Matriz de Riesgos e Informe

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Medidas de Control/Salvaguardas
Portátiles y tablets de consultores y soporte técnico	Pérdida o robo de dispositivos	Uso fuera de la oficina, movilidad constante	Alto	Medio	Alto	Cifrado de disco, bloqueo remoto, políticas MDM, formación en seguridad
Acceso remoto a VPN	Acceso no autorizado	Contraseñas débiles, mala gestión de credenciales	Alto	Medio	Alto	Autenticación multifactor, política de contraseñas robustas, monitorización de accesos
Datos de clientes e informes de proyectos	Fuga de información	Envío por email no cifrado, almacenamiento local no cifrado	Muy Alto	Medio	Muy Alto	Cifrado de emails, uso de repositorios seguros, formación en protección de datos
Red local de la sede	Intrusión externa	Firewall local de menor capacidad	Alto	Bajo	Medio	Revisión de configuración de firewall, actualizaciones, auditoría periódica
Soporte técnico	Uso de dispositivos externos (USB)	Posible malware en dispositivos de diagnóstico	Alto	Bajo	Medio	USBs controlados y cifrados, antivirus actualizado, políticas de uso de medios externos
Personal (consultores/ soporte)	Ingeniería social	Desconocimiento de ataques de phishing	Alto	Alto	Muy Alto	Formación periódica, simulacros de phishing, filtros antispam
Acceso a documentación técnica	Modificación no autorizada	Falta de control de versiones y permisos	Alto	Bajo	Medio	Control de versiones, permisos granulares, auditoría de cambios

Comunicaciones internas	Interceptación de tráfico	VPN mal configurada o uso indebido de WiFi público	Alto	Medio	Alto	Configuración correcta de VPN, prohibición de WiFi público sin VPN, monitorización

INFORME DE RIESGOS (sede regional Barcelona)

1. Objetivo del informe

El presente informe detalla los principales riesgos de seguridad detectados en la sede regional de Barcelona, para cumplir con la Auditoría de Seguridad Informática.

2. Resumen de hallazgos

Los activos más críticos en esta sede son los dispositivos móviles (portátiles y tablets), el acceso remoto mediante VPN y la información confidencial de clientes. La movilidad de los consultores y el soporte técnico implica una exposición elevada a amenazas como pérdida de dispositivos, fugas de datos o ataques de ingeniería social. Además, los firewalls locales tienen menor capacidad que la sede central, aumentando la probabilidad de intrusiones si no se refuerzan las configuraciones de red.

3. Riesgos más relevantes:

- **Robo/Pérdida de dispositivos:** alto impacto por la sensibilidad de la información.
- **Acceso indebido a la red vía VPN:** requiere medidas estrictas de control de acceso.
- **Fuga de información por malas prácticas:** envío de documentación sin cifrado.
- **Ingeniería social:** riesgo elevado por falta de formación específica y rotación de personal.

4. Medidas de control recomendadas

- Reforzar el cifrado de todos los dispositivos móviles y portátiles.
- Implementar bloqueo remoto y gestión centralizada de dispositivos (MDM).
- Revisar y endurecer políticas de contraseñas y MFA para VPN.
- Obligar al cifrado de emails que contengan datos confidenciales.
- Reforzar la configuración de firewalls locales con auditorías trimestrales.
- Capacitar al personal en detección de phishing y buenas prácticas de seguridad.
- Restringir el uso de USBs y controlar los medios de diagnóstico del soporte técnico.
- Monitorizar el acceso a la documentación técnica mediante permisos granulares y auditorías.

5. Conclusión

La sede de Barcelona presenta riesgos asociados principalmente a la movilidad y manejo de información confidencial. Es imprescindible fortalecer la cultura de seguridad, la protección de dispositivos y el control de acceso remoto para mitigar los riesgos identificados.