DASSAULT SYSTEMES

PIATTAFORMA 3DEXPERIENCE
SICUREZZA E PRIVACY DEL CLOUD

White paper

SOMMARIO

INTRODUZIONE

LA NOSTRA FILOSOFIA

Il cloud computing rappresenta un cambiamento di paradigma nel nostro modo di fare business. Le organizzazioni stanno eseguendo le applicazioni, gestendo i dati e spostando le operazioni verso il cloud per trarre vantaggio dalla velocità e dalla semplicità delle disposizioni sul cloud, oltre a trarre vantaggio dall'efficacia operativa della manutenzione, dei servizi IT e della sicurezza da parte di fornitori specializzati.

Dassault Systèmes fornisce servizi basati sul cloud sin dalla creazione della piattaforma **3D**EXPERIENCE® nel 2012. Abbiamo creato un ecosistema completo basato sul cloud, la piattaforma **3D**EXPERIENCE Cloud, che consente ai nostri clienti di usufruire di risorse cloud sicure, flessibili e scalabili. La nostra missione è supportare i nostri clienti con fiducia e affidabilità in ogni aspetto delle nostre soluzioni.

Il nostro approccio alla gestione del rischio è articolato e proattivo, basato sulle Best practice e progettato per anticipare le minacce alla sicurezza in tutte le nostre operazioni. Utilizziamo un Sistema di gestione della privacy e della sicurezza delle informazioni (ISPMS) certificato ISO/IEC 27001:2017 e ISO/IEC 27701:2019 e soggetto a controlli di routine. Il nostro ISPMS si basa sui valori fondamentali di riservatezza, integrità, disponibilità e responsabilità.

Questo white paper illustra l'approccio di Dassault Systèmes alla sicurezza e alla conformità della **3D**EXPERIENCE, la nostra piattaforma basata sul cloud in cui i clienti accedono alle applicazioni, all'archivio dei dati e alle risorse scalabili di computing. In questo white paper affrontiamo gli aspetti principali delle nostre pratiche di sicurezza, privacy e conformità nel cloud.

LA NOSTRA DEFINIZIONE DI MISSIONE PER LA SICUREZZA DELLE INFORMAZIONI E LA PRIVACY

La definizione della missione per la sicurezza delle informazioni e la privacy di Dassault Systèmes è la seguente[1].

Gestisci l'esposizione ai rischi per la sicurezza delle informazioni e proteggi le informazioni di identificazione personale (PII) per la piattaforma **3D**EXPERIENCE Software as a Service (SaaS) e migliora continuamente la riservatezza, l'integrità e la disponibilità delle informazioni e la protezione di quanto segue:

- Proprietà intellettuale del cliente e dati degli utenti, PII inclusi
- Reputazione e proprietà intellettuale di Dassault Systèmes
- Disponibilità e resilienza del cloud
- Conformità alle normative e agli standard applicabili in materia di sicurezza informatica e protezione dei dati

La presente definizione di missione è a disposizione dei dipendenti come informazione documentata e delle parti interessate su richiesta.

DICHIARAZIONE DI NON RESPONSABILITÀ

Questi contenuti rappresentano le procedure di sicurezza, privacy, qualità e conformità della piattaforma **3D**EXPERIENCE Cloud a partire da marzo 2022. Il contenuto delle nostre procedure qui riportate è soggetto a modifiche a esclusiva discrezione di Dassault Systèmes. "Noi" e "nostro" utilizzati in questo documento si riferiscono specificamente a Dassault Systèmes.

1. Ciò corrisponde all'informativa sulla privacy e la sicurezza delle informazioni ISO 27001.

DASSAULT SYSTÈMES: UN'ORGANIZZAZIONE INCENTRATA SULLA SICUREZZA E SULLA PRIVACY

PIATTAFORMA 3DEXPERIENCE SAAS PER LA SICUREZZA INFORMATICA E LA GOVERNANCE DELLA PRIVACY

Dassault Systèmes R&D gestisce un Sistema di gestione della privacy e della sicurezza delle informazioni (ISPMS) controllato a livello centrale per la piattaforma **3D**EXPERIENCE SaaS con certificazione ISO/IEC 27001:2017 e ISO/IEC 27701:2019 da SGS International Certification Services (SGS-ICS). L'ambito della certificazione comprende:

1. Progettazione, sviluppo, consegna, distribuzione, operazioni cloud e supporto della piattaforma **3D**EXPERIENCE SaaS.

2. Gestione della privacy dei dati quando Dassault Systèmes agisce come:

a. Responsabile del trattamento per la gestione dei dati personali forniti nel contesto della piattaforma **3D**EXPERIENCE SaaS.

b. Elaboratore per PII sotto il controllo di un cliente ed elaborato nella piattaforma **3D**EXPERIENCE SaaS.

Il nostro ISPMS è amministrato e sottoposto a revisione da parte del Comitato esecutivo ricerca e sviluppo di Dassault Systèmes. È basato su un Sistema di gestione della qualità (QMS) ben consolidato, utilizzato sulla piattaforma **3D**EXPERIENCE ed è certificato ISO 9001:2015 da SGS-ICS.

QMS e ISPMS condividono molti processi fondamentali e di supporto basati su una metodologia Secure Software Development Lifecycle (Secure SDLC). L'ISPMS include anche ulteriori processi basati sul rischio incentrati sulla sicurezza delle informazioni e sulla protezione dei dati.

Tutti i processi e i controlli ISPMS vengono continuamente valutati per verificarne la conformità e l'efficacia dal programma **3D**EXPERIENCE Compliance Audit di Dassault Systèmes R&D. Le azioni correttive risultanti e i miglioramenti continui vengono monitorati nella piattaforma **3D**EXPERIENCE.

I criteri di verifica si basano sui requisiti di controllo e sui sistemi di gestione ISO 9001, ISO 27001 e ISO 27701. Tutti i controlli secondo ISO 27001 Allegato A e ISO 27701 Allegati A e B sono inclusi nell'ambito del sistema di gestione in quanto Dassault Systèmes agisce sia in qualità di responsabile del trattamento dei PII sia di elaboratore PII (vedere la sezione Protezione e privacy dei dati, pag. 11).

L'ISPMS è supportato da una definizione di missione per la sicurezza delle informazioni e la privacy (Informativa sulla privacy) della piattaforma **3D**EXPERIENCE e da obiettivi annuali. Gli obiettivi forniscono traguardi misurabili e indicatori delle prestazioni chiave (KPI) monitorati dai team operativi. Gli obiettivi di sicurezza informatica e protezione dei dati vengono rivisti regolarmente per verificarne l'idoneità nell'ambito del processo di pianificazione annuale di Dassault Systèmes.

IL NOSTRO PERSONALE ADDETTO ALLA SICUREZZA, ALLA PRIVACY E ALLA CONFORMITÀ

Comitato esecutivo ricerca e sviluppo

Il Comitato esecutivo ricerca e sviluppo di Dassault Systèmes è in ultima analisi responsabile dell'efficacia del Sistema di gestione della privacy e della sicurezza delle informazioni (ISPMS) della piattaforma **3D**EXPERIENCE con il supporto del General Counsel di Dassault Systèmes per quanto riguarda i requisiti di protezione e privacy dei dati. Il Comitato esecutivo ricerca e sviluppo dimostra attivamente il suo impegno nei confronti dell'ISPMS e delle aspettative dei clienti attraverso vari mezzi, tra cui:

- Garantire che la Politica sulla sicurezza e la privacy delle informazioni e gli obiettivi annuali siano compatibili con la direzione strategica dell'organizzazione;
- Garantire l'integrazione dei requisiti ISPMS nei processi aziendali dell'organizzazione;
- Garantire la disponibilità delle risorse necessarie per l'ISPMS;
- Comunicare l'importanza dell'ISPMS;
- Garantire che l'ISPMS raggiunga i risultati previsti;
- Dirigere e supportare le persone per contribuire all'efficacia dell'ISPMS;
- Promuovere il miglioramento continuo dei processi e delle operazioni ISPMS.

Team per la sicurezza informatica, la privacy dei dati e la conformità

Dassault Systèmes dispone di un modello di ruolo aziendale che definisce la missione, la descrizione, i risultati finali, i KPI, il profilo del ruolo e le competenze associate a ciascuna posizione o ruolo.

Un team di Chief Information Security Officer (CISO) e responsabili della sicurezza hanno la responsabilità generale di implementare il programma per la sicurezza delle informazioni di Dassault Systèmes. Sono responsabili della definizione,

del mantenimento e dell'applicazione a livello globale delle policy, degli standard, delle linee guida e delle procedure di sicurezza delle informazioni.

La sicurezza informatica e la privacy dei dati di Dassault Systèmes nel settore Ricerca e sviluppo hanno la responsabilità di garantire che l'ISPMS di **3D**EXPERIENCE sia pianificato, implementato, mantenuto e migliorato continuamente in conformità ai requisiti ISO 27001 e ISO 27701. Sono responsabili del monitoraggio della conformità e dell'efficacia dell'ISPMS e della relativa segnalazione alla direzione esecutiva nell'ambito di riunioni di governance standard.

Un Group Data Protection Officer (DPO) informa e consiglia Dassault Systèmes sulla protezione dei dati personali per garantire la best practice, la responsabilità e la crescita sostenibile di Dassault Systèmes. Il Group DPO è l'interlocutore privilegiato delle autorità di vigilanza per la protezione dei dati e riferisce al General Counsel di Dassault Systèmes la conformità e l'efficacia dell'ISPMS.

Un team R&D Compliance & Risk gestisce un programma di verifica della conformità interna per valutare la conformità di Dassault Systèmes ai processi interni e alle certificazioni di settore come ISO 9001, ISO 27001 e ISO 27701. I risultati delle verifiche e i corrispondenti piani di azioni correttivi e preventivi (CAPA) sono gestiti nella piattaforma.

Un team di Group Internal Audit definisce e valuta la conformità e l'efficacia del framework di valutazione dei controlli interni (ICE) di Dassault Systèmes attraverso un programma di controllo interno a livello aziendale. Il framework di controllo interno aiuta a mitigare i rischi attraverso l'istituzione e la verifica dei controlli generali e dei controlli generali informatici (ITGC).

INSERIMENTO E FORMAZIONE PER TUTTI I DIPENDENTI

I dipendenti che entrano a far parte di Dassault Systèmes devono accettare di rispettare il nostro codice di condotta, lo statuto IT e le policy sulla protezione dei dati. Tutti i nuovi dipendenti seguono una formazione obbligatoria sull'etica e sulla conformità in materia di sicurezza e privacy, tra cui:

- Prevenzione delle minacce alla sicurezza dei dati.
- Protezione dei dati fisici e delle workstation; policy sulla pulizia della scrivania.
- Protezione e riservatezza dei dati personali.
- Comportamento aziendale etico; principi delle leggi anticorruzione e sulla concorrenza.
- Gestione degli incidenti; riconoscimento e segnalazione di potenziali minacce.

Promuoviamo costantemente la sicurezza e la privacy in tutta l'organizzazione.

LA SICUREZZA NEL TELELAVORO

Quando lavorano in remoto, i dipendenti Dassault Systèmes possono accedere ai dati, alle applicazioni e alle utility della piattaforma solo tramite una VPN. Ciò si applica sia ai dispositivi aziendali sia a quelli personali. Sono consentiti solo dispositivi personali registrati e approvati con accesso VPN.

I NOSTRI PARTNER PER LA SICUREZZA DEL CLOUD

Lavoriamo a stretto contatto con i nostri provider di infrastrutture cloud (IaaS), incluso 3DS Outscale, per garantire sicurezza e conformità in tutte le nostre attività. Tra gli altri criteri, i nostri provider IaaS devono essere certificati ISO 27001.

I NOSTRI STANDARD DI SICUREZZA

Il nostro approccio alla sicurezza informatica è radicato negli standard di settore più rispettati. Gli esperti indipendenti di sicurezza informatica collaborano attivamente per stabilire gli standard globali per i provider di software. OWASP, NIST e ISO/IEC sono tre enti esperti che guidano i nostri team di sicurezza informatica e privacy con best practice, requisiti, controlli, test e altri strumenti per ridurre i rischi e mitigare le vulnerabilità.

OWASP: OPEN WEB APPLICATION SECURITY PROJECT[1]

OWASP ha lo scopo di consentire alle organizzazioni di sviluppare e mantenere applicazioni estremamente sicure. OWASP Foundation è la principale fonte di ricerca all'avanguardia, framework prevalenti e informazioni essenziali relative alla sicurezza delle applicazioni.

Con l'aiuto di alleanze globali, OWASP offre:

- Strumenti, standard e metodologie per la sicurezza delle applicazioni
- Risorse per lo sviluppo sicuro del codice, revisioni del codice di sicurezza e test di sicurezza delle applicazioni
- Librerie e controlli di sicurezza standard

Le principali pubblicazioni di OWASP includono:

- I 10 principali rischi per la sicurezza delle applicazioni web
- Procedure di codifica sicure
- Guida alla revisione dei codici
- Standard per la verifica della sicurezza delle applicazioni

NIST: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY[2]

NIST è la principale fonte di soluzioni di misurazione critiche e standard equi per l'elettronica, il software e altre tecnologie. NIST Special Publication (SP) 800-53 definisce i controlli di sicurezza e i controlli sulla privacy per sistemi informativi e organizzazioni.

NIST SP 800-53 è progettato per proteggere le operazioni e le risorse organizzative, gli individui e altre entità da "una serie diversificata di minacce e rischi, tra cui attacchi ostili, errori umani, disastri naturali, guasti strutturali, entità di intelligence straniere e rischi per la privacy". Questi controlli riguardano la sicurezza e la privacy sia dal punto di vista della funzionalità sia della sicurezza.

ISO/IEC: ORGANIZZAZIONE INTERNAZIONALE PER LA STANDARDIZZAZIONE E LA COMMISSIONE ELETTROTECNICA INTERNAZIONALE[3]

ISO/IEC è un comitato tecnico congiunto che lavora per promuovere gli standard nell'IT e nella tecnologia delle comunicazioni. Il nostro ISPMS per la piattaforma **3D**EXPERIENCE SaaS è certificata ISO/IEC 27001:2017 e ISO/IEC 27701:2019, mentre il nostro QMS è certificato ISO 9001:2015, entrambi da SGS-ICS (vedere la sezione "Piattaforma **3D**EXPERIENCE SaaS per la sicurezza informatica e la governance della privacy", pag. 4).

ISO 9001 specifica i requisiti per un sistema di gestione della qualità quando un'organizzazione:

a. deve dimostrare la propria capacità di fornire costantemente prodotti e servizi che soddisfino i requisiti legali e normativi applicabili del cliente, e

b. mira a migliorare la soddisfazione del cliente attraverso l'applicazione efficace del sistema, inclusi i processi per il miglioramento del sistema e la garanzia di conformità al cliente e i requisiti legali e normativi applicabili.

Il nostro Sistema di gestione della qualità (QMS) è basato sui processi utilizzati per la progettazione, lo sviluppo, la consegna, l'implementazione, le operazioni cloud e il supporto della piattaforma **3D**EXPERIENCE. Molte delle nostre pratiche di sicurezza delle applicazioni sono integrate nel nostro QMS.

ISO/IEC 27001 specifica i requisiti per stabilire, implementare, mantenere e migliorare continuamente un Sistema di gestione della sicurezza delle informazioni (ISMS). ISO/IEC 27001 Allegato A articola i controlli previsti per ogni aspetto, dalla protezione dei servizi applicativi sulle reti pubbliche alla protezione delle transazioni di sicurezza delle applicazioni, all'applicazione di una policy di sviluppo sicura, alla limitazione delle modifiche ai pacchetti software, al rispetto dei principi di progettazione sicura dei sistemi e così via.

ISO/IEC 27701 specifica i requisiti e fornisce indicazioni per stabilire, implementare, mantenere e migliorare continuamente un Sistema di gestione delle informazioni sulla privacy (PIMS) sotto forma di estensione a ISO/IEC 27001 e ISO/IEC 27002 per la gestione della privacy nel contesto dell'organizzazione. Lo standard fornisce indicazioni per i responsabili del trattamento PII e gli elaboratori PII, che sono responsabili del trattamento PII. L'allegato A specifica gli obiettivi di controllo e i controlli per i responsabili del trattamento PII e l'allegato B specifica gli obiettivi di controllo e i controlli per gli elaboratori PII.

1. Ulteriori informazioni: www.owasp.org
2. Ulteriori informazioni: csrc.nist.gov
3. Ulteriori informazioni: iso.org/isoiec-27001-information-security

PRINCIPALI FUNZIONI DI SICUREZZA

AUTENTICAZIONE E AUTORIZZAZIONE

Il meccanismo di autenticazione e autorizzazione per la piattaforma **3D**EXPERIENCE Cloud è **3D** Passport, un login personalizzato che consente agli utenti di accedere in modo sicuro a tutti i ruoli, le app e i servizi. Gli amministratori mantengono le politiche di autenticazione utente come la complessità delle password, la scadenza e la configurazione dei modelli per rilevare i tentativi di sblocco della password non autorizzati.

Funzioni di 3D Passport

Privacy dei dati

Ogni utente delle nostre soluzioni online ha accesso all'Informativa sulla privacy di Dassault Systèmes e deve accettarla quando crea il proprio **3D** Passport. Gli utenti possono esercitare i propri diritti in conformità alle policy e ai processi di Dassault Systèmes inviando una richiesta tramite un modulo Web.

Inoltre, un'azienda può anche presentare la propria informativa sulla privacy agli utenti per richiederne l'accettazione. In questo caso, l'amministratore della piattaforma caricherà la propria informativa sulla privacy tramite il dashboard Gestione piattaforma.

Single Sign-on (SSO)

Grazie allo scambio dei dati di autenticazione e autorizzazione in un formato standard, **3D** Passport garantisce una perfetta esperienza di accesso singolo in tutte le app della piattaforma **3D**EXPERIENCE Cloud.

Autenticazione multifattore (MFA)

È possibile raggiungere un livello di sicurezza maggiore, sfruttando le funzionalità MFA della piattaforma. Ad esempio, dopo che la MFA è stata configurata da un amministratore, l'utente può utilizzare un'app mobile per generare un codice da inserire insieme alla password e ottenere una maggiore protezione.

CONTROLLO DEGLI ACCESSI

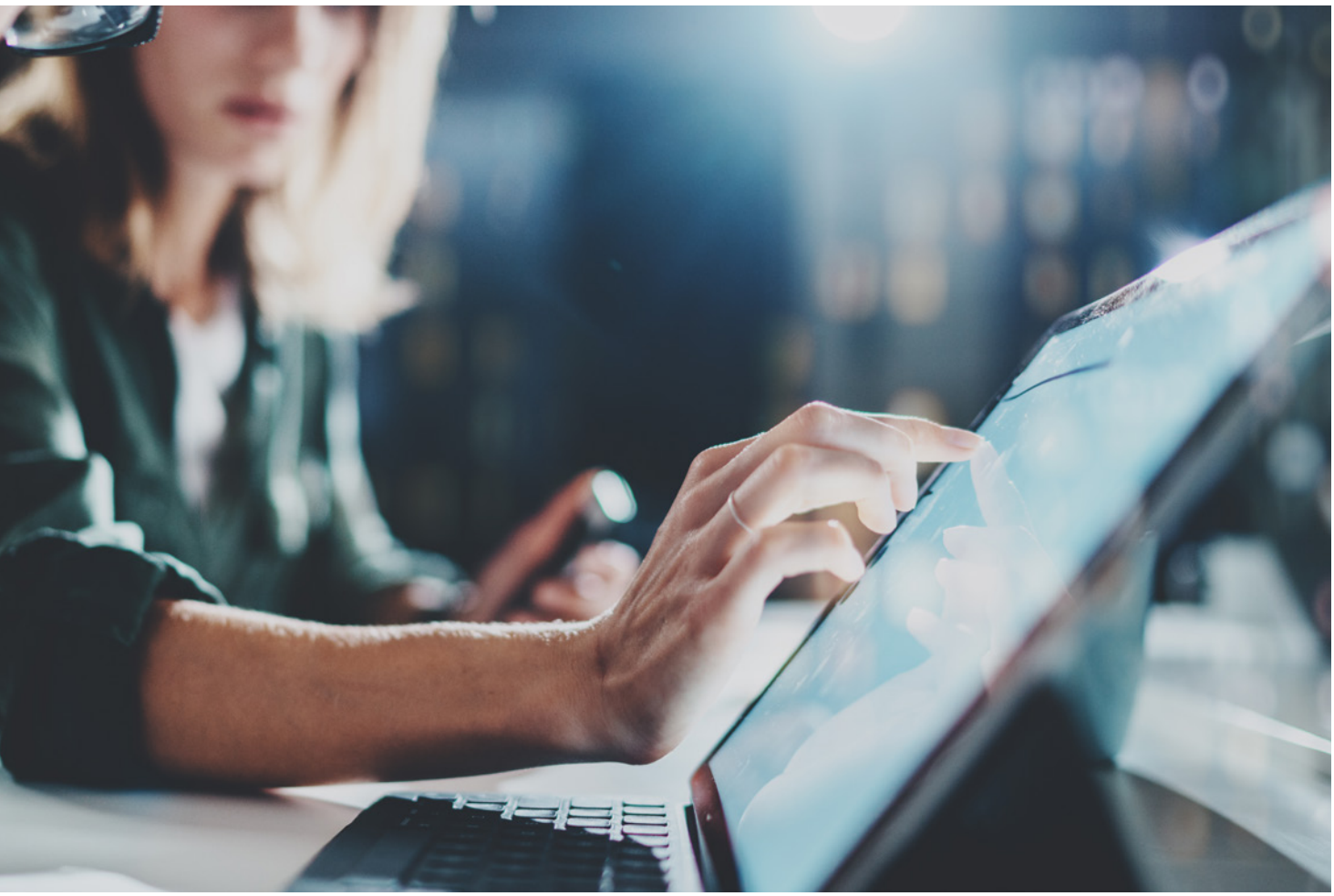
Il controllo degli accessi regola chi può accedere, visualizzare o utilizzare le risorse nel nostro ambiente di cloud computing. Queste autorizzazioni contribuiscono a proteggere i dati dei clienti, oltre a supportare la conformità dei clienti e i processi di certificazione realizzabili sulla piattaforma **3D**EXPERIENCE Cloud.

CRITTOGRAFIA

I dati in transito sono protetti mediante un protocollo di crittografia end-to-end HTTPS/TLS per proteggere l'integrità e la riservatezza.

ALTA DISPONIBILITÀ E ANTI-DDOS

Tutti i servizi sono protetti da un servizio proxy per il bilanciamento del carico ad alta disponibilità e alte prestazioni, che si integra con meccanismi di attacco e blacklist anti-DDoS (Distributed Denial of Service).



SICUREZZA OPERATIVA

LE NOSTRE OPERAZIONI CLOUD

Le nostre soluzioni cloud sono realizzate e gestite su una struttura a tre livelli. Identifichiamo e monitoriamo le minacce ed eseguiamo la mitigazione a ogni livello utilizzando standard di settore per considerare e assegnare le priorità ai rischi.

Software as a Service (SaaS)

Il livello più alto è il Software as a Service (SaaS) o il livello delle applicazioni. È qui che gli utenti della piattaforma **3D**EXPERIENCE Cloud accedono e utilizzano le loro applicazioni.

Platform as a Service (PaaS)

Il livello centrale è il livello Platform as a Service (PaaS) o il livello della piattaforma. È qui che viene realizzata e utilizzata la nostra piattaforma **3D**EXPERIENCE. Questo livello ci consente di gestire in modo sicuro il rapporto con i nostri fornitori di infrastrutture e di archiviare i database con cui il nostro livello SaaS interagisce.

Il nostro team PaaS determina la configurazione, il sistema operativo, la struttura e le risorse virtuali che compongono la piattaforma **3D**EXPERIENCE Cloud e determina il modo in cui riceviamo le informazioni dai nostri fornitori di infrastrutture cloud.

Le strategie di mitigazione dei rischi critici per i nostri livelli SaaS e PaaS includono autenticazione, controllo degli accessi basato sui ruoli, crittografia, monitoraggio e controllo, DAST e SAST, hardening del middleware, hardening del server e controlli SSL/TLS.

Infrastructure as a Service (IaaS)

L'Infrastructure as a Service (IaaS) o il livello dell'infrastruttura è il luogo in cui si trovano le nostre risorse di cloud computing. Forniscono funzionalità di virtualizzazione e gestiscono i backup e i servizi di ripristino in caso di emergenza.

Questo livello offre scalabilità a Dassault Systèmes e ai nostri clienti, con potenza di elaborazione e archiviazione aggiuntivi disponibili su richiesta.

I nostri principali provider di servizi cloud sono 3DS Outscale, un'azienda del Gruppo Dassault Systèmes e Amazon Web Services.

IL MODELLO DI RESPONSABILITÀ CONDIVISA

In un modello di cloud computing, i provider di servizi cloud e gli utenti cloud hanno la responsabilità condivisa di garantire il massimo livello di sicurezza e conformità per i servizi online. Ogni parte è responsabile dei diversi aspetti della sicurezza del cloud:

- Il provider cloud è responsabile della sicurezza dell'infrastruttura cloud.
- Il provider delle piattaforme (Dassault Systèmes) è responsabile della configurazione, della gestione e del funzionamento della sicurezza.
- Il cliente è responsabile della sicurezza a livello di applicazione, compresa la gestione amministratore/tenant.
- Seguiamo le best practice di sicurezza per rafforzare e gestire l'ambiente cloud, in conformità con le best practice dei nostri fornitori di servizi cloud oltre alle linee guida CSA (Cloud Security Alliance) e NIST.

Per ulteriori informazioni, fare riferimento a Best practice di Outscale.

DISPONIBILITÀ SLA (CONDIZIONI DEL CONTRATTO DI SERVIZIO)

Il nostro obiettivo è garantire la disponibilità dei nostri servizi online per almeno il 99,5% del tempo in cui i servizi online non sono soggetti a (i) interruzione pianificata del servizio o (II) interruzione conseguente a richiesta del cliente.

Per ulteriori informazioni, consulta il Contratto di servizio per i servizi online.

GESTIONE DELLE VULNERABILITÀ

Nell'ambito delle nostre misure per monitorare e mitigare continuamente le vulnerabilità, applichiamo una valutazione completa dei rischi per identificare, analizzare e valutare i rischi e selezionare i controlli di trattamento del rischio basati su NIST SP 800-53, ISO/IEC 27001 e ISO/IEC 27701.

Utilizziamo un sistema di gestione delle vulnerabilità multilivello basato sulle best practice NIST, che combina sistemi interni ed esterni per identificare, testare e controllare le vulnerabilità. Una parte importante del nostro sistema di gestione delle vulnerabilità è l'utilizzo di scanner di rete e di vulnerabilità. Se è stata identificata una vulnerabilità che richiede un intervento di correzione, questa viene registrata e attribuita la priorità in base alla gravità, quindi monitorata fino a quando non viene risolta.

Utilizziamo analisi del codice statico (SAST), analisi dinamica (DAST) e test di penetrazione manuali intensivi, oltre ai controlli basati sulle best practice OWASP per aggiungere continuamente nuove misure di sicurezza contro potenziali minacce.

Metodi di rilevamento delle minacce

I nostri metodi di rilevamento delle minacce includono:

Prevenzione del malware

Vietiamo l'uso di software non autorizzati e formiamo i dipendenti in merito all'uso accettabile dell'apparecchiatura. Abbiamo controlli tecnici per identificare il codice dannoso e svolgiamo corsi di formazione sulla consapevolezza dei dipendenti. Inoltre, abbiamo messo in atto procedure per garantire una risposta efficiente e rapida in caso di incidenti da parte di malware.

Monitoraggio

Monitoriamo l'efficacia del controllo e gli eventi di sicurezza a tutti i livelli del cloud, inclusi middleware, rete, sistema operativo e accesso al sistema operativo. Il monitoraggio automatizzato fornisce dati in tempo reale sulle prestazioni operative e funzionali.

Gestione degli incidenti

Adottiamo un approccio sistematico per identificare, classificare, registrare e comunicare gli incidenti relativi alla sicurezza e alla privacy. Tutti gli incidenti vengono valutati dal punto di contatto in base alla nostra scala di classificazione e gestiti tramite i nostri processi stabiliti di gestione degli incidenti e di violazione dei dati.

Gestione delle vulnerabilità a livello di applicazione

L'esecuzione di SaaS e PaaS su cloud sicuri richiede l'identificazione continua e la mitigazione delle vulnerabilità, che sono comuni tra le tecnologie di informazione e comunicazione. Nell'ambito del nostro Secure Software Development Lifecycle (Secure SDLC) abbiamo integrato diverse misure chiave per identificare le vulnerabilità del software e convalidare i nostri controlli di sicurezza esistenti. Queste misure includono scansioni statiche e dinamiche in varie fasi di sviluppo, oltre a test di penetrazione manuali estesi.

Test di sicurezza delle applicazioni statiche (SAST)

SAST valuta automaticamente il codice sorgente durante il processo di sviluppo per risolvere i problemi prima che il codice venga passato alla fase successiva di Secure SDLC. Collaboriamo con un fornitore SAST leader di Gartner.

Test di sicurezza delle applicazioni dinamiche (DAST)

DAST valuta automaticamente la piattaforma attraverso il front-end per individuare i punti deboli dell'architettura e le potenziali vulnerabilità della sicurezza. Il nostro DAST viene eseguito utilizzando strumenti di sicurezza leader del settore.

Test di penetrazione manuale

Professionisti della sicurezza autorizzati di terze parti simulano manualmente gli attacchi sulla piattaforma **3D**EXPERIENCE Cloud o un set specifico di app per confermare il loro stato di sicurezza.

Test di ingegneria della qualità interfunzionale

I nostri team di Quality Engineering indipendenti contribuiscono al processo di verifica della sicurezza eseguendo regolarmente scenari di minacce. La loro ampia conoscenza dei prodotti e il forte comando dei concetti chiave di sicurezza rappresentano un ulteriore livello di verifica e convalida della sicurezza.

Middleware, gestione delle vulnerabilità dei sistemi operativi e di rete

Utilizziamo più controlli di vulnerabilità e scansione con credenziali per identificare le risorse presenti su Internet, utilizzando uno scanner di vulnerabilità leader di Gartner per identificare in modo rapido ed efficiente i potenziali difetti della nostra rete e delle nostre risorse.

GESTIONE DELLE PATCH

Applichiamo regolarmente gli aggiornamenti software, incluse le patch funzionali e di sicurezza. Le interruzioni di servizio pianificate si verificano regolarmente, come stabilito nel nostro SLA. Inoltre, i nostri processi di gestione delle patch e degli incidenti tengono conto delle patch di sicurezza di emergenza che possono essere applicate in poche ore, con interruzioni occasionali non pianificate del servizio.

MONITORAGGIO DELLA SICUREZZA E GESTIONE DEGLI INCIDENTI

Il nostro sistema completo di monitoraggio della sicurezza e gestione degli incidenti identifica, analizza e risponde in tempo reale alle minacce alla sicurezza. Da un lato, adottiamo un doppio approccio per identificare e correggere le vulnerabilità e rispondere rapidamente agli incidenti di sicurezza.

Monitoraggio della sicurezza

Registri ed eventi vengono raccolti e analizzati a livello centrale tramite la nostra soluzione SIEM (Security, Incident and Event Management) e monitorati 24/7 ore su 24, 7 giorni su 7 dal nostro team SOC (Security Operations Center) dedicato. La nostra piattaforma SIEM raccoglie i dati a livello centrale e utilizza un motore di correlazione avanzato per identificare in modo proattivo gli eventi di sicurezza, analizzando grandi volumi di dati dei log di sicurezza per identificare tentativi di attività dannose.

Il nostro servizio di monitoraggio e supervisione della piattaforma **3D**EXPERIENCE Cloud include decine di indicatori su tutti i livelli del cloud per monitorare funzionalità, prestazioni e sicurezza.

Processi di risposta agli incidenti

Il nostro team SOC monitora e valuta continuamente i rischi identificati dalla nostra soluzione SIEM in base alla natura dell'incidente. Affrontiamo immediatamente gli incidenti in base alla nostra valutazione del rischio, seguendo la nostra procedura di gestione degli incidenti secondo le linee guida NIST SP 800-61. Ciò include le fasi principali di contenimento, eradicazione, recupero e notifica.

Nell'ambito del nostro processo di gestione delle patch, le patch di emergenza vengono eseguite in poche ore (vedere la sezione Gestione delle patch).

PIANI DI RIPRISTINO AZIENDALE (BCP) E PIANI DI RIPRISTINO IN CASO DI EMERGENZA (DRP)

I piani di ripristino aziendale (BCP) e i piani di ripristino in caso di emergenza (DRP) sono fondamentali per qualsiasi fornitura di software basata sul cloud. Il nostro BCP si occupa della pianificazione del ripristino completo di servizi informatici, servizi software, connessioni e dati in caso di perdita. Il nostro DRP è in grado di gestire le procedure di limitazione o inversione delle perdite in caso di eventi importanti.

Per il BCP/DRP seguiamo le best practice del settore, tra cui:

1. Mantenere un piano coerente per il backup e il recupero dei dati dei clienti garantendo che tutti i componenti del piano siano accessibili in caso di gravi disastri.

2. Conservare copie dei dati critici al di fuori dell'area di produzione, lontano dal data center principale.

3. Mantenere aggiornati i nostri BCP/DRP e garantire che tengano conto di eventuali cambiamenti nell'ambiente di produzione.

4. Esercizio annuale del BCP/DRP.

5. Sfruttare le funzionalità di virtualizzazione, come il bilanciamento del carico e i sistemi di failover, per ridurre al minimo le interruzioni del servizio.

Puntiamo a un obiettivo del tempo di recupero (RTO) e a un obiettivo del punto di recupero (RPO) aggressivi per garantire la continuità operativa dei nostri clienti in tutti gli scenari.

Backup e recupero dei dati

In linea con il nostro Contratto di servizio, garantiamo backup giornalieri dei dati di clienti e utenti, conservati in conformità allo SLA. Eseguiamo backup continui a caldo e a freddo per ridurre al minimo i tempi di inattività e massimizzare la protezione dei dati.

I dati dei clienti della piattaforma **3D**EXPERIENCE Cloud continuano a essere disponibili per il recupero per un periodo definito, come specificato nello SLA.

Per ulteriori informazioni, consulta il Contratto di servizio per i servizi online.

PROTEZIONE E PRIVACY DEI DATI

Le nostre soluzioni cloud sono progettate per rispettare la privacy dei nostri clienti e utenti. Seguiamo standard elevati per garantire che tutti i PII siano archiviati e gestiti in modo sicuro, in conformità alle leggi e agli standard pertinenti, come il regolamento generale europeo sulla protezione dei dati 2016/679 (GDPR).

Responsabile del trattamento

I responsabili del trattamento, come definito nel GDPR, devono stabilire politiche e procedure per il trattamento dei dati personali, compresa la determinazione del periodo di conservazione, la conformità alla minimizzazione dei PII e la gestione delle richieste degli interessati. Dassault Systèmes agisce in qualità di responsabile del trattamento durante l'elaborazione di PII in relazione ai processi aziendali interni e ai sistemi informativi.

Un cliente delle soluzioni SaaS di Dassault Systèmes è responsabile della gestione della PII gestita nella soluzione e agisce pertanto in qualità di responsabile del trattamento.

Lo scopo del GDPR e di altre leggi sulla protezione dei dati è rafforzare i diritti fondamentali dei residenti ampliando i diritti in materia di privacy e permettendo agli individui di esercitare il controllo sui propri dati personali. In qualità di azienda globale, Dassault Systèmes è conforme al GDPR, oltre ad altre leggi sulla protezione dei dati in cui opera Dassault Systèmes. Il GDPR e altre leggi specifiche per paese sono citati nell'Informativa sulla privacy di Dassault Systèmes, disponibile all'indirizzo 3ds.com.

Per la piattaforma **3D**EXPERIENCE Cloud, Dassault Systèmes svolge il ruolo di responsabile del trattamento per quanto segue:

- **3D** Passport ad eccezione delle offerte di cloud privati
- **3D** Passport creato da un individuo tramite il sito 3ds.com
- Community pubbliche **3D**EXPERIENCE disponibili sulle piattaforme pubbliche Dassault Systèmes
- Supporto clienti Dassault Systèmes
- **3D**EXPERIENCE Marketplace

Oltre al GDPR, altre leggi e normative locali sulla protezione dei dati sono monitorate dai responsabili della protezione dei dati di Dassault Systèmes su base regionale e sono applicate da processi e procedure locali.

3D Passport è il profilo di autenticazione creato per utente. L'elaborazione della PII all'interno di **3D** Passport è responsabilità di Dassault Systèmes. La PII associata a **3D** Passport viene archiviata in Europa con alcune eccezioni specifiche a causa dei requisiti normativi.

Elaboratore

Quando Dassault Systèmes fornisce offerte basate sul cloud, come la piattaforma **3D**EXPERIENCE Cloud, Dassault Systèmes agisce come elaboratore per la seconda fase di elaborazione e archiviazione. In tale veste, Dassault Systèmes elabora la PII in conformità all'accordo contrattuale sottoscritto tra le parti.

Dassault Systèmes ricopre il ruolo di elaboratore, come definito nel GDPR, per quanto segue:

- Offerte Dassault Systèmes sul cloud (private e pubbliche) fornite a clienti e partner aziendali
- **3D** Passport per offerte di cloud privati

Quando si agisce in qualità di elaboratore, i dati della piattaforma saranno archiviati da un provider IaaS di terze parti (ad esempio 3DS Outscale o Amazon Web Services) in un data center locale.

CONCLUSIONI

Dassault Systèmes mette la sicurezza e la privacy al centro delle proprie operazioni. Le nostre misure di sicurezza informatica e protezione dei dati si basano sugli standard più affidabili del settore e vengono applicate sistematicamente tramite formazione, requisiti di progettazione, controlli di sicurezza, misure di privacy e verifiche e test di terze parti. Miglioriamo continuamente le nostre misure di sicurezza e privacy con spirito di innovazione ed eccellenza, garantendo il miglior supporto possibile ai nostri clienti.

La piattaforma **3D**EXPERIENCE® migliora le applicazioni del marchio al servizio di 11 settori industriali ed offre un'ampia gamma di esperienze di soluzioni industriali.

Dassault Systèmes, the **3DEXPERIENCE** Company, è un catalizzatore per il progresso umano. Mettiamo a disposizione di aziende e privati ambienti di collaborazione virtuali in cui immaginare innovazioni per un mondo sostenibile. Creando riproduzioni virtuali esatte del mondo reale con le nostre applicazioni e la piattaforma **3DEXPERIENCE**, i nostri clienti ampliano i confini dell'innovazione, dell'apprendimento e della produzione.

I 20.000 dipendenti di Dassault Systèmes offrono valore a oltre 270.000 aziende di tutte le dimensioni e di tutti i settori industriali in oltre 140 Paesi. Per ulteriori informazioni, visitare il sito web **www.3ds.com/it**.

3DEXPERIENCE®

DASSAULT SYSTEMES | The **3D**EXPERIENCE® Company

Europa/Medio Oriente/Africa
Dassault Systèmes
10, rue Marcel Dassault
CS 40501
78946 Vélizy-Villacoublay Cedex
Francia

Americhe
Dassault Systèmes
175 Wyman Street
Waltham, MA 02451
USA

Asia/Pacifico
Dassault Systèmes K.K.
ThinkPark Tower,
2-1-1 Osaki, Shinagawa-ku,
Tokyo 141-6020
Giappone