Seguridad de Smartsheet

Una vista exhaustiva de las capacidades, prácticas y protecciones de Smartsheet en materia de seguridad

Resumen ejecutivo

En Smartsheet, entendemos que las plataformas de software como un servicio (SaaS) de grado empresarial deben ofrecer múltiples capas de defensa e infinidad de protecciones y controles de TI a fin de proteger los datos confidenciales de la empresa. También es importante que estas soluciones sean flexibles y se integren en los sistemas y procesos existentes de seguridad de datos.

En el presente informe técnico, se exponen las capacidades, protecciones y prácticas de Smartsheet en materia de seguridad y gobernanza. Esencialmente, nos concentraremos en las capacidades controladas por el cliente que Smartsheet recomienda implementar para mantener un entorno de trabajo seguro, conforme y bien gestionado. Tenga en cuenta que este informe técnico no incluye las capacidades de seguridad que todavía no están disponibles de manera generalizada.

Descripción general

Con el propósito de proteger a su organización, recomendamos implementar controles en torno a tres áreas principales: gestión de identidades y accesos, gobernanza de datos y configuración global de la cuenta. Además de estos temas, este documento incluye información general sobre las prácticas de seguridad, privacidad y cumplimiento de Smartsheet.

- **La gestión de identidades y accesos** tiene como eje principal controlar la forma en la que sus usuarios obtienen acceso a Smartsheet, lo que garantiza que la función y la identidad de cada usuario dentro de la plataforma sean acordes con su estructura y políticas organizativas. Asimismo, discutiremos cómo garantizar la seguridad al colaborar con usuarios externos, en función de sus preferencias de seguridad.

- **La gobernanza de datos** debe ejecutarse tanto a nivel del usuario como en toda la organización. En el caso de los usuarios, el enfoque de mínimo privilegio es el predeterminado para Smartsheet e incluye controles adicionales disponibles para restringir y controlar aún más la visibilidad, de modo que los usuarios solo estén expuestos a lo que necesiten cuando lo necesiten. A nivel de la organización, explicaremos tanto los mecanismos simples (p. ej., el uso compartido seguro y los informes de usuarios) como las capacidades avanzadas opcionales disponibles (p. ej., las políticas de salida de datos).

- **La configuración global de la cuenta** le permite personalizar la estética de su entorno de Smartsheet para que sea acorde con la marca de su organización. Incluso algo tan simple como una señal visual que confirma que los usuarios están dentro del entorno protegido de la organización puede servir para garantizar la seguridad. Garantice la coherencia fijando la marca y la personalización para que todos y cada uno de los recursos creados sean acordes con su marca.

- **Las prácticas de seguridad, privacidad y cumplimiento** aluden a las acciones y protecciones que Smartsheet mantiene fuera de nuestra plataforma y cuyo propósito es garantizar que los datos de los clientes estén plenamente protegidos. Smartsheet implementó estrategias de defensa exhaustivas y líderes del sector a través de una combinación de personas, procesos y tecnologías que protegen la confidencialidad, integridad y disponibilidad de los entornos y recursos de Smartsheet.

Índice

Gestión de identidades

La gestión de la identidad de un usuario en Smartsheet y, por ende, su acceso al sistema es tan importante como gestionar los datos en la plataforma.

En las primeras instancias de implementación de Smartsheet, usted decidirá qué método de autenticación quiere usar. Smartsheet ofrece diferentes opciones: correo electrónico y contraseña, y métodos de inicio de sesión único (SSO) de Google, Microsoft, proveedores de SAML 2.0 y Apple.

Puede seleccionar uno o más métodos para su organización, aunque sugerimos aplicar un solo método de autenticación de SSO para todos los usuarios y desactivar los otros métodos. También recomendamos agregar otra capa de seguridad implementando la autenticación de múltiples factores (MFA) cuando configure su SSO.

Smartsheet dispone de un robusto conjunto de API de REST. La API de Smartsheet utiliza OAuth 2.0 para la autenticación y autorización. Se requiere un encabezado HTTP que contenga un token de acceso para autenticar cada solicitud. Para mayor seguridad, utilice OAuth 2.0 para cualquier integración que cree como práctica recomendada.

Gestión de accesos

La gestión de los usuarios y su acceso es una función administrativa central que puede afectar tanto la seguridad como la adopción de Smartsheet en la organización. Las organizaciones deben encontrar un delicado equilibrio entre fomentar la colaboración y, al mismo tiempo, gestionar los riesgos que conlleva la distribución cada vez mayor de los datos y los equipos. Para respaldar este concepto, Smartsheet ofrece tres modelos de gobernanza diferenciados de acuerdo con las principales formas en que los clientes intentan gestionar la aplicación.

Modelos de gobernanza de Smartsheet

El primer enfoque es nuestro modelo descentralizado (federado), en el que las unidades de negocio individuales controlan sus propias compras y planes de forma directa. En este modelo, TI no suele participar en la administración, y la facturación del plan, la gobernanza y la administración de usuarios se dejan a discreción de cada departamento. Por lo general, este modelo es el indicado para las empresas que recién inician su recorrido en Smartsheet.

Nuestro segundo enfoque es el modelo centralizado (consolidado), en el que los planes de Smartsheet se consolidan en una sola suscripción gestionada por TI. Esto facilita un control directo sobre los gastos, la administración de usuarios y los controles de seguridad. Este modelo es más adecuado para los equipos de TI que quieren supervisar de cerca todos los aspectos de su experiencia en Smartsheet.

Por último, nuestro modelo compartido (híbrido) está ideado como un enfoque intermedio, es decir, TI controla la configuración de la organización mediante el Administrador del plan Empresarial, y los administradores de sistemas de la línea de negocios se encargan de forma directa de la administración de usuarios y licencias. La facturación también está separada por planes, lo que permite la facturación por departamento, o un modelo en el que el gasto en Smartsheet se incorpora a los presupuestos departamentales en lugar de facturarse de manera centralizada a TI.

A fin de garantizar un alto nivel de seguridad, Smartsheet recomienda nuestros modelos compartidos o centralizados, que proporcionan un control de TI más directo sobre sus planes.

Gestión de usuarios

A medida que varios equipos de su empresa adoptan Smartsheet de forma independiente para sus propias necesidades, pueden crearse múltiples planes separados. Las fusiones y adquisiciones pueden contribuir a un entorno con múltiples planes de Smartsheet.

Para gestionar usuarios en estos planes a través del modelo descentralizado, es conveniente habilitar la Detección de cuentas para cada uno de esos planes. A medida que los nuevos usuarios se exponen a Smartsheet, esto les permite a ellos o a cualquier persona del dominio de la organización ver una lista de los planes de Smartsheet asociados con su empresa, lo que proporciona un medio centralizado para solicitar unirse a uno de esos planes existentes, en lugar de iniciar uno nuevo. Dichas solicitudes se envían automáticamente a sus administradores de sistemas (a través del Centro de administración de Smartsheet) para su revisión y aprobación.

Si tiene varios planes separados y quiere gestionar los usuarios con el modelo centralizado, es posible que tenga que llevar a cabo una consolidación de cuentas. Nota: Los clientes con capacidades avanzadas, como Dynamic View, Conectores de aplicación premium y Control Center, deberán comunicarse con el Soporte de Smartsheet para pedir asistencia adicional con ciertos aspectos de la consolidación.

Si está usando el modelo compartido y el Administrador del plan Empresarial, una práctica recomendada consiste en organizar los planes en torno a departamentos, equipos o centros de costos. De este modo, podrá definir una política para asignar usuarios automáticamente a los planes relevantes según su afiliación a una de estas entidades.

Administración de usuarios

Smartsheet entiende que es posible que agregar usuarios de uno en uno no pueda ajustarse a escala, ya que la adopción crece hasta decenas, cientos o, incluso, miles de usuarios. En ese sentido, cuando recién esté empezando, le recomendamos aprovechar la función de importación masiva de usuarios de nuestro Centro de administración. A través de esta, puede agregar fácilmente hasta 1000 usuarios de una sola vez en su organización de Smartsheet. Del mismo modo, también puede utilizar la actualización masiva para editar en masa las funciones de los usuarios existentes.

Las fusiones o adquisiciones suelen dar lugar a cambios de marca, lo que hace que los usuarios reciban nuevas direcciones de correo electrónico. La Combinación de usuarios permite actualizar de forma masiva las direcciones de correo electrónico principales de los usuarios y eliminar las cuentas duplicadas.

En un plan consolidado de Smartsheet, se pueden usar otras dos capacidades para optimizar aún más la administración de usuarios, además de automatizarla:

- El Aprovisionamiento automático de usuarios (UAP) automatiza el proceso de agregar usuarios a una cuenta empresarial. A medida que los usuarios se registren o inicien sesión en Smartsheet con la dirección de correo electrónico de su empresa, se agregarán automáticamente a su cuenta. Además, puede elegir si se deben conceder licencias a los usuarios o si deben unirse automáticamente a la cuenta como colaboradores sin licencia (gratuitos).

    - Si adoptó nuestro modelo consolidado, le sugerimos que active el UAP para que los empleados se unan automáticamente a la cuenta central controlada por TI.

    - Si utiliza nuestro modelo compartido (y si su organización documentó la información del departamento/centro de costos para su lista de usuarios), le recomendamos activar el UAP, ya que esa información se puede importar para asociar automáticamente a los usuarios con el plan adecuado cuando soliciten una licencia. También puede utilizarse para automatizar la migración de usuarios sin licencia entre planes.

- La Integración de directorios le permite sincronizar directamente sus usuarios de Microsoft Azure Active Directory (AD) en Smartsheet. Conecte Smartsheet a su automatización existente en Azure AD para automatizar completamente la incorporación y la baja de usuarios, a fin de minimizar el riesgo de que los usuarios retengan o vuelvan a visitar sus cuentas de Smartsheet. Como ventaja adicional, los atributos de AD a nivel de usuario (p. ej., departamento, centro de costos o división) se incluyen en un Informe de devolución de Smartsheet, que está disponible en el Centro de administración y se puede usar para facilitar la devolución interna. Una práctica recomendada es sincronizar todos los usuarios del Directorio con la cuenta de Smartsheet de su organización. Así evita que esos usuarios creen cuentas de Smartsheet adicionales de "TI en la sombra" al iniciar sesión por primera vez. Como segunda capa de defensa, también puede dejar el UAP activado para que capte a todos los usuarios que aún no estén sincronizados a través del Directorio.

Cuando una persona abandona su organización, es importante eliminar su acceso a Smartsheet. Ofrecemos dos formas de hacerlo. Cuando elimina a un usuario, este desaparece de su cuenta de Smartsheet, al igual que los recursos que posee; sin embargo, esto puede provocar que se eliminen los elementos que aún se estén utilizando, lo que podría dañar las soluciones que dependen de esos datos. En su lugar, Smartsheet recomienda desactivar los usuarios. Esto sigue impidiendo totalmente que el usuario acceda a Smartsheet, pero preserva la accesibilidad a su contenido y elimina cualquier consideración necesaria en torno a la estabilidad de la solución o las transferencias de propiedad.

Tipos de funciones y usuarios en Smartsheet

Independientemente de su método de aprovisionamiento de usuarios, deberá determinar las funciones en Smartsheet para las personas de su organización.

Cabe destacar que asignar una función a una persona no le otorga acceso a los recursos de Smartsheet de su organización. Los recursos también se deben compartir de forma directa con dichas personas. En ese sentido, tanto las funciones como los permisos de acceso a recursos determinarán lo que las partes interesadas pueden ver y hacer en Smartsheet. Smartsheet admite las siguientes funciones principales:

- Usuario con licencia: Usar funciones con licencia, como la creación de hojas

- Administrador de grupo: Crear y gestionar grupos de Smartsheet*

  * Las funciones de Administrador de grupo también deben ser Usuarios con licencia.

- Administrador del sistema: Gestionar usuarios, configuración de la cuenta y controles de seguridad

Recomendamos encarecidamente asignar al menos dos Administradores del sistema activos a la cuenta de Smartsheet de su organización, de forma tal que no se produzcan alteraciones si un Administrador del sistema no está disponible en algún momento.

Los Administradores de grupo pueden crear grupos de Smartsheet, lo que les permite a los usuarios compartir contenido con el grupo, en lugar de pedirles a los usuarios que compartan con cada miembro de forma individual. Los Administradores de grupo solo pueden gestionar grupos de los que son propietarios. En caso necesario, para limitar la colaboración externa, restrinja la membresía a los grupos únicamente a las partes interesadas de su organización.

Si no asigna ninguna de las funciones anteriores a un usuario, su acceso se limitará solo a los recursos de Smartsheet (hojas, informes, paneles o WorkApps) que se le hayan compartido. Para crear recursos en Smartsheet, las partes interesadas deben ser Usuarios con licencia y pueden solicitar una licencia directamente a través de la aplicación Smartsheet. Los Administradores del sistema pueden hacer un seguimiento de las solicitudes y responder a ellas de manera individual o masiva a través de la sección Administración de solicitud de licencia del Centro de administración. Si usted ya tiene establecido un proceso para gestionar las solicitudes de licencia, debería pensar en aprovechar una Pantalla de actualización personalizada para indicar a los usuarios que presenten sus solicitudes de licencia a través de dichos procesos internos.

Colaboradores externos

Toda parte interesada fuera de su dominio a quien se le comparten recursos de Smartsheet se define como colaborador externo. Smartsheet dota de facultades a su organización para colaborar libremente con cualquier parte externa de confianza, sin costos asociados para este tipo de colaboradores. Para garantizar la seguridad en las colaboraciones externas, lo conveniente es aprovechar tres controles centrales de administración:

El Uso compartido seguro le permite especificar dominios o direcciones de correo electrónico que son de confianza y están autorizados para la colaboración externa.

Los Informes de acceso a las hojas ofrecen una lista de los colaboradores externos que tienen acceso al contenido de Smartsheet de su organización.

La función Revocar el acceso a los elementos, ubicada en el Centro de administración, permite eliminar a los colaboradores externos del contenido al que ya no necesitan acceder.

Gobernanza de datos

La gobernanza eficaz de los datos es indispensable para que las empresas de hoy en día garanticen que la información que es propiedad de la organización se cree, utilice, comparta y proteja de acuerdo con la normativa vigente, las políticas de la empresa y las prácticas recomendadas del sector.

Estos controles son necesarios no solo a efectos normativos, sino también para garantizar la eficiencia, la confidencialidad y la continuidad del negocio:

A nivel del usuario, la organización debe proporcionar herramientas eficaces para restringir la visibilidad y mostrar solamente a las partes interesadas la información relevante.

A nivel de la organización, la empresa debe disponer de herramientas pertinentes para la creación y la ejecución eficaz de políticas.

Gobernanza de datos a nivel del usuario

La mayoría de los usuarios están familiarizados con los niveles de permiso en Smartsheet (Observador, Editor, Administrador y Propietario). Dynamic View y WorkApps proporcionan controles y flexibilidad adicionales y más granulares, lo que permite brindar capacidades eficaces de gobernanza de datos a nivel del usuario. Limitar el acceso solo al contenido más relevante ayuda a garantizar la eficacia del proceso (ya que los usuarios deben centrarse necesariamente en los elementos que necesitan atención), pero también garantiza la seguridad, porque se amplía el enfoque de Smartsheet de mínimo privilegio por defecto a una escala más granular.

Dynamic View

No todos los procesos de negocios garantizan una transparencia plena. Para muchos procesos (gestión de pedidos, colaboración con proveedores, proyectos en los que participan equipos mixtos internos y externos), hace falta un control estricto de qué se comparte y con quiénes.

Dynamic View permite la colaboración sin afectar la confidencialidad. Con Dynamic View, los propietarios de las hojas pueden compartir de forma selectiva las filas y los campos de interés con colaboradores específicos, sin compartir las hojas subyacentes. Esto permite varios casos de uso en los que usuarios empresariales específicos pueden compartir de forma selectiva elementos con proveedores, equipos mixtos internos y externos, o entre organizaciones, lo que invita a colaborar solo en determinados campos. Todos tienen acceso a la información que necesitan, y solo a la que necesitan.

WorkApps

WorkApps le permite agilizar su trabajo y simplificar la colaboración usando aplicaciones fáciles de navegar diseñadas directamente a partir de sus hojas, formularios, paneles, informes y mucho más. Puede adaptar la experiencia de la aplicación a los miembros de su equipo con base en la función de cada persona, y trabajar juntos a partir de los mismos conjuntos de datos subyacentes. Ajuste sus aplicaciones a escala con la misma seguridad de grado empresarial y multinivel que la plataforma Smartsheet.

WorkApps elimina la necesidad de compartir los recursos subyacentes constitutivos de una WorkApp. Puede crear una WorkApp con una vista filtrada de hojas e informes seleccionados, pero no es necesario compartir ninguna de esas hojas o informes con el usuario final. El usuario solo ve dichos recursos en la vista de la "WorkApp".

Controles de políticas de gobernanza de datos a nivel de la organización

Smartsheet dota de facultades a los administradores para garantizar que las capacidades de la plataforma se utilicen en el marco de las políticas de gobernanza de la organización. Estos controles permiten a los administradores implementar una buena gobernanza de datos para garantizar que los datos se gestionen correctamente y que solo lo hagan las personas que deban interactuar con ellos.

Los administradores pueden elegir cómo quieren que los usuarios interactúen con determinadas funciones. ¿Deberían los propietarios de la hoja tener la capacidad de publicar sus hojas y crear nuevas automatizaciones? ¿Tiene algún sistema de almacenamiento específico desde el que deban adjuntarse los archivos? ¿Deben los colaboradores externos tener la capacidad de descargar el contenido compartido con ellos? Estos son ejemplos de preguntas que los administradores deben plantearse para evaluar con eficacia cuáles son los controles adecuados que deben implementarse en toda la organización.

Estos controles de políticas también abarcan el uso compartido seguro. Si desea limitar el uso compartido de datos y recursos a direcciones de correo electrónico o dominios específicos, esta es la herramienta indicada. Como se mencionó anteriormente, el uso compartido seguro también determina si su organización puede compartir elementos de Smartsheet con otras organizaciones, como proveedores y socios.

Control del widget de contenido web

Los paneles admiten la capacidad de incrustar contenido interactivo, entre ellos, videos, diagramas y documentos. Los administradores pueden activar o desactivar esta función, además de definir una lista aprobada de dominios compatibles con el widget de contenido web. Como práctica recomendada, le sugerimos limitar esta función a los dominios internos de la empresa.

Permisos de automatización

Controle quiénes pueden recibir automatización de las hojas. Las opciones son las siguientes: Limitado (solo permite acciones a los usuarios que tienen uso compartido de la hoja) o Ilimitado (la automatización se aplica a cualquier dirección de correo electrónico e integración de terceros, como Slack). Le recomendamos que revise este control para asegurarse de que su configuración se ajuste al nivel deseado de colaboración interna y externa de su organización.

Controles de archivos adjuntos

Determine si los miembros del plan pueden cargar archivos de sus propias computadoras al adjuntar un enlace (URL) a un sitio o desde servicios de almacenamiento en la nube de terceros, como Google Drive, OneDrive, Box, Dropbox, Evernote o Egnyte. Para evitar la ingesta de datos de fuentes no aprobadas, habilite solamente los proveedores de archivos adjuntos cuyo uso esté aprobado por las políticas internas de su organización.

Controles de publicación

Al publicar una hoja, un informe o un panel, se genera una URL única a la que cualquier persona puede acceder sin iniciar sesión en Smartsheet y un código iFrame que puede insertar dentro del código fuente de un sitio web para mostrar la hoja o el informe.

Puede deshabilitar la publicación de hojas, informes, paneles y iCal, y el botón Publicar desaparecerá del recurso de Smartsheet. También puede restringir el acceso a los elementos publicados únicamente a las personas que se encuentren dentro de su organización de Smartsheet. Observamos que los clientes preocupados por la seguridad suelen permitir la publicación, pero limitan el acceso a los elementos publicados a las personas de su cuenta.

Uso compartido seguro

Utilice esta capacidad para restringir el uso compartido por dominio o por direcciones de correo electrónico específicas (p. ej., para asegurarse de que las hojas se compartan únicamente con las personas que tienen dirección de correo electrónico de la empresa). Smartsheet recomienda encarecidamente implementar el uso compartido seguro para controlar la colaboración externa. Además, para simplificar las actualizaciones y el mantenimiento de su lista de uso compartido seguro, le sugerimos recopilar cualquier solicitud de actualización a través de un formulario web de Smartsheet.

Controles de presentaciones de formularios sin conexión

Cuando se utiliza la aplicación para dispositivos móviles, Smartsheet habilita automáticamente el envío de formularios sin conexión a fin de admitir casos de uso en los que los usuarios pueden no disponer de una conexión estable (p. ej., en una obra en construcción). Este control ofrece a los administradores la capacidad de desactivar (o volver a activar) el envío de formularios sin conexión a fin de controlar si un usuario puede iniciar la aplicación para dispositivos móviles sin conexión para enviar formularios.

Controles de integraciones de comunicación

Smartsheet admite Google Chat, Microsoft Teams, Slack y Cisco Webex como servicios de comunicación compatibles. Los administradores de cuenta pueden habilitar uno o más servicios, a su discreción.

Registros e informes

Puede descargar informes que abarquen diferentes aspectos del uso de Smartsheet en toda su organización, para tener una visibilidad permanente del uso de la plataforma, los usuarios, el contenido, la facturación y el acceso.

Informe de acceso a las hojas

Se genera un archivo Excel con los nombres de todas las hojas, informes y paneles que son propiedad de usuarios con licencia de la cuenta, el nombre del espacio de trabajo en el que se guardan estos elementos (si corresponde), los colaboradores con uso compartido de cada hoja y la marca de tiempo de la última modificación. Recomendamos revisar este informe con regularidad para auditar la lista de colaboradores externos que tienen acceso a recursos que son propiedad de personas de su organización.

Informe de elementos publicados

Se genera un archivo Excel que incluye todos los elementos publicados. Este informe, ideal para la seguridad de los datos o para saber quién publicó determinados elementos, se puede usar para configurar el control de publicación según sea necesario.

Informe de lista de usuarios

Se genera un archivo Excel que incluye a todos los miembros (tanto invitados como activos) de la cuenta, una marca de tiempo que indica cuándo se los agregó a la cuenta, sus niveles de acceso (Administrador del sistema, Administrador de grupo, etc.), la cantidad de hojas de su propiedad y la marca de tiempo del último inicio de sesión en Smartsheet.

Informe del historial de inicios de sesión

Los Administradores del sistema de cuentas con múltiples usuarios pueden utilizar el Centro de administración para recibir por correo electrónico un archivo en formato Excel con el historial reciente de inicios de sesión.

Informe de devolución

Los clientes que utilizan la integración de directorios pueden usar los Informes de devolución, disponibles en el Centro de administración, para facilitar la devolución interna. Esta función permite agregar columnas por división, departamento y centro de costos al informe existente creado cuando los clientes descargan su lista de usuarios, lo que proporciona los datos necesarios para realizar informes de devolución interna.

Para un seguimiento más detallado de las acciones del usuario en hojas, paneles y celdas, puede utilizar el Registro de actividad, el Historial de celda y las Columnas del sistema.

- **Registro de actividad:** Ofrece un registro de auditoría de los cambios introducidos en un recurso, quién los realizó y cuándo. Esto incluye ediciones, como la eliminación de filas (con los datos que se eliminaron), quién visualizó el elemento y cambios en los permisos de uso compartido.

- **Historial de celda:** Muestra un registro de los cambios realizados a nivel de la celda, con detalles de quién los introdujo, cuáles fueron esos cambios y cuándo se hicieron. Los usuarios pueden utilizar fácilmente la función de copiar y pegar desde el Historial de celda para restaurar información anterior que puede haberse eliminado o cambiado por error.

- **Columnas del sistema:** Muestran el momento en que se editó cada fila por última vez y el colaborador que implementó el cambio.

Controles avanzados de gobernanza de datos

Smartsheet ofrece una serie de capacidades avanzadas que proporcionan control de la gobernanza de datos a los clientes con necesidades de seguridad de datos particularmente estrictas. Estas capacidades se incluyen en Smartsheet Advance Platinum y Smartsheet Safeguard.

Claves de cifrado administradas por el cliente

Smartsheet utiliza el cifrado para proteger los datos de los clientes y ayudarlos a mantener el control sobre ellos. Las claves de cifrado administradas por el cliente (CMEK) están pensadas para organizaciones que tienen datos confidenciales o regulados, que las obligan a administrar su propia clave de cifrado. Las CMEK permiten a las organizaciones empresariales utilizar aplicaciones SaaS en la nube para, al mismo tiempo, mantener un control de los datos comparable con el de una instalación local y agregar una capa de cifrado administrada por el cliente al almacenamiento de datos de Smartsheet a fin de ejecutar políticas avanzadas de seguridad y gobernanza de datos.

Nota: Para utilizar las CMEK, los clientes deben tener acceso a Amazon Web Services Key Management Service (AWS KMS), ya que las claves del cliente se configuran y administran de forma directa dentro de AWS.

Smartsheet utiliza CMEK para cifrar los datos de su organización de forma que estén bajo su control en todo momento. En concreto, Smartsheet no almacena ni controla estas claves de cifrado, y debe solicitar y recuperar las claves del Key Management Service (KMS) de AWS de nuestro cliente cada vez que Smartsheet necesita acceder a los datos de su hoja.

Como su organización controla las CMEK almacenadas en el Key Management System de AWS, usted puede revocar el acceso de Smartsheet a las CMEK y, por ende, el acceso a sus datos en cualquier momento. Si elimina las claves maestras en el Key Management System de AWS, su organización puede borrar en efecto sus datos de los sistemas de Smartsheet. Cualquier agente malintencionado que cuente con una copia de la base de datos de Smartsheet, el código fuente y las claves de cifrado en la nube no podrá leer los datos cifrados con las CMEK.

Políticas de salida de datos

El uso compartido de datos siempre plantea cierto nivel de riesgo, pero cuando se trata de contenidos particularmente confidenciales, es primordial garantizar que los datos de la empresa permanezcan únicamente en su cuenta y bajo su control.

Los Administradores del sistema pueden utilizar las políticas de salida de datos para proteger la información confidencial mediante un control minucioso de cómo se pueden exportar los datos tanto dentro como fuera de su organización.

Las políticas de salida de datos se pueden implementar para evitar que los colaboradores internos y externos realicen las siguientes acciones en hojas, informes y paneles:

- Guardar como nuevo
- Guardar como plantilla
- Enviar como adjunto
- Publicar
- Imprimir
- Exportar

Los usuarios que intenten una acción restringida recibirán una notificación de que el comportamiento está prohibido debido a la política de salida de datos que implementó su organización.

Estos límites tienen como objetivo evitar que los colaboradores guarden o compartan información confidencial con fines malintencionados.

Informes de eventos

Para garantizar la seguridad de la información, muchas empresas requieren un control constante de la manera en que se utilizan las aplicaciones empresariales como Smartsheet. Es prudente mantener la visibilidad en lo siguiente:

- Quiénes crean hojas
- Quiénes crean espacios de trabajo
- Quiénes eliminan objetos
- Quiénes compartieron una hoja y con quiénes

Los Informes de eventos ofrecen visibilidad detallada del comportamiento y la actividad de los usuarios dentro de la cuenta de Smartsheet de su organización. Esta función le permite supervisar la pérdida de datos e identificar patrones de uso anómalos, para que pueda ejecutar con más rigor las políticas de seguridad y cumplimiento de la organización.

Los Informes de eventos ofrecen un feed de datos JSON de los eventos de uso en Smartsheet (“Eventos”) dentro de un plan (org), al que se accede por medio de la API de Informes de eventos. El servicio genera informes de más de 120 eventos en Smartsheet y almacena hasta 6 meses de datos, a partir de la fecha en que se activa el feed.

Para aprovechar este feed, los datos de los Informes de eventos suelen integrarse en otros sistemas de seguridad que ofrecen capacidades de supervisión, notificación, creación y ejecución de políticas, y prevención de pérdida de datos (DLP). Empresas de terceros venden estas aplicaciones, por lo general, sistemas CASB (agente de seguridad de acceso a la nube), sistemas SIEM (gestión de información y eventos de seguridad) o una combinación de CASB y SIEM en simultáneo. A veces, las empresas desarrollan sus propios sistemas de supervisión y respuesta, en lugar de confiar en los que suministran terceros.

Casos de uso clave de los Informes de eventos:

- Prevención de pérdida de datos
- Manejo de información personal identificable (PII)
- Gobernanza de datos
- Perspectivas sobre la colaboración

Controles de conservación de datos

Cuanto más contenido tenga la organización en cualquier aplicación SaaS, más riesgo asume su empresa.

Los Controles de conservación de datos de Smartsheet ofrecen a las organizaciones la capacidad de crear una política que dicte cuándo deben eliminarse los contenidos, en función de los criterios que quieran ejecutar.

Estas políticas pueden basarse en la fecha en que se creó una hoja o en la última vez que se modificó, lo que garantiza que únicamente el contenido activo o reciente se mantenga dentro de su instancia de Smartsheet y limita su perfil de riesgo.

Configuración global de la cuenta

La seguridad de la cuenta no se limita a características técnicas, como el cifrado de datos, la clasificación o las opciones de autenticación. Puede ser algo tan sencillo como incluir el logotipo de su organización en todos y cada uno de los elementos que le pertenecen.

Los controles de la Configuración global de la cuenta le permiten implementar marcas visuales (y otras restricciones) para que los usuarios sepan que están accediendo a la información correcta.

Los Administradores del sistema pueden añadir logotipos a nivel global para que la implementación de Smartsheet cumpla con los requisitos de marca de la organización. Utilice el bloqueo de marca para asegurarse de que todos los recursos nuevos lleven la misma marca.

Los controles de personalización y la configuración de la cuenta de Smartsheet también sirven para configurar pantallas de bienvenida personalizadas. Puede crear pantallas de ayuda personalizadas con descripciones de cómo comenzar, pantallas de solicitud de licencia para ayudar a los usuarios a comunicarse con usted o pantallas de bienvenida personalizadas con su marca que aparezcan cuando el usuario inicie sesión. Las pantallas pueden incluir el requisito de que el usuario apruebe las condiciones del servicio antes de acceder a más información.

Combinar una identidad visual coherente con información personalizada permite a los usuarios saber que están accediendo a las herramientas y la información correctas, además de que mejora su seguridad.

Prácticas de Smartsheet en materia de seguridad, privacidad y cumplimiento

Mediante un enfoque integral, los programas de ciberseguridad, privacidad y protección de datos de Smartsheet parten de políticas estratégicas de seguridad de la información definidas y respaldadas por el Comité Directivo de Seguridad de la Información (ISSC) y el equipo directivo de Smartsheet. Estas políticas están diseñadas para alinearse con las prácticas estratégicas de gestión de riesgos de la organización, gestionar y supervisar proactivamente los riesgos de seguridad, promover la seguridad mediante la madurez de los procesos y una arquitectura de sistemas eficaz, y permitir a los usuarios tomar decisiones prudentes sobre los riesgos de seguridad mediante la capacitación y la concienciación.

Seguridad de los datos

Incorporamos seguridad en nuestra plataforma para garantizar la protección de su recurso más valioso: sus datos. Smartsheet contrata a terceros para que realicen auditorías de nuestras prácticas de seguridad, incluida una evaluación y certificación SOC 2 Tipo II, además de evaluaciones técnicas de seguridad de terceros con empresas de pruebas de penetración. Además, el programa de gestión de vulnerabilidades de Smartsheet automatiza la identificación y corrección de vulnerabilidades de redes y sistemas en todos los entornos corporativos y de producción de Smartsheet. Smartsheet utiliza el cifrado para preservar sus datos y ayudarlo a mantener el control sobre ellos. Esto es lo que Smartsheet puede ofrecerle de forma confiable: todos los datos se almacenan de forma duradera con cifrados aprobados por el Instituto Nacional de Estándares y Tecnología (NIST), tecnología de seguridad de la capa de transporte (TLS), cifrado AES de 256 bits en reposo y el servicio S3 de Amazon para almacenar y administrar los archivos cargados.

Privacidad

En Smartsheet, valoramos su privacidad y respetamos su derecho a saber cómo se recopila y utiliza su información. En nuestro Aviso de privacidad, se describe de qué manera Smartsheet recopila, utiliza y divulga la información personal y de otro tipo que recopilamos a través de nuestros sitios web, nuestras aplicaciones para dispositivos móviles y la plataforma Smartsheet de ejecución del trabajo.

- Reconocemos los derechos de privacidad de nuestros clientes potenciales, clientes y socios, y respetamos las normativas de privacidad globales, incluido el Reglamento General de Protección de Datos (GDPR) de la Unión Europea.

- Ofrecemos un Acuerdo de procesamiento de datos a los clientes que necesitan condiciones específicas para el procesamiento de contenido que incluye información personal. Si determinó que necesita un DPA con Smartsheet, puede enviar un formulario en el que acepta las condiciones del DPA a través de smartsheet.com/legal/DPA

Gestión operativa

Implementamos políticas y procedimientos diseñados para garantizar que sus datos estén seguros y respaldados en varias ubicaciones físicas. Nuestros equipos evalúan constantemente las nuevas amenazas de seguridad e implementan medidas correctivas actualizadas orientadas a prevenir el acceso no autorizado o el tiempo de inactividad no planificado del Servicio de suscripción. El acceso a todos los sistemas y datos de producción de Smartsheet está limitado a los miembros autorizados del equipo de Operaciones técnicas de Smartsheet, en función de los principios de mínimo privilegio y según corresponda. Smartsheet publica información sobre el estado de los sistemas en su sitio dedicado a tal fin. Por lo general, Smartsheet notifica a los clientes de incidentes significativos del sistema por correo electrónico o mensaje de texto, siempre y cuando se hayan suscrito a las actualizaciones automáticas en el sitio de estado de Smartsheet.

Seguridad, continuidad y redundancia del centro de datos

Trabajamos con socios de servicios de alojamiento (hosting) reconocidos del sector para asegurarnos de que pueda brindar servicios a su organización de forma segura en una plataforma de confianza. Contamos con redundancia de datos en varios sitios y alojamiento en las instalaciones de AWS, que cuentan con el aval de las certificaciones SOC 1, SOC 2, ISO 27001 y FISMA. Nuestro servicio de supervisión incluye protocolos de escaneo biométrico, vigilancia continua y gestión de entornos de producción las 24 horas del día, los 7 días de la semana. Smartsheet dispone de procesos y planes internos para hacer frente a eventos que amenacen la continuidad del negocio y contemplar casos de recuperación ante desastres. Estos planes se revisan y evalúan una vez al año, y se distribuyen al personal pertinente de toda la organización. Nuestros centros de datos están geográficamente aislados entre sí (aprox. 965 km), a fin de evitar que se vean afectados de forma simultánea en caso de un desastre natural a gran escala.

Auditorías y certificaciones

Las siguientes auditorías y certificaciones relacionadas con la seguridad y la privacidad corresponden a los servicios de aplicaciones centrales dentro de Smartsheet.

- **SOC 2/SOC 3:** Smartsheet se somete a exámenes y pruebas anuales como parte del proceso de auditoría SOC. Los informes de auditoría externa resultantes avalan el diseño y la eficacia operativa de los controles internos en todo nuestro negocio, incluidas la seguridad, la disponibilidad y la confidencialidad.

- **Certificación del Escudo de la privacidad entre la UE y EE. UU., y entre Suiza y EE. UU.:** Los datos de los clientes enviados a los Servicios cubiertos están dentro del ámbito de una certificación anual del marco del Escudo de la privacidad entre la UE y EE. UU. y del marco del Escudo de la privacidad entre Suiza y EE. UU., administrados por el Departamento de Comercio de EE. UU. La certificación actual está disponible en privacyshield.gov/list; para encontrarla, busque “Smartsheet”.

- **FedRAMP (moderado):** La Junta de Autorización Conjunta (JAB) seleccionó a Smartsheet para el programa FedRAMP Connect, que priorizó a Smartsheet Gov para la certificación con base en la demanda de organismos gubernamentales federales. Smartsheet Gov es un entorno de Smartsheet separado, autorizado por FedRAMP, que facilita al Gobierno de EE. UU. el uso de Smartsheet para gestionar el trabajo y cumplir con los requisitos de seguridad y cumplimiento.

- **Ley Sarbanes-Oxley de 2002:** Smartsheet es una sociedad cotizante y, como tal, tiene la obligación de cumplir con la Ley Sarbanes-Oxley (SOX). El cumplimiento de la SOX permite crear un equipo interno coherente y mejora la comunicación entre los equipos implicados en las auditorías.

Tal y como se advierte en nuestra página web de información legal, Smartsheet utiliza una infraestructura suministrada por Amazon Web Services, Inc. (“AWS”) para alojar los datos de los clientes. La información sobre las auditorías y certificaciones relacionadas con la seguridad y la privacidad recibidas por AWS, como la certificación ISO 27001 y los informes SOC, está disponible en el sitio web de seguridad de AWS y en el sitio web de cumplimiento de AWS. Para ver la lista completa de nuestras certificaciones y otros informes técnicos y hojas de datos, visite la página de cumplimiento en Smartsheet Trust Center.

Conclusión y recursos adicionales

El trabajo de hoy (y de mañana) necesita una plataforma moderna de gestión del trabajo que sea fácil de usar y segura. Gracias a nuestro enfoque e inversiones permanentes, desarrollamos Smartsheet desde cero con estrictos requisitos y capacidades de confidencialidad de datos. Además de lo que está disponible hoy, tenemos una serie de funciones de seguridad adicionales actualmente en desarrollo. Para obtener más información sobre las capacidades, los programas y las protecciones de Smartsheet en materia de seguridad, visite smartsheet.com/trust y los siguientes recursos adicionales:

Ayuda en línea para Administradores del sistema de Smartsheet
Funciones de Smartsheet según el plan
Integraciones de Smartsheet
Documentación de la API de Smartsheet

sales@smartsheet.com
(844) 324-2360
smartsheet.com
/smartsheet
/company/smartsheet-com
@smartsheetplatform
/@smartsheet
/smartsheet
/smartsheet