

## **Mejores Prácticas para la Seguridad para Analistas de datos**

*Por NetGuard Solutions*

En un mundo cada vez más digitalizado, la seguridad informática ya no es responsabilidad exclusiva de equipos especializados: profesionales de todos los roles y sectores de TI —incluyendo analistas de datos— deben adoptar buenas prácticas para proteger sistemas, información sensible y la reputación de su organización.

Los datos respaldan esta urgencia. Estudios recientes muestran que un alto porcentaje de las brechas de seguridad se originan en errores humanos —como contraseñas débiles, configuración inapropiada o descuidos con el correo electrónico— y no necesariamente en sofisticados ataques técnicos. En concreto, uno de los reportes más recientes indica que las credenciales comprometidas están detrás de más de la mitad de los incidentes.

Para profesionales de datos —que manipulan volúmenes sensibles de información, acceden a bases, dashboards, pipelines y reportes— esto implica una doble responsabilidad: asegurar la calidad de los análisis y proteger la integridad y privacidad de los datos. Aquí algunas **mejores prácticas esenciales**:

- **Usar contraseñas seguras y únicas**, idealmente con generadores de contraseña, y combinar con **autenticación multifactor (MFA)** para dificultar el acceso a actores maliciosos.
- **Mantener actualizado software, librerías y entornos de datos**, ya que vulnerabilidades conocidas pueden ser explotadas.
- **Configurar correctamente los accesos a bases de datos, almacenamiento en la nube o data-warehouses**, asegurando que sólo usuarios autorizados tengan privilegios mínimos necesarios.
- **Adoptar la política de “mínimos privilegios”**, es decir, que cada usuario —analista, desarrollador o administrador— tenga solo los permisos estrictamente necesarios para cumplir su función.
- **Capacitarse y sensibilizar al equipo**: muchos incidentes suceden por desconocimiento, descuido o malas prácticas (por ejemplo, compartir credenciales, responder phishing, uso de dispositivos personales sin protección).

En NetGuard Solutions creemos que la seguridad no debe ser un muro que frene la innovación, sino un pilar que sostiene la confianza, tanto interna como externa. Adoptar estas prácticas no solo reduce riesgos: fortalece tu reputación, protege a tus clientes o usuarios y aporta valor diferencial.

Te invitamos a reflexionar: en un contexto donde los datos son uno de los activos más valiosos de una organización —y a la vez de los más vulnerables— —la seguridad digital debe ser una prioridad transversal, que involucré a todos los miembros del equipo TI, no

solo a los expertos. Con disciplina, buenas prácticas y concienciación, podemos construir entornos de datos robustos, confiables y preparados ante amenazas modernas.

**Fuentes:**

- <https://www.brightdefense.com/resources/data-breach-statistics/>
- <https://www.keevee.com/data-breach-statistics>
- <https://b2b-cyber-security.de/es/Informe-de-violaci%C3%B3n-de-datos-que-inicialmente-reduce-los-costos-de-p%C3%A9rdida-de-datos/>
- <https://thestandardcio.com/2025/08/19/ciberataques-latam-eset-report-2025/>