



# Auditoría Ofimática

***Auditoria ofimática es la que se realiza sobre el sistema informatizado que genera, procesa, almacena, recupera, comunica y presenta datos relacionados con el funcionamiento del software de oficina***

### Herramientas que incluyen:

- Aplicaciones de productividad personal
- Administradores de Bases de Datos
- Hojas de cálculo
- Procesadores de Textos
- Presentadores de ideas
- Gráficos


El escritorio virtual y el trabajo cooperativo.

## **PROBLEMAS se deben a Características específicas que presenta el ambiente ofimático**

La distribución de las aplicaciones por los diferentes departamentos de la organización en lugar de encontrarse en una única ubicación centralizada;

El traslado de la responsabilidad sobre ciertos controles de los sistemas de información a usuarios finales no dedicados profesionalmente a la informática,

## Como consecuencia de estas características

- 
- adquisiciones poco planificadas;
  - desarrollos ineficaces e ineficientes,
  - falta de conciencia de los usuarios acerca de la seguridad de la información;
  - utilización de copias ilegales de aplicaciones informáticas,
  - procedimientos de copias de seguridad deficientes;
  - escasa formación de personal;
  - ausencia de documentación suficiente, entre otros aspectos.

# CONTROLES

Los controles han sido agrupados siguiendo el criterio de:

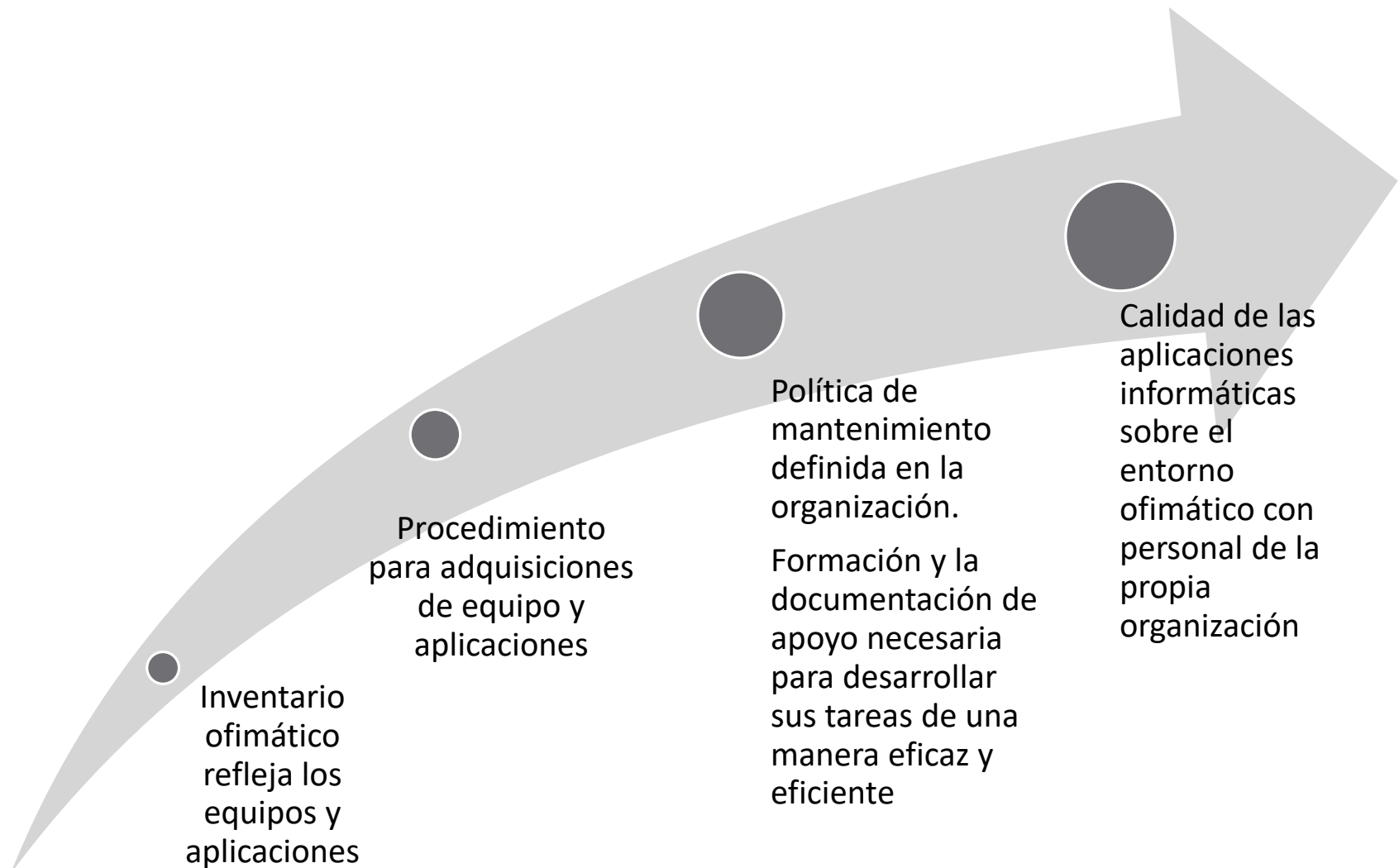
Economía

- Economía, eficacia y eficiencia;

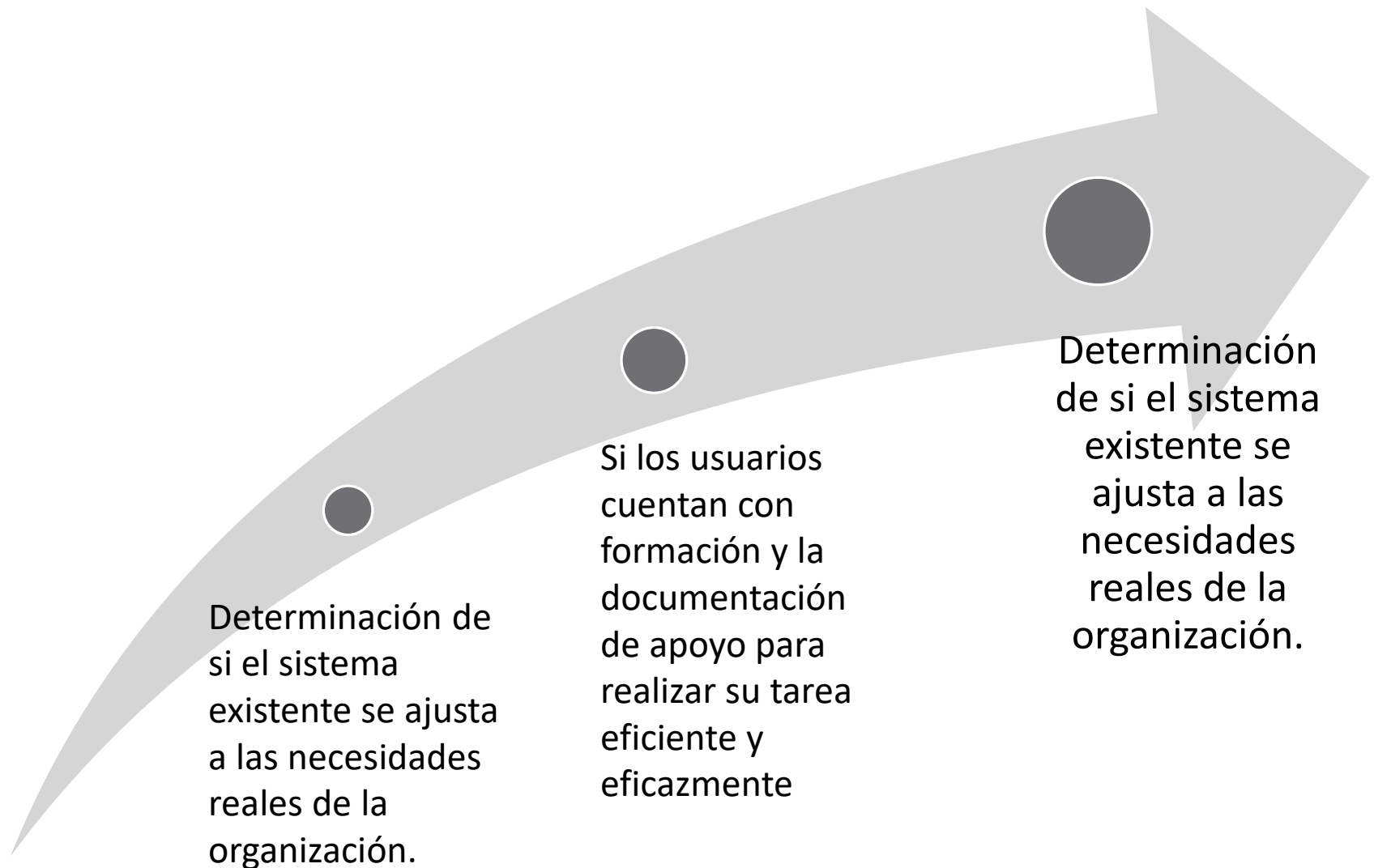
Seguridad

- Seguridad y condicionantes legales,


# ECONOMÍA, EFICACIA Y EFICIENCIA



# ECONOMÍA, EFICACIA Y EFICIENCIA



# SEGURIDAD



● Proporcionan información reservada tales como agendas, contactos, informes confidenciales, estadísticas,

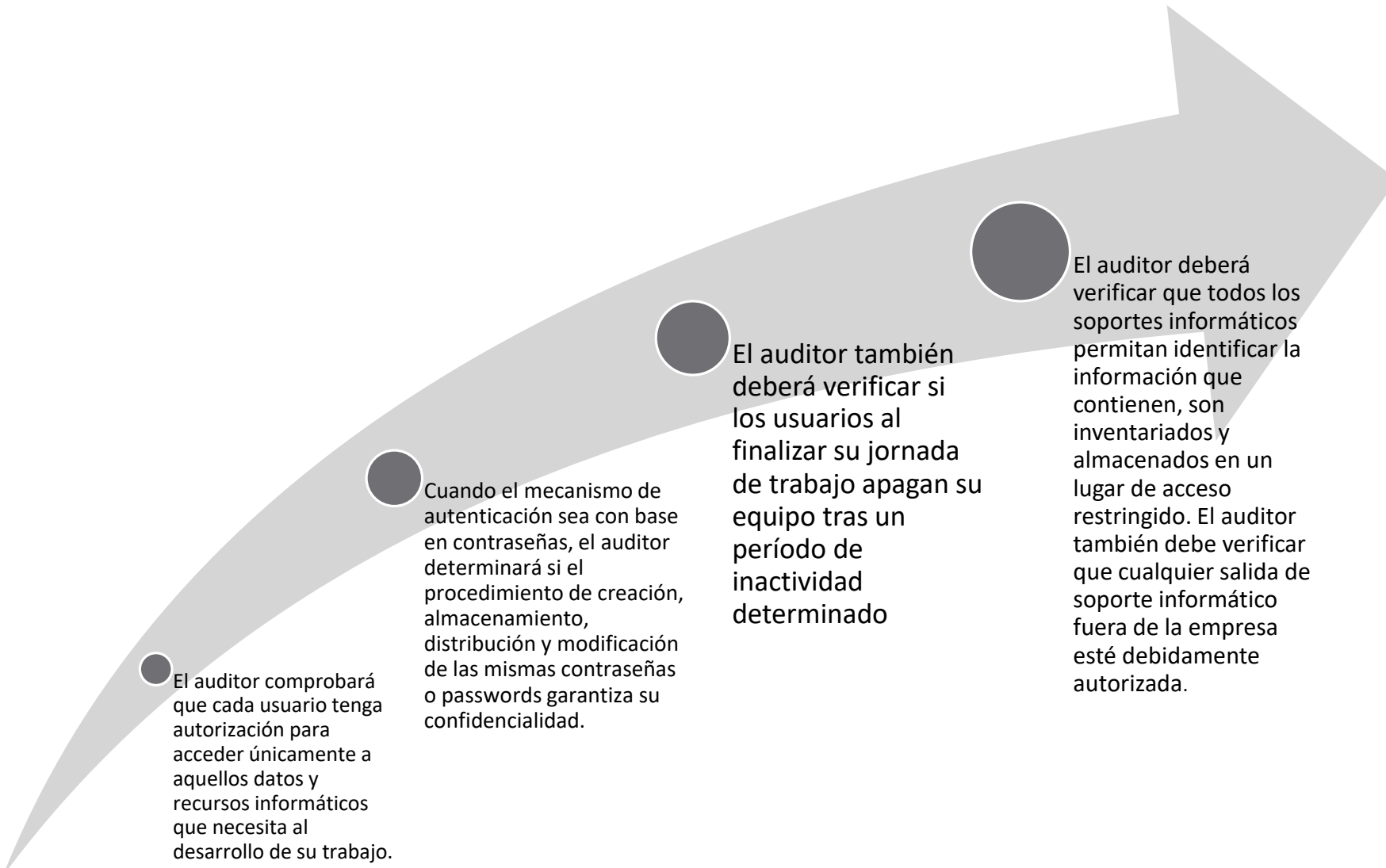
● Garantizar políticas y procedimientos de seguridad para garantizar la confidencialidad, integridad y disponibilidad de la información almacenada en la base de datos.

● Examinar la documentación y comprobará los procedimientos de clasificación de la información, control de acceso, identificación y autenticación, gestión de reportes, gestión de incidencias y controles de auditoría.

● El auditor deberá comprobar que el procedimiento de clasificación de la información establecido ha sido elaborado atendiendo a la sensibilidad e importancia de la misma, y deberá comprobar que toda la información ha sido clasificada en función de los criterios establecidos.

● Verificar funciones, obligaciones y responsabilidades en materia de seguridad, de cada puesto de trabajo están claramente definidas y documentadas,





El auditor comprobará que cada usuario tenga autorización para acceder únicamente a aquellos datos y recursos informáticos que necesita al desarrollo de su trabajo.

Cuando el mecanismo de autenticación sea con base en contraseñas, el auditor determinará si el procedimiento de creación, almacenamiento, distribución y modificación de las mismas contraseñas o passwords garantiza su confidencialidad.

El auditor también deberá verificar si los usuarios al finalizar su jornada de trabajo apagan su equipo tras un período de inactividad determinado

El auditor deberá verificar que todos los soportes informáticos permitan identificar la información que contienen, son inventariados y almacenados en un lugar de acceso restringido. El auditor también debe verificar que cualquier salida de soporte informático fuera de la empresa esté debidamente autorizada.

**1. Evaluación del inventario ofimático; si refleja con exactitud los equipos y aplicaciones de la oficina existente en cada una de las áreas.**

Aspectos a evaluar:

**A) Examinar el proceso de adquisición de hardware y aplicaciones.**

**Actividades:**

1. Comprobar si se han establecido políticas y estándares, relacionados con la adquisición, uso y control de los recursos de hardware y aplicaciones.
2. Comprobar si existe un plan de compras o adquisiciones de recursos informáticos con base en las necesidades actuales de la institución.
3. Examinar como se lleva a cabo el proceso de compra de los recursos de hardware y aplicaciones de la institución.

## **B) Evaluar la fiabilidad del inventario ofimático de cada una de las áreas de la institución.**

- a) Comprobar que en la institución existan mecanismos que garanticen que los equipos y aplicaciones adquiridas son debidamente inventariados.
- b) Elaborar una relación exhaustiva de los equipos informáticos, aplicaciones y archivos que residen en la institución.
- c) Contrastar la relación elaborada con el inventario oficial y adquisiciones de la institución.
- d) Verificar si la jefatura de los departamentos usuarios, participan activamente en el proceso de actualización del inventario ofimático de la institución.
- e) Comprobar que se evalúan periódicamente los cambios de ubicación de los recursos informáticos.
- f) Verificar si cada empleado firma su hoja de afectación de equipos

## **C) Examinar el inventario de licencias de software**

1. Comprobar la existencia de un procedimiento de control para la adquisición y registro de licencias.
2. Verificar que todo software instalado en la institución cuenta con licencia actualizada

## **2-Evaluación de la calidad de las aplicaciones del entorno ofimático de desarrollo por personal de la propia institución.**

### **A) Comprobar la existencia de un departamento responsable del control del desarrollo de aplicaciones de toda la institución.**

- a) Verificar si existen procedimientos generales de petición, autorización, programación y entrega de aplicaciones.
- b) Constatar si existen otros departamentos que desarrollen aplicaciones de uso interno, sin el control del centro de información.
- c) Verificar que las aplicaciones se realizan sobre un entorno de desarrollo, evitando operar directamente sobre los datos reales de explotación.
- d) Verificar si existe un registro de incidencias de las aplicaciones, así como de las reclamaciones manifestadas por los clientes y usuarios, a fin de detectar aquellas aplicaciones que podrían estar funcionando de manera irregular.

## **B) Evaluar las situaciones de integración y de incompatibilidad entre las nuevas aplicaciones instaladas y las existentes con anterioridad.**

### Actividades:

- a) Verificar si existen procedimientos formales para la autorización, aprobación, adquisición de nuevas aplicaciones y cambios de versiones dentro de la institución
- b) Comprobar si se han analizado los problemas de integración y las incompatibilidades que pueden presentar las nuevas aplicaciones previas a su implantación, que constan en actas, informes, etc.
- c) Comprobar si se ha elaborado un plan de capacitación de los usuarios, con la finalidad de que los cambios no impacten negativamente en funcionamiento de la institución.
- d) Verificar que el personal capacitado cuente con la documentación básica de operatividad de las aplicaciones, con el propósito de acceder a ella en caso de una ocurrencia.

### **C. Evaluar si la(s) aplicación(es) existente se ajusta a las necesidades reales de la institución.**

#### **Actividades:**

- a) Revisar las actividades que se ejecutan en cada equipo, a fin de determinar tareas que necesitan ser automatizados o precisen actualizar los equipos existentes.
- b) Comprobar que los puestos de trabajo, debido a su escasa actividad no se encuentre sobredimensionados.
- c) Elaborar una relación con recomendaciones sobre descatalogación de productos obsoletos, redistribuciones y adquisiciones de nuevos equipo y aplicaciones.