FORMACIÓN PROFESIONAL

# Auditoría de Sistemas de Información

Fundamentos, Estándares Internacionales y Normativa Española/Europea

ISACA • COBIT • ISO 27001

RGPD • ENS • NIS2

Unidad Didáctica 1

# Objetivos de Aprendizaje

## AL FINALIZAR ESTA UNIDAD, SERÁS CAPAZ DE:

### Comprender los criterios generales

Dominar los fundamentos de auditoría IT y su aplicación práctica en entornos empresariales

### Identificar el marco normativo

Reconocer la normativa española y europea aplicable a auditoría de sistemas de información

### Aplicar conceptos éticos

Integrar principios deontológicos en contextos reales de auditoría profesional

### Diferenciar tipos de pruebas

Distinguir entre pruebas de cumplimiento y sustantivas, así como técnicas de muestreo

### Categorizar hallazgos

Clasificar hallazgos según impacto normativo bajo ENS y GDPR

### Utilizar herramientas CAAT

Aplicar herramientas de auditoría asistida por ordenador con validez jurídica eIDAS

### Competencia Transversal

**Cumplimiento legal** + **Excelencia técnica**

FUNDAMENTOS

# Introducción a la Auditoría de Sistemas de Información

## Definición

**Según ISACA:** Proceso sistemático para recopilar y evaluar evidencias determinando si los sistemas de información salvaguardan activos, mantienen integridad de datos, operan eficazmente y cumplen leyes.

**Según el IIA:** Actividad de aseguramiento y consultoría objetiva e independiente diseñada para agregar valor y mejorar las operaciones.

## Objetivos Principales

- **Evaluar controles:** Verificar efectividad de controles internos
- **Verificar cumplimiento:** Asegurar adherencia a normativas
- **Identificar riesgos:** Detectar amenazas y vulnerabilidades
- **Agregar valor:** Recomendar mejoras estratégicas

## Seguridad de la Información (CIA)

**C**

**Confidencialidad**

Protección contra acceso no autorizado

**I**

**Integridad**

Precisión y protección contra modificación

**A**

**Disponibilidad**

Acceso cuando se requiere

## Importancia en la Era Digital

### Transformación Digital

Las organizaciones dependen críticamente de la tecnología para operar, aumentando la necesidad de controles robustos.

### Ciberamenazas Crecientes

Ransomware, phishing y ataques APT requieren auditorías proactivas para detectar vulnerabilidades.

### Marco Regulatorio Complejo

Cumplimiento de RGPD, NIS2, ENS y otros requiere verificación continua mediante auditorías.

### Confianza de Stakeholders

Clientes, inversores y reguladores exigen evidencia de controles efectivos y gestión de riesgos.

### Concepto Clave

La auditoría IT no busca solo detectar problemas, sino **agregar valor** mediante recomendaciones que mejoren la eficiencia y reduzcan riesgos.

# ¿Qué es la Auditoría Informática?

*Definición, alcance y objetivos*

- Proceso sistemático de obtención y evaluación objetiva de evidencias sobre los sistemas de información
- Objetivos: verificar la eficacia de controles, seguridad, integridad y disponibilidad de los datos
- Tipos: auditoría de sistemas, de red, de aplicaciones, forense, de cumplimiento y de hacking ético
- Diferencia entre auditoría interna (equipo propio) y externa (empresa especializada independiente)
- El auditor debe poseer independencia, objetividad, competencia técnica y código deontológico
- Resultado final: informe técnico con hallazgos, vulnerabilidades y recomendaciones priorizadas

MARCO NORMATIVO

# Estándares Internacionales Clave

## ISACA

Information Systems Audit and Control Association

- **CISA:** Certificación de Auditor de Sistemas de Información
- **COBIT:** Framework de gobierno y gestión de TI
- **Estándares de Auditoría:** Guías para auditoría de SI
- **CISM, CRISC, CGEIT:** Otras certificaciones especializadas

## ISO 27000

Familia de normas de seguridad de la información

- **ISO 27001:** Requisitos para SGSI (certificable)
- **ISO 27002:** Código de prácticas de controles
- **ISO 27005:** Gestión de riesgos de seguridad
- **ISO 27007:** Directrices para auditoría de SGSI

## ISO 19011

**Directrices para auditoría** de sistemas de gestión

- ✓ Principios de auditoría
- ✓ Gestión de programas
- ✓ Competencia de auditores

## NIST CSF

**Marco de ciberseguridad** del NIST (EE.UU.)

- ✓ Identificar - Proteger
- ✓ Detectar - Responder
- ✓ Recuperar

## ITIL 4

**Gestión de servicios TI** y mejores prácticas

- ✓ Sistema de valor
- ✓ Prácticas de gestión
- ✓ Modelos de operación

### Sinergias entre Estándares

Los estándares no son mutuamente excluyentes; se **complementan**. COBIT proporciona el marco de gobierno, ISO 27001 los requisitos de seguridad, e ISO 19011 la metodología de auditoría. La integración efectiva crea un ecosistema robusto de gobernanza, riesgo y cumplimiento (GRC).

CERTIFICACIÓN PROFESIONAL

# ISACA y la Certificación CISA

## ¿Qué es ISACA?

Organización internacional líder en **gobernanza, control y seguridad de la información**. Fundada en 1969, cuenta con más de 170,000 miembros en 180 países.

- Desarrolla estándares y frameworks (COBIT)
- Ofrece certificaciones reconocidas globalmente
- Publica investigaciones y guías de mejores prácticas
- Promueve la educación continua

## Certificación CISA

**Certified Information Systems Auditor** - Estándar de excelencia para auditores de SI desde 1978. Más de 164,000 profesionales certificados.

### Requisitos para la Certificación

1. **Aprobar el examen CISA**
   150 preguntas en 4 horas
2. **Experiencia laboral**
   5 años en auditoría, control o seguridad de SI
3. **Código de ética profesional**
   Adherirse a los estándares de ISACA
4. **Educación continua (CPE)**
   120 horas cada 3 años (mínimo 20/año)

## Dominios del Examen CISA

| | | |
|---|---|---|
| **Dominio 1** | **Proceso de Auditoría de SI**<br>Planificación, ejecución y reporte según estándares ISACA | 18% |
| **Dominio 2** | **Gobierno y Gestión de TI**<br>Estructuras organizativas, estrategia y marcos de gobierno | 18% |
| **Dominio 3** | **Adquisición, Desarrollo e Implementación**<br>Ciclo de vida de sistemas y controles de cambio | 12% |
| **Dominio 4** | **Operaciones y Resiliencia del Negocio**<br>Gestión de servicios, continuidad y recuperación | 26% |
| **Dominio 5** | **Protección de Activos de Información**<br>Seguridad lógica, física y controles criptográficos | 26% |

## Beneficios de la Certificación CISA

- **Reconocimiento global** en 160+ países
- **Salario promedio** de $110,000 USD/año
- **Ventaja competitiva** en el mercado laboral
- **Desarrollo profesional** continuo

FRAMEWORK DE GOBIERNO

# COBIT 2019: Gobierno y Gestión de TI

## COBIT 2019

Control Objectives for Information Technologies

Framework integral desarrollado por **ISACA** para gobernar y gestionar la tecnología de la información. Proporciona un conjunto completo de mejores prácticas para alinear TI con objetivos de negocio.

- **40 procesos** de gobierno y gestión
- **231 prácticas** específicas
- **1,202 actividades** detalladas

## Principios del Marco

1. Identificar componentes clave y sus relaciones
2. Permitir agregado flexible de nuevo contenido
3. Alineado a estándares y regulaciones relevantes

## Principios del Sistema

1. Componentes holísticos que trabajan juntos
2. Dinámico y adaptable al contexto
3. Distinguir gobierno vs. gestión
4. Adecuado a necesidades empresariales
5. Cobertura end-to-end de la empresa

## Los 5 Dominios de COBIT 2019

### EDM

**Evaluar, Dirigir y Monitorear**

Gobierno corporativo de TI, asegurando entrega de beneficios y optimización de riesgos y recursos.

### APO

**Alinear, Planificar y Organizar**

Gestión de arquitectura empresarial, riesgos, seguridad, recursos y calidad de datos.

### BAI

**Construir, Adquirir e Implementar**

Desarrollo y gestión de programas, definición de requisitos, cambios organizacionales.

### DSS

**Entregar, Servicio y Soporte**

Operaciones de TI, gestión de servicios, seguridad, continuidad y gestión de problemas.

### MEA

**Monitorear, Evaluar y Mejorar**

Monitoreo del desempeño, conformidad con requisitos internos y externos.

## Alineación con Otros Estándares

COBIT 2019 integra y alinea con **ISO 27001, ISO 20000, ITIL 4, NIST, TOGAF, CMMI y PMI** . Esto permite a las organizaciones usar múltiples frameworks de manera complementaria, evitando duplicidad de esfuerzos.

GESTIÓN DE SEGURIDAD

# ISO 27001: Sistema de Gestión de Seguridad de la Información

## ¿Qué es ISO 27001?

Estándar internacional que especifica requisitos para establecer, implementar, mantener y mejorar continuamente un **Sistema de Gestión de Seguridad de la Información (SGSI)**.

- **Protege activos** de información
- **Garantiza CIA** (Confidencialidad, Integridad, Disponibilidad)
- **Gestiona riesgos** de seguridad
- **Demuestra compromiso** ante clientes y partes interesadas

## Estructura de Cláusulas (Anexo SL)

**4 Contexto de la organización**
Entender el contexto, partes interesadas, alcance

**5 Liderazgo**
Compromiso de la dirección, política, roles

**6 Planificación**
Evaluación de riesgos, tratamiento, objetivos

**7 Soporte**
Recursos, competencia, comunicación

**8 Operación**
Planificación operacional, evaluación de riesgos

**9 Evaluación del desempeño**
Monitoreo, auditoría interna, revisión

**10 Mejora**
No conformidades, acciones correctivas

### Ciclo PHVA (Planificar-Hacer-Verificar-Actuar)

Enfoque de mejora continua aplicado al SGSI.

## Anexo A: 93 Controles (2022)

| | |
|---|---|
| **Organizacionales** — Políticas, roles, evaluación de riesgos, gestión de incidentes | 37 |
| **Personas** — Selección, términos de contratación, concienciación | 8 |
| **Físicos** — Perímetros de seguridad, controles de acceso físico | 14 |
| **Tecnológicos** — Criptografía, seguridad de redes, desarrollo seguro | 34 |

## Novedades ISO 27001:2022

- 11 controles nuevos: inteligencia de amenazas, cloud, DLP, codificación segura
- Reorganización en 4 temas (vs. 14 dominios anteriores)
- Mayor alineación con tendencias actuales de ciberseguridad

### Certificación

Acreditación por organismos acreditados (IAS, ENAC), reconocimiento global IAF MLA.

Fundamentos Legales

# Marco Normativo de Referencia: UE y España

## EU NORMATIVA EUROPEA

**GDPR**
Reg. UE 2016/679 - Protección de datos

**Directiva NIS2**
Seguridad redes y sistemas

**Reglamento eIDAS**
Identidad electrónica y servicios de confianza

**Cybersecurity Act**
Marco de ciberseguridad europeo

**Guías ENISA**
Agencia de Ciberseguridad UE

**ETSI Standards**
Estándares técnicos europeos

## ES NORMATIVA ESPAÑOLA

**ENS**
RD 311/2022 - Esquema Nacional de Seguridad

**LOPDGDD**
Ley Orgánica 3/2018 - Protección de datos

**Ley de Auditoría de Cuentas**
Marco regulatorio de auditores

**Normas CCN-STIC**
Guías técnicas del CCN-CERT

**Guías AEPD**
Agencia Española de Protección de Datos

**Marco Español de Ciberseguridad**
Estrategia nacional

**ISO 27001 / COBIT:** Soporte técnico complementario que operacionaliza requisitos legales en controles prácticos

Contexto Actual

# Panorama de la Auditoría Informática en España/UE

**35%**
Crecimiento

Demanda de auditores IT (2020-2024)

**Sector Público**
Obligatorio

Todas las administraciones bajo ENS

**NIS2**
Ampliación

Más entidades obligadas a auditoría

## Sectores Regulados

- Banca
- Salud
- Energía
- Telecomunicaciones

## Organismos Clave

**ICJCE / ROAC**
Certificación de auditores

**AEPD**
Control y sanción en protección de datos

**ENISA**
Guías técnicas europeas

**CCN**
Certificación y estándares sector público

**NIS2:** Amplía significativamente el número de entidades obligadas a realizar auditorías de ciberseguridad, incluyendo más sectores críticos

# Marco Normativo Vigente en España y la UE

### RGPD (UE) 2016/679

Reglamento General de Protección de Datos. Aplicable desde mayo 2018. Multas de hasta 20M€ o el 4% del volumen de negocio global anual.

### LOPDGDD (LO 3/2018)

Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales. Adapta el RGPD al ordenamiento español e incorpora derechos digitales.

### Directiva NIS2 (2022/2555)

Sustituye a NIS1. Amplía sectores obligados (energía, transporte, banca, salud, agua...). Transposición antes de octubre 2024.

### ENS – RD 311/2022

Esquema Nacional de Seguridad. Obligatorio para AAPP y proveedores. Categorías: BÁSICA, MEDIA y ALTA según impacto.

### Ley 36/2015 Seguridad Nacional

Marco para la protección de infraestructuras críticas. Coordinado por el CNPIC y el CCN-CERT.

### Código Penal (arts. 197-200)

Tipifica delitos contra la intimidad, el descubrimiento y revelación de secretos, intrusión informática y daños a sistemas informáticos.

# RGPD: Principios y Obligaciones para la Auditoría

*Impacto directo en auditorías de seguridad informática*

- Principio de responsabilidad proactiva (accountability): la organización debe demostrar cumplimiento activo
- Derecho a la portabilidad, al olvido, de acceso, rectificación y limitación del tratamiento
- Obligación de realizar EIPD (Evaluación de Impacto) cuando el tratamiento suponga alto riesgo
- Designación de DPO (Delegado de Protección de Datos) obligatoria en ciertos supuestos
- Notificación de brechas de seguridad a la AEPD en 72 horas y al interesado si alto riesgo
- Registro de actividades de tratamiento (RAT): documento obligatorio para todas las organizaciones
- Medidas técnicas y organizativas: pseudoanonimización, cifrado, control de accesos, backups
- Auditoría de protección de datos: verificar cumplimiento y detectar riesgos de privacidad

# ENS: Esquema Nacional de Seguridad

- Marco legal obligatorio para AAPP (RD 311/2022)
- 3 categorías: BÁSICA, MEDIA, ALTA
- 93 medidas de seguridad agrupadas en marco organizativo, operacional y protección
- Ciclo de mejora continua: Plan-Do-Check-Act
- Conformidad mediante auditoría bienal (cat. MEDIA/ALTA)
- CCN-STIC: guías técnicas de referencia para implantación
- INES: Informe Nacional del Estado de la Seguridad
- Certificación ENS por entidades acreditadas ENAC
- Declaración de Aplicabilidad (DdA) documentada
- Interoperabilidad con ISO 27001:2022

Ética Profesional

# Código Deontológico de la Función de Auditoría

## PRINCIPIOS FUNDAMENTALES (ICJCE/IFAC)

### INTEGRIDAD

Actuar con honestidad en todo proceso de auditoría

### OBJETIVIDAD

Sin sesgos ni conflictos de interés

### CONFIDENCIALIDAD

Protección de datos (LOPDGDD art. 5)

### COMPETENCIA

Formación continua y cualificación ROAC

### COMPORTAMIENTO PROFESIONAL

Cumplir normativa vigente

## ESPECIAL ATENCIÓN

- **Tratamiento de datos personales** durante auditoría (GDPR art. 28)
- **Gestión de información sensible** según ENS Medidas de Seguridad

## Marco Normativo de Referencia

- Código deontológico ICJCE
- Estándares éticos IFAC
- Ley de Auditoría de Cuentas

Requisitos Legales

# Independencia y Objetividad

## INDEPENDENCIA SEGÚN LEY DE AUDITORÍA DE CUENTAS

### INCOMPATIBILIDADES

1. **Servicios de consultoría**
   No haber prestado servicios en los últimos **2 años**
2. **Relaciones laborales**
   No tener vínculos laborales con la entidad auditada
3. **Intereses económicos**
   No tener participación financiera en la entidad

### SALVAGUARDAS

1. **Rotación de socios**
   Cambio obligatorio cada **7 años**
2. **Revisión por pares**
   Obligatoria para garantizar calidad
3. **Declaración firmada**
   Documento de independencia obligatorio

### SANCIONES POR INCUMPLIMIENTO

**Invalidez del informe de auditoría** + **sanciones ROAC/AEPD** según gravedad

Estructura del Equipo

# Composición del Equipo Auditor

| | |
|---|---|
| Líder Auditor | ROAC/ICJCE, 5+ años experiencia en auditoría |
| Especialista IT | ENS, ISO 27001, CCN-STIC, ciberseguridad |
| Experto Legal | LOPDGDD, GDPR, eIDAS, normativa sectorial |
| Analista CAAT | ACL, IDEA, Python, SQL, análisis de datos |

## COMPETENCIAS BLANDAS REQUERIDAS

- Comunicación efectiva
- Ética profesional
- Pensamiento crítico
- Trabajo en equipo

Organización del Trabajo

# Roles y Responsabilidades dentro del Equipo

## MATRIZ RACI EN PROYECTOS DE AUDITORÍA IT

### R RESPONSABLE

Ejecuta la tarea

**Ejemplo:** Analista CAAT realiza extracción de datos

### A APROBADOR

Valida y firma

**Ejemplo:** Líder auditor firma informes finales

### C CONSULTADO

Aporta información

**Ejemplo:** DPO, CISO, legal interno

### I INFORMADO

Recibe actualizaciones

**Ejemplo:** Dirección, comité de auditoría

## COORDINACIÓN CON DPO (Data Protection Officer)

- **Obligatorio** cuando se traten datos personales (GDPR art. 37)
- **Registro** de actividades de tratamiento de la auditoría
- **EIPD** si procede (Evaluación de Impacto en Protección de Datos)

# Conceptos Fundamentales del Análisis de Riesgos

## Activo

Todo elemento con valor para la organización: hardware, software, datos, servicios, personal, instalaciones e imagen corporativa.

## Amenaza

Causa potencial de un incidente que puede causar daños a activos. Pueden ser accidentales, deliberadas o de origen natural.

## Vulnerabilidad

Debilidad de un activo que puede ser explotada por una amenaza. Se clasifican según CVSS v3.1 (0-10) y CVE en NVD/MITRE.

## Riesgo

Probabilidad × Impacto. Es la combinación de la probabilidad de que se materialice una amenaza y el impacto sobre el negocio.

## Impacto

Consecuencia de la materialización de una amenaza: pérdida económica, reputacional, legal o de disponibilidad del servicio.

## Salvaguarda

Medida de protección que reduce la probabilidad o el impacto de una amenaza. Pueden ser preventivas, detectoras o correctoras.

# Metodologías de Análisis y Gestión de Riesgos

- MAGERIT v3 (CCN): metodología española de referencia para AAPP. Catálogo de activos, amenazas y salvaguardas estandarizado
- NIST SP 800-30 r1: guía de gestión de riesgos para sistemas federales de EEUU, ampliamente adoptada a nivel global
- ISO 31000:2018: marco internacional de gestión de riesgos. Principios, marco y proceso de evaluación
- OCTAVE (Carnegie Mellon): Operationally Critical Threat, Asset, and Vulnerability Evaluation
- FAIR (Factor Analysis of Information Risk): cuantificación económica del riesgo de ciberseguridad
- EBIOS Risk Manager (Francia): metodología alineada con ISO 27005 para análisis de escenarios de ataque

# Principales Tipos de Amenazas y Vulnerabilidades (2024-2025)

*Según ENISA Threat Landscape 2024 y OWASP Top 10*

- Ransomware: sigue siendo la principal amenaza. Grupos como LockBit, ALPHV/BlackCat y RansomHub son los más activos en 2024
- Ataques a la cadena de suministro (Supply Chain): compromiso de software legítimo para infectar miles de organizaciones
- Ingeniería social y phishing: deepfakes de voz/vídeo potenciados por IA generativa aumentan la efectividad
- Explotación de vulnerabilidades 0-day: Log4Shell, MOVEit, Citrix Bleed demuestran el impacto global
- Ataques a APIs (OWASP API Security Top 10): BOLA, autenticación rota, SSRF son vectores críticos
- Amenazas a entornos OT/ICS y IoT: infraestructuras críticas cada vez más expuestas a ciberataques
- Filtraciones de datos masivas: IA generativa facilita el abuso de datos robados para fraude personalizado

# Fases de una Auditoría de Seguridad

1. Planificación y definición del alcance
2. Recopilación de información (OSINT/RECON)
3. Análisis y evaluación de vulnerabilidades
4. Explotación controlada (si aplica)
5. Post-explotación y escalada de privilegios
6. Documentación de hallazgos y evidencias
7. Elaboración del informe de auditoría
8. Presentación de resultados al cliente
9. Plan de remediación y seguimiento
10. Re-auditoría y verificación de correcciones

METODOLOGÍA

# El Proceso de Auditoría de Sistemas de Información

## 01 Planificación

- ✓ Definir alcance y objetivos
- ✓ Evaluación de riesgos
- ✓ Asignación de recursos
- ✓ Programa de auditoría
- ✓ Revisión documental

## 02 Ejecución

- ✓ Reunión de apertura
- ✓ Recopilación de evidencias
- ✓ Entrevistas y observación
- ✓ Pruebas técnicas
- ✓ Identificación de hallazgos

## 03 Informe

- ✓ Estructura del informe
- ✓ Conclusiones y hallazgos
- ✓ Recomendaciones
- ✓ Comunicación de resultados
- ✓ Opinión del auditor

## 04 Seguimiento

- ✓ Plan de acciones correctivas
- ✓ Verificación de implementación
- ✓ Auditorías de seguimiento
- ✓ Cierre de hallazgos
- ✓ Mejora continua

## Técnicas de Recopilación de Evidencias

- **Entrevistas** con personal clave
- **Revisión documental**
- **Pruebas técnicas** (CAATs)
- **Observación** directa de procesos
- **Muestreo** estadístico
- **Trazabilidad** de procesos

## Estructura del Informe de Auditoría

1. **Resumen ejecutivo** - Conclusiones principales y opinión
2. **Alcance y objetivos** - Propósito y límites de la auditoría
3. **Metodología** - Enfoque y criterios utilizados
4. **Hallazgos** - Descripción de problemas identificados
5. **Recomendaciones** - Acciones correctivas propuestas
6. **Conclusión** - Opinión global del auditor

CLASIFICACIÓN

# Tipos de Auditoría IT

## Por Quién la Realiza

### Auditoría Interna

Realizada por profesionales de la propia organización.

- Enfoque en mejora continua
- Evaluación de controles internos
- Identificación de eficiencias
- Reporta a dirección/comité de auditoría

### Auditoría Externa

Realizada por profesionales independientes sin vínculo laboral.

- Verificación de cumplimiento normativo
- Certificación (ISO 27001, ENS)
- Mayor objetividad e independencia
- Reporta a stakeholders externos

## Por Naturaleza

**Auditoría de Cumplimiento (Compliance)**

Verifica adherencia a regulaciones (RGPD, ENS, NIS2, ISO 27001).

**Auditoría Operativa**

Evalúa eficiencia y eficacia de procesos de TI.

**Auditoría Financiera**

Verifica controles sobre sistemas contables y financieros.

**Auditoría Forense**

Investigación de incidentes de seguridad o fraudes.

**Auditoría de Seguridad**

Evaluación de controles de seguridad (pentesting, vulnerabilidades).

## Auditorías Específicas de TI

**Desarrollo**

Ciclo de vida, controles de cambio, calidad

**Operaciones**

Centros de datos, backup, monitoreo

**Red**

Arquitectura, firewalls, segmentación

**Aplicaciones**

Controles de acceso, validación, auditoría

Tipologías Especializadas

# Tipos de Auditoría en SI (II)

## TIPOLOGÍAS ESPECIALIZADAS

### AUDITORÍA FORENSE

- **Evidencia digital** con validez legal (LECrim, eIDAS)
- **Cadena de custodia** obligatoria
- Para **procedimientos judiciales** o sancionadores

**Ámbito:** Delitos informáticos, fraudes, investigaciones

### AUDITORÍA DE CUMPLIMIENTO

- **Verificación ENS, GDPR, NIS2**
- **Checklist** de controles normativos
- Informe para **reguladores** (AEPD, CCN)

**Ámbito:** Cumplimiento legal, certificaciones, inspecciones

### AUDITORÍA DE SEGURIDAD

- **Tests técnicos** (pentesting, vulnerabilidades)
- **CCN-STIC 800+** para sector público
- **ISO 27001** para sector privado

**Ámbito:** Infraestructuras, aplicaciones, redes

**Nota:** Estas tipologías no son excluyentes. Una auditoría puede combinar elementos de las tres según el alcance y objetivos del trabajo

IMPLEMENTACIÓN

# Herramientas y Técnicas de Auditoría

## Técnicas de Recopilación

**Entrevistas**

Estructuradas, semi-estructuradas o abiertas con personal clave.

**Cuestionarios**

Formularios estandarizados para recopilar información sistemática.

**Checklists**

Listas de verificación basadas en requisitos normativos.

**Observación Directa**

Presencia física para observar procesos y controles en acción.

## Herramientas Técnicas (CAATs)

**Análisis de Datos**

ACL, IDEA, Excel avanzado para análisis de grandes volúmenes.

**Escaneo de Vulnerabilidades**

Nessus, OpenVAS, Qualys para identificar debilidades técnicas.

**Pruebas de Penetración**

Metasploit, Burp Suite, Kali Linux para simular ataques.

**SIEM**

Splunk, ELK Stack, QRadar para análisis de logs y eventos.

## Software GRC

Plataformas integrales de Gobierno, Riesgo y Cumplimiento.

- Gestión de auditorías
- Evaluación de riesgos
- Seguimiento de hallazgos

## Documentación

Herramientas para gestión de evidencias e informes.

- Plantillas estandarizadas
- Workpapers electrónicos
- Trazabilidad de evidencias

## Mejores Prácticas

- ✓ **Independencia** del auditor
- ✓ **Objetividad** en evaluaciones
- ✓ **Confidencialidad** de información
- ✓ **Competencia** profesional
- ✓ **Due professional care**

Verificación Normativa

# Auditoría de Cumplimiento Normativo: GDPR y ENS

## CHECKLIST DE CONTROLES CLAVE

### EU GDPR (Art. 32 – Seguridad del Tratamiento)

- ☑ **Cifrado** de datos personales
- ☑ **Confidencialidad, integridad, disponibilidad**
- ☑ **Restauración** de acceso tras incidente
- ☑ **Evaluación periódica** de medidas

### ES ENS (RD 311/2022)

- ☑ **Medidas Básicas** (todos los sistemas)
- ☑ **Medidas Medias** (información moderada)
- ☑ **Medidas Altas** (información crítica)
- ☑ **Certificación** cada 2 años (nivel Alto)

### CONSECUENCIAS DEL INCUMPLIMIENTO

**Sanciones AEPD** (hasta 20M€ o 4% VT) + **Invalidación ENS** (imposibilidad de operar en sector público)

Soporte Técnico

# Integración de Marcos: COBIT e ISO como Soporte Técnico

## MAPEO DE MARCOS NORMATIVOS

| | | |
|---|---|---|
| **GDPR Art. 32** | A.12 Operaciones seguras | DSS05 Gestionar servicios de seguridad |
| **ENS Medidas** | A.9 Control de accesos | APO12 Gestionar riesgos |
| **NIS2 Incidentes** | A.16 Gestión de incidentes | MEA03 Monitorear y evaluar |
| **eIDAS Evidencia** | A.12.4 Logging y monitoreo | BAI09 Gestionar activos |

### Requisitos Legales

Establecen **qué** debe cumplirse (obligaciones)

### ISO 27001 / COBIT

Definen **cómo** cumplirlo (controles)

### Valor Añadido

**Operacionalizan** requisitos legales en controles técnicos

Metodología

# Pruebas de Auditoría: Clasificación y Propósito

## CLASIFICACIÓN DE PRUEBAS

### PRUEBAS DE CUMPLIMIENTO

**¿El control existe y funciona?**

Verifican la existencia y operatividad de controles establecidos

**Ejemplo práctico:**

¿Hay política de contraseñas según ENS? ¿Se aplica correctamente?

**Evidencia:**

- Documentos y políticas
- Entrevistas
- Observación directa

### PRUEBAS SUSTANTIVAS

**¿Los datos son correctos y completos?**

Validan la integridad y exactitud de la información

**Ejemplo práctico:**

¿Los logs de acceso coinciden con la realidad? ¿Hay inconsistencias?

**Evidencia:**

- Análisis de datos
- Recálculo y reconciliación
- Confirmación externa

### OBJETIVO COMÚN

Obtener **evidencia suficiente, competente y relevante** para sustentar las conclusiones del informe de auditoría

Ejemplo Práctico

# Pruebas de Cumplimiento: Verificación de Controles Normativos

## CONTROL: Cifrado de datos personales en reposo

NORMA: ENS Medida 8.2 + GDPR Art. 32

### 1 Inspección

Revisar política de cifrado documentada y aprobada

### 2 Entrevista

Cuestionar al responsable de seguridad sobre implementación

### 3 Observación

Verificar configuración de cifrado en sistemas de producción

### 4 Re-ejecución

Probar cifrado con datos de prueba y verificar resultado

✅ **CUMPLE**
Control implementado y operativo

❌ **NO CUMPLE**
Control inexistente o no operativo

⚠️ **PARCIAL**
Cumple con deficiencias menores

Ejemplo Práctico

# Pruebas Sustantivas: Validación de Integridad de la Información

**OBJETIVO: Validar integridad de logs de historiales**

NORMA: ENS Medidas Altas + LOPDGDD Art. 28

### 1 Recálculo

Comparar logs registrados con accesos reales del sistema

### 2 Confirmación

Validar con responsables de área sobre actividades registradas

### 3 Análisis CAAT

Detectar anomalías y patrones sospechosos con herramientas

### 4 Trazabilidad

Cadena de custodia de evidencias digitales

**ALTERACIÓN DE LOGS**

**Incumplimiento grave ENS** (pérdida de certificación) + **Posible delito** (alteración de evidencias)

Técnicas de Selección

# Tipos de Muestreo en Auditoría Informática

| | |
|---|---|
| Aleatorio Simple | Población homogénea, sin sesgos aparentes. Cada elemento tiene igual probabilidad de selección. |
| Estratificado | Población heterogénea dividida por niveles de riesgo. Mayor representatividad de estratos críticos. |
| Juicio Profesional | Áreas críticas (ENS Alto, GDPR datos sensibles). Basado en experiencia y conocimiento del auditor. |
| Sistemático | Cada N-ésimo elemento (logs, transacciones). Intervalo fijo después de punto aleatorio inicial. |

## CONSIDERACIONES LEGALES

- **Representatividad** para procedimientos sancionadores (AEPD)
- **Documentar** metodología de selección (cadena de custodia)
- **Tamaño muestral** justificado según riesgo normativo

Tecnología Auditoría

# Herramientas CAAT: Eficiencia y Trazabilidad

## COMPUTER ASSISTED AUDIT TOOLS (CAAT)

### BENEFICIOS

**Cobertura 100%**
De la población, no solo muestra

**Detección anomalías**
Patrones y tendencias sospechosas

**Auditoría continua**
En tiempo real

**Trazabilidad completa**
De evidencias digitales

### HERRAMIENTAS COMUNES

**ACL / IDEA**
Herramientas comerciales especializadas

**Python + pandas**
Open source, flexibilidad y potencia

**ELK Stack**
Logs y análisis de seguridad

**SQL / Power BI**
Análisis de datos y visualización

**eIDAS:** Validez jurídica de evidencias digitales generadas con CAATs certificados

# Herramientas de Reconocimiento y Escaneo de Red

## Nmap 7.95

Escáner de puertos y servicios. Uso: nmap -sV -sC -O target. Scripts NSE para detección avanzada. Integrado en Kali Linux.

## Wireshark / TShark

Analizador de protocolos de red. Captura y análisis de tráfico en tiempo real. Filtros BPF para análisis forense.

## Netdiscover / Nessus

Descubrimiento de hosts activos (ARP). Nessus: escáner de vulnerabilidades líder con más de 200.000 plugins.

## OpenVAS / Greenbone

Alternativa open source a Nessus. GVM 22.4+: gestión completa de vulnerabilidades con dashboard web.

## Masscan / Zmap

Escaneo masivo de Internet a velocidades de 25M paquetes/segundo. Útil para reconocimiento de grandes rangos IP.

## Shodan / Censys

Motores de búsqueda de dispositivos conectados. Identifican servicios expuestos, versiones y vulnerabilidades conocidas.

# Herramientas de Auditoría Web y Contraseñas

### Burp Suite Pro / OWASP ZAP

Proxy de interceptación para auditoría web. Escáner activo/pasivo de vulnerabilidades OWASP. ZAP 2.14 es la alternativa open source.

### Nikto

Escáner de servidores web. Detecta más de 6.700 archivos peligrosos y versiones desactualizadas de software.

### SQLmap

Herramienta automatizada de detección y explotación de inyecciones SQL. Soporta MySQL, PostgreSQL, Oracle, MSSQL...

### John the Ripper / Hashcat

Cracking de contraseñas offline. Hashcat GPU acelera hasta 100Gx/s en MD5. Soporta +300 tipos de hash.

### Hydra / Medusa

Ataques de fuerza bruta online a servicios: SSH, FTP, HTTP, SMB, RDP, etc. Uso educativo en entornos controlados.

### OWASP Amass / Subfinder

Enumeración de subdominios e infraestructura. Esencial en reconocimiento pasivo de superficie de ataque.

# Frameworks y Plataformas de Auditoría

## Kali Linux 2024.x

Distribución Linux de referencia para pentesting. +600 herramientas preinstaladas. Versiones: Desktop, Cloud y ARM.

## Metasploit Framework

Framework de explotación más utilizado. +2.000 módulos de exploit. Interfaz Msfconsole. Armitage para uso gráfico.

## Cobalt Strike

Plataforma comercial para Red Team. Beacons C2, lateral movement y post-explotación avanzada. Imitado por adversarios.

## OSINT Framework

Recopilación de inteligencia de fuentes abiertas. Maltego, theHarvester, Recon-ng, SpiderFoot, Shodan...

# Herramientas del Sistema Operativo para Auditoría

*Utilidades nativas de diagnóstico de red y sistema*

- ping / ping6: verificación de conectividad ICMP, medición de latencia y detección de hosts activos
- traceroute / tracert: trazado de rutas, identificación de saltos y detección de dispositivos intermedios
- nslookup / dig: consultas DNS, enumeración de registros (A, MX, TXT, NS, SOA, AXFR)
- netstat / ss: estado de conexiones TCP/UDP, puertos en escucha, procesos asociados
- arp -a: tabla ARP local, útil para detectar ARP spoofing y mapear red local
- ipconfig / ifconfig / ip a: configuración de interfaces de red y routing
- tasklist / ps aux: listado de procesos en ejecución para detectar procesos sospechosos
- Sysinternals Suite (Windows): Process Explorer, Autoruns, TCPView para análisis forense

# Tipos de Cortafuegos y Tecnologías

## Packet Filtering (L3/L4)

Filtra paquetes por IP origen/destino, puerto y protocolo. Base de firewalls tradicionales. Stateless (sin seguimiento de sesión).

## Stateful Inspection (L4)

Seguimiento del estado de las conexiones TCP. Detecta paquetes fuera de secuencia. Más seguro que el filtrado simple.

## Application Layer (WAF/L7)

Inspección profunda de paquetes (DPI). Web Application Firewall: protege contra OWASP Top 10. ModSecurity, Cloudflare WAF.

## NGFW (Next Generation)

Integra IPS, control de aplicaciones, SSL inspection y threat intelligence. Líderes: Palo Alto, Fortinet FortiGate, Check Point.

## UTM (Unified Threat Management)

Firewall + antivirus + IPS + filtrado web + VPN en un solo dispositivo. Ideal para PYME. Sophos, WatchGuard, Cisco Meraki.

## FWaaS / Cloud Firewall

Firewall como servicio en la nube. Zscaler, Prisma Access, Azure Firewall. Esencial en arquitecturas SASE/Zero Trust.

# Auditoría de Cortafuegos: Aspectos Clave

*Qué revisar en una auditoría de firewall*

- Revisión del ruleset: identificar reglas permisivas (any/any), reglas duplicadas, oscuras u obsoletas
- Verificar el principio de mínimo privilegio: solo se permite el tráfico estrictamente necesario
- Análisis de reglas implícitas: comportamiento por defecto (deny-all vs. allow-all) al final del ruleset
- Segmentación de red: revisión de zonas (LAN, DMZ, WAN, OT) y control de flujos entre zonas
- Logging y monitorización: verificar que los registros de tráfico bloqueado/permitido están activos
- Gestión de cambios: existe proceso formal de solicitud, aprobación y revisión de cambios de reglas
- Pruebas de evasión: técnicas de fragmentación, tunelización (DNS tunneling, ICMP tunneling) y bypass
- Inspección TLS/SSL: necesidad de man-in-the-middle corporativo para inspeccionar tráfico cifrado

# Arquitecturas de Red y DMZ

- DMZ (Zona Desmilitarizada): servidores web, email, DNS públicos separados de la LAN interna
- Arquitectura dual-homed: firewall con al menos 3 interfaces (WAN / DMZ / LAN)
- Screened subnet: dos firewalls para mayor segmentación
- Zero Trust Network Access (ZTNA): verificación continua, sin perímetro de confianza implícita
- Micro-segmentación: SDN para aislar cargas de trabajo en entornos virtualizados y cloud
- VLAN segmentation: aislamiento de redes por función (usuarios, servidores, IoT, OT/ICS)
- IDS/IPS: Snort 3, Suricata 7. Integrados en NGFW o como sonda inline/offline
- Honeypot / Honeynet: sistemas señuelo para detectar atacantes internos o externos
- NAC (Network Access Control): 802.1X, Cisco ISE, validación de postura antes de acceder a la red
- SIEM integration: correlación de logs de firewall con otros eventos de seguridad

SECCIÓN 5

# HALLAZGOS Y COMUNICACIÓN DE RESULTADOS

Documentación, Categorización y El Informe de Auditoría

Estructura del Hallazgo

# Requerimientos de los Hallazgos de Auditoría

## LOS 5 ATRIBUTOS DE UN HALLAZGO (ICJCE/IGAE)

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| **CONDICIÓN** | **CRITERIO** | **CAUSA** | **EFECTO** | **RECOMEND.** |
| ¿Qué se encontró? | ¿Qué debería ser? | ¿Por qué ocurrió? | ¿Qué impacto tiene? | ¿Cómo solucionarlo? |
| Situación real observada | Norma/ENS/GDPR aplicable | Raíz del problema | Riesgo/sanción potencial | Acción correctiva |

## EJEMPLO PRÁCTICO

**Falta cifrado** en base de datos de clientes (Condición) vs. **ENS Medida 8.2** que exige cifrado de información sensible (Criterio). Causa: presupuesto insuficiente. Efecto: exposición a sanciones AEPD hasta 20M€. Recomendación: implementar cifrado TDE en 30 días.

Clasificación de Hallazgos

# Categorización: Observaciones vs. No Conformidades

| | ✅ | ❌ |
|---|---|---|
| **Incumplimiento** | No directo | Sí, normativo explícito |
| **Impacto Legal** | Bajo | Medio/Alto |
| **Sanción AEPD** | No aplica | Posible |
| **ENS** | Mejora oportuna | Invalida certificación |
| **Plazo Corrección** | 6-12 meses | Inmediato/30 días |
| **Ejemplo** | Documentación incompleta | Sin cifrado GDPR datos sensibles |

**NO CONFORMIDAD CRÍTICA**

**Notificación obligatoria** a regulador (AEPD, CCN) cuando el riesgo supere el umbral establecido en la normativa aplicable

Papeles de Trabajo

# Documentación y Trazabilidad de Hallazgos

## REQUISITOS LEGALES

### Ley de Auditoría de Cuentas

- **Conservación mínima:** 5 años desde fecha del informe
- **Acceso restringido** y confidencial

### GDPR (Art. 5)

- **Minimización** de datos en papeles de trabajo
- **Derecho de supresión** cuando aplique

### eIDAS

- **Sello de tiempo** en evidencias digitales
- **Firma electrónica cualificada** para informes

### Cadena de Custodia

- **Registro** de quién, cuándo y cómo accede
- **Crítico** para procedimientos sancionadores/judiciales

**Recomendación:** Implementar sistema de gestión documental con control de versiones, trazabilidad completa y acceso basado en roles

El Informe de Auditoría

# Comunicación de Resultados: El Informe de Auditoría

## ESTRUCTURA DEL INFORME (ICJCE/ROAC)

1. **Objetivos y alcance de la auditoría**
   Definición clara del trabajo realizado
2. **Marco normativo aplicado**
   ENS, GDPR, NIS2, LOPDGDD
3. **Metodología y muestreo utilizado**
   Técnicas y alcance de las pruebas
4. **Hallazgos detallados**
   5 atributos de cada hallazgo
5. **Categorización**
   Observación / No Conformidad
6. **Recomendaciones y plan de acción**
   Acciones correctivas propuestas
7. **Plazos de seguimiento**
   Fechas de implementación y revisión

### DESTINATARIOS

- Dirección de la entidad
- DPO (Data Protection Officer)
- Comité de Auditoría
- Reguladores (AEPD, CCN)

### GDPR Art. 33

**Notificación de brecha** en 72 horas si procede tras identificación durante auditoría

**Calidad del informe:** Debe ser claro, conciso, objetivo y basado en evidencias. Cada hallazgo debe ser trazable a su soporte documental

# El Informe de Auditoría

*Estructura, contenidos y buenas prácticas*

- Resumen ejecutivo: síntesis de hallazgos y riesgo global para la dirección no técnica
- Metodología empleada: herramientas, técnicas y restricciones del alcance
- Hallazgos técnicos: clasificados por criticidad (Crítica, Alta, Media, Baja, Informativa)
- Sistema de puntuación CVSS v3.1: métrica estándar para calificar la gravedad de vulnerabilidades
- Evidencias: capturas de pantalla, logs y pruebas de explotación documentadas
- Recomendaciones: soluciones técnicas priorizadas con estimación de coste/esfuerzo
- Plan de remediación: cronograma con responsables y fechas de resolución estimadas

EU **ENISA** - guias.enisa.europa.eu

- Guías sobre auditoría de ciberseguridad
- Marcos de referencia europeos
- Actualizaciones sobre NIS2 y Cybersecurity Act

ES **CCN** - ccn.cni.es

- Normas CCN-STIC para sector público
- Certificaciones y formación especializada
- Alertas de seguridad y buenas prácticas

ES **AEPD** - aepd.es

- Guías interpretativas de GDPR/LOPDGDD
- Doctrina en procedimientos sancionadores
- Canal de notificación de brechas

🏛️ **ICJCE** - icjce.es

- Código Deontológico y Normas Técnicas de Auditoría
- Formación continua y cualificación ROAC
- Foro profesional y actualización normativa