

INFORME ENS

Esquema Nacional de Seguridad

Empresa: TFG_PYME

Fecha del informe: 10 de June de 2025

ANALISIS INTEGRAL DE CIBERSEGURIDAD

Este informe contiene un analisis completo del cumplimiento del Esquema Nacional de Seguridad (ENS) nivel Alto, incluyendo:

- Evaluacion de cumplimiento de controles ENS
- Diagnostico detallado de vulnerabilidades
- Analisis de incidentes de seguridad detectados
- Simulacion de ataques y pruebas de penetracion
- Optimizacion de recursos y estimacion de costes
- Recomendaciones y plan de accion prioritario

INDICE

1. RESUMEN EJECUTIVO	3
2. CUMPLIMIENTO ENS POR FAMILIAS	4
3. DIAGNOSTICO DETALLADO	5
4. ANALISIS DE VULNERABILIDADES	6
5. INCIDENTES DE SEGURIDAD	7
6. SIMULACION DE ATAQUES	8
7. OPTIMIZACION DE RECURSOS	9
8. PLAN DE ACCION PRIORITARIO	10
9. CONCLUSIONES Y RECOMENDACIONES	11
10. ANEXOS	12

NOTA IMPORTANTE:

Este informe ha sido generado automaticamente mediante el analisis de los resultados obtenidos de las 8 herramientas especializadas del sistema TFG ENS PYME. Los datos reflejan el estado actual de cumplimiento y seguridad de la organizacion en el momento de la evaluacion.

1. RESUMEN EJECUTIVO

METRICAS CLAVE

Fecha del Analisis: 10/06/2025

Controles ENS Evaluados: 62 controles

Cumplimiento Global: 41.9

Vulnerabilidades Detectadas: 15 vulnerabilidades

Incidentes de Seguridad: 13 incidentes

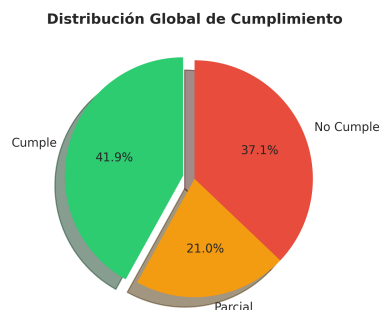
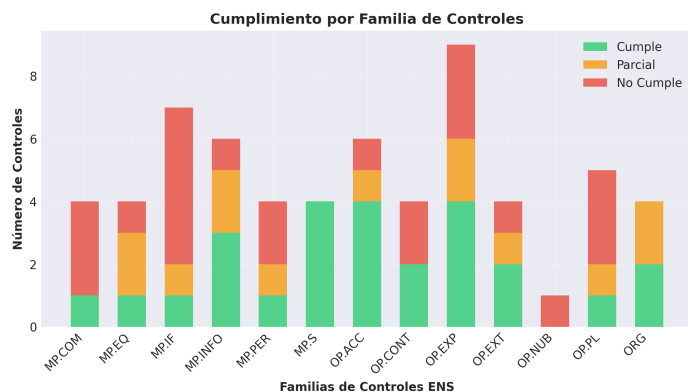
Inversion Estimada: 30,760

Estado General de Cumplimiento

MEJORABLE - Se requieren mejoras significativas en la seguridad.

2. CUMPLIMIENTO ENS POR FAMILIAS

Dashboard de Cumplimiento ENS



METRICAS CLAVE DE CUMPLIMIENTO ENS

- Total de Controles Evaluados: 62
- Porcentaje de Cumplimiento Global: 41.9%
- Controles que Cumplen Completamente: 26
- Controles con Cumplimiento Parcial: 13
- Controles No Cumplidos: 23
- Familias de Controles Analizadas: 13

ESTADO GENERAL DEL CUMPLIMIENTO: MEJORABLE

Analisis Detallado por Familia

MP.COM: 1/4 controles (25.0 cumplimiento)

MP.EQ: 1/4 controles (25.0 cumplimiento)

MP.IF: 1/7 controles (14.3 cumplimiento)

MP.INFO: 3/6 controles (50.0 cumplimiento)

MP.PER: 1/4 controles (25.0 cumplimiento)

MP.S: 4/4 controles (100.0 cumplimiento)

OP.ACC: 4/6 controles (66.7 cumplimiento)

OP.CONT: 2/4 controles (50.0 cumplimiento)

OP.EXP: 4/9 controles (44.4 cumplimiento)

OP.EXT: 2/4 controles (50.0 cumplimiento)

OP.NUB: 0/1 controles (0.0 cumplimiento)

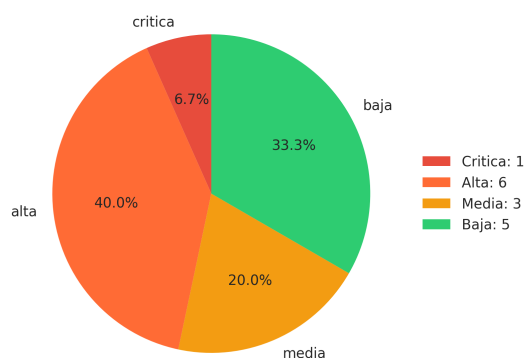
OP.PL: 1/5 controles (20.0 cumplimiento)

ORG: 2/4 controles (50.0 cumplimiento)

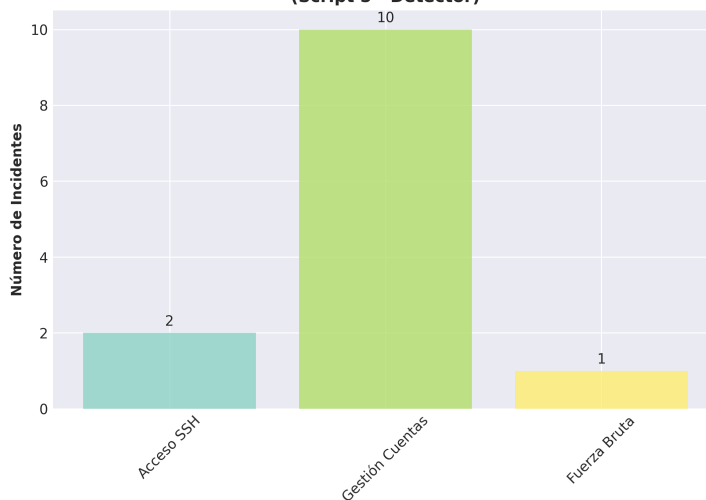
3. ANALISIS DE VULNERABILIDADES E INCIDENTES

Analisis de Vulnerabilidades e Incidentes

Vulnerabilidades por Severidad
(Script 4 - Auditor)



Incidentes Detectados por Tipo
(Script 5 - Detector)



Auditoria de Permisos y Accesos (Script 4)

Total de vulnerabilidades detectadas: 15

Distribucion por severidad:

Critica: 1 vulnerabilidades

- UID duplicado en Linux

Alta: 6 vulnerabilidades

- Cuenta bloqueada en Linux
- Cuenta bloqueada en Linux
- Cuenta bloqueada en Linux
- ... y 3 mas

Media: 3 vulnerabilidades

- Usuario con shell inusual en Linux
- Periodo de expiracion de contrasena incorrecto
- Cadencia minima de cambio de contrasena inadecuada

Baja: 5 vulnerabilidades

- Cuentas en grupos privilegiados
- Cuentas en grupos privilegiados
- Cuentas en grupos privilegiados
- ... y 2 mas

Deteccion de Incidentes (Script 5)

Total de incidentes detectados: 13

Informe ENS Profesional - TFG_PYME

Incidentes por tipo:

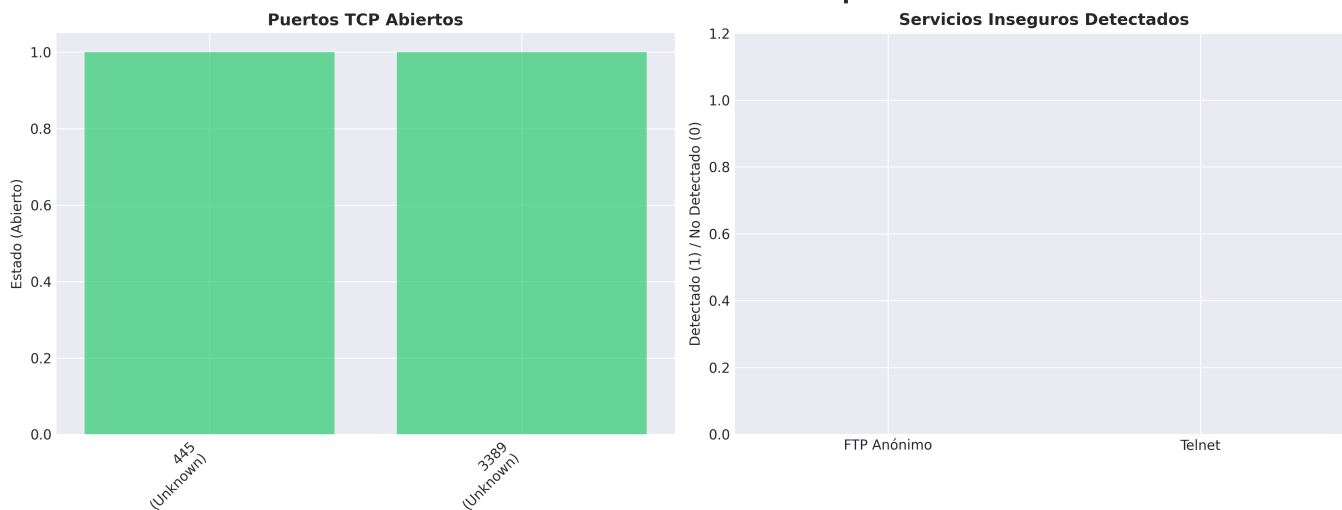
Acceso SSH: 2 incidentes

Gestion Cuentas: 10 incidentes

Fuerza Bruta: 1 incidentes

4. SIMULACION DE ATAQUES

Analisis de Simulacion de Ataques



TARGET ANALIZADO: 192.168.100.2

RESUMEN DE HALLAZGOS:

- Total de Vulnerabilidades: 2
- Puertos TCP Abiertos: 2
- Puertos UDP Abiertos: 4

VULNERABILIDADES DETECTADAS:

- 2 puertos TCP abiertos
- 4 puertos UDP abiertos/filtrados

NIVEL DE RIESGO

MEDIO

Resultados de la Simulacion

Target analizado: 192.168.100.2

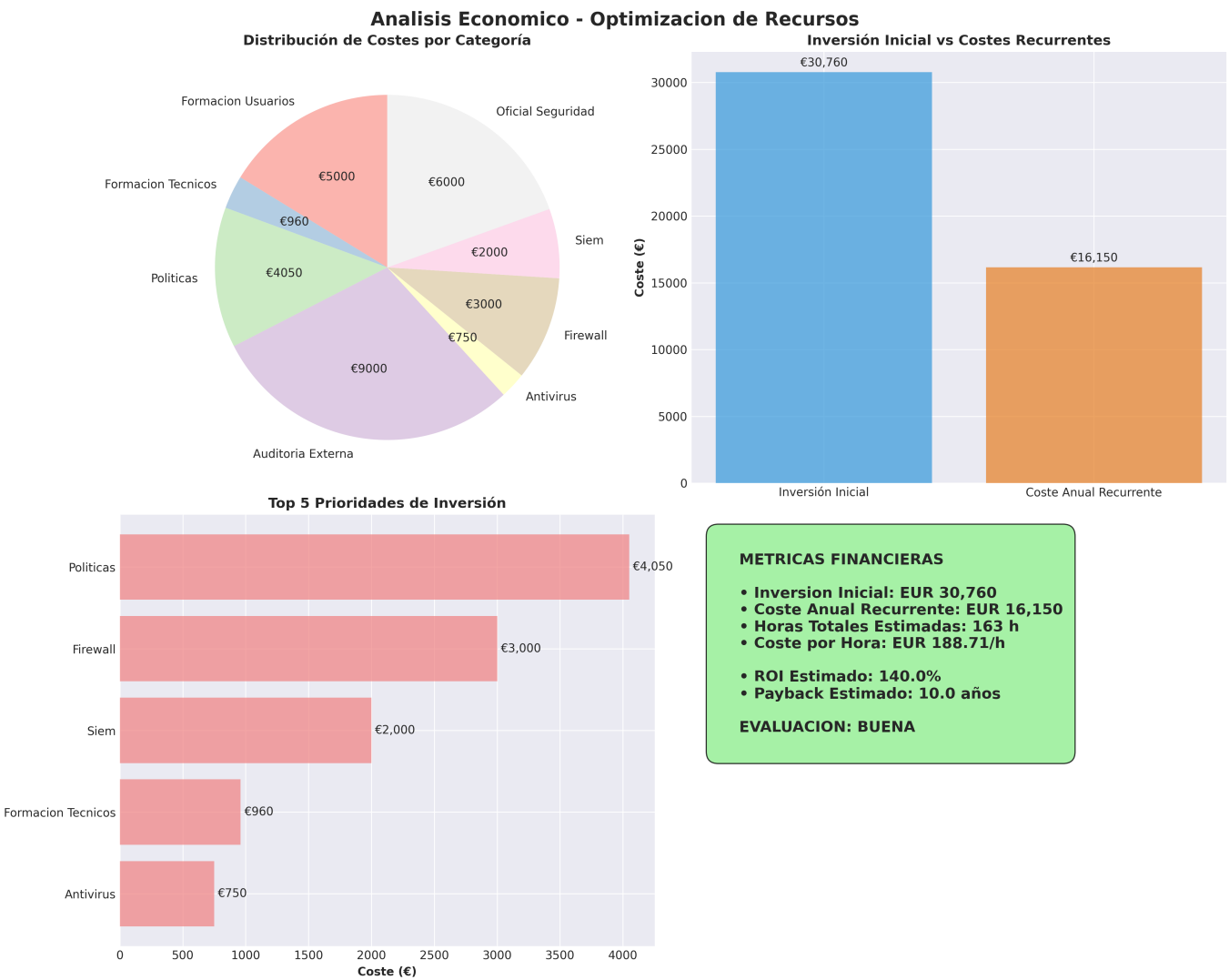
Total de vulnerabilidades identificadas: 2

Vulnerabilidades Identificadas

2 puertos TCP abiertos

4 puertos UDP abiertos/filtrados

5. OPTIMIZACION DE RECURSOS Y COSTES



METRICAS CLAVE

Inversion Inicial: 30,760
Coste Recurrente Anual: 16,150
Horas Totales Estimadas: 163 h
ROI Estimado: 140.0

Plan de Prioridades de Inversion

1. Antivirus: 750
2. Formacion Tecnicos: 960
3. Siem: 2,000
4. Firewall: 3,000
5. Politicas: 4,050

6. CONCLUSIONES Y RECOMENDACIONES

Conclusiones Principales

- La organizacion requiere mejoras significativas en ciberseguridad.
- Se han identificado multiples vulnerabilidades que requieren atencion inmediata.
- La frecuencia de incidentes sugiere la necesidad de mejores controles preventivos.
- La inversion estimada de 30,760 es necesaria para alcanzar el cumplimiento ENS.

Recomendaciones Especificas

- Priorizar la implementacion de controles de seguridad criticos
- Establecer un programa de formacion continua en ciberseguridad
- Implementar monitorizacion y respuesta a incidentes 24/7
- Realizar evaluaciones de seguridad periodicas
- Mantener actualizado el plan de continuidad de negocio

NOTA FINAL:

Este informe representa una evaluacion integral del estado de ciberseguridad de la organizacion. Se recomienda revisar este analisis trimestralmente y actualizar las medidas segun la evolucion de las amenazas y el crecimiento de la organizacion.