TERMINOS Y CONDICIONES LEGALES

CMFLca es una firma de consultoría empresarial que opera bajo estándares de calidad y confiabilidad para apoyar a las pequeñas y medianas empresas en la gestión de sus operaciones. Como parte de este ecosistema, **ERP506.com y FEKII.com** son marcas asociadas que proporcionan servicios especializados relacionados con servidores privados. **Estas marcas se dedican exclusivamente a la custodia de información y la seguridad de acceso mediante servidores encriptados**, garantizando la confidencialidad y protección de los datos empresariales.

Los servicios e ingresos generados por **ERP506.com y FEKII.com** derivan únicamente del acceso a estos servidores y de la custodia de la información confiada por sus usuarios. Cada servidor y usuario cuenta con herramientas diseñadas bajo estándares **GNU LGPL**, lo que asegura un marco confiable y de código abierto para su operación. Sin embargo, **la responsabilidad de actualizar, dar soporte técnico o garantizar el mantenimiento continuo de los sistemas no recae sobre CMFLca**, ya que dichas herramientas están diseñadas para operar bajo un modelo autónomo y de autogestión.

El objetivo de este documento es brindar una orientación general sobre la implementación y gestión de servidores y la seguridad informática para pequeñas y medianas empresas (PYMEs). Esta guía no sustituye la asesoría técnica profesional ni garantiza la solución de necesidades específicas. Se recomienda siempre evaluar el contexto único de cada empresa antes de tomar decisiones técnicas o de seguridad.

Avisos Importantes:

1. **Limitaciones de Responsabilidad.**

   La información proporcionada aquí es genérica y puede no abordar todas las necesidades específicas de tu empresa. Es responsabilidad de cada organización evaluar sus propios requerimientos y riesgos de seguridad, así como implementar las medidas necesarias para proteger su infraestructura y datos.

2. **Riesgos Tecnológicos**

   - Toda tecnología, por robusta que sea, está sujeta a vulnerabilidades. Aunque se adopten medidas preventivas, ningún sistema puede garantizar una seguridad absoluta frente a amenazas internas o externas.
   - Las configuraciones inadecuadas, el software no actualizado o el uso inapropiado de herramientas de seguridad pueden incrementar significativamente los riesgos.

3. **Consultoría Profesional**

   Se recomienda encarecidamente buscar asesoría de expertos certificados en seguridad informática y administración de servidores para implementar soluciones específicas que cumplan con los estándares de la industria.

4. **Cambios y Actualizaciones**

   Los avances tecnológicos y las amenazas de seguridad evolucionan constantemente. Por ello, es fundamental mantener actualizados los sistemas, las políticas y los procedimientos de seguridad.

5. **Cumplimiento Legal**

   - Cada empresa es responsable de cumplir con las normativas locales e internacionales aplicables a la gestión de datos y seguridad (como RGPD, PCI DSS, o ISO/IEC 27001).
   - Este documento no sustituye la asesoría legal sobre las obligaciones de protección de datos o ciberseguridad.

6. **Implementación y Monitoreo**
   La implementación de medidas de seguridad requiere supervisión continua, auditorías periódicas y una respuesta proactiva ante posibles incidentes.

Nota final: Este disclaimer no garantiza la ausencia de riesgos ni reemplaza la contratación de servicios especializados. Las PYMEs deben realizar evaluaciones internas y externas para garantizar la seguridad de sus operaciones y la continuidad del negocio.