

# NEWSLETTER

## CIBERSEGURIDAD

> abril 2024



### FRASE DEL MES:

¿Están preparados para el futuro digital? En nuestro boletín de hoy, exploraremos cómo una estrategia de backup sólida puede ser su mejor aliado contra la pérdida de datos y las amenazas cibernéticas."



### ✓ CONSEJOS DE CONCIENTIZACIÓN SOBRE BACKUP:

1. **Planificación proactiva:** No esperes a que ocurra un desastre para respaldar tus datos. Establece una rutina de respaldo regular para garantizar que siempre tengas una copia de seguridad actualizada.
2. **Diversificación de almacenamiento:** No pongas todos tus huevos en una sola cesta. Utiliza diferentes métodos y ubicaciones de almacenamiento para tus copias de seguridad, como almacenamiento en la nube, dispositivos externos y servidores locales.
3. **Pruebas de restauración:** No subestimes la importancia de probar tus backups periódicamente. Una copia de seguridad que no se puede restaurar con éxito en realidad no es una copia de seguridad. Practica la restauración de datos para asegurarte de que tus sistemas de backup estén funcionando correctamente.



SOLUCIONES & TECNOLOGIA S.A.S.

Sus desafíos digitales, nuestras soluciones personalizadas

[www.solytec.com.co](http://www.solytec.com.co)

Especialistas en Ciberprotección



datasafecloud

# ✓ Guardianes Digitales: Agradecimiento y Consejos en Ciberseguridad

## Consejo en Backup:

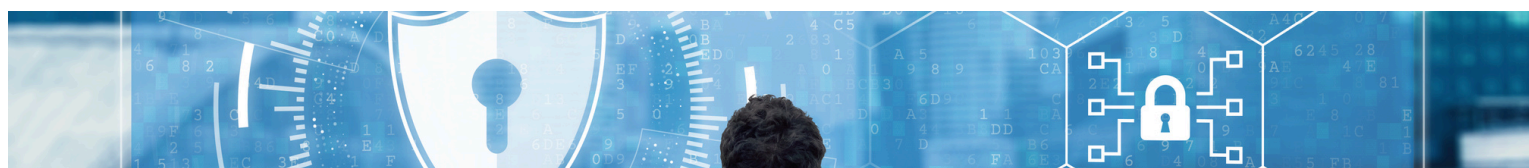
En el mundo digital actual, donde los datos son el activo más valioso, la seguridad de la información es fundamental. Uno de los pilares de una sólida estrategia de ciberseguridad es un plan de backup efectivo. Te recomendamos seguir el enfoque de 3-2-1 para respaldar tus archivos críticos:

- 1. Tres copias de seguridad:** Mantén al menos tres copias independientes de tus datos. Esto asegura redundancia y te protege en caso de que una copia se corrompa o se vuelva inaccesible.
- 2. Dos dispositivos diferentes:** Almacena tus copias de seguridad en al menos dos tipos diferentes de dispositivos. Por ejemplo, puedes combinar el almacenamiento en la nube con unidades externas o servidores locales. Esto ayuda a mitigar el riesgo de perder datos debido a un fallo en un solo tipo de dispositivo.
- 3. Una copia fuera del sitio:** Asegúrate de tener al menos una copia de seguridad almacenada fuera de tu ubicación principal. Esto es crucial en caso de desastres naturales, robos o ataques cibernéticos que puedan afectar físicamente a tu lugar de trabajo.

Este enfoque no solo te protege contra la pérdida de datos debido a fallas de hardware, errores humanos o ataques maliciosos, sino que también puede ayudarte a recuperarte más rápidamente de un incidente de seguridad. Recuerda revisar regularmente tus procesos de backup y realizar pruebas de restauración para garantizar que tus datos estén protegidos y accesibles cuando más los necesites. La seguridad de tus datos es una responsabilidad que no puedes permitirte descuidar."

---

¡Mantén tus datos seguros y protegidos como los guardianes digitales que eres!



**datasafecloud**  
Ciberprotección como servicio



SOLUCIONES & TECNOLOGIA S.A.S.  
Sus desafíos digitales, nuestras soluciones personalizadas

[www.solytec.com.co](http://www.solytec.com.co)

Especialistas en Ciberprotección

[info@solytec.com.co](mailto:info@solytec.com.co)