



Análisis de Vulnerabilidad de Seguridad de Activos de Información On-Premise del AMV

2025



ÁREA METROPOLITANA DE VALLEDUPAR

1. Introducción

Este análisis tiene como objetivo identificar y evaluar las vulnerabilidades de seguridad en los activos de información on-premise. de la entidad Área Metropolitana de Valledupar. La finalidad es establecer un punto de partida para implementar medidas correctivas que permitan proteger la confidencialidad, integridad y disponibilidad de la información institucional.

2. Alcance

Este análisis se enfoca en los activos de información ubicados esencialmente dentro de las instalaciones de la entidad, incluyendo:

Equipos de cómputo (PC y portátiles)

Dispositivos de red (módems, conmutadores, enrutadores)

Servidor local (en caso de implementación con el nuevo proyecto de modernización)

Sistemas operativos instalados (Windows 7, 10 y 11)

Aplicaciones ofimáticas y administrativas

Acceso físico a los activos

3. Inventario de activos

Tipo de activo	Cantidad	Sistema Operativo	Ubicación	Conectividad
PC de escritorio	14	Windows 10 y 11	Oficinas administrativas	Cableado de módem y WiFi
Portátiles	3	Windows 10 y 11	Oficinas administrativas	Cableado de módem y WiFi
Módems	1	-	Sala de comunicaciones	
Servidor (propuesta)	1	Servidor Windows / Linux	Sala	Cableado estructurado
Impresoras Ofimática	3	Compatible windows	Oficinas administrativas	Red local y WiFi
Scanner	1	Compatible windows	Oficinas administrativas	Cableado directo

4. Identificación de Vulnerabilidades



4.1. Hardware

Falta de control de acceso físico a equipos y sala de comunicaciones.

Mantenimiento preventivo irregular.

Uso de dispositivos antiguos sin soporte (ej. PC con Windows 7).

4.2. Software

Sistemas operativos sin soporte oficial (Windows 7).

Falta de actualizaciones automáticas en algunos equipos.

Ausencia de antivirus corporativo centralizado.

Licencias de software no verificadas o caducadas.

4.3. Red

Falta de segmentación de red.

Conexiones Wi-Fi abiertas o con contraseñas débiles.

Sin firewall perimetral o sin configuración avanzada.

Ausencia de monitoreo de tráfico de red.

4.4. Políticas de seguridad

Contraseñas débiles o compartidas entre usuarios.

Falta de capacitación en seguridad de la información.

Acceso de usuarios sin control de privilegios.

5. Análisis de Riesgos

Vulnerabilidad	Impacto	Probabilidad	Nivel de Riesgo	Recomendación
Uso de Windows 7	Alto	Alta	Crítico	Migrar a sistemas soportados
Contraseñas	Medio	Alta	Alto	Implementar políticas
Red Wi-Fi sin cifrado fuerte	Alto	Medios de comunicación	Alto	Acceso usuarios con control de privilegios



Vulnerabilidad	Impacto	Probabilidad	Nivel de Riesgo	Recomendación
Sin antivirus centralizado (Servidor)	Medio	Alta	Alto	Instalar solución de antivirus corporativo en servidores.
Ausencia de copia de seguridad automatizada	Alto	Medios de comunicación	Alto	Implementar sistema de respaldo automatizado

6. Conclusiones y Recomendaciones Generales

Se identifican múltiples vulnerabilidades de nivel crítico y alto.

Es imprescindible realizar un plan de mitigación de riesgos, priorizando la actualización de sistemas y la protección de la red.

Debe desarrollarse una política integral de seguridad informática, incluyendo control de acceso, respaldo, actualizaciones y gestión de incidentes.

Requiere capacitación básica para usuarios sobre buenas prácticas en el manejo de la información.

7. Próximos Pasos

Migrar o retirar los equipos con Windows 7.

Segmentar la red y reforzar la seguridad Wi-Fi.