione e di prova. Le patch, i service pack e gli aggiornamenti sono tutti testati in queste piattaforme prima di essere implementate nelle piattaforme online.

Le TF attualmente supportate sono:

Livello	Tecnologie supportate
Browser dell'utente finale	Chrome, Edge, IE (versione attuale e le due precedenti)
Server web	Server HTTPs (TLS)
Server delle applicazioni	WildFly
Sistema operativo	Linux, Windows
Database	Oracle RDBMS
Directory	LDAP
Telecomunicazioni	Progettate secondo le specifiche esigenze o connessione all'hub di connettività

Kyriba supporta attivamente più TF per mantenere la conformità ai requisiti interni ed esterni e l'indipendenza software dei propri servizi. Le TF sono progettate per grandi piattaforme in grado di servire un vasto numero di client.

6.2. SaaS, Internet, Intranet

La soluzione è una piattaforma SaaS che serve migliaia di client che accedono alla piattaforma tramite Internet. Sono disponibili due modalità di accesso al firewall front-end:

- certificati X.509 da qualsiasi punto del globo
- certificati X.509 con filtraggio IP facoltativo. Questa modalità è dedicata a chi desidera eseguire i client in una modalità simil-Intranet con punti di accesso a Kyriba limitati. In questo assetto, gli utenti dei client possono connettersi al servizio solo da uno degli IP inseriti in una specifica lista. La lista degli IP approvati può operare al livello:
- del client: si applica a tutti gli utenti o a un determinato insieme di IP aziendali diversi
- dell'utente: si predispone un elenco delle eccezioni degli IP utente per utente (per es., i dirigenti possono accedere all'applicazione da località diverse).

Nella maggior parte dei casi, la lista degli IP approvati opera al livello del client (si applica a tutti gli utenti), con la possibilità di predisporre un elenco delle eccezioni degli IP utente per utente.

6.3. Scambio di dati con la piattaforma di Kyriba

La soluzione di Kyriba è progettata per comunicare con varie entità:

- banche (estratti conto, documenti di conferma, pagamenti, ecc.)
- ERP (previsioni, pagamenti, ecc.)
- fornitori di contenuti (tassi, valori, dati, ecc.)
- fornitori di servizi terzi (transazioni FX, flussi di cassa da operazioni di investimento, ecc.)

6.4. Kyriba Connectivity

Le componenti di comunicazione con banche e terze parti sono implementate direttamente nella piattaforma tramite server dedicati, ciascuno dei quali copre un certo numero di protocolli e formati.

Si può accedere a Kyriba Connectivity tramite link sicuri che operano su Internet e che consentono di inviare e ricevere file dagli istituti finanziari. Laddove sia richiesto, è possibile firmare elettronicamente i file di rimessa. In questo caso, Kyriba Connectivity invita l'utente a firmare il file utilizzando una soluzione di firma elettronica appropriata (per es., smartcard) e applica il requisito della doppia firma nel caso in cui sia richiesto dal protocollo o da regole aziendali interne definite dal cliente.

I clienti possono anche usare Kyriba Connectivity per automatizzare lo scambio dei dati con la propria infrastruttura IT interna (ERP o altro software interno). Generalmente la comunicazione usa i protocolli SFTP, FTPS e REST.

Kyriba Connectivity utilizza anche le API REST, destinate principalmente a coprire:

- l'utilizzo delle API di terze parti (della banca, dell'ERP, di fornitori di servizi terzi)
- l'utilizzo delle API aperte di Kyriba (gestione dei dati, scambio di dati, saldi, pagamenti, integrazione ERP, ecc.)

La gamma dei protocolli supportati da Kyriba Connectivity viene periodicamente ampliata grazie all'installazione di nuovi server di comunicazione e all'espansione geografica di Kyriba stessa. In alcuni paesi Kyriba collabora con partner che hanno una connettività testata con le principali banche della regione. In questi casi, collabora direttamente con tali partner per integrare i dati acquisiti nell'applicazione di Kyriba.

6.5. Personalizzazione delle comunicazioni

La componente connettività/hub di comunicazione della piattaforma di Kyriba è progettata per ricevere file, messaggi e altri dati da molte fonti e inviare dati a vari destinatari. La soluzione è stata progettata come prodotto a versioni aggiornabili e tutte le modifiche e le migliorie vengono realizzate dal team di sviluppo di Kyriba e implementate a intervalli di tempo predefiniti.

La soluzione è stata progettata per integrare facilmente ogni fornitore di servizi di comunicazione e Kyriba Connectivity può essere facilmente estesa in qualsiasi momento aggiungendo protocolli standard. In alcuni casi, le connessioni a determinate banche potrebbero servirsi di protocolli o meccanismi di accesso non standard. In questi casi, la connessione può essere personalizzata al fine di trovare il modo più efficiente di ricevere i file dalla banca, prendendo in considerazione i formati, il volume, il protocollo, la sicurezza e la frequenza dei file infragiornalieri. Kyriba può anche ricevere feed di dati da sistemi interni (per es., Bloomberg) già adottati dal cliente.

Il sistema di comunicazione con le banche è monitorato costantemente e viene ampliato man mano che nuovi clienti richiedono specifiche connettività o ogni qualvolta Kyriba decide di entrare in nuovi mercati. I nostri clienti beneficiano dunque di questo approccio alla connettività bancaria, che si traduce in minori costi per l'aggregazione delle transazioni e in una maggiore efficienza operativa.

6.6. Formati bancari

Kyriba è in grado di ricevere estratti conto e avvisi di pagamento dagli istituti finanziari e di generare pagamenti e file di rimessa e trasmettere i file prodotti dal sistema ERP del cliente agli istituti finanziari. Nel nostro catalogo sono presenti oltre 400 formati, sotto-formati e varianti utilizzati dagli istituti finanziari in tutto il mondo. Kyriba è fortemente impegnata a supportare gli standard più diffusamente accettati quali SWIFT MT e ISO XML UNIFI 20022. Inoltre, laddove necessario, supportiamo e aggiungiamo i formati locali e, una volta rilasciati, i nuovi formati vengono messi a disposizione di tutti i clienti in tutto il mondo.

La Payment Factory di Kyriba copre trasferimenti, addebiti diretti, fatture in entrata, fatture in uscita, transazioni finanziarie e messaggi di Supply Chain Finance. Kyriba può anche generare file di rimessa e inviare i file generati dal sistema ERP o da altre applicazioni del cliente alle banche connesse all'azienda. Siamo in grado di trasmettere qualsiasi tipo di file. Inoltre, per oltre 60 formati, inclusi XML UNIFI 20022 (compatibili o meno con SEPA), MT101, EDI820, ecc., siamo in grado di controllare la validità della struttura del file sulla base dello standard associato. Nell'attuare un flusso di lavoro di approvazione, i firmatari potranno vedere il contenuto del file.

6.7. Mobile

Kyriba Mobile estende le funzionalità di base della gestione della tesoreria ai dispositivi mobile. Kyriba Mobile è disponibile come app gratuita nell'App Store di Apple e nel Marketplace di Android e i clienti di Kyriba possono accedere utilizzando le stesse credenziali di login usate per accedere alla piattaforma web di Kyriba. Kyriba Mobile è compatibile con tutti gli iPad e gli iPhone con iOS 5 o superiore. Kyriba Mobile utilizza le stesse tecnologie di sicurezza per l'accesso elencate sopra (TLS, firewall front-end, ecc.).

7. Sviluppo e implementazione

7.1. Obiettivi dello sviluppo

Il processo di sviluppo di Kyriba e le configurazioni tecniche sono stati attentamente pianificati per concentrarsi sui seguenti obiettivi:

- **Reattività**
  Crediamo fortemente che rispondere rapidamente alle esigenze dei clienti sia importante per fornire un'esperienza di servizio di qualità e lavoriamo per ottimizzare il nostro staff in vista di una rapida gestione delle richieste dei nostri clienti come aggiunte al codice, prototipi e patch per avviare la produzione in breve tempo.
- **Stabilità**
  Prima di implementare nell'ambiente di produzione le nuove versioni, svolgiamo sempre test di controllo qualità esaustivi sulle pre-release.
- **Frequenza**
  Il nostro ritmo di rilascio delle nuove versioni è agile e aggressivo e si attesta su rilasci mensili con implementazione di patch secondo necessità. Ciascuna nuova versione viene installata nei siti di produzione e messa a disposizione di tutti i clienti.
- **Tracciabilità**
  Il nostro processo di sviluppo è organizzato rigorosamente e include specifiche, sviluppo, testing e implementazione.

7.2. Sviluppo agile

Il processo di sviluppo di Kyriba si basa sulle migliori pratiche di sviluppo del software e in particolare su quelle impiegate per lo sviluppo di soluzioni software per il cloud. Esso è inoltre organizzato in modo da garantire un'elevata tracciabilità dello sviluppo e del processo di validazione.

Il processo di sviluppo di Kyriba si basa su due infrastrutture tanto agili quanto all'avanguardia:

- **Scrum**
  Scrum viene usato per i più importanti progetti di evoluzione del prodotto con iterazioni ogni due settimane che consentono un'elevata frequenza delle consegne mantenendo i rischi tecnici e funzionali al minimo. Ciascun progetto dura dalle due alle dieci iterazioni ed è sviluppato sotto la responsabilità di un team di tre-sei persone.
- **Kanban**
  Kanban viene usato per l'attività di manutenzione ordinaria, con l'obiettivo di ottimizzare i tempi di consegna e incrementare la reattività. Il processo è fluido e caratterizzato da frequenti consegne di fix.

Lo sviluppo avviene in base al modello Trunk Based Development e prevede controlli di qualità prima della fusione. La programmazione adotta la maggior parte delle pratiche XP (per es., integrazione continua, revisione del codice, pair programming, TDD).

La qualità e la non regressione sono assicurate e monitorate tramite test automatici su vasta scala realizzati per mezzo di un'infrastruttura di testing basata sui dati. Per il nostro lavoro quotidiano usiamo i migliori strumenti SaaS, tra cui:

- Bitbucket/GIT come controllo di versione distribuito del source
- JIRA per il monitoraggio dei task distribuito

- JIRA Agile per i dashboard agili
- Fogli di calcolo per conservare insiemi di dati dei test (per le specifiche eseguibili).

Attraverso questo processo, siamo in grado di effettuare consegne frequenti e ciascuna nuova versione viene installata nei siti di produzione e messa a disposizione di tutti i clienti.

7.3. Ambiente di sviluppo delle tecnologie

L'applicazione è stata creata usando gli strumenti della famiglia Java, che forniscono un ambiente in grado di supportare i nostri obiettivi, tra cui la possibilità di implementare la nostra soluzione su una vasta gamma di sistemi operativi (per es., Windows e varie versioni di Linux).

7.4. Processo di testing e implementazione

Supportiamo, testiamo e monitoriamo diverse fondamenta tecniche, che vengono implementate in una piattaforma ospitata nei nostri centri di testing e ogni patch, service pack o nuova versione sono testati su queste piattaforme prima di essere implementati in quelle online (cfr. la sezione 5, Fondamenta tecniche).

Prima di raggiungere la piattaforma di produzione finale, il nuovo codice viene implementato in una serie di piattaforme intermedie. Su ciascuna piattaforma viene eseguita una serie di validazioni e di test prima dell'implementazione finale nelle piattaforme di produzione.

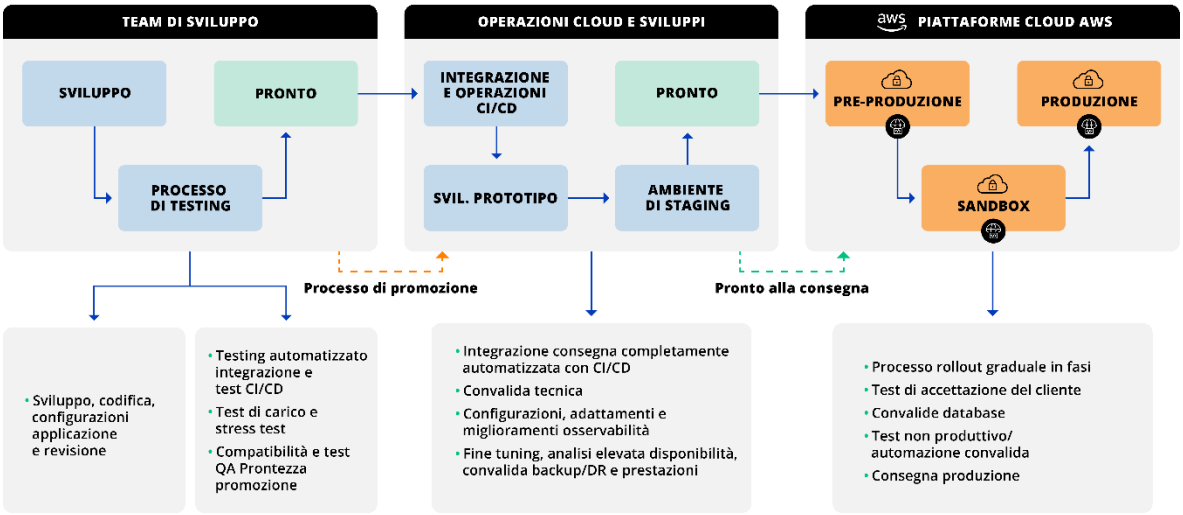

Figura 5: Processo di implementazione

Per tutte le fondamenta tecniche e le architetture di piattaforma esiste una piattaforma prototipi e Kyriba garantisce il supporto per queste componenti. Similmente, validiamo tutte le nuove versioni, le patch e i service pack prima dell'implementazione. La piattaforma prototipi viene usata anche per validare il processo di implementazione automatizzato, l'ottimizzazione e gli aggiornamenti delle tecnologie (per es., sistemi operativi, middleware).

Tutti gli aggiornamenti e le nuove versioni vengono messi a disposizione dei clienti gratuitamente e la loro implementazione non richiede ai clienti un nuovo ciclo di implementazione del progetto. Ciò vale per qualsiasi modulo che il cliente abbia già autorizzato. In ogni dato momento, ferma restando la pianificazione dei rilasci, tutti i nostri clienti usano la versione di Kyriba più recente.

Gli aggiornamenti sono progettati e implementati in modo tale da non interferire con le configurazioni personalizzate dei clienti. Tutto questo è reso possibile dal team di testing interno di Kyriba. I clienti possono scegliere di non usare determinate nuove funzionalità per impostazione predefinita, ma esse resteranno sempre disponibili nel caso in cui il cliente cambiasse idea.

Informazioni su Kyriba

Kyriba permette a CFO, tesorieri e responsabili IT di trasformare il modo in cui ottimizzano le soluzioni tecnologiche finanziarie, riducono il rischio della migrazione dell'ERP nel cloud e attivano la liquidità per renderla un mezzo dinamico e in tempo reale di crescita e creazione di valore. Con 2.000 clienti in tutto il mondo, tra cui un quarto delle società Fortune 500 ed Eurostoxx 50, la pionieristica piattaforma di servizi Kyriba Connectivity integra applicazioni interne per la tesoreria, la gestione del rischio, i pagamenti e il Working Capital con fonti esterne quali banche, ERP, piattaforme di trading e fornitori di dati di mercato. Con la sua piattaforma di connettività, Kyriba gestisce ogni anno 1,3 miliardi di transazioni bancarie e 200 milioni di pagamenti in 140 paesi. Kyriba è una piattaforma SaaS sicura e scalabile che sfrutta l'intelligenza artificiale, automatizza i flussi di lavoro dei pagamenti e permette a migliaia di multinazionali e banche di massimizzare le opportunità di crescita, proteggersi da perdite, frodi e rischi finanziari e ridurre i costi operativi. Kyriba ha sede a San Diego e i suoi uffici si trovano a Dubai, Francoforte, Londra, Minsk, Parigi, Shangai, Singapore, Tokyo, Varsavia e in altre importanti località del mondo. Per ulteriori informazioni, visita www.kyriba.it.