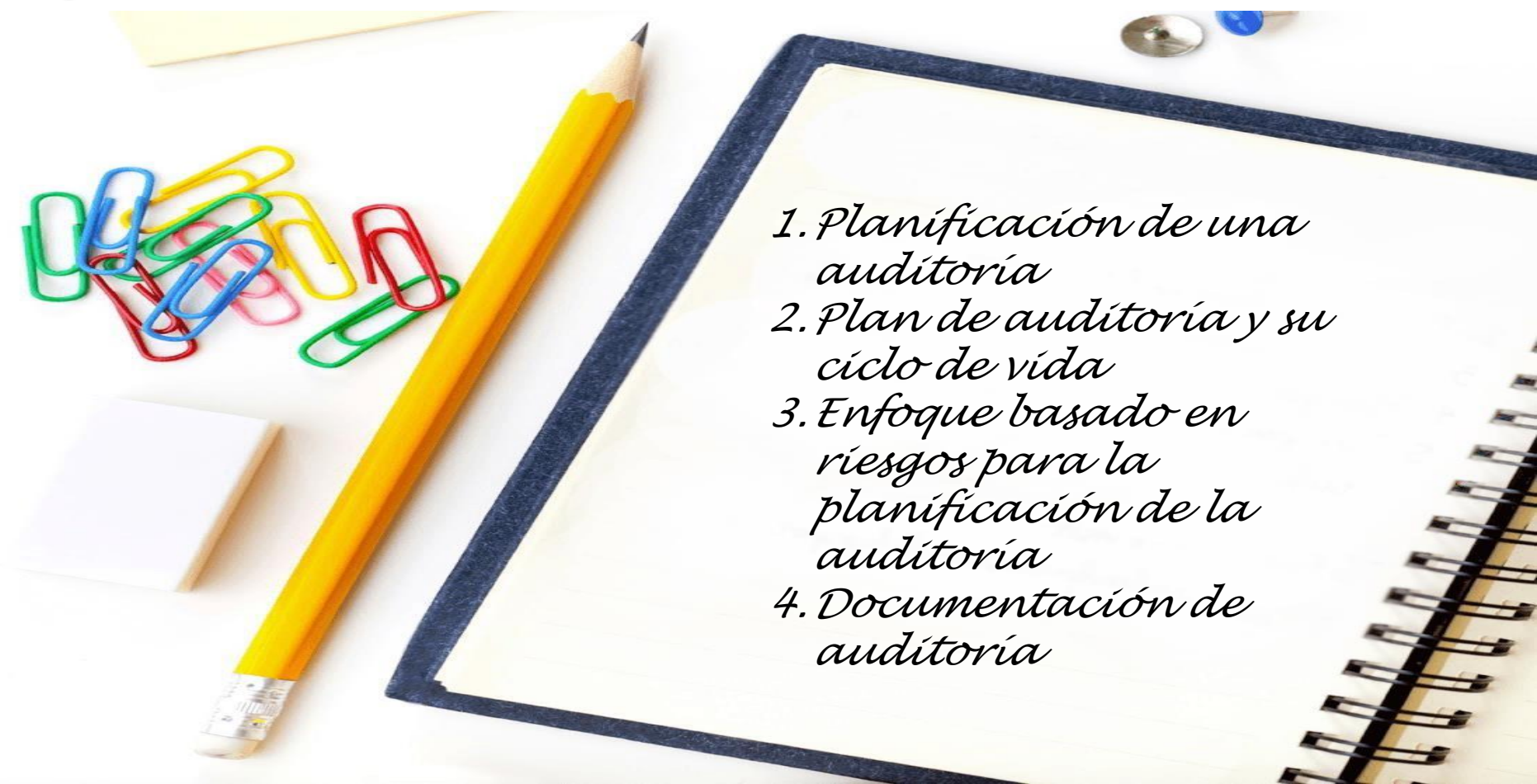


AUDITORÍA Y CONTROL DE SISTEMAS

LA PLANIFICACIÓN DEL PROCESO DE AUDITORÍA

Agenda

- 
1. *Planificación de una auditoría*
 2. *Plan de auditoría y su ciclo de vida*
 3. *Enfoque basado en riesgos para la planificación de la auditoría*
 4. *Documentación de auditoría*

Estatuto de auditoría *(Estándar de auditoría y aseguramiento de SI 1001)*

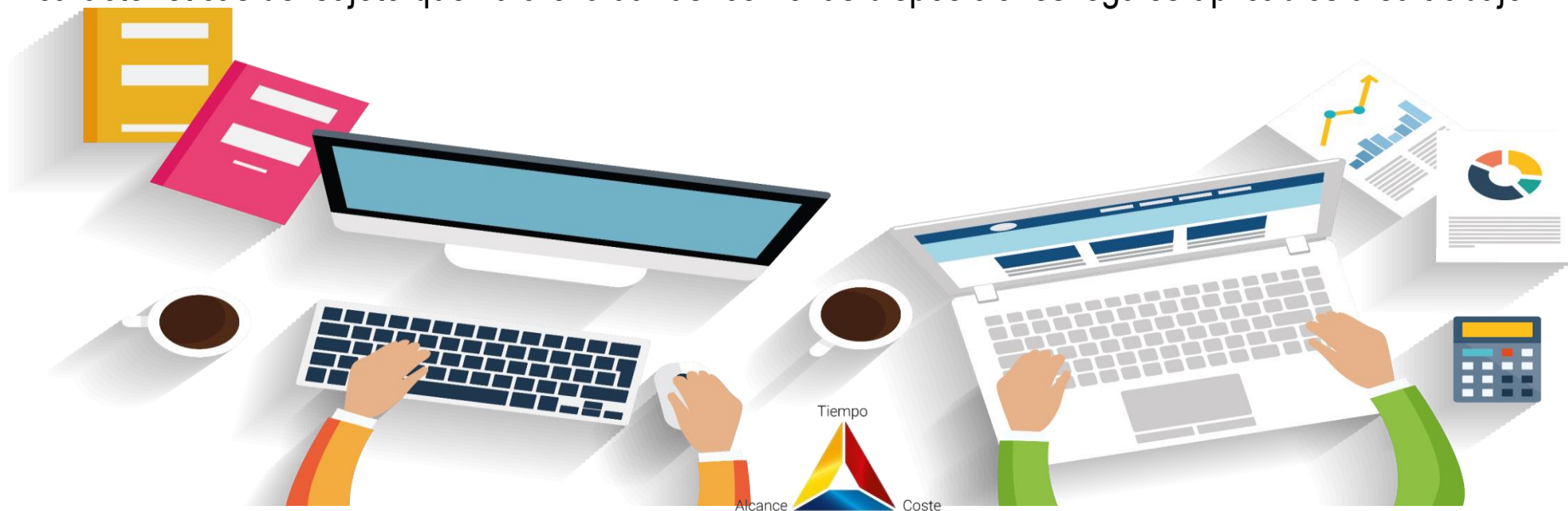
- Conocido como *Audit charter*
- Es un documento de carácter **normativo** **e informativo**
- Menciona el alcance, la organización, las funciones, las responsabilidades y los mecanismos de comunicación del área de auditoría.
- Formaliza el esquema de trabajo de la función informática en la empresa.



Planificación de una Auditoría *(Estándar de auditoría y aseguramiento de SI 1201)*

Definición

La planificación de una auditoria implica **desarrollar una estrategia general para su ejecución**, a fin de asegurar que el auditor tenga un cabal conocimiento y comprensión de las actividades y de las características del sujeto que va a evaluar así como las disposiciones legales aplicables a su trabajo.



Planificación de una Auditoría



Plan Anual de Auditoría

- Incluye todas las auditorías que se van a hacer en la organización
- Es aprobado por el Comité de Auditoría o equivalente (Alto Nivel Directivo)
- Se elabora bajo un enfoque de Gestión de Riesgos.
- El orden de elaboración puede variar en cada entidad, dependiendo entre otros del nivel de complejidad, tamaño, control interno, sistemas de información y estructura organizacional.

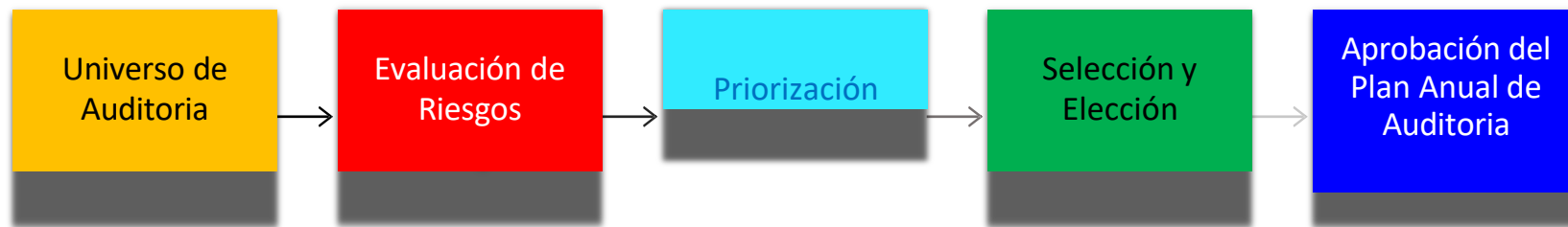


Plan de Auditoría

- Corresponde el plan de una auditoría en particular
- Realizado por el Jefe / Gerente de Auditoría, o el responsable de cada una.
- Basado en las Normas de auditoría otros aplicables
- Forman parte del Plan Anual de Auditoría.
- El Gerente de Auditoría aprueba el alcance y objetivo definido por el Jefe del equipo de Auditoría.
- Comprende la evaluación de riesgos del sujeto a auditar.

Planificación de una Auditoría

Elaboración del Plan Anual de Auditoría



Ver “*PA - 1 - Ejemplo Plantilla de Selección de Universo - Basado en Riesgos*”

ENFOQUE BASADO EN RIESGOS PARA LA PLANIFICACIÓN DE LA AUDITORÍA

Plan Anual de Auditoría

Determinación del Universo:

Riesgos Empresariales

Strategic

Governance Risk

- Board Performance
- Tone at the Top / Corporate Culture
- Enterprise Risk Management – Risk Mitigations

Planning & Resource Allocation Risk

- Organizational Structure Change
- Strategic Planning
- Long Term Planning
- JV's, Alliances and Partnerships
- Decision Speed

Technology change Risk – *AMS, smart grid*

- Industry Changes (Gas Generation)

Customer Demand Changes Risk

- Customer Demand Changes

Competition Risk

- Client Services / Satisfaction
- Communication Strategy and Plan

Enterprise Portfolio Risk

- Alliance/Partnerships
- Trademark/Brand Name
- Wholly Owned Affiliates

Government Policy Risk

- Regulatory Changes

Political Risk

- Political Changes

Lifecycle Risk

- Industry & Demand (30+ Year Rate Base Projection)

Organizational Structure Risk

- Performance Management (STIP/LTIP)

Business Development Risk

- Mergers and Acquisition and Divestiture
- Opportunity Capture
- Executing Captured Opportunity
- Due Diligence: Risk Assessment & Management

Major Initiatives Risk

- Planning and Execution
- Measurement and Monitoring
- Technology Implementations
- Business Acceptance

Communication/Investor Relation Risk

- Government/Media/Public Relations
- Land Owner Consultation & Relations
- Stakeholder/Investor Relations
- Reputation Management
- Crisis Management
- Regulatory/Legal Response Plan

Operational

People Risk

- Employee Fraud and Investigations
- Organizational Capacity & Capabilities
- Employee & labor relations
- Contractor Management & Excessive Usage
- Health & Welfare & Safety
- Excessive Recruitment and Turnover
- Timely & Effective Training and Development

Project/Operations Management Risk

- Contract Commitments
- Scheduling & Forecasting
- Documentation & Standards
- Design, Mapping and Drafting
- Procurement / Competitive Bidding
- Vendor Selection / Contract Management
- Vendor / Contractor Management
- Project Execution (Stage Gate) & Management
- Change Notice & Management
- New Technology: Smart Grid
- Client & Service Interaction
- Quality Assurance & Control
- Incident Management & Investigation
- Safety & Reliability
- Fleet Purchases, Maintenance and Management
- Asset Management
- Environment Management Strategy
- Land Management Strategy
- Performance Management Gaps/KPI's
- Physical Security/Disturbance Analysis
- Privacy & Confidentiality
- Business Continuity / Disaster Recovery

External Risk

- Catastrophic/Natural Disaster/Weather
- Sabotage / Terrorist
- 3rd Party Contractor Mgmt./Reporting (Earned Value)
- Customer/3rd Party/Land Manager Fraud
- Supplier Performance
- Supplier Availability /Sole Source
- Availability of Goods and Services

IT & Control Center Risk

- Third Party Suppliers and Outsourcing
- Control Center Operations
- Programs and Change Management
- Security and Privacy (Firewalls, Access Management)
- Physical Environment
- Staffing/Operations/Disaster Recovery
- Data Security
- Infrastructure
- Authentication and Database

Compliance

Code of Conduct Risk

- Ethics / Conflict of Interest
- 1-800 Ethics Line Management
- Fraud (Anti Fraud Program)

Legal Risk

- Contracts
- Stranded Asset Issue
- IP and Patents
- Liability Protection, Regulation & Insurance
- Anti-Corruption

Regulatory Risk

- Due Diligence Process
- GTA Hearing, IR & Processes
- AESQ/AUC/Prudency Audits & Enforcement
- Alberta Reliability Standards
- Labor Standards
- Engineering Standards
- Environment
- Quality, Health and Safety
- Data Protection, Availability, and Privacy
- International Laws and Standards (i.e. FCPA)
- Tax Compliance
- Customs
- Discriminatory Practices

Financial

Rate Base and Cost Recovery Risk

- Regulated Tariff: Unapproved Costs/Prudence
- Deferral (DACDA) and Reserve Accounts
- Capital Budgeting and Cost Management (ABC)
- Transmission and Miscellaneous Revenue
- Customer Deposits

Financial Accounting & Reporting Risk

- Accounts Payable / Receivable
- Inventory, Prepaid Expenses & Deposits
- Budget & Planning Forecasts
- Accounting/External Reporting - IFRS
- Fund Investment & Evaluation
- Management/Internal Reporting
- Inter-affiliate Transactions (SNC-ATP)
- ICFR: C-SOX / Disclosure Controls
- Payroll & Expense Reporting
- Capital Overhead Allocation (i.e. E&S)
- Taxes and Insurance

Liquidity, Credit, and Equity Risk

- Corporate Funding / Equity Management
- Access to Capital Markets
- Debt Maturity Profile
- Flexibility in Capital Spending Budget
- Contingency Funding
- Collateral Requirements
- Capital Availability
- Fund Diversification
- Credit Risk Management/Credit Downgrade

Cash Flow Risk

- Daily Operational Funding
- Cash Flow Projections/Forecasting

Profitability Risk

- Return on Capital / Debt

Market Sensitivity Risk

- Commodity Price
- Commodity Volatility
- Interest Rates
- Security Prices
- Foreign Exchange

Volume Risk

- Attrition
- Economic Factors
- Variable Load

Market Liquidity Risk

- Market Tightness, Depth, and Resilience

Investment Performance Risk

- Reserve Fund



Plan Anual de Auditoría

Determinación del Universo:

Riesgos Tecnológicos



PLAN DE AUDITORÍA

Plan de Auditoría

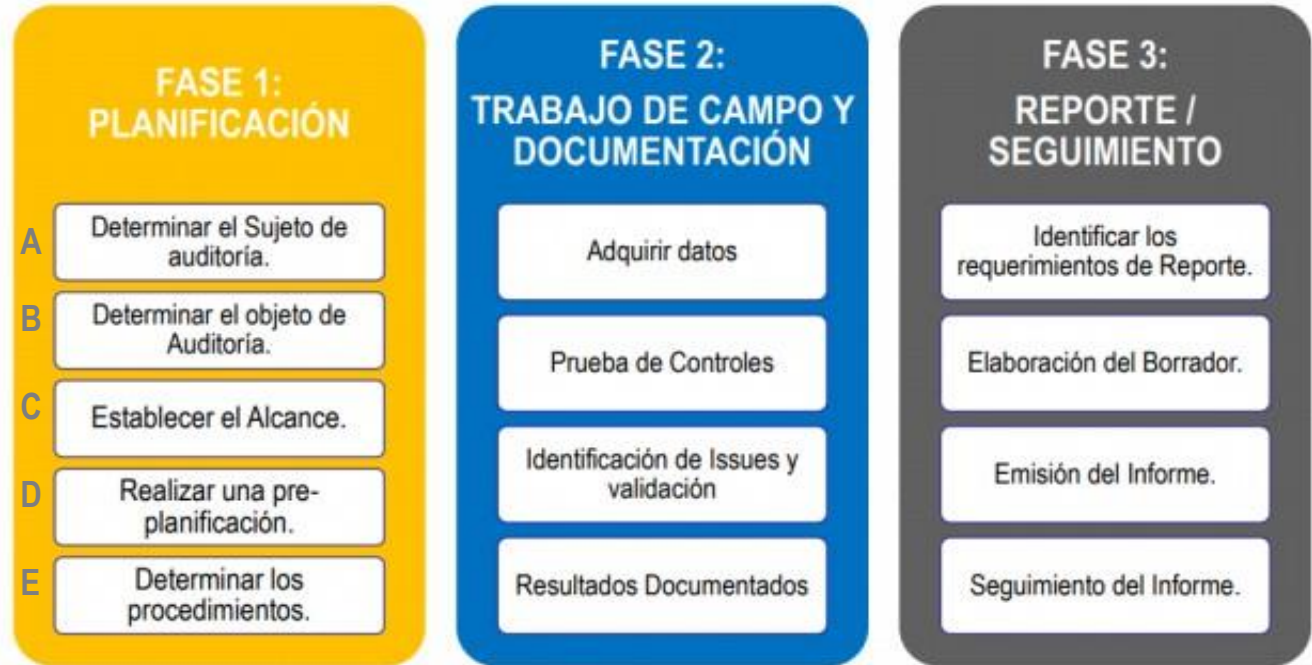


Figura 1. Adaptado y Traducido de «Information System Auditing: Tools and Techniques. Creating Audit Programs», p.6, ©2016 Information Systems Audit and Control Association, Inc. (ISACA). Recuperado de http://www.isaca.org/Knowledge-Center/Research/Documents/IS-auditing-creating-audit-programs_whp_eng_0316.PDF?regnum=. Fecha de consulta: 16.04.2018

Plan de Auditoría

Fase de Planificación

FASE DE PLANIFICACIÓN



Plan de Auditoría

Determinar el sujeto de la auditoria

A. Sujeto de Auditoría

Consiste en identificar el “ELEMENTO” a ser auditado. Existendos escenarios.

1. El sujeto tiene como marco un proceso empresarial específico el cual deberá estar incluido en todas las fases. Por ejemplo, el proceso de ventas, el proceso de marketing, entre otros.
2. El sujeto es un proceso, procedimiento, sistema, tecnología o locación física. Por ejemplo:
 - Proceso de gestión del cambio
 - Proceso de seguridad de la información
 - Cloud Computing
 - Sistema de planificación de recursos empresariales (ERP)
 - Centro de datos, Red privada virtual (VPN)
 - Gobierno y gestión de TI
 - Base de datos.

Plan de Auditoría

Determinar el objetivo de la auditoria

B. Objetivo de Auditoría: Objetivo General y Criterios – objetivos específicos

Los objetivos se dividen en dos (2)

Objetivo General.-

El Objetivo General es el propósito primordial que se quiere alcanzar al realizar la Auditoria Informática, expresándose de manera global.

Criterios.-

Es un conjunto de requisitos que el auditor tiene que verificar su cumplimiento, existencia, idoneidad en el sujeto de auditoría.

Objetivos específicos (basado en Criterios de auditoría).-

Describen los aspectos específicos, los que sumados dan respuesta al objetivo general de la Auditoria.

$$\text{Obj Esp 1} + \text{Obj Esp 2} + \dots + \text{Obj Esp N} = \text{Obj Gen}$$

Plan de Auditoría

Determinar el alcance de la auditoria

C. Alcance de Auditoría

Consiste en identificar los sistemas, funciones o unidades específicos de la organización que se incluirán en la revisión.

Por ejemplo:

- a) **Sujeto**: Proceso de Gestión de Cambios a Programas de la organización.
- b) **Objeto**: Determinar si el proceso de Gestión de Cambios a Programas cuenta con un adecuado control interno y se lleva a cabo utilizando de manera eficiente y eficaz los recursos asignados.
- c) **Alcance**: Se validarán los cambios hechos al módulo de cobranzas.

Plan de Auditoría

Realizar una pre planificación de la auditoria

D. Realizar una Pre - Planificación

Una vez definido el alcance, se debe establecer los objetivos específicos de la auditoria, para lo cual el auditor se apoya en tres fuentes de información:

1. **Evaluación de riesgos**: para establecer el alcance final de una auditoría basada en el riesgo. También puede incluir la evaluación de riesgos realizadas por otros tipos de auditorías (por ejemplo, cumplimiento). Realizar una evaluación del riesgo ayuda a **justificar el compromiso y refinar el alcance** y pre planning focus. Ver “*MRC-1-Plantilla Matriz de Riesgos y Controles*”
2. **Entrevista**: Esta fase se construye producto de la entrevista a auditados clave, con el objetivo de preguntar sobre las actividades o áreas de interés que deben incluirse en el alcance de la contratación, los requisitos de cumplimiento normativo, entre otros
3. **Establecer el Equipo de Auditoría**
4. **Presupuesto**
5. **Cronograma de Trabajo**
6. **Fuentes de Información**
7. **Criterios**

Plan de Auditoría

D. Realizar una Pre - Planificación

Cronograma del Trabajo

| CRONOGRAMA Y PLAZOS DE ENTREGA DE DOCUMENTOS | | | |
|--|-------------------|-------------------|--------------|
| FASES /ACTIVIDADES | FECHAS | | DIAS HABILES |
| | DEL | AL | |
| FASE 1: PLANIFICACIÓN | 12/01/2022 | 25/01/2022 | 10 |
| ACREDITAR E INSTALAR EL EQUIPO DE AUDITORÍA | 12/01/2022 | 13/01/2022 | 2 |
| DETERMINAR DEL SUJETO, OBJETIVO, ALCANCE, CRITERIOS, INTEGRANTES DEL EQUIPO DE AUDITORÍA, PRESUPUESTO, CRONOGRAMA DE TRABAJO Y PROCEDIMIENTOS DE AUDITORÍA | 14/01/2022 | 21/01/2022 | 6 |
| ELABORAR Y APROBAR DEL PLAN DE AUDITORÍA DEFINITIVO | 24/01/2022 | 25/01/2022 | 2 |
| FASE 2: TRABAJO DE CAMPO Y DOCUMENTACIÓN | 26/01/2022 | 30/03/2022 | 46 |
| ADQUIRIR DATOS PARA APLICAR PROCEDIMIENTOS DE AUDITORÍA | 26/01/2022 | 9/02/2022 | 11 |
| PROBAR CONTROLES (APLICAR PROCEDIMIENTOS DE AUDITORÍA) | 10/02/2022 | 14/03/2022 | 23 |
| IDENTIFICAR HALLAZGOS Y VALIDAR. IDENTIFICAR CONTROLES INTERNOS ELABORAR, COMUNICAR, REVISAR DESCARGOS DE HALLAZGOS. | 15/03/2022 | 22/03/2022 | 6 |
| DOCUMENTAR EVIDENCIAS | 23/03/2022 | 30/03/2022 | 6 |
| FASE 3: REPORTE Y SEGUIMIENTO | 31/03/2022 | 13/04/2022 | 10 |
| IDENTIFICAR LOS REQUERIMIENTOS DEL REPORTE Y ELABORAR BORRADOR DEL INFORME | 31/03/2022 | 7/04/2022 | 6 |
| EMITIR EL INFORME | 8/04/2022 | 12/04/2022 | 3 |
| REVISAR, APROBAR, COMUNICAR Y PLANEAR SEGUIMIENTO | 13/04/2022 | 13/04/2022 | 1 |

Plan de Auditoría de Sistemas

E. Determinar los procedimientos

En esta etapa del proceso de auditoría, el equipo de auditoría debe tener suficiente información para identificar y seleccionar el enfoque o estrategia de auditoría y comenzar a desarrollar el **programa de auditoría**. Algunas de las actividades específicas en este paso vinculadas a la evaluación de los controles existentes son:

- Identificar y obtener políticas, estándares y directrices departamentales para su revisión.
- Identificar los requisitos de cumplimiento normativo.
- Identificar una lista de individuos para entrevistar.
- Identificar métodos (incluyendo herramientas) para realizar la evaluación.
- Desarrollar herramientas y metodología de auditoría para probar y verificar los controles.
- Desarrollar scripts de prueba.
- Identificar criterios para evaluar la prueba.
- Definir una metodología para evaluar que la prueba y sus resultados son precisos (y repetibles si necesario).

PROGRAMA DE AUDITORÍA

| PROGRAMADO INICIALES DEL AUDITOR | PROCEDIMIENTOS DE AUDITORÍA | | TERMINADO | | |
|--|-------------------------------------|---|------------------------|--------------|--------------|
| | | | FECHA DE CONCLUSIÓN | HECHO POR | REF. DOC. |
| | OBJETIVO ESPECÍFICO N° 1 | VERIFICAR QUE EL CONTROL IMPLEMENTACIÓN DE MEDIDAS NECESARIAS PARA ASEGURAR QUE LAS PARTIDAS PRESUPUESTALES INCLUYA RECURSOS SUFICIENTES PARA EL PAGO DE LICENCIAS DE SOFTWARE POR ADQUIRIR, EN LOS CASOS QUE PROCEDA DICHO PAGO. | | | |
| MAC | PROCEDIMIENTO N° 1 | | | | |
| | DETALLE | Verificar si en el último año se asignó una partida presupuestaria para la adquisición de software o programas y determine si las mismas se ejecutaron de acuerdo con una programación determinada. | | | |
| MCS | PROCEDIMIENTO N° 2 | | | | |
| | DETALLE | Identificar quien toma la decisión de adquisición del software en la entidad, evaluando si se encuentra sustentado en informes técnicos dichas adquisiciones. Verificar si se cuenta con políticas para la adquisición de estos. | | | |
| VAC | PROCEDIMIENTO N° 3 | | | | |
| | DETALLE | Verificar si se lleva algún tipo de control de costos por concepto de mantenimiento de software. | | | |

Documentación Básica de Auditoría

Papeles de trabajo



Toda la documentación generada durante la realización de una auditoría por parte del equipo auditor es denominada *papeles de trabajo (work papers)*.

Características:

- Facilitan la elaboración del informe final
- Deben incluir notas y explicaciones de la forma de trabajo efectuado por el equipo auditor, las razones que le asistieron para seguir ciertos procedimientos u omitir otros y su opinión respecto a la calidad de la información examinada
- Le pertenecen al equipo auditor, aunque el auditado podría solicitar se incluyan en el informe final



El Informe de auditoría

Documento que se elabora a lo largo de la auditoría y que recoge los hallazgos más significativos identificados en ella.

Muestran finalmente, el resultado de la evaluación de los criterios planteados al inicio de la auditoría.

Versiones:

- Resumen ejecutivo: versión corta de carácter gerencial
- Informe técnico: para las partes interesadas en corregir los hallazgos
- Informe en extenso: resumen ejecutivo + informe técnico + anexos que pueden incluir los papeles de trabajo



Estructura del informe final de auditoría

1. Título que indique el área y objetivo general de la auditoría, junto con el período de tiempo que le corresponda.
2. Breve introducción del proceso seguido: declaración de objetivos específicos, limitaciones, alcance, período cubierto, breve descripción de los procesos, referencias, marco legal y definiciones de términos si fuese necesario.
3. Áreas involucradas y auditadas junto con la relevancia e impacto de la auditoría en ellas.
4. Niveles de distribución del documento (público y sus accesos correspondientes)
5. Conformación del equipo de auditoría con los roles desarrollados. En algunos casos se puede incluso hacer mención a nombres de personas mientras que en otros se prefiere hacer referencia a cargos administrativos.

Técnicas de recopilación de evidencia

- Revisión de las estructuras organizacionales de TI.
- Revisión de políticas y procedimientos de TI.
- Revisión de estándares.
- Revisión de documentación.
- **Entrevistas.**



Referencias bibliográficas

- [ISACA, 2009] ISACA International. The Risk IT Framework. ISACA Publishing, USA (2009)
- [ISO, 2018a] The International Organization for Standardization. ISO 31000:2018 Risk Management- Principles and Guidelines. ISO, Suiza (2018).
- [ISO, 2018b] International Stardart Organization. *Norma ISO/IEC 19011:2018. Directrices para la auditoría de Sistemas de Gestión*. ISO, Suiza (2018)

¿Consultas?



LA PLANIFICACIÓN DEL PROCESO DE AUDITORÍA