Documentación de Producto

Asei Backup Online en infraestructura "Premium" y R.G.P.D

INFRAESTRUCTURA PREMIUM

La infraestructura del servicio de Asei es la columna vertebral de nuestra credibilidad y nos permite ofrecer servicios en la nube de clase empresarial de forma extremadamente segura, escalable y fiable. Todos nuestros productos y soluciones están respaldadas por una infraestructura de nube altamente resistente, redundante y que está constantemente supervisado y respaldado por un líder en la industria del DataCenter.

Centros de Datos

Asei dispone de almacenes en dos centros de datos de nivel empresarial en lugares estratégicos en Europa. Las instalaciones están diseñadas para el 99,999 por ciento de fiabilidad y cuentan con la mayoría de las certificaciones existentes en materia de seguridad: SSAE 16, HIPAA, PCI compatible, ISO 9001 /ISO 27001, etc. Cada centro de datos dispone de avanzadas características de seguridad, potencia, controles ambientales y capacidades de red.

Estos DataCenters pertenecen a Amazon Inc. El DataCenter principal utilizado se encuentra en FrankFurt (Alemania) y los datos de backup se sincronizan asíncronamente con el DataCenter de Dublín (Irlanda) conforme a los requisitos RGPD.

Seguridad e Integridad de los Datos

Asei Backup Online protege y preserva los datos de los cuales se hace backup mediante el compromiso de los más altos estándares de seguridad – y utilizando sistemas de ingeniería que aseguren la integridad de los datos. Asei utiliza las normas más estrictas para el cifrado de datos y la transmisión de los mismos a la red.

Asei se adhiere a los más altos estándares de seguridad para proteger los datos subidos a los DataCenter. Insistimos en que nuestro servicio cumple las más estrictas normas aceptadas internacionalmente para el cifrado de datos, incluyendo el algoritmo de **cifrado AES de 256bits**.

Segura, la Red siempre Activa

Alto rendimiento y conectividad a Internet desde los DataCenter utilizados es crucial para que la prestación de servicios en la nube sea rápida y fiable. Laconectividad de red de los DataCenter de Amazon tiene una redundancia sin precedentes, utilizando varios troncales de acceso y con seguridad activa en cada capa del sistema.

Si desea conocer más sobre los sistemas de seguridad aplicados a los DataCenter de Amazon le proponemos consultar su hoja de datos de los procesos de seguridad aplicados:

https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

Seguimiento y Gestión

El equipo de soporte de Asei Backup Online monitoriza todas las copias que se producen diariamente. Se comprueba que las copias de seguridad programas se realicen correctamente y en caso de producirse cualquier problema o incidente durante dos ciclos de copia se contacta con el administrador indicado del sistema para avisar y en caso de ser necesario, actuar como servicio de soporte para resolver el problema e incidencia que se produzca.

Además, nuestros agentes de copia, una vez terminada la ejecución de los backup puede informar de manera automática a quien se desee, por medio de un correo electrónico, del resultado final de la copia de seguridad.

Adecuación a la R.G.P.D.

Las empresas se deben adecuar a la R.G.P.D. de acuerdo a su nivel sobre las medidas de seguridad que deben de tomar.

El servicio de **Asei Backup Online BASIC en infraestructura Premium** se adecuada al **nivel básico** sobre medidas de seguridad.

El servicio de **Asei Backup Online BACRI en infraestructura Premium** **puede ser adecuado al nivel medio y alto** sobre medidas de seguridad siempre que el responsable de los ficheros cumpla con las obligaciones establecidas para ello indicadas en este apartado.

En este resumen vamos a indicar las medidas que tiene que cumplir una empresa en materia de Copias de Seguridad y recuperación de datos:

Obligaciones que afectan a datos de todos los niveles (Básico, Medio y Alto)

Se deberán garantizar la restauración de datos al momento anterior a producirse la pérdida. Se requiere realizar copias de seguridad al menos una vez a la semana (artículo 94.1 del Reglamento de Desarrollo de la RGPD (RRGPD), RD 1720/2007)

- **Realizando una programación adecuada del plan de copias se cumple perfectamente esta obligación. Normalmente, se realizan copias diarias de la información modificada.**

Obligaciones que afectan a datos de nivel Medio y Alto

Es necesaria una autorización para la ejecución de procedimientos de restauración de datos (RRGPD artículo 100.2)

- **El usuario que va a realizar la restauración (siempre que las copias se hayan encriptado previamente) debe introducir una clave de desencriptación. Sin dicha clave es imposible realizar la restauración.**
  Esta contraseña debe ser guardada por el responsable del tratamiento de la información de forma segura. Además, es posible proteger la consola de restauración con una contraseña maestra para impedir accesos no autorizados.

Obligaciones que afectan a datos de nivel Alto

Almacenamiento externo de copias y procedimientos de restauración de datos (RGPD artículo 100.2)

- **Es la funcionalidad principal de las herramientas de Backup Online.**

ARTICULOS DE LA NORMA A CONSIDERAR

Veamos qué dice la norma:

Identificación de soportes (Art. 13)

Mantener un control de la salida de soportes.

Asegurarse que el desecho de soportes no pone en riesgo la confidencialidad.

- **No es aplicable a herramientas de Backup Online ya que no hay soportes físicos a manejar.**
- **Sí es aplicable cuando el backup se realiza en soportes físicos (NAS, Disco Duro externos, pendrive, etc).**

Artículo 101.2 - Cifrado de los datos

La distribución de soportes que contengan datos de carácter personal se realizará cifrando dichos datos garantizando que dicha información no sea vista ni manipulada durante su transporte. Para la encriptación se recomienda un cifrado de 128 bits

- **No es aplicable a herramientas de Backup Online ya que no hay soportes físicos a manejar.**
- **Sí es aplicable cuando el backup se realiza en soportes físicos (NAS, Disco Duro externos, pendrive, etc).**

Artículo 103 – Registro de accesos

El administrador no tiene acceso a los datos salvo autorización expresa del cliente. En el caso de necesitar ejecutar una recuperación en el datacenter, el usuario debe proporcionar su clave de seguridad. El acceso queda registrado.

- **El encargado de realizar la restauración (siempre que las copias se hayan encriptado previamente) debe introducir una clave de desencriptación. Sin dicha clave es imposible realizar la restauración.**
  Esta contraseña debe ser guardada por el responsable del tratamiento de la información de forma segura. Además, es posible proteger la consola de restauración con una contraseña maestra para impedir accesos no autorizados.

Artículo 102 – Copias de seguridad en un lugar diferente al que se encuentran los equipos informáticos que los tratan

Es la funcionalidad principal de las herramientas de backup online. Obligatorio en las copias para la protección de datos de Nivel Alto.

Artículo 104 – Transmisión de datos por redes de telecomunicaciones

Los datos se transmiten cifrados y comprimidos, bajo un protocolo de comunicación seguro SSL (https).

- **La norma indica la transmisión con protocolos seguros SSL (https). Asei lo cumple.**
- **Respecto al cifrado de los datos, la norma recomienda un cifrado de 128 bits. Asei Backup Online puede cifrar la información con algoritmos de 256 bits.**

Artículo 94.2 – Verificación periódica de la copia de seguridad

El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de seguridad y de recuperación de los datos

- **Este punto queda exento de la responsabilidad de Asei Backup Online y esta verificación recae en el responsable del fichero. Este responsable del fichero deberá de ser asignado en el momento de la contratación del servicio. Asei dispone del servicio BACRI para delegar este trabajo en técnicos cualificados de Asei.**