IRON MOUNTAIN®

Documento técnico

Seguridad en Iron Mountain InSight®

Resumen ejecutivo

Acerca de la seguridad en Iron Mountain

Iron Mountain incorpora un enfoque de seguridad exhaustivo que abarca la incorporación de contenido, el almacenamiento y el procesamiento de documentos digitales, así como el alojamiento en un centro de datos seguro. Iron Mountain usa el marco de ciberseguridad (CSF) del Instituto Nacional de Normas y Tecnología (NIST) como su marco de seguridad empresarial. Ofrecemos una implementación segura de servicios, almacenamiento de datos con protección de la privacidad de los usuarios finales, comunicación entre los servicios y soporte administrativo con separación de responsabilidades.

Formación

Iron Mountain trabaja con sectores altamente regulados que requieren formación sobre seguridad y privacidad para sus trabajadores.Los empleados realizan varios cursos de seguridad y formación a lo largo del año según lo establecido por nuestro programa de formación empresarial. La formación incluye concienciación anual en materia de seguridad, formación sobre privacidad de datos, formación sobre código seguro, y formación sobre el código de ética y conducta empresarial. Trabajamos con los clientes para verificar los antecedentes del personal. Para trabajar con nosotros, es necesario realizar una comprobación previa de antecedentes, tal como exigen diversos requisitos locales o de nuestros clientes.

Productos de Iron Mountain InSight

I. Programas de cumplimiento

Iron Mountain InSight ha establecido un programa de cumplimiento de seguridad amplio y específico que se adapta a las necesidades normativas y del sector de los clientes. Esto incluye el cumplimiento de las normas de seguridad y privacidad de los datos.

Certificaciones de cumplimiento

- ISO-27001: InSight cuenta con esta certificación desde 2020. Se trata de una norma internacional que ayuda a las organizaciones a gestionar la seguridad de sus activos de información. Proporciona un marco de gestión para implementar un sistema de gestión de la seguridad de la información (ISMS) para garantizar la confidencialidad, la integridad y la disponibilidad de todos los datos.
- SOC2 Tipo 2: Iron Mountain cuenta con la certificación SOC2 Tipo 2 para InSight desde 2020. El informe SOC2 Tipo 2 es una auditoría de control de una organización de servicios (SOC) que aborda

la manera que tiene un proveedor de servicios de gestionar la información confidencial en la nube.

Cumplimiento de las normativas del sector

- InSight es compatible con la norma 21 CFR, Parte 11.
- StateRAMP: se recibió el estado Ready (Listo) en enero del 2024.
- FedRAMP (NIST 800-53/37): pruebas realizadas por terceros según los controles de la norma NIST 800-53 Revisión 4, así como los requisitos adicionales de FedRAMP. InSight ha recibido el estado Authorizations to Operate (ATO) de FedRAMP, así como el estado Ready (Listo).

Privacidad de los datos

- Reglamento General de Protección de Datos (RGPD): InSight se ha sometido a una evaluación del RGPD y hay disponible una copia del informe previa solicitud.
- Ley de responsabilidad y portabilidad de seguros médicos (HIPAA): InSight cumple con la ley HIPAA y ha implementado medidas para proteger la privacidad y la seguridad de la información personal identificable (PII).

II. Descripción general sobre seguridad operativa

Gestión de acceso e identidades

- Implementamos y aplicamos un control de acceso basado en funciones para los usuarios con privilegios; su uso y asignación están restringidos. La autenticación multifactor (MFA) es obligatoria para limitar el acceso a los usuarios autenticados. Se implementan unos privilegios mínimos para usuarios y procesos autorizados.

Supervisión

- Análisis de seguridad: el entorno de InSight incluye un sistema de supervisión que analiza los sistemas y las imágenes de los contenedores, y detecta vulnerabilidades.
- Pruebas de seguridad de aplicaciones: InSight realiza pruebas de seguridad de aplicaciones estáticas y dinámicas (SAST y DAST, respectivamente), así como pruebas de penetración manuales.
- Supervisión del sistema y registros de auditoría: InSight incluye un sistema de gestión de eventos e información de seguridad (SIEM) que contempla actividades y tareas como la gestión de registros, la supervisión en tiempo real de eventos de seguridad, la correlación y la activación de alertas de eventos de seguridad, y el almacenamiento de registros de auditoría.
- Respuesta ante incidentes: nuestro equipo de respuesta e incidentes cibernéticos (CIRT) es responsable de clasificar los eventos de auditoría que sean de especial interés para el sistema de información Iron Mountain InSight, así como de realizar revisiones y análisis de los registros de auditoría.
- Gestión de incidentes: nuestro equipo de respuesta e incidentes cibernéticos (CIRT) mantiene un plan de respuesta cibernética para identificar y detectar amenazas, proteger los sistemas, responder ante una amenaza y recuperar los sistemas en tiempo real; dicho plan incluye la supervisión y la elaboración de registros de nuestros productos e infraestructura. También mantenemos programas de concienciación y formación de los empleados que incluyen políticas y procedimientos internos de seguridad de la información.

Continuidad del negocio

- El tiempo de recuperación objetivo (RTO) de InSight para las aplicaciones empresariales de nivel 1 es de entre 10 y 24 horas, y el punto de recuperación objetivo (RPO) fue de 1 hora en nuestra última prueba del plan de continuidad del negocio (BCP) realizada en el 4.º trimestre del 2023.El RTO y el RPO se pueden modificar en función de las necesidades del cliente.

Recuperación ante desastres

- La prueba de recuperación ante desastres de InSight está diseñada para que podamos recuperar de forma eficaz objetos, bases de datos e índices en caso de eliminación o actualización accidental, ya que dichos elementos son las fuentes de datos persistentes para la aplicación InSight dentro del RTO o RPO indicados, tal y como se documenta en nuestro plan de continuidad del negocio (BCP).

Planificación de la capacidad

- Nuestra planificación de la capacidad tiene como objetivo supervisar el rendimiento de las cargas de trabajo y permitir que la capacidad satisfaga las demandas actuales y futuras.Esto incluye la medición del rendimiento y la supervisión

para no alcanzar en ningún momento el límite de la capacidad.

Aplicación de parches y gestión de vulnerabilidades

- La aplicación de parches y la gestión de vulnerabilidades, el antimalware, el cifrado de los discos de los puntos finales y la prevención de intrusos se gestionan a través de nuestras soluciones de gestión de puntos finales y activos de tecnología de la información.

Cifrado

- Todos los datos se cifran en tránsito y en reposo siguiendo las normas federales de procesamiento de información (FIPS 140-2) y mediante estándares del sector, como el estándar de cifrado avanzado (AES) 256 y las claves gestionadas por servicio.

III. Privacidad de los datos

Residencia de datos

- La residencia de datos hace referencia al lugar donde se almacenan los datos del cliente en reposo. Para ayudar a cumplir con los requisitos de residencia de datos, InSight tiene la capacidad de controlar dónde se almacenan los datos, así como personalizar y restringir el almacenamiento de datos en determinadas regiones.

Protección de los datos

- InSight aplica las medidas técnicas, organizativas y administrativas adecuadas, incluidos el cifrado y la autenticación multifactor (MFA), para que los datos de los clientes permanezcan seguros en todo momento. InSight puede implementar un firewall de aplicaciones web (WAF) a petición del cliente.

Evaluaciones del impacto en la protección de datos (DPIA)

- Iron Mountain maneja información privada e información personal identificable en nombre de otras personas. Como responsable o encargado del tratamiento de los datos, Iron Mountain puede gestionar o procesar la información del cliente sin tener en cuenta el contenido real o el origen de los datos.
- Cuando actuemos como responsable o encargado del tratamiento de los datos dentro del Espacio Económico Europeo (EEE) y Suiza (o accedamos a datos del EEE o Suiza desde Estados Unidos), los datos se procesarán de acuerdo con los Principios del Escudo de Privacidad aplicables.
- Llevamos a cabo evaluaciones de impacto en la protección de datos (DPIA) con respecto al tratamiento de los datos personales, y lo hacemos de manera periódica y según lo establecido.

NOTA: Consulta la política de privacidad de Iron Mountain para obtener información sobre los tipos de datos personales que transferimos y procesamos y el propósito por el cual lo hacemos, así como para conocer los terceros con los que compartimos tales datos.

Elevate the power of your work

Iron Mountain lleva más de 70 años siendo tu mejor socio estratégico para cuidar de tu información y tus activos. Somos líderes mundiales en servicios de almacenamiento y gestión de la información y contamos con la confianza de más de 225 000 organizaciones de todo el mundo, entre las que se incluyen más del 90 % de las empresas de la lista Fortune 1000. Protegemos, desbloqueamos y ampliamos el valor de tu trabajo, sin importar cómo sea, donde se encuentre o cómo se almacene.

ARG: 4630-5100 / 4630-4100 | ironmountain.com/es-ar
CHIL: (562) 23957000 | ironmountain.com/es-cl
COL: 1 742 1904 | ironmountain.com/es-co
MX: 8008994766 | ironmountain.com/es-mx
PE: 01 - 711 4000 | ironmountain.com/es-pe

Acerca de Iron Mountain

Iron Mountain Incorporated (NYSE:IRM), fundada en 1951, es líder mundial en servicios de almacenamiento y gestión de la información. Con la confianza de más de 225 000 organizaciones de todo el mundo y con una red de propiedades de más de 9,1 millones de metros cuadrados repartidos en más de 1400 instalaciones ubicadas en más de 60 países, Iron Mountain almacena y protege miles de millones de activos de información, que incluyen información crítica para el negocio, datos altamente confidenciales y artefactos culturales e históricos. Al ofrecer soluciones que incluyen almacenamiento seguro, gestión de la información, transformación digital, destrucción segura, así como centros de datos, almacenamiento y logística de obras de arte, y servicios en la nube, Iron Mountain ayuda a las organizaciones a reducir costos y riesgos, cumplir la normativa, recuperarse de desastres y permitir una forma de trabajar más digital. Visita www.ironmountain.com para obtener más información.