Comunicado Oficial STRATOSPHERE.
Campaña de revisión y actualización Veeam Backup.

Como su proveedor de servicios en la nube, nos es importante participar en la **protección y continuidad de sus operaciones** a través de la administración de su servicio de Veeam Backup. Para mantener la eficacia y la alineación con su operación, es crucial que en conjunto revisemos periódicamente la configuración de sus respaldos.
Por ello, le solicitamos atentamente su colaboración para **validar los siguientes aspectos** de sus Jobs(tareas de respaldo programadas) de Veeam Backup, dado que pudieran haber cambiado las políticas de su organización desde la configuración/entrega inicial le pedimos revise las siguientes preguntas y sea tan amable de contactarnos para poder verificar en conjunto que su respaldo está respondiendo a sus necesidades.

- **Contenido de los Jobs:** ¿Se están respaldando todos los datos, sistemas y aplicaciones críticos para su negocio? ¿Hay algún nuevo elemento que deba incluirse o alguno que ya no sea necesario posterior a su configuración inicial?
- **Periodicidad de los Jobs:** ¿La frecuencia de los respaldos (diaria, semanal, etc.) sigue siendo la adecuada para sus objetivos de punto de recuperación (RPO) y de tiempo de recuperación (RTO)?
- **Retención de los Jobs:** ¿Los períodos de retención de sus respaldos son consistentes con sus políticas internas y requisitos regulatorios? Es necesario validar su crecimiento y prever que no haya procesos truncos por no contar con espacio suficiente.

Agradeceremos que **nos confirme su conformidad** con: 1. La configuración actual, 2. Si la configuración se ajustó posterior a la entrega, 3. Nos indique cualquier ajuste que considere necesario. Esta validación nos permitirá asegurarnos de que su estrategia de respaldo esté perfectamente alineada con la evolución de su negocio y sus prioridades.

Estamos a su disposición para cualquier consulta, para programar una sesión asistida y revisar juntos la configuración de sus Jobs de Veeam Backup.

Por favor, solicite un ticket a nuestra mesa de servicio: soportesd@stratospherecorp.com o al número de teléfono customer service: +52 1 55 8500 8011.

Además de esta revisión, le compartimos algunas otras recomendaciones y buenas prácticas.

Es fundamental que tome en cuenta lo siguiente, para que complemente su servicio de Veeam Backup y fortalezca su postura de continuidad del negocio:

1. **Conozca sus RPO y RTO:** Defina claramente el tiempo máximo de pérdida de datos aceptable (RPO - Recovery Point Objective) y el tiempo máximo que su negocio puede estar inactivo (RTO - Recovery Time Objective) después de un incidente. Esto guía la estrategia de sus respaldos.

2. **Pruebas de Recuperación Regulares:** Un respaldo no es efectivo si no se puede recuperar. Es fundamental realizar pruebas de recuperación periódicas para validar la integridad de sus respaldos y la capacidad de su sistema para restaurar la información en caso de una contingencia real. Sugerimos levante un ticket para solicitar un acompañamiento en dicha recuperación.

3. **Principio 3-2-1:** Una estrategia robusta de respaldo sigue la regla 3-2-1:
    - **3 copias de su información:** Una copia de producción y dos respaldos.
    - **2 formatos diferentes:** Por ejemplo, disco y cinta, o disco y nube o 2 Data Centers de nube diferentes, cómo Stratosphere que tiene 2 Data Centers en el país con acceso a múltiples puntos en el mudo debido a pertenecemos a una federación internacional.
    - **1 copia offsite (fuera de sitio):** Una copia de los datos debe estar en una ubicación física diferente para protegerse contra desastres locales.
4. **Monitoreo Constante:** Revise los informes de sus trabajos de respaldo para identificar cualquier fallo o advertencia y abordarlo de inmediato. Nosotros realizamos este monitoreo, pero su conocimiento, atención y seguimiento a las alertas que le llegan es igualmente valioso.

5. **Plan de Recuperación ante Desastres (DRP):** Tener un plan documentado sobre cómo se recuperará su negocio después de un desastre es tan importante como los respaldos mismos. Este plan debe incluir roles, responsabilidades, procedimientos y objetivos. Por favor comparta con nosotros los momentos en que debemos interactuar con ustedes y permítanos participar en sus simulaciones, dichas simulaciones deben ser programadas por lo menos cada 3 a 6 meses máximo.

6. **Protección contra Ransomware:** Asegúrese de que sus respaldos estén protegidos contra ataques de ransomware, idealmente con copias inmutables o en ubicaciones aisladas de la red de producción con software antivirus y de seguridad que debe tener su propia instancia tanto en lo local como en la nube.

7. **Sugerencia de firewall sino lo tiene**

    Para asegurar la máxima protección de sus activos en la nube, es fundamental comprender la responsabilidad compartida en materia de ciberseguridad. Si bien nuestra infraestructura de nube es inherentemente segura y nosotros nos encargamos de proteger la plataforma subyacente, usted es el responsable

principal de la seguridad dentro de su propia instancia (sus datos, aplicaciones y sistemas operativos) tanto física como virtual.

Piénselo así: nosotros construimos y protegemos un edificio con sistemas de seguridad robustos (la infraestructura de la nube). Sin embargo, usted es quien debe asegurar las puertas, ventanas y el contenido dentro de su propia oficina (su instancia en la nube). Las vulnerabilidades específicas de sus aplicaciones, configuraciones, datos y accesos recaen bajo su esfera de control y requieren su atención.

Esto significa que, aunque nuestra plataforma le brinda una base sólida respecto a la estabilidad de sus recursos virtuales, es crucial que implemente y mantenga sus propias medidas de seguridad que protejan su propia instancia, como:

- Configuración segura de sus sistemas operativos y aplicaciones.
- Gestión de identidades y accesos (IAM) robusta.
- Protección contra malware y virus.
- Monitoreo de actividades y detección de intrusiones dentro de su instancia.
- Parcheo y actualizaciones de seguridad constantes.

Tenga en cuenta que Stratosphere cuenta con sistemas de seguridad en sus Centros de Datos y en la bóveda de información para el servicio BaaS, sin embargo, el Cliente es el único responsable de instalar antivirus, antimalware o cualquier programa/servicio para la protección de su información dentro de los equipos y recursos virtuales. Por lo anterior, Stratosphere no tiene ninguna responsabilidad, de ataques cibernéticos, virus o similares que generen alguna falla, error, vulneración y/o mal funcionamiento imputable al Cliente, comprometiendo así las copias de seguridad y su contenido.

No dude en recurrir a nosotros para asesorarle y ofrecerle herramientas que le ayuden a fortalecer la seguridad de su instancia en la nube. No dude en contactarnos si tiene alguna pregunta o si desea discutir cómo podemos colaborar para asegurar sus operaciones.
Agradecemos de antemano su pronta atención a este importante asunto.

Team Stratosphere.