# Documentación de Firewalls / IDS / IPS

## TechSys Solutions S.L.

## Sede Barcelona

### 1. Introducción

**Objetivo**: Describir la configuración, políticas y procedimientos de seguridad perimetral.
**Alcance**: Sede de Barcelona. Protección de los departamentos de Consultora y Atención al Cliente.

### 2. Inventario de Dispositivos

| Nombre del dispositivo | Modelo/Fabricante | Ubicación | Estado | Versión Firmware | Fecha Instalación |
|---|---|---|---|---|---|
| Firewall Local Barcelona | No especificado | Sede Barcelona | Operativo | No documentado | No documentado |
| | | | | | |

*Nota: Se requiere auditoría física para completar datos.*

### 3. Topología y Arquitectura

- **VPN** hacia Madrid con MFA obligatorio.
- **Segmentación**: Separación de redes entre Consultora y Atención al Cliente.
- **Interfaces**: Falta documentación de interfaces WAN, LAN, VPN y segmentación.
- **Rutas**: Se deben definir rutas hacia Madrid y servicios en la nube.
- **Alta disponibilidad**: No implementada.

### 4. Políticas de Seguridad (Firewalls)

- **Reglas Configuradas**:
    - VPN sede Madrid: IPsec AES-256 (permitido)
    - Acceso por departamentos: segmentado
    - HTTP/HTTPS: permitido para todos
    - Servicios Cloud: OneDrive, Google Drive permitidos
    - IMAP SSL (993), SMTP (587): permitidos
    - SSH (22): restringido
- **Justificación**: Cada regla documentada con razón de negocio.
- **Orden de reglas**: Seguridad crítica > acceso interno > servicios > acceso general

- **Política por defecto**: Denegar todo.
- **Cambios recientes**: No registrados formalmente. Se requiere sistema de control de cambios.

## 5. Configuración de IDS/IPS

- No implementado.
- Recomendación: Urgente implementar IDS/IPS en modo detección/preventivo.

## 6. Procedimientos de Gestión

- **Actualización de reglas**: No documentada. Debe establecerse cronograma, pruebas y rollback.
- **Cambio de reglas**: Solicitud > Aprobación > Implementación.
- **Responsables**: TI, Administrador de red, Responsable de seguridad IT.

## 7. Monitorización y Logs

- **Eventos**: accesos, informes, tickets, administración.
- **Retención**: No especificada.
- **Herramientas**: Dashboards internos, TLS 1.3.
- **Revisión de alertas**: No existe procedimiento formal. Debe incluir escalado y tiempos de respuesta.

## 8. Pruebas de Funcionamiento

- No realizadas formalmente. Deben establecerse pruebas periódicas de reglas, VPN y segmentación.
- Documentar con capturas y logs.

## 9. Copias de Seguridad de Configuración

- No documentadas.
- Se requiere definir ubicación, periodicidad y proceso de restauración.

## 10. Revisión y Mantenimiento

- **Revisiones**: certificados anuales, accesos mensuales.
- **Auditorías**: no existen registros formales. Implementar internas y externas.
- **Mantenimiento preventivo**: no definido. Requiere cronograma y registro de tareas.

---

## Recomendación Final

Asignar recursos para la creación formal de este documento y la implementación de IDS/IPS y alta disponibilidad. La documentación es crítica para el cumplimiento de ISO 27001 y la seguridad general de TechSys Solutions S.L.