INFORME FINAL DE AUDITORÍA DE SISTEMAS

# CARÁTULA

Entidad Auditada: [Nombre de la entidad o dependencia]

Ubicación: [Ciudad, distrito, provincia, país]

Período auditado: [Desde dd/mm/aaaa hasta dd/mm/aaaa]

Equipo Auditor: [Nombres y roles del equipo auditor]

Fecha del informe: [dd/mm/aaaa]

# ÍNDICE

1. Resumen Ejecutivo
2. Antecedentes
3. Objetivos de la Auditoría
4. Alcance de la Auditoría
5. Normativa y Criterios de Evaluación
6. Metodología y Enfoque
7. Hallazgos y Observaciones
8. Análisis de Riesgos
9. Recomendaciones
10. Conclusiones
11. Plan de Acción y Seguimiento
12. Anexos

# 1. RESUMEN EJECUTIVO

Este apartado se desarrolla al final de la auditoría realizada y es una descripción breve y concisa del propósito de la auditoría, principales hallazgos, conclusiones y recomendaciones más relevantes.

# 2. ANTECEDENTES

Contexto general de la entidad, naturaleza de sus sistemas de información, estructura organizativa, y antecedentes de auditorías previas (si las hubiera).

# 3. OBJETIVOS DE LA AUDITORÍA

Definición del objetivo general y los objetivos específicos, orientados a evaluar aspectos como:

* Seguridad de la información
* Continuidad del negocio
* Gestión de cambios y configuración
* Cumplimiento normativo
* Integridad y disponibilidad de datos
* etc

# 4. ALCANCE DE LA AUDITORÍA

Ámbitos evaluados (tecnológico, organizacional, normativo, etc.)  
Sistemas y procesos incluidos  
Unidades o áreas auditadas  
Periodo auditado

# 5. NORMATIVA Y CRITERIOS DE EVALUACIÓN

Lista de normas, marcos de referencia o políticas aplicadas como base para la auditoría. Ejemplos:

* COBIT 2019
* ISO/IEC 27001:2022
* Ley de Protección de Datos Personales [local]
* Políticas internas de TI de la entidad

# 6. METODOLOGÍA Y ENFOQUE

Descripción del enfoque utilizado (basado en riesgos, cumplimiento, mixto) y métodos aplicados:

* Entrevistas con usuarios y responsables de TI
* Inspección de documentos y registros
* Pruebas técnicas (análisis de logs, escaneo de vulnerabilidades)
* Revisión de configuraciones
* Aplicación de listas de verificación

# 7. HALLAZGOS Y OBSERVACIONES

Presentación detallada de los hallazgos, estructurados por áreas evaluadas. Cada hallazgo debe incluir:  
Descripción del hallazgo  
Evidencia objetiva  
Grado de criticidad (alto, medio, bajo)  
Criterio vulnerado  
Causa y efecto

# 8. ANÁLISIS DE RIESGOS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Hallazgo | Riesgo asociado | Impacto | Probabilidad | Nivel de Riesgo |

# 9. RECOMENDACIONES

¿Qué debe hacerse al respecto para mejorar, corregir o mitigar los riesgos?. Propuestas técnicas y organizativas para mitigar los riesgos y subsanar los hallazgos. Cada recomendación debe estar vinculada al hallazgo correspondiente.

# 10. CONCLUSIONES

¿Qué se ha encontrado? ¿Cuál es el estado general del sistema auditado?. Síntesis evaluativa sobre el estado de control y gestión de los sistemas de información auditados. Indicar si los controles existentes son adecuados, eficaces y cumplen con la normativa aplicable.

# 11. PLAN DE ACCIÓN Y SEGUIMIENTO

|  |  |  |  |
| --- | --- | --- | --- |
| Hallazgo | Recomendación | Responsable | Fecha Comprometida |

# 12. ANEXOS

Incluir documentos de respaldo como:  
  
- Cuestionarios aplicados  
- Capturas de pantalla  
- Registros de logs  
- Políticas internas revisadas  
- Cualquier otro elemento que sustente los hallazgos