ANEXO 6 – Manual de Operación y Mantenimiento

6.1. Acceso y gestión

- Acceso administrativo únicamente desde VLAN 99 (Gestión) o desde IP de origen en lista blanca, mediante HTTPS (GUI) o SSH (CLI), con autenticación multifactor (MFA).
- Cuentas nominales por técnico; prohibido el uso de cuentas genéricas compartidas.
- Registro de todas las sesiones de administración en el syslog centralizado.

6.2. Copias de seguridad

- Backup automático diario de la configuración, exportado a repositorio externo al propio UTM.
- Backup adicional manual antes de cualquier cambio relevante de políticas o firmware.
- Retención mínima de 90 días de copias de configuración.

6.3. Actualizaciones

- Firmas de IPS/antivirus: actualización automática diaria.
- Firmware del sistema: revisión mensual de versiones disponibles; aplicación en ventana de mantenimiento planificada, previa prueba en entorno de laboratorio si el cambio es mayor (major release).
- Licencias: revisión trimestral de vigencia y renovación con 60 días de antelación al vencimiento.

6.4. Monitorización

- Supervisión continua de CPU, memoria, sesiones concurrentes y estado de los enlaces (WAN, VPN, HA si aplica) desde el NMS.
- Alertas automáticas ante: caída de túnel VPN, uso de CPU >80% sostenido, fallo de conmutación HA, certificado SSL próximo a caducar.
- Revisión semanal de los informes de IPS/antivirus y de las categorías más bloqueadas por el filtrado web.

6.5. Gestión de cambios

- Toda modificación de reglas de firewall se solicita, documenta y aprueba antes de su aplicación (procedimiento de change management).
- Cambios de bajo riesgo: aplicación directa con registro posterior.
- Cambios de riesgo medio/alto: prueba previa en laboratorio o ventana de mantenimiento.

6.6. Procedimiento ante incidencias

Incidencia	Procedimiento
Caída de la VPN Site-to-Site	Verificar interfaz WAN, revisar log IKE/IPsec, comprobar disponibilidad del extremo remoto, reiniciar túnel
Bloqueo indebido de una aplicación legítima	Identificar categoría/firma en el log, crear excepción puntual documentada, revisar en el siguiente comité de cambios
Fallo de conmutación HA (si aplica)	Comprobar heartbeat entre nodos, forzar failover manual, sustituir nodo defectuoso
Saturación de CPU/sesiones	Identificar origen del tráfico anómalo, aplicar limitación temporal, evaluar ampliación de dimensionamiento