¿Por qué usar DRaaS? Beneficios, razones para usarlo

DRaaS (recuperación ante desastres como servicio) es un modelo de servicio de informática de nube que permite a las organizaciones recuperar el acceso a la infraestructura de TI y reestablecer su funcionamiento tras un desastre, mediante copias de seguridad de los datos y de la infraestructura de TI que se almacenan en entornos de nube.

Beneficios

Algunos de los beneficios de DRaaS son:

- Reducción de costes: Elimina la necesidad de invertir en hardware, software y personal dedicados para la recuperación ante desastres, ya que se paga sólo por los recursos que se utilizan en caso de una emergencia.
- Rentabilidad: DRaaS puede ser más rentable en comparación con los enfoques tradicionales de recuperación de desastres que requieren importantes gastos de capital para hardware, software e infraestructura. Con DRaaS, las empresas a menudo pueden pagar por los servicios que necesitan mediante suscripción, lo que puede resultar más económico y permitir un mejor control de los costes.
- Mayor flexibilidad: Permite adaptar el plan de recuperación a las necesidades específicas de cada organización, eligiendo el nivel de servicio, el tiempo de recuperación y el punto de recuperación que se desee.

Esto otorga a las empresas la forma de elegir el nivel de recuperación que necesitan, como la conmutación por error de todo el sitio, la conmutación por error parcial o la recuperación de aplicaciones o datos individuales, en función de los requisitos específicos de su negocio.

- Mayor escalabilidad: Otro de los beneficios es que podemos aumentar o disminuir los recursos de recuperación según la demanda, sin tener que preocuparse por la capacidad o el rendimiento. Esto permite a las empresas ajustar sus recursos de recuperación ante desastres en función de sus necesidades cambiantes. A medida que crecen los volúmenes de datos o evolucionan los requisitos empresariales, DRaaS puede adaptarse fácilmente para acomodar estos cambios sin requerir inversiones iniciales significativas en hardware o infraestructura adicional.
- Mayor fiabilidad: Una ventaja más, es que ofrece una mayor garantía de recuperación que los métodos tradicionales, ya que se basa en proveedores especializados que cuentan con infraestructuras robustas y redundantes, así como con protocolos y herramientas de prueba y monitorización.
- Gestión simplificada: Los proveedores de este tipo de servicios suelen encargarse de la gestión, supervisión y mantenimiento del entorno de recuperación ante desastres, lo que puede aliviar la carga del personal informático interno y liberar recursos para otras tareas críticas. Esto puede ser especialmente beneficioso para las pequeñas y medianas empresas (PYMES) con recursos informáticos limitados.
- Tiempo de recuperación más rápido: Estas soluciones de recuperación ante desastres como servicio, están diseñadas para proporcionar tiempos de recuperación rápidos en caso de desastre, lo que ayuda a las empresas a reanudar sus operaciones rápidamente y minimizar el impacto del tiempo de inactividad en sus operaciones, clientes e ingresos.

- Conocimientos y experiencia: Los proveedores de DRaaS suelen tener conocimientos y experiencia en la gestión de entornos de recuperación de desastres, incluidas las mejores prácticas para la protección de datos, copias de seguridad, replicación y recuperación. Esto puede proporcionar a las empresas acceso a habilidades y conocimientos especializados que pueden no estar disponibles internamente.

DRaaS es una solución ideal para las organizaciones que quieren proteger sus datos y su continuidad de negocio ante posibles desastres naturales, ciberataques o fallos humanos, sin tener que asumir altos costes ni complejidades técnicas.

Relación de DraaS, Capex y Opex

DRaaS, o recuperación ante desastres como servicio, puede tener implicaciones tanto para los gastos de capital (CapEx) como para los gastos operativos (OpEx) de las empresas.

CapEx: Los enfoques tradicionales de recuperación ante desastres suelen requerir importantes inversiones iniciales en hardware, software e infraestructura, que se consideran gastos de capital (CapEx). Estas inversiones pueden incluir la compra y el mantenimiento de servidores redundantes, dispositivos de almacenamiento, equipos de red y otros componentes de infraestructura. Sin embargo, con DRaaS, las empresas normalmente no necesitan hacer inversiones sustanciales en CapEx, ya que la infraestructura y los recursos necesarios para la recuperación de desastres son propiedad y están mantenidos por el proveedor de DRaaS. Esto puede ayudar a las empresas a evitar grandes costes iniciales y, potencialmente, liberar capital para otras necesidades empresariales.

OpEx: DRaaS suele funcionar mediante suscripción o pago por uso, lo que implica gastos operativos continuos (OpEx). Las empresas suelen pagar una cuota periódica al proveedor de

DRaaS por los servicios que utilizan, que pueden incluir replicación de datos, copia de seguridad, almacenamiento, supervisión y gestión del entorno de recuperación ante desastres. Los gastos OpEx de DRaaS suelen ser predecibles y pueden presupuestarse como gastos operativos, lo que permite un mejor control de costes y planificación financiera.

Por el contrario, los enfoques tradicionales de recuperación ante desastres pueden requerir gastos operativos continuos para mantener y gestionar la infraestructura, así como posibles costes adicionales para actualizaciones de hardware, licencias de software, mantenimiento y otros requisitos operativos.

Una de las ventajas de DRaaS es que puede desplazar algunos de los costes iniciales de CapEx asociados a la recuperación ante desastres tradicional a gastos OpEx continuos, lo que proporciona a las empresas más flexibilidad en su presupuestación y gestión financiera. DRaaS permite a las empresas pagar por los servicios que necesitan cuando los necesitan, sin tener que realizar importantes inversiones iniciales en infraestructura. Sin embargo, es importante considerar cuidadosamente el coste total de propiedad (TCO) y comparar las implicaciones CapEx y OpEx de DRaaS frente a los enfoques tradicionales de recuperación de desastres para determinar la opción más rentable para las necesidades particulares de una empresa.

Cumplimiento de requisitos y certificaciones

Los proveedores de DRaaS suelen cumplir varios requisitos y certificaciones para

ra
ga
ra
nt
iz
ar
la
se
gu
ri
da
d,
fi
ab
il
id
ad
y
co
nf
id
en
ci
al
id
ad
de
su
s
se
rv
ic
io
s.
Re
la
ci

on
em
os
al
gu
na
s
co
ns
id
er
ac
io
ne
s
cl
av
e
re
la
ci
on
ad
as
co
n
el
cu
mp
li
mi
en
to
de
re
qu
is

itos y certificaciones en el contexto de DRaaS:

- Seguridad y privacidad de los datos: Los proveedores de DRaaS pueden cumplir con las normas y regulaciones de la industria relacionadas con la seguridad y privacidad de los datos, como el Reglamento General de Protección de Datos (GDPR), la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA), el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) y otros. El cumplimiento de estos requisitos puede implicar la aplicación de medidas técnicas y organizativas adecuadas para proteger los datos contra el acceso no autorizado, garantizar el cifrado de los datos en tránsito y en reposo, realizar auditorías de seguridad periódicas y mantener estrictos controles de acceso.

- Acuerdos de nivel de servicio (SLA): Estás mismas empresas pueden ofrecer SLA que especifiquen el nivel de disponibilidad del servicio, el rendimiento y los objetivos de tiempo de recuperación de datos (RTO) y los objetivos de punto de recuperación (RPO) a los que se comprometen. El cumplimiento de los acuerdos de nivel de servicio puede implicar la supervisión y la elaboración de informes sobre el rendimiento del servicio, la disponibilidad y las métricas de recuperación de datos para garantizar que se cumplen los niveles de servicio acordados.
- Certificaciones específicas del sector: Del mismo modo estás Compañías pueden obtener certificaciones específicas del sector que demuestren su cumplimiento de normas o requisitos específicos relevantes para los sectores de sus clientes. Por ejemplo, en sectores muy regulados como la sanidad o las finanzas, los proveedores de DRaaS pueden obtener certificaciones como HITRUST, SOC 2, ISO 27001 o FedRAMP, que garantizan su cumplimiento de las normativas y requisitos específicos del sector.
- Auditorías y evaluaciones: Los ofertantes de DRaaS pueden someterse a auditorías y evaluaciones por parte de organizaciones de terceros para evaluar su cumplimiento de las normas, reglamentos y mejores prácticas del sector. Estas auditorías y evaluaciones pueden incluir evaluaciones de vulnerabilidad, pruebas de penetración, auditorías de seguridad y otras evaluaciones para garantizar que la infraestructura, los procesos y los controles el oferente de estás soluciones y, que cumplen las normas exigidas.
- Informes de cumplimiento y documentación: Los vendedores de DRaaS pueden proporcionar a los clientes informes de cumplimiento, certificaciones y otra documentación que demuestre su conformidad con los requisitos pertinentes. Esto puede ayudar a los clientes a cumplir sus propias obligaciones de cumplimiento y los requisitos

normativos.

Al considerar un abastecedor de DRaaS, es importante evaluar su cumplimiento de los requisitos y certificaciones pertinentes para garantizar que sus servicios cumplen las normas de seguridad, privacidad y reglamentación necesarias para su empresa. Revisar las certificaciones del proveedor, los acuerdos de nivel de servicio, los informes de auditoría y otra documentación puede proporcionar información valiosa sobre su compromiso con el cumplimiento y ayudarle a tomar una decisión informada.

Proveedores

Los proveedores de DRaaS (recuperación de desastres como servicio) son empresas u organizaciones que ofrecen soluciones basadas en la nube para que las empresas repliquen y almacenen sus datos críticos, aplicaciones e infraestructura de TI en una ubicación remota y externa, proporcionando capacidades de recuperación de desastres en caso de desastre o fallo del sistema. Estos son algunos de los proveedores de DRaaS más

conocidos:

1. Amazon Web Services (AWS) Disaster Recovery
2. Microsoft Azure Site Recovery
3. IBM Resiliency Orchestration
4. Google Cloud Disaster Recovery
5. VMware Site Recovery
6. Datto
7. Zerto
8. Acronis Cyber Disaster Recovery
9. Veeam Disaster Recovery
10. Infrascale

Nosotros en HostDime estamos certificados en tecnologías Veeam, que es la solución que más empleamos con nuestros clientes, si bien hay solicitudes de soluciones en Acronis y otros.

Estos proveedores ofrecen una amplia gama de funciones y capacidades, como replicación de datos, conmutación por error y recuperación por error automatizadas, recuperación de máquinas virtuales, recuperación de redes y aplicaciones, supervisión y gestión, y planes de recuperación personalizables.

Las ofertas y capacidades específicas pueden variar de un proveedor a otro, por lo que es importante evaluar y elegir el proveedor de DRaaS que mejor se adapte a las necesidades y requisitos específicos de su empresa. También se recomienda tener en cuenta factores como la fiabilidad, la seguridad, el rendimiento, el soporte y el coste a la hora de seleccionar un proveedor de DRaaS.

Veeam Disaster Recovery

Veeam Disaster Recovery es una solución integral de recuperación de desastres como servicio (DRaaS) ofrecida por Veeam, proveedor líder de soluciones de gestión de datos y backup. Veeam Disaster Recovery ayuda a las empresas a garantizar la continuidad del negocio y la disponibilidad de los datos en caso de desastre o fallo del sistema mediante la replicación de sus datos críticos, aplicaciones y máquinas virtuales a una ubicación remota y externa.

Algunas de las características clave de Veeam Disaster Recovery incluyen:

- Replicación: Veeam permite a las empresas replicar sus máquinas virtuales, aplicaciones y datos en tiempo real o casi real a un sitio secundario o una ubicación basada en la nube para la protección fuera del sitio.
- Failover y Failback automatizados: Veeam proporciona capacidades automatizadas de failover y failback, lo que permite a las empresas cambiar rápidamente y sin

problemas al entorno replicado en caso de desastre o fallo del sistema, y luego volver al entorno primario cuando se restaura.

- Monitorización y gestión: Veeam ofrece capacidades completas de monitorización y gestión, incluyendo la monitorización del proceso de replicación, pruebas automatizadas de las máquinas virtuales replicadas y gestión centralizada de todo el proceso de recuperación ante desastres a través de una única consola.
- Planes de recuperación personalizables: Veeam permite a las empresas crear planes de recuperación personalizables que definen el orden y la prioridad de las máquinas virtuales y aplicaciones a recuperar en caso de desastre, proporcionando flexibilidad y control sobre el proceso de recuperación.
- Seguridad y conformidad: Veeam proporciona cifrado de datos en tránsito y en reposo, garantizando la seguridad y confidencialidad de los datos replicados. También ayuda a las empresas a cumplir los requisitos de conformidad proporcionando funciones como políticas de retención de datos, auditoría e informes.
- Integración con Veeam Backup & Replication: Veeam Disaster Recovery se integra perfectamente con Veeam Backup & Replication, lo que permite a las empresas aprovechar su infraestructura de backup Veeam existente para fines de replicación y recuperación ante desastres, simplificando la gestión y reduciendo costes.

Ediciones 2018-23

Leer también: Recuperación de desastres como servicio (DRaaS); ventajas y desventajas;