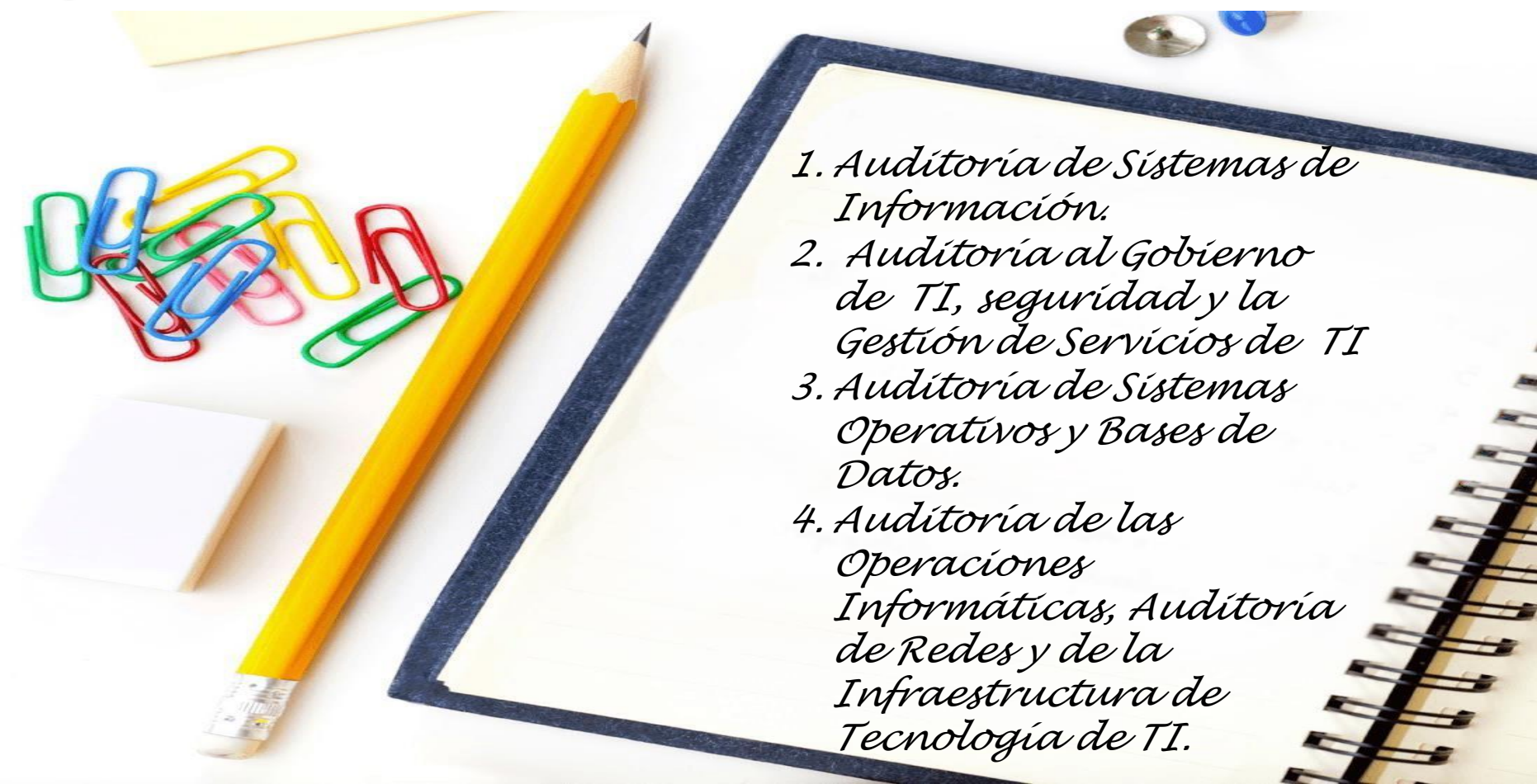


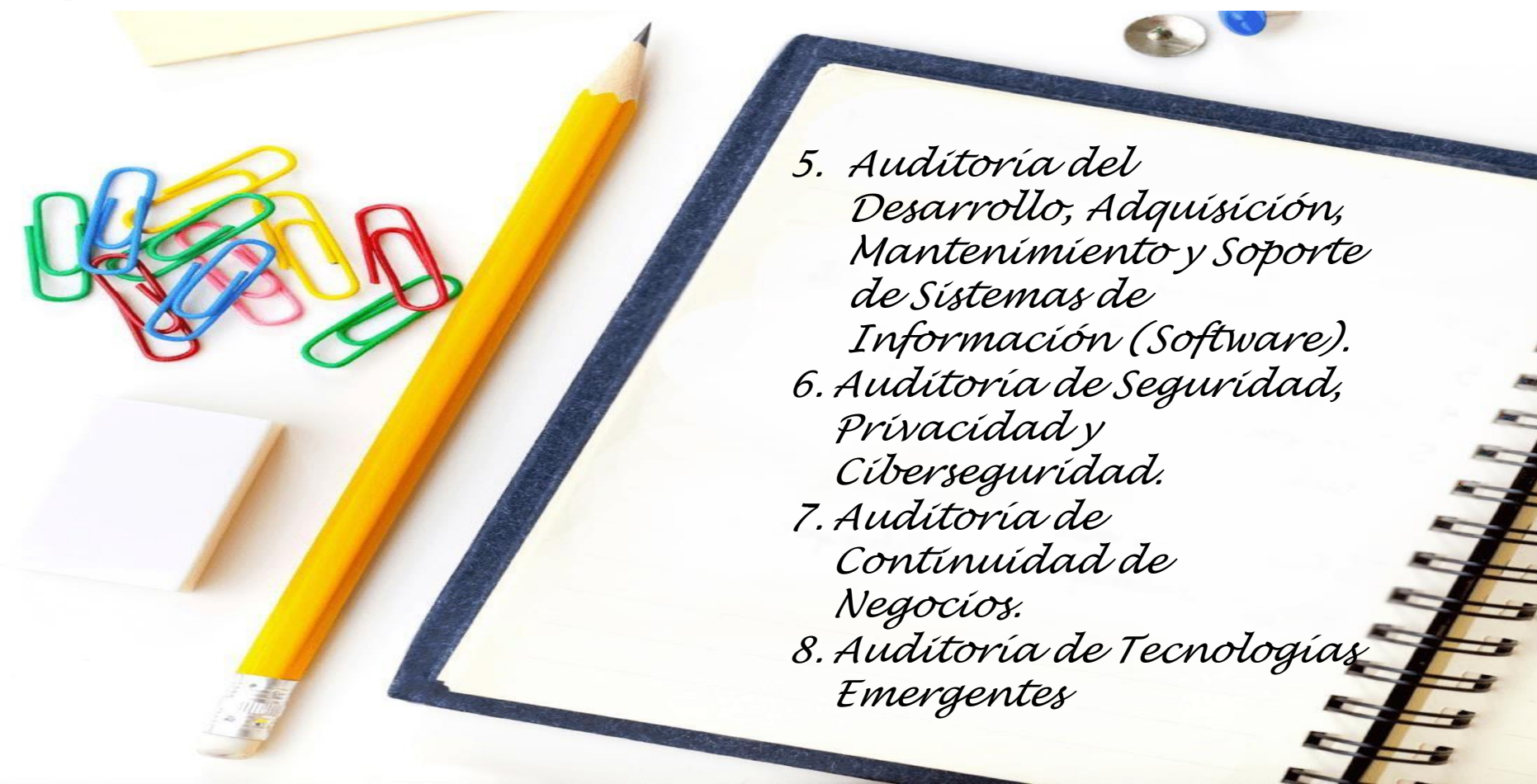
AUDITORÍA Y CONTROL DE SISTEMAS

TIPOS DE AUDITORÍAS DE SISTEMAS

Agenda

- 
1. *Auditoría de Sistemas de Información.*
 2. *Auditoría al Gobierno de TI, seguridad y la Gestión de Servicios de TI*
 3. *Auditoría de Sistemas Operativos y Bases de Datos.*
 4. *Auditoría de las Operaciones Informáticas, Auditoría de Redes y de la Infraestructura de Tecnología de TI.*

Agenda

- 
5. *Auditoría del Desarrollo, Adquisición, Mantenimiento y Soporte de Sistemas de Información (Software).*
 6. *Auditoría de Seguridad, Privacidad y Ciberseguridad.*
 7. *Auditoría de Continuidad de Negocios.*
 8. *Auditoría de Tecnologías Emergentes*

TIPOS DE AUDITORÍAS DE SISTEMAS

Auditoría de Sistemas de Información

Definición

Este proceso **recolecta y evalúa la evidencia para determinar si los sistemas de información de una organización y sus recursos relacionados:**

- ✓ Manejan información relevante y confiable
- ✓ Proveen soporte a los procesos de negocio y a lograr de forma efectiva los objetivos organizacionales
- ✓ Usan eficientemente los recursos y constituyen inversiones eficientes
- ✓ Proveen una certeza razonable de que los objetivos de negocio, operacionales y de control relacionados con estos sistemas serán alcanzados y que cualquier desviación será evitada o detectada forma oportuna.



Auditoría al Gobierno de TI, al Gobierno de Seguridad de la Información, a la Gestión de Servicios de TI

Definición

Gobierno de TI

Este proceso **recolecta y evalúa la evidencia para determinar si la estructura organizacional de la empresa permite alcanzar los objetivos de negocio, haciendo que las TI sean seguras (riesgos) y aporten valor.**

Gobierno de la Seguridad de la Información

Este proceso **recolecta y evalúa la evidencia para determinar si la organización mantiene seguras las TIC y la información relacionada, garantizando los objetivos del negocio.**

Gestión de Servicios de TI

Este proceso **recolecta y evalúa la evidencia para verificar si los servicios de TI otorgan valor a la organización y a las partes interesadas.**



Auditoría de Sistemas Operativos y Bases de Datos

Definición

Este proceso **recolecta y evalúa la evidencia para determinar:**

- ✓ Si los sistemas operativos son adecuados a la infraestructura de la organización.
- ✓ Si permiten el correcto funcionamiento de los sistemas de información que aloja.
- ✓ Si las bases de datos están convenientemente diseñadas, operadas, mantenidas, optimizadas y protegidas
- ✓ Existe segregación de funciones en el personal a cargo de base de datos y desarrollo de aplicaciones.



Auditoría de las Operaciones Informáticas, Auditoría de Redes y de la Infraestructura de Tecnología de TI

Definición

Este proceso **recolecta y evalúa la evidencia para determinar:**

- ✓ Las operaciones informáticas se realizan de manera adecuada, siguiendo las políticas y procedimientos vigentes.
- ✓ La infraestructura de red, telecomunicaciones y hardware es idónea, da soporte adecuado a los procesos de negocio aportando valor para la consecución de los objetivos de negocio.

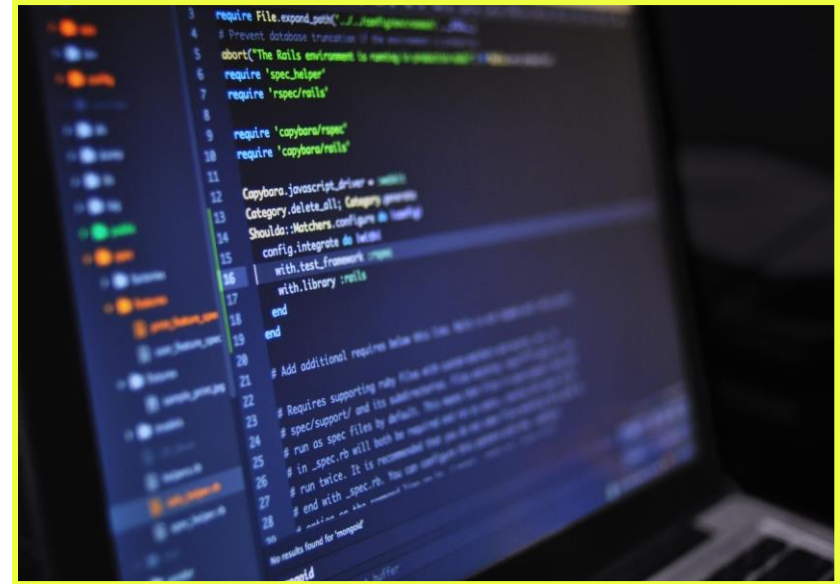


Auditoría del Desarrollo, Adquisición, Mantenimiento y Soporte de Sistemas de Información (Software).

Definición

Este proceso **recolecta y evalúa la evidencia para determinar (donde aplique):**

- ✓ Si el desarrollo de software genera productos de calidad, al seguir buenas prácticas relacionadas.
- ✓ Si el proceso de adquisición es adecuado, conforme a la regulación vigente y siempre procurando los intereses de la organización.
- ✓ Si el mantenimiento de los sistemas de información es brindado de manera oportuna y adecuada.
- ✓ Si el soporte a la operativa de los sistemas (help desk) es el adecuado
- ✓ El personal responsable (interno o externo) tiene las competencias adecuadas.



Auditoría de Seguridad, Privacidad y Ciberseguridad

Definición

Este proceso **recolecta y evalúa la evidencia para determinar**:

- ✓ Si los activos de información y la información misma, se encuentra convenientemente protegidos.
- ✓ Si la información personal se encuentra conveniente protegida, de acuerdo a la regulación vigente.
- ✓ Si la infraestructura de TI se encuentra suficientemente preparada para hacer frente a un ciberataque.

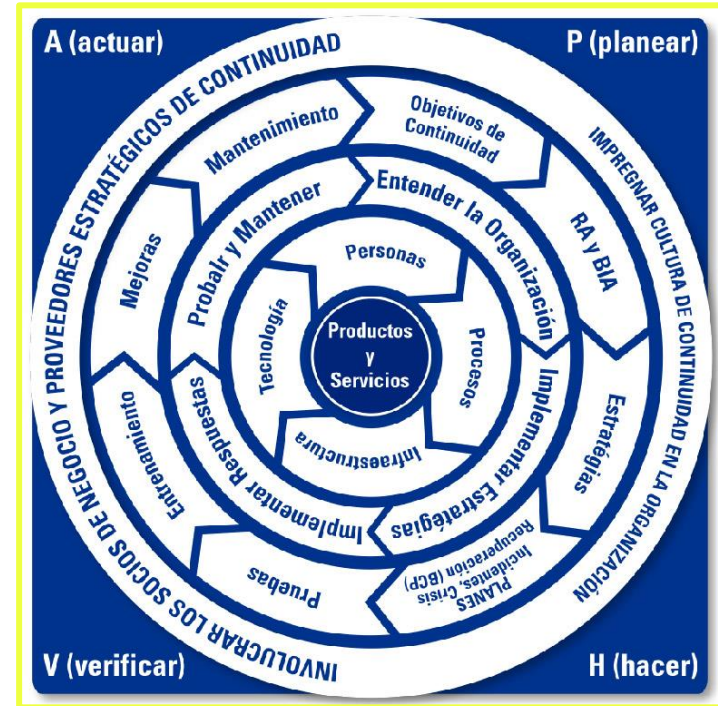


Auditoría de Continuidad de Negocios

Definición

Este proceso **recolecta y evalúa la evidencia para determinar**:

- ✓ Si se han definido los procedimientos y planes adecuados, suficientes y necesarios para hacer frente a cualquier amenaza que ponga en riesgo la ejecución de los procesos de negocio, procurando su reactivación de manera celera y dentro de márgenes de costos aceptados por la organización.
- ✓ Si los planes de continuidad de negocios, recuperación ante desastres, contingencia de TI son adecuados
- ✓ Si el personal responsable se encuentra suficientemente preparado para ejecutar los planes.



Auditoría de Tecnologías Emergentes

Definición

El uso de tecnologías emergentes como Big Data, Data Analytics, IoT, Cloud Computing, entre muchas otras también puede ser sujeto de auditoría con el objetivo de determinar:

- ✓ Si el costo-beneficio de la tecnología emergente es adecuado.
- ✓ Si los riesgos que traen estas nuevas tecnologías están convenientemente identificados y tratados (lo que se convierte en una auditoría de seguridad)
- ✓ Si proveen información relevante y confiable
- ✓ Si logran de forma efectiva las metas organizacionales



Referencias bibliográficas

- ISACA (2018). Certified Information Systems Auditor (CISA) Exam Preparation Guide. ISACA Publishing, USA (2018).
- Tupia (2011). Principios de auditoría de sistemas y tecnologías de información. Tupia Consultores Y Auditores S.A.C., Perú.

¿Consultas?



AUDITORÍA DE SISTEMAS DE INFORMACIÓN Y OTROS TIPOS TECNOLÓGICOS RELACIONADOS