

Informe de Auditoría de Seguridad Informática

TechSys Solutions S.L.

Sede Barcelona

1. Objetivo del Informe

Evaluar el cumplimiento de la política de seguridad de la información, identificar vulnerabilidades técnicas y organizativas, y proponer acciones correctivas para mejorar la protección de los activos críticos en la sede de Barcelona.

2. Resumen Ejecutivo

- **Nº de hallazgos detectados:** X (tomamos “X” como un número)
 - **Clasificación de riesgos:**
 - Críticos: X
 - Altos: X
 - Medios: X
 - Bajos: X
 - **Estado general:** [Satisfactorio / Con deficiencias que requieren atención inmediata / Riesgo alto]
-

3. Hallazgos y Recomendaciones

Nº	Hallazgo	Nivel de Riesgo	Evidencia	Recomendación	Responsable	Fecha Límite
1						
2						

4. Clasificación de los Riesgos

Basado en el modelo MAGERIT, los riesgos se han clasificado considerando:

- Probabilidad de ocurrencia
 - Impacto en la confidencialidad, integridad y disponibilidad
 - Grado de exposición según el activo
-

5. Plan de Acción y Seguimiento

El Comité de Seguridad deberá:

- Revisar este informe en la próxima reunión mensual
 - Priorizar los hallazgos críticos y altos
 - Asignar recursos para la implementación de las recomendaciones
 - Documentar el cierre de acciones en el sistema de gestión de seguridad (SGSI)
-

6. Conclusiones

La sede de Barcelona presenta un nivel de seguridad **[moderado/alto/bajo]** con áreas de mejora. La implementación del plan de acción propuesto es esencial para mitigar riesgos reales y cumplir con la política interna y normativa aplicable (LOPDGDD, ENS si aplica).