UAI

UNIVERSIDAD ABIERTA INTERAMERICANA

FACULTAD DE TECNOLOGIA INFORMATICA INGENIERIA EN SISTEMAS INFORMÁTICOS

AUDITORIA DE SISTEMAS

Actividad Nro 1

Docentes: Casco, Maria Eugenia

Alumno: Di Domenico, Nicolás.

Comisión: 5° A.

Turno: Mañana.

Año: 2025.

1. ¿Qué factores crees que podrían aumentar el riesgo de auditoría en un sistema informático y cómo podrían impactar en la confiabilidad de los resultados de una auditoría?

Los factores que pueden aumentar el riesgo de auditoría en un sistema informático incluyen:

- Deficiencias en los controles internos: cuando no existen controles preventivos, detectivos o correctivos, el riesgo residual aumenta y se compromete la confiabilidad de la información auditada.

- Frecuencia de fallos tecnológicos: fallos en software crítico, pérdida de datos o interrupciones del servicio incrementan la posibilidad de errores en la información financiera.

- Accesos no autorizados: la falta de seguridad en el acceso puede alterar registros clave, afectando la veracidad de los resultados.

- Riesgos humanos: errores de los usuarios o fraudes intencionales elevan la posibilidad de información inexacta.

Con respecto al impacto, estos factores reducen la confiabilidad de la auditoría porque generan información incompleta, manipulada o errónea, lo que puede llevar a conclusiones equivocadas y decisiones erradas.

2. Imagina que eres el auditor de un sistema de gestión de datos financieros en una empresa. ¿Qué tipos de riesgos (tecnológicos, operativos o humanos) identificarías como prioritarios y por qué?

Riesgos tecnológicos

1. Pérdida de datos por fallas en servidores → Alto
2. Ciberataques o accesos no autorizados al sistema → Alto
3. Errores en actualizaciones de software financiero → Medio
4. Caídas de la red que impiden el acceso a la información → Medio

Riesgos operativos

1. Errores en la carga o procesamiento de transacciones → Alto
2. Falta de respaldo periódico de la base de datos → Alto
3. Procesos manuales sin validaciones automáticas → Medio
4. Retrasos en la conciliación de cuentas por fallos logísticos internos → Medio

Riesgos humanos

1. Manipulación fraudulenta de datos contables → Alto
2. Uso indebido de credenciales (compartir contraseñas) → Alto
3. Desconocimiento o falta de capacitación en el sistema → Medio
4. Errores involuntarios en la digitación de datos → Bajo/Medio

Los riegos prioritarios son los de impacto alto (pérdida de datos, ciberataques, fraudes humanos y errores críticos en procesos financieros), porque comprometen directamente la integridad, disponibilidad y confiabilidad de la información financiera auditada.

3. ¿Cómo puede la falta de controles adecuados en un sistema informático afectar la evaluación de riesgos de auditoría y la seguridad de la información de una organización?

En un sistema informático los controles se dividen en preventivos, detectivos y correctivos. La ausencia de cada uno genera impactos directos en la seguridad de la información y en la evaluación de riesgos de auditoría:

1. **Falta de controles preventivos**
    - Qué son: buscan evitar que ocurran incidentes (ej. contraseñas seguras, segregación de funciones, validaciones de entrada de datos).
    - Impacto en la seguridad: sin ellos, aumentan las vulnerabilidades y cualquier amenaza puede concretarse fácilmente (ej. un usuario no autorizado accede a datos financieros).
    - Impacto en la auditoría: el auditor no puede confiar en que el sistema evita errores o fraudes antes de que sucedan. Esto eleva el riesgo de auditoría, porque la información revisada puede estar ya contaminada desde el origen.

2. **Falta de controles detectivos**
    - Qué son: sirven para identificar incidentes una vez ocurridos (ej. registros de auditoría, monitoreo de accesos, reportes de inconsistencias).
    - Impacto en la seguridad: sin estos controles, un acceso indebido o una modificación de datos puede pasar inadvertida, comprometiendo la integridad y trazabilidad de la información.
    - Impacto en la auditoría: el auditor no dispone de evidencias confiables para evaluar lo sucedido, porque no existen logs ni alertas que respalden las conclusiones. Esto limita la posibilidad de medir el riesgo real.

3. **Falta de controles correctivos**

    - Qué son: buscan mitigar el daño después de un incidente (ej. respaldos, planes de recuperación, políticas de restauración de datos).
    - Impacto en la seguridad: si ocurre una pérdida de datos o un fallo del sistema, la organización no puede recuperarse, afectando gravemente la disponibilidad de la información.
    - Impacto en la auditoría: la ausencia de estos controles implica que, frente a un incidente, no hay garantías de continuidad operativa ni de veracidad en la información recuperada. Esto aumenta el riesgo residual y resta confiabilidad a los informes de auditoría.

Bibliografía

Pirani. (s.f.). *Guía de gestión de riesgos desde cero*. Recuperado del PDF provisto por la cátedra.

Pirani. (s.f.). *Guía para realizar la evaluación del riesgo*. Recuperado del PDF provisto por la cátedra.

UAI. (2022). *La Auditoría de Sistemas y sus Alcances*. Presentación en PowerPoint provista por la cátedra.