

GAKORK GESTOR DE CONTRASEÑAS

Gakork es un gestor de contraseñas de código abierto basado en Psono capaz de ser alojado en un servidor local. Tanto las contraseñas como las comunicaciones están cifradas para una seguridad de extremo a extremo y un almacenamiento seguro. Es ideal para empresas que quieran compartir contraseñas entre sus empleados.



¿A quién va dirigido?

- A todas las empresas que quieran mantener sus contraseñas a salvo y centralizadas en un servidor local.
- A empresas que quieran mejorar su gestión de las claves.
- A empresas que quieran tener un gestor de contraseñas colaborativo sin necesidad de alojarlo en sistemas de terceros.

¿Qué solución tecnológica cubre?

- Tener un sistema de contraseñas minimiza el uso de tenerlas en medios no seguros como cuadernos, post-it, teléfono móvil...
- Permite el almacenamiento de las contraseñas en un sistema centralizado y compartirlas con los usuarios indicados.
- Permite autenticación de doble factor

GAKORK GESTOR DE CONTRASEÑAS

Gakork es un gestor de contraseñas de código abierto basado en Psono capaz de ser alojado en un servidor local. Tanto las contraseñas como las comunicaciones están cifradas para una seguridad de extremo a extremo y un almacenamiento seguro. Es ideal para empresas que quieran compartir contraseñas entre sus empleados.



Ventajas

- Tener las contraseñas en un servidor local y no en uno público disminuye los riesgos de ciberataque.
- Poder compartir contraseñas y directorios con usuarios de la aplicación.
- Posibilidad de compartir contraseñas con usos restringidos mediante link para usuarios no registrados.
- Análisis de contraseñas para evitar duplicados, antiguas o débiles.
- Posibilidad de crear grupos para compartir en bloque.
- Gestión de permisos sobre las contraseñas (editar, leer y compartir).
- Posibilidad de habilitar la autenticación en dos pasos.
- Encriptación de varios niveles, empezando por una capa de encriptación del lado del cliente, que permite una verdadera encriptación de extremo a extremo para compartir contraseñas, seguida de encriptación SSL y de almacenamiento.