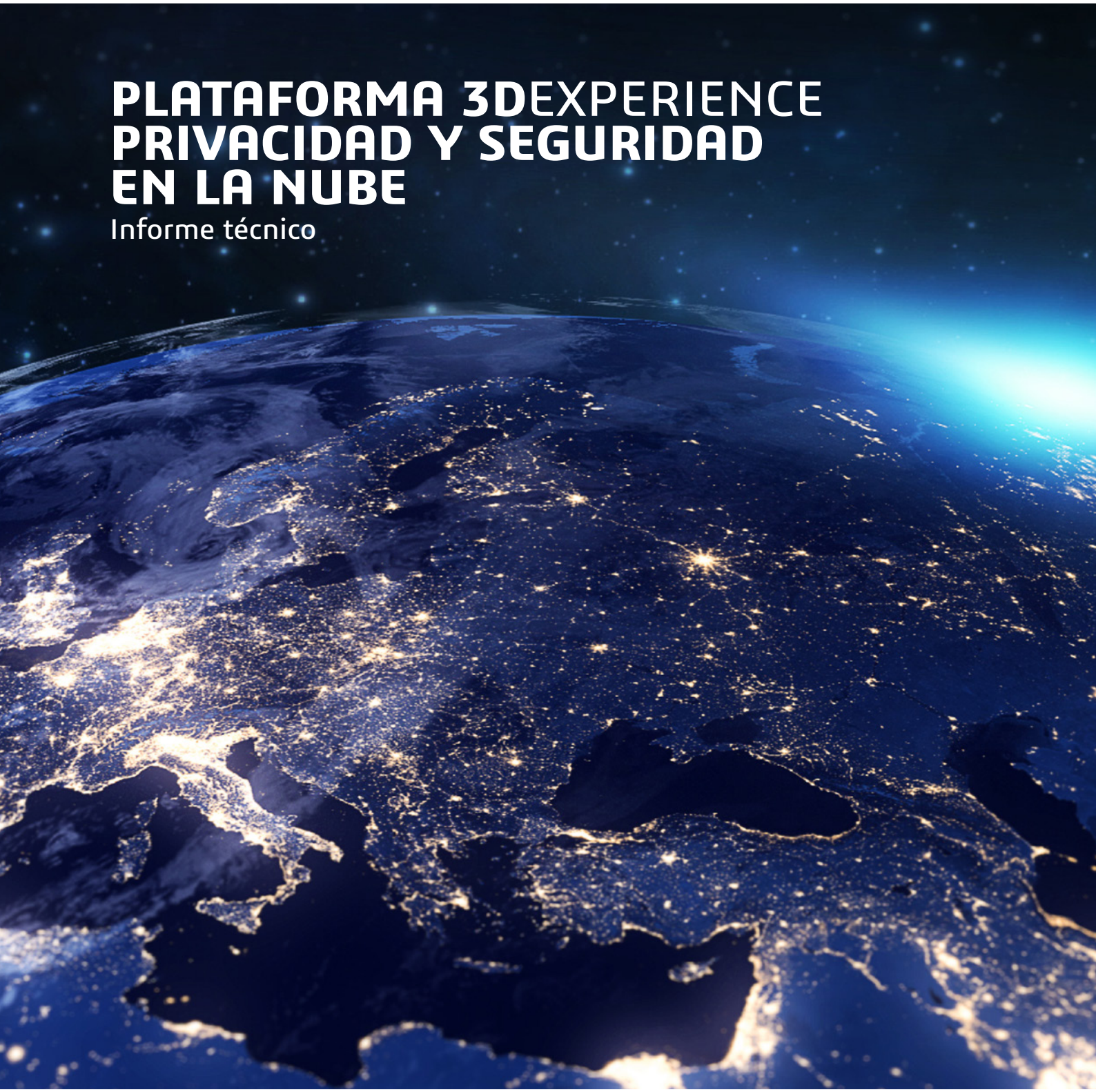
DASSAULT SYSTEMES

PLATAFORMA 3DEXPERIENCE
PRIVACIDAD Y SEGURIDAD EN LA NUBE

Informe técnico



CONTENIDO

INTRODUCCIÓN

NUESTRA FILOSOFÍA

La computación en la nube representa un cambio de paradigma en la forma en que hacemos negocios. Las organizaciones ejecutan aplicaciones, gestionan datos y migran operaciones a la nube para beneficiarse de la velocidad y la simplicidad que ofrecen los servicios de la nube, así como de la eficacia operativa del mantenimiento, los servicios de TI y la seguridad de proveedores especialistas.

Dassault Systèmes lleva proporcionando servicios basados en la nube desde la creación de la plataforma **3D**EXPERIENCE® en 2012. Hemos desarrollado un ecosistema completamente basado en la nube, la plataforma **3D**EXPERIENCE en la nube, que permite a nuestros clientes beneficiarse de recursos de la nube seguros, flexibles y escalables. Nuestra misión es apoyar a nuestros clientes ofreciéndoles confianza y fiabilidad en todos los aspectos de las soluciones que ofrecemos.

El enfoque que adoptamos en la gestión de riesgos es polifacético y proactivo, se basa en las prácticas recomendadas y está diseñado para anticiparse a las amenazas de seguridad en nuestras operaciones. Ejecutamos un sistema de gestión de privacidad y seguridad de la información (ISPMS) que cuenta con las certificaciones ISO/IEC 27001:2017 e ISO/IEC 27701:2019 y está sujeto a auditoría de rutina. Nuestro ISPMS se basa en los valores fundamentales de la confidencialidad, la integridad, la disponibilidad y la responsabilidad.

Este informe técnico describe el enfoque de Dassault Systèmes en lo relativo a la seguridad y el cumplimiento de **3D**EXPERIENCE, nuestra plataforma basada en la nube en la que los clientes acceden a aplicaciones, almacenamiento de datos y recursos informáticos escalables. En este informe técnico, abordamos los aspectos fundamentales de nuestras prácticas de seguridad, privacidad y cumplimiento en la nube.

NUESTRA DECLARACIÓN DE OBJETIVOS SOBRE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

La Declaración de objetivos sobre privacidad y seguridad de la información de Dassault Systèmes es la siguiente[1].

Gestionar la exposición al riesgo de la seguridad de la información y proteger la información de identificación personal (PII) del software como servicio (SaaS) de la plataforma **3D**EXPERIENCE, así como mejorar continuamente la confidencialidad, la integridad y la disponibilidad de la información, y proteger lo siguiente:

- La propiedad intelectual del cliente y los datos del usuario, PII incluida.
- La reputación y la propiedad intelectual de Dassault Systèmes.
- La disponibilidad y la resiliencia de la nube.
- El cumplimiento de las normas y regulaciones de ciberseguridad y la protección de datos aplicables.

Esta declaración de objetivos está disponible para los empleados como información documentada y para las partes interesadas, previa solicitud.

DECLINACIÓN DE RESPONSABILIDAD

Este contenido representa las prácticas de seguridad, privacidad, calidad y cumplimiento de la plataforma **3D**EXPERIENCE en la nube de marzo de 2022. El contenido de las prácticas que aquí se establece está sujeto a cambios según el criterio exclusivo de Dassault Systèmes. "Nosotros" y "nuestro", tal como se utilizan en este documento, se refieren específicamente a Dassault Systèmes.

1. Corresponde a ISO 27001 Política de privacidad y seguridad de la información.

DASSAULT SYSTÈMES: UNA ORGANIZACIÓN CENTRADA EN LA SEGURIDAD Y LA PRIVACIDAD

CONTROL DE LA PRIVACIDAD Y LA CIBERSEGURIDAD DEL SAAS DE LA PLATAFORMA 3DEXPERIENCE

El área de I+D de Dassault Systèmes ejecuta un sistema de gestión de privacidad y seguridad de la información (ISPMS) controlado de forma centralizada para el SaaS de la plataforma **3D**EXPERIENCE. Este sistema cuenta con las certificaciones ISO/IEC 27001:2017 e ISO/IEC 27701:2019 otorgadas por los Servicios de Certificación Internacional SGS (SGS-ICS). El alcance de la certificación incluye:

1. El diseño, el desarrollo, la entrega, la implementación, las operaciones en la nube y la compatibilidad del SaaS de la plataforma **3D**EXPERIENCE.

2. La gestión de la privacidad de los datos en los casos en los que Dassault Systèmes actúa como:

a. Responsable del tratamiento en la gestión de datos personales proporcionados en el contexto del SaaS de la plataforma **3D**EXPERIENCE.

b. Encargado del tratamiento de PII bajo el control de un cliente y que se trata en el SaaS de la plataforma **3D**EXPERIENCE.

Nuestro ISPMS está administrado por el Comité Ejecutivo de Investigación y Desarrollo de Dassault Systèmes y sujeto a revisiones de gestión por su parte. Se ha desarrollado sobre los cimientos de un sólido sistema de gestión de calidad (QMS) que se ejecuta en la plataforma **3D**EXPERIENCE y que cuenta con la certificación ISO 9001:2015 de SGS-ICS.

El QMS y el ISPMS comparten muchos procesos fundamentales y de respaldo que se basan en la metodología del ciclo de vida de desarrollo de software seguro (Secure SDLC). El ISPMS incluye también procesos adicionales basados en riesgos que se centran en la seguridad de la información y la protección de los datos.

Para garantizar el cumplimiento y la efectividad, todos los procesos y controles del ISPMS se evalúan continuamente a través del programa de Auditoría de cumplimiento de **3D**EXPERIENCE del área de I+D de Dassault Systèmes. Las medidas correctivas y las mejoras continuas resultantes se supervisan en la plataforma **3D**EXPERIENCE.

Los criterios de auditoría se basan en los requisitos de control y de sistema de gestión ISO 9001, ISO 27001 e ISO 27701. Todos los controles del Anexo A de la norma ISO 27001 y los controles del Anexo A y B de la norma ISO 27701 se incluyen en el alcance del sistema de gestión, ya que Dassault Systèmes actúa como responsable del tratamiento de PII y como encargado del tratamiento de PII (consulte Privacidad y protección de datos, p. 11).

El ISPMS está respaldado por la Declaración de objetivos sobre privacidad y seguridad de la información (Declaración de la política) de la plataforma **3D**EXPERIENCE y por los objetivos anuales. Los objetivos proporcionan metas medibles e Indicadores clave de rendimiento (KPI) que los equipos operativos supervisan. Durante el proceso de planificación anual de Dassault Systèmes, los objetivos de ciberseguridad y protección de datos se revisan con regularidad para determinar su idoneidad.

NUESTRO PERSONAL DE SEGURIDAD, PRIVACIDAD Y CUMPLIMIENTO

Comité Ejecutivo de I+D

El Comité Ejecutivo de I+D de Dassault Systèmes es el responsable, en última instancia, de la eficacia del sistema de gestión de privacidad y seguridad de la información (ISPMS) de la plataforma **3D**EXPERIENCE. Cuenta con el apoyo del Consejo General de Dassault Systèmes en lo relativo a la privacidad y los requisitos de protección de datos. El Comité Ejecutivo de I+D demuestra activamente su compromiso con el ISPMS y con las expectativas de los clientes de diversas formas, como las siguientes:

- Garantizar que la Política de privacidad y seguridad de la información y los objetivos anuales sean compatibles con la dirección estratégica de la organización;
- garantizar la integración de los requisitos del ISPMS en los procesos de negocio de la organización;
- garantizar que los recursos necesarios para el ISPMS estén disponibles;
- comunicar la importancia del ISPMS;
- asegurarse de que el ISPMS logre los resultados previstos;
- orientar y ofrecer apoyo al personal para que contribuya a la eficacia del ISPMS;
- promover la mejora continua de los procesos y operaciones del ISPMS.

Equipos de Ciberseguridad, Privacidad de Datos y Cumplimiento

Dassault Systèmes cuenta con un modelo de funciones de la empresa en el que se definen la misión, la descripción, los resultados finales, los KPI, el perfil de la función y las habilidades asociadas a cada puesto o función.

Un equipo compuesto por directores de Seguridad de la Información (CISO) y líderes en materia de seguridad tiene la responsabilidad general de implementar el Programa de seguridad de la información de Dassault Systèmes. Este equipo es el responsable de establecer, mantener y garantizar el cumplimiento de las políticas, los estándares, las pautas y los procedimientos de seguridad de la información a nivel mundial.

Los equipos de Ciberseguridad y Privacidad de Datos del área de I+D de Dassault Systèmes son los responsables de garantizar que el ISPMS de **3D**EXPERIENCE se planifique, implemente, mantenga y mejore continuamente de acuerdo con los requisitos de ISO 27001 e ISO 27701. Son los responsables de supervisar el cumplimiento y la efectividad del ISPMS y de informar sobre estas cuestiones al equipo directivo como parte de las reuniones habituales de dirección.

El delegado de protección de datos (DPO) del Grupo informa y asesora a Dassault Systèmes sobre la protección de PII con el fin de garantizar la aplicación de las prácticas recomendadas, la asunción de responsabilidades y el crecimiento sostenible de Dassault Systèmes. El DPO del Grupo es el interlocutor principal con las autoridades de control en materia de protección de datos e informa sobre el cumplimiento y la efectividad del ISPMS al Consejo General de Dassault Systèmes.

El equipo de Cumplimiento y Riesgo de I+D ejecuta un programa de auditoría de cumplimiento interno para evaluar el cumplimiento de Dassault Systèmes con procesos internos y certificaciones del sector, como ISO 9001, ISO 27001 e ISO 27701. Los resultados de las auditorías y los planes de medidas correctivas y preventivas (CAPA) correspondientes se gestionan en la plataforma.

Un equipo de Auditoría Interna del Grupo define y evalúa el cumplimiento y la efectividad del Marco de evaluación de control interno (ICE) de Dassault Systèmes a través de un programa de auditoría interna a nivel empresarial. El Marco de control interno ayuda a mitigar los riesgos, ya que establece y verifica los Controles generales y los Controles generales de tecnología de la información (ITGC).

PROCESO DE INCORPORACIÓN Y FORMACIÓN PARA TODOS LOS EMPLEADOS

Los empleados que se incorporan a Dassault Systèmes deben aceptar cumplir con nuestro código de conducta, nuestros estatutos de TI y las políticas de protección de datos. Todos los nuevos empleados realizan una formación obligatoria sobre ética y cumplimiento que aborda la seguridad y la privacidad, y en la que se incluyen cuestiones como las siguientes:

- Prevención de amenazas a la seguridad de los datos.
- Protección de datos físicos y estaciones de trabajo; política de escritorio limpio.
- Protección y confidencialidad de los datos personales.
- Comportamiento empresarial ético; principios de las legislaciones en materia de competencia y anticorrupción.
- Gestión de incidentes; reconocimiento y notificación de posibles amenazas.

Fomentamos constantemente la concienciación en materia de seguridad y privacidad en toda la organización.

SEGURIDAD EN EL TELETRABAJO

Cuando los empleados de Dassault Systèmes trabajan de forma remota, únicamente pueden acceder a los datos, aplicaciones y utilidades de la plataforma a través de una VPN. Lo anterior se aplica tanto a dispositivos personales como a equipos de la empresa. Solo se permite el acceso VPN a dispositivos personales registrados y aprobados.

NUESTROS PARTNERS EN SEGURIDAD EN LA NUBE

Trabajamos estrechamente con nuestros proveedores de infraestructura en la nube (IaaS), como 3DS Outscale, para garantizar la seguridad y el cumplimiento en todas nuestras operaciones. Exigimos a nuestros proveedores de IaaS que cuenten con la certificación ISO 27001, entre otros criterios.

NUESTROS ESTÁNDARES DE SEGURIDAD

Nuestro planteamiento en materia de ciberseguridad se basa en los estándares más respetados del sector. Expertos independientes en ciberseguridad colaboran activamente para definir estándares a nivel mundial aplicables a los proveedores de software. El OWASP, el NIST y la ISO/IEC son tres organismos expertos que proporcionan orientación a nuestros equipos de ciberseguridad y privacidad a través de prácticas recomendadas, requisitos, controles, pruebas y otras herramientas que tienen por objetivo reducir el riesgo y mitigar las vulnerabilidades.

OWASP: PROYECTO ABIERTO DE SEGURIDAD DE APLICACIONES WEB[1]

El OWASP se dedica a posibilitar que las organizaciones puedan desarrollar y mantener aplicaciones muy seguras. La Fundación OWASP es la fuente principal de investigación de vanguardia, marcos comunes e información vital relacionada con la seguridad de las aplicaciones.

Con la ayuda de alianzas internacionales, el OWASP proporciona:

- Herramientas, normas y metodologías de seguridad para aplicaciones.
- Recursos para el desarrollo de código seguro, revisiones de códigos de seguridad y pruebas de seguridad de aplicaciones.
- Bibliotecas y controles de seguridad estándar.

Entre las principales publicaciones del OWASP se incluyen:

- Top 10 Riesgos de seguridad en aplicaciones web
- Prácticas de codificación segura
- Guía de revisión del código
- Estándar de verificación de seguridad en aplicaciones

NIST: INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA DE EE. UU.[2]

El NIST es la fuente de referencia para soluciones de medición esenciales y estándares equitativos en electrónica, software y otras tecnologías. La Publicación Especial (SP) NIST 800-53 define controles de seguridad y controles de privacidad para organizaciones y sistemas de información.

La NIST SP 800-53 está diseñada para proteger a las operaciones y los activos de las organizaciones, a las personas y a otras entidades de "un conjunto diverso de amenazas y riesgos, incluidos ataques hostiles, errores humanos, desastres naturales, fallos estructurales, entidades de inteligencia extranjera y riesgos de privacidad". Estos controles abordan la seguridad y la privacidad desde las perspectivas de la funcionalidad y la confianza.

ISO/IEC: ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN Y COMISIÓN ELECTROTÉCNICA INTERNACIONAL[3]

La ISO/IEC es un comité técnico conjunto que trabaja para promover normas en las áreas de la tecnología de la información y la tecnología de las comunicaciones. Nuestro ISPMS para el SaaS de la plataforma **3D**EXPERIENCE cuenta con las certificaciones ISO/IEC 27001:2017 e ISO/IEC 27701:2019, y nuestro sistema de gestión de calidad (QMS) cuenta con la certificación ISO 9001:2015, ambos por parte de SGS-ICS (consulte "Control de la privacidad y la ciberseguridad del SaaS de la plataforma **3D**EXPERIENCE", p. 4).

La norma ISO 9001 define los requisitos de los sistemas de gestión de calidad cuando la organización:

a. debe demostrar su capacidad de proporcionar de manera coherente productos y servicios que satisfagan al cliente y cumplan con los requisitos legales y normativos aplicables, y

b. tiene como objetivo mejorar la satisfacción del cliente a través de la aplicación efectiva del sistema, incluidos los procesos para mejorar el sistema y garantizar la conformidad con el cliente y los requisitos legales y normativos aplicables.

Nuestro sistema de gestión de calidad (QMS) está anclado en los procesos que se utilizan en el diseño, el desarrollo, la entrega, la implementación, las operaciones en la nube y el respaldo de la plataforma **3D**EXPERIENCE. Muchas de las prácticas de seguridad para aplicaciones que implementamos están integradas en nuestro QMS.

La ISO/IEC 27001 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (ISMS). El Anexo A de la ISO/IEC 27001 articula los controles esperados para todos los aspectos, por ejemplo, la protección de los servicios de aplicaciones en redes públicas, la protección de las transacciones de seguridad de aplicaciones, la aplicación de una política de desarrollo seguro, la restricción de cambios a los paquetes de software, la conformidad con los principios de ingeniería de sistemas seguros, etc.

La ISO/IEC 27701 especifica los requisitos y proporciona orientación para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de información de privacidad (PIMS) como una extensión a la ISO/IEC 27001 y la ISO/IEC 27002 para la gestión de la privacidad dentro del contexto de la organización. La norma proporciona orientación a los responsables del tratamiento de PII y los encargados del tratamiento de PII que tienen la responsabilidad de tratar PII. El Anexo A especifica los objetivos de control y los controles para los responsables del tratamiento de PII y el Anexo B especifica los objetivos de control y los controles para los encargados del tratamiento de PII.

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

CARACTERÍSTICAS CLAVE DE SEGURIDAD

AUTENTICACIÓN Y AUTORIZACIÓN

El mecanismo de autenticación y autorización para la plataforma **3D**EXPERIENCE en la nube es **3D** Passport, un inicio de sesión personalizado que permite a los usuarios acceder de forma segura a todas sus funciones, aplicaciones y servicios. Los administradores pueden mantener políticas de autenticación de usuarios como patrones de longitud de contraseña, de caducidad y de configuración para detectar intentos a la fuerza de desbloquear las contraseñas.

Características de 3D Passport

Privacidad de los datos

Todos los usuarios de nuestras soluciones en línea tienen acceso a la Política de privacidad de Dassault Systèmes y deben aceptarla al crear su **3D** Passport. Los usuarios pueden ejercer sus derechos de acuerdo con las políticas y los procesos de Dassault Systèmes mediante el envío de una solicitud a través de un formulario web.

Además, las empresas también pueden presentar sus políticas de privacidad a los usuarios para que las acepten. En este caso, el administrador de la plataforma puede cargar su política de privacidad mediante el panel de Gestión de plataformas.

Inicio de sesión único (SSO)

Al intercambiar datos de autenticación y autorización en un formato estándar, **3D** Passport proporciona una experiencia sencilla de inicio de sesión único en las aplicaciones de la plataforma **3D**EXPERIENCE en la nube.

Autenticación de varios factores (MFA)

Se puede lograr un mayor nivel de seguridad al aprovechar las capacidades de MFA de la plataforma. Por ejemplo, una vez que un administrador ha configurado la MFA, el usuario puede utilizar una aplicación móvil para generar un código que se tendrá que introducir junto con la contraseña para brindar una mayor seguridad.

CONTROL DE ACCESO

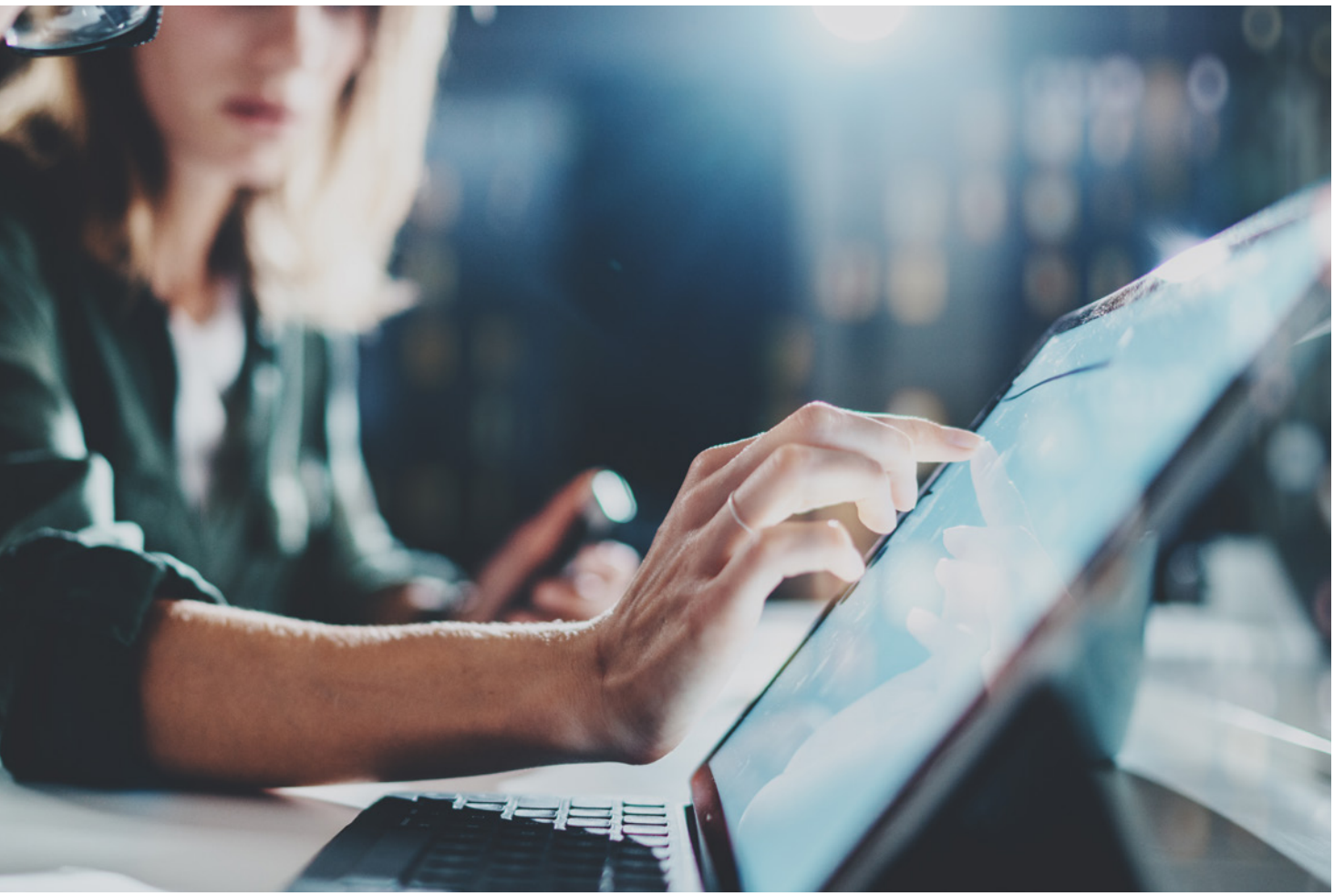
El control de acceso regula quién puede acceder, ver o utilizar recursos en nuestro entorno de computación en la nube. Estas autorizaciones ayudan a proteger los datos del cliente, así como a respaldar los procesos de certificación y cumplimiento del cliente que se pueden lograr en la plataforma **3D**EXPERIENCE en la nube.

CIFRADO

Los datos en tránsito se protegen mediante un protocolo de cifrado HTTPS/TLS de extremo a extremo para proteger la integridad y la confidencialidad.

ALTA DISPONIBILIDAD Y ANTI-DDOS

Todos los servicios están protegidos por un servicio de proxy de equilibrio de carga, alto rendimiento y alta disponibilidad que se integra con mecanismos antiataques DDoS (denegación de servicio distribuido) y de lista negra.



SEGURIDAD OPERATIVA

NUESTRAS OPERACIONES EN LA NUBE

Nuestras soluciones basadas en la nube se desarrollan y ejecutan en una estructura de tres capas. Identificamos y supervisamos las amenazas y llevamos a cabo la mitigación en cada capa aplicando los estándares de la industria a la hora de analizar y priorizar los riesgos.

Software como servicio (SaaS)

En la capa más alta está el software como servicio (SaaS) o la capa de aplicaciones. Aquí es donde los usuarios de la plataforma **3D**EXPERIENCE en la nube acceden a sus aplicaciones y las utilizan.

Plataforma como servicio (PaaS)

La capa media es la plataforma como servicio (PaaS) o capa de plataforma. Aquí es donde nuestra plataforma **3D**EXPERIENCE se construye y ejecuta. Esta capa nos permite gestionar de forma segura la relación con nuestros proveedores de infraestructura y almacenar las bases de datos con las que interactúa nuestra capa de SaaS.

Nuestro equipo de PaaS determina la configuración, el sistema operativo, la estructura y los recursos virtuales que conforman la plataforma **3D**EXPERIENCE en la nube, y determina cómo recibimos la información de nuestros proveedores de infraestructuras en la nube.

Las estrategias fundamentales de mitigación de riesgos para nuestras capas de SaaS y PaaS incluyen la autenticación, el control de acceso basado en funciones, el cifrado, la supervisión y la auditoría, DAST y SAST, el fortalecimiento del software intermedio, el fortalecimiento de servidores y las comprobaciones SSL/TLS.

Infraestructura como servicio (IaaS)

La infraestructura como servicio (IaaS) o capa de infraestructura es donde se encuentran nuestros recursos de computación en la nube. Proporciona capacidades de virtualización y mantiene las copias de seguridad y los servicios de recuperación ante desastres.

Esta capa proporciona escalabilidad a Dassault Systèmes y a nuestros clientes, y ofrece potencia de procesamiento y almacenamiento adicionales disponibles bajo petición.

Nuestros principales proveedores de la nube son 3DS Outscale, una empresa del Grupo Dassault Systèmes, y Amazon Web Services.

EL MODELO DE RESPONSABILIDAD COMPARTIDA

En un modelo de computación en la nube los proveedores de la nube y los usuarios de la nube tienen una responsabilidad compartida a la hora de garantizar el más alto nivel de seguridad y cumplimiento para con los servicios en línea. Cada parte es responsable de determinadas cuestiones para lograr la seguridad en la nube:

- El proveedor de la nube es responsable de la seguridad de la infraestructura de la nube.
- El proveedor de la plataforma (Dassault Systèmes) es responsable del funcionamiento, la configuración y la gestión de la seguridad.
- El cliente es responsable de la seguridad en la capa de la aplicación, incluida la gestión de administradores o tenants.
- Seguimos las prácticas recomendadas de seguridad para reforzar y operar el entorno de la nube y tenemos en cuenta las prácticas recomendadas de nuestros proveedores de nube, además de las pautas de la CSA (Alianza de Seguridad en la Nube) y el NIST.

Para obtener más información, consulte Prácticas recomendadas de Outscale.

SLA (ACUERDO DE NIVEL DE SERVICIO) DE DISPONIBILIDAD

Tenemos el objetivo de ofrecer una disponibilidad para nuestros servicios en línea equivalente a que, como mínimo, el 99,5 % del tiempo estos servicios no sufran (i) una interrupción del servicio planificada o (ii) una interrupción resultado de una solicitud del cliente.

Para obtener más información, consulte nuestro Acuerdo de nivel de servicio para servicios en línea.

GESTIÓN DE VULNERABILIDADES

Como parte de las medidas que tomamos para supervisar y mitigar vulnerabilidades de forma continua, llevamos a cabo una evaluación integral de riesgos con el fin de identificar, analizar y evaluar los riesgos y seleccionar los controles de tratamiento de los mismos de acuerdo con NIST SP 800-53, ISO/IEC 27001 e ISO/IEC 27701.

Empleamos un sistema de gestión de vulnerabilidades de varias capas que se basa en las prácticas recomendadas del NIST, y que combina sistemas externos e internos para identificar, probar y controlar vulnerabilidades. Una parte importante de nuestro sistema de gestión de vulnerabilidades consiste en el uso que hacemos de escáneres de vulnerabilidades y redes. Si se identifica una vulnerabilidad que debe ser solucionada, se registra y prioriza en función de la gravedad. Después, se realiza un seguimiento hasta que se ha solucionado.

Utilizamos análisis de código estáticos (SAST), análisis dinámicos (DAST) y pruebas de penetración manuales intensivas, así como controles basados en las prácticas recomendadas del OWASP para incorporar continuamente nuevas medidas de seguridad contra posibles amenazas.

Métodos de detección de amenazas

Nuestros métodos de detección de amenazas incluyen:

Prevención de malware

Prohibimos el uso de software no autorizado y formamos a los empleados sobre el uso aceptable de los equipos. Contamos con controles técnicos para identificar códigos maliciosos y llevamos a cabo formaciones de concienciación para los empleados. Además, hemos implementado procedimientos para garantizar una respuesta eficiente y rápida en caso de que se produzca un incidente de malware.

Supervisión

Supervisamos la eficacia de los controles y los eventos de seguridad en todas las capas de la nube, incluido el software intermedio, la red, el acceso al SO y el SO. La supervisión automatizada proporciona datos en tiempo real sobre el rendimiento operativo y funcional.

Gestión de incidentes

Aplicamos un planteamiento sistemático para identificar, clasificar, registrar y comunicar incidentes de seguridad y privacidad. Todos los incidentes son evaluados por el punto de contacto en función de nuestra escala de clasificación y se gestionan a través de los procesos establecidos de gestión de incidentes y filtración de datos.

Gestión de vulnerabilidades en la capa de aplicaciones

Para ejecutar SaaS y PaaS en la nube de forma segura, es necesario identificar y mitigar continuamente vulnerabilidades comunes en las tecnologías de la información y la comunicación. Como parte de nuestro ciclo de vida de desarrollo de software seguro (Secure SDLC), integramos varias medidas clave para identificar vulnerabilidades de software y validar nuestros controles de seguridad existentes. Estas medidas incluyen análisis estáticos y dinámicos en diversas etapas del desarrollo, así como pruebas exhaustivas de penetración manuales.

Prueba de seguridad de aplicaciones estática (SAST)

La SAST evalúa automáticamente el código fuente durante el proceso de desarrollo para solucionar problemas antes de pasar al siguiente paso del ciclo de vida de desarrollo de software seguro. Trabajamos con un proveedor de SAST líder según Gartner.

Prueba de seguridad de aplicaciones dinámica (DAST)

La DAST evalúa automáticamente la plataforma a través de la interfaz de usuario en busca de debilidades arquitectónicas y posibles vulnerabilidades de seguridad. Ejecutamos la DAST con herramientas de seguridad líderes en el sector.

Prueba de penetración manual

Profesionales de seguridad externos autorizados simulan manualmente ataques en la plataforma **3D**EXPERIENCE en la nube o en un conjunto específico de aplicaciones para confirmar su nivel de seguridad.

Prueba de ingeniería de calidad interfuncional

Nuestros equipos independientes de Ingeniería de Calidad contribuyen al proceso de verificación de la seguridad mediante la ejecución periódica de escenarios de amenazas. Su amplio conocimiento del producto y su dominio de conceptos clave de seguridad constituyen una capa adicional de verificación y validación de la seguridad.

Gestión de vulnerabilidades de sistemas operativos, redes y software intermedio

Utilizamos varias comprobaciones de vulnerabilidades y análisis acreditados para identificar activos orientados a Internet. Además, empleamos un escáner de vulnerabilidades líder según Gartner para identificar de manera rápida y eficiente posibles fallos en nuestra red y nuestros activos.

GESTIÓN DE PARCHES

Aplicamos periódicamente actualizaciones de software, incluidos parches funcionales y relacionados con la seguridad. Las interrupciones de servicio planificadas se producen regularmente según lo establecido en nuestro SLA. Además, nuestros procesos de gestión de parches y gestión de incidentes tienen en cuenta los parches de seguridad de emergencia que se pueden aplicar en cuestión de horas, lo que implica interrupciones ocasionales del servicio no planificadas.

SUPERVISIÓN DE SEGURIDAD Y GESTIÓN DE INCIDENTES

Nuestro sistema integral de supervisión de seguridad y gestión de incidentes identifica, analiza y responde a las amenazas de seguridad en tiempo real. Adoptamos un doble planteamiento que consiste, por un lado, en identificar y corregir vulnerabilidades y, por otro, en responder rápidamente a los incidentes de seguridad.

Supervisión de seguridad

Los registros y los eventos se recopilan y analizan de forma centralizada a través de nuestra solución SIEM (administración de eventos, incidentes y seguridad) y nuestro equipo especializado del SOC (Centro de Operaciones de Seguridad) los supervisa de forma ininterrumpida. Nuestra plataforma SIEM recopila datos de forma centralizada y utiliza un motor de correlación avanzado para identificar proactivamente los eventos de seguridad. Analiza grandes volúmenes de datos del registro de seguridad para identificar intentos de actividad maliciosa.

Nuestro servicio de supervisión y control de la plataforma **3D**EXPERIENCE en la nube cuenta con múltiples indicadores en las capas de la nube para supervisar la funcionalidad, el rendimiento y la seguridad.

Procesos de respuesta a incidentes

Nuestro equipo del SOC supervisa y evalúa continuamente los riesgos que identifica nuestra solución SIEM en función de la naturaleza del incidente. Respondemos a los incidentes de inmediato de acuerdo con nuestra evaluación del riesgo y el procedimiento de gestión de incidentes siguiendo las pautas de la NIST SP 800-61. Lo anterior incluye las fases principales de contención, erradicación, recuperación y notificación.

Como parte del proceso de gestión de parches, se implementan parches de emergencia en cuestión de horas (consulte Gestión de parches).

PLANES DE RECUPERACIÓN DEL NEGOCIO (BCP) Y PLANES DE RECUPERACIÓN ANTE DESASTRES (DRP)

Los planes de recuperación del negocio (BCP) y los planes de recuperación ante desastres (DRP) son fundamentales para cualquier proveedor de software basado en la nube. Nuestro BCP aborda la planificación para restaurar por completo los servicios informáticos, los servicios de software, las conexiones y los datos en caso de pérdida. Nuestro DRP aborda los procedimientos para limitar o revertir las pérdidas en caso de eventos importantes.

En lo relativo al BCP y al DRP, seguimos las prácticas recomendadas del sector, que incluyen:

1. Mantener un plan coherente sobre la copia de seguridad y la recuperación de los datos del cliente, y garantizar que todos los componentes del plan sean accesibles en caso de un desastre importante.

2. Mantener copias de los datos esenciales fuera de nuestra región de producción, alejados de nuestro centro de datos principal.

3. Mantener actualizados nuestros BCP y DRP y garantizar que incorporen cualquier cambio que se realice en el entorno de producción.

4. Probar nuestros BCP y DRP anualmente.

5. Aprovechar las capacidades de virtualización, como los sistemas de equilibrio de carga y conmutación por error, para garantizar interrupciones mínimas del servicio.

Nuestra meta es lograr un objetivo de tiempo de recuperación (RTO) y un objetivo de punto de recuperación (RPO) imponentes para garantizar la continuidad del negocio de nuestros clientes en todas las situaciones.

Copia de seguridad y recuperación de datos

En consonancia con nuestro Acuerdo de nivel de servicio, nos aseguramos de realizar copias de seguridad diarias de los datos de nuestros clientes y usuarios. Mantenemos las copias siguiendo lo dispuesto en el SLA. Realizamos copias de seguridad en caliente y en frío constantemente para minimizar el tiempo de inactividad y maximizar la protección de los datos.

Los datos del cliente de la plataforma **3D**EXPERIENCE en la nube siguen estando disponibles para su recuperación durante un período definido, según se especifica en el SLA.

Para obtener más información, consulte nuestro Acuerdo de nivel de servicio para servicios en línea.

PRIVACIDAD Y PROTECCIÓN DE DATOS

Nuestras soluciones en la nube se desarrollan respetando la privacidad de nuestros clientes y usuarios. Seguimos altos estándares para garantizar que toda la PII se almacena y gestiona de manera segura, de acuerdo con las leyes y normativas pertinentes, como el Reglamento General de Protección de Datos europeo 2016/679 (RGPD).

Responsable del tratamiento

Los responsables del tratamiento, según lo definido en el RGPD, deben determinar las políticas y los procedimientos para el tratamiento de datos personales, incluido el período de conservación del almacenamiento, el cumplimiento de la minimización de PII y la gestión de las solicitudes de los sujetos de los datos. Dassault Systèmes actúa como responsable del tratamiento cuando procesa PII relacionada con sus procesos comerciales internos y sistemas de información.

El cliente de las soluciones de SaaS de Dassault Systèmes es responsable de la gestión de PII almacenada en la solución y, por lo tanto, actúa como responsable del tratamiento.

El RGPD y otras leyes de protección de datos tienen como objetivo fortalecer los derechos fundamentales de los ciudadanos al ampliar sus derechos de privacidad y darles el control sobre su PII. Como empresa internacional, Dassault Systèmes cumple con el RGPD, así como con otras leyes de protección de datos en las jurisdicciones en las que Dassault Systèmes opera. El RGPD y otras leyes específicas del país se incluyen en la Política de privacidad de Dassault Systèmes disponible en 3ds.com.

En el caso de la plataforma **3D**EXPERIENCE en la nube, Dassault Systèmes actúa en el papel de responsable del tratamiento para lo siguiente:

- **3D** Passport salvo para ofertas de nube privadas.
- **3D** Passport creado por un usuario a través de 3ds.com.
- Comunidades públicas de **3D**EXPERIENCE disponibles en las plataformas públicas de Dassault Systèmes.
- Asistencia al cliente de Dassault Systèmes
- **3D**EXPERIENCE Marketplace

Además del RGPD, los delegados regionales de protección de datos de Dassault Systèmes supervisan el resto de leyes y regulaciones locales de protección de datos, cuya aplicación se garantiza a través de procesos y procedimientos locales.

3D Passport es el perfil de autenticación creado por el usuario. El tratamiento de PII en **3D** Passport es responsabilidad de Dassault Systèmes. La PII asociada a **3D** Passport se almacena en Europa con algunas excepciones específicas debido a los requisitos normativos.

Encargado del tratamiento

Cuando Dassault Systèmes proporciona ofertas basadas en la nube, como la plataforma **3D**EXPERIENCE en la nube, Dassault Systèmes actúa como encargado del tratamiento de la PII que se le pide que trate y almacene. En esta función, Dassault Systèmes procesa la PII según el acuerdo contractual firmado entre las partes.

Dassault Systèmes actúa en el papel de encargado del tratamiento, según lo definido en el RGPD, en los siguientes casos:

- Las ofertas de la nube públicas y privadas de Dassault Systèmes a clientes y socios comerciales.
- **3D** Passport para ofertas de nube privadas.

Cuando actúa como encargado del tratamiento, un proveedor de IaaS externo almacena los datos de la plataforma (p. ej., 3DS Outscale o Amazon Web Services) en un centro de datos local.

CONCLUSIÓN

Para Dassault Systèmes la seguridad y la privacidad son una prioridad en las operaciones. Nuestras medidas de ciberseguridad y protección de datos se basan en los estándares más respetados del sector y se aplican sistemáticamente a través de formaciones, requisitos de diseño, controles de seguridad, medidas de privacidad y pruebas y auditorías externas. Mejoramos continuamente las medidas de seguridad y privacidad en nuestro afán por innovar y lograr la excelencia, garantizando que apoyamos a nuestros clientes de la mejor manera posible.

La plataforma **3D**EXPERIENCE® impulsa nuestras aplicaciones y ofrece un extenso portfolio de experiencias que dan solución a 11 industrias diferentes.

Dassault Systèmes, The **3DEXPERIENCE** Company, es un catalizador del progreso humano. Proporcionamos a las empresas y a las personas entornos virtuales de colaboración para dar rienda suelta a la imaginación en materia de innovación sostenible. Mediante la creación de "gemelos virtuales" de elementos reales con nuestras aplicaciones y plataforma **3DEXPERIENCE**, los clientes traspasan los límites de la innovación, el aprendizaje y la producción.

Los 20 000 empleados de Dassault Systèmes están aportando valor a más de 270 000 clientes de todo tipo, de cualquier sector y en más de 140 países. Si desea obtener más información, visite **www.3ds.com/es**.

3DEXPERIENCE®

DASSAULT SYSTEMES | The 3DEXPERIENCE® Company

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

América
Dassault Systèmes
175 Wyman Street
Waltham, MA, 02451
EE. UU.

Asia-Pacífico
Dassault Systèmes K.K.
ThinkPark Tower,
2-1-1 Osaki, Shinagawa-ku,
Tokyo 141-6020
Japón