AUDITORÍA INFORMÁTICA

ING. WENDY OBREGÓN MARTÍNEZ, MG.

ACTIVIDAD1: PRÁCTICA 1

Unidad 1: Fundamentos de la Auditoría Informática

ALCIVAR FUENTES HANSEL ADRIAN

17 DE NOVEMBER DE 2025

Comprender el concepto y la estructura del control interno y representar los 5 componentes de COSO con sus principios aplicados a un proceso real.

El control interno es un conjunto de políticas, procedimientos y actividades diseñadas para garantizar el logro de los objetivos institucionales y la integridad de la información. Su relevancia radica en que permite prevenir errores, evitar fraudes, asegurar la continuidad operativa y fortalecer la gestión organizacional (Marín, 2014).

PROCESO DE BACKUPS

El proceso de *backup* o copia de seguridad implica seleccionar los datos importantes, crear copias de seguridad de esos datos y almacenarlas en un lugar seguro y separado de los originales

1. **Construye un mapa visual (diagrama) que muestre: proceso → riesgos clave → controles → componente COSO.**

Se consideran 10 procesos y 10 controles. Además, se clasifican de acorde a la componente adecuada de COSO

Proceso	Riesgo claves	Control Asociado	Clasificación Componente COSO
Registro de respaldos (logs del software de backup).	Fallos al no ejecutarse los respaldos programados.	Backups automáticos programados.	Actividades de Control
Reporte de ejecución automática.	No detectar errores en la ejecución del backup.	Monitoreo de logs y alertas de fallo.	Actividades de Control
Capturas de pantalla de respaldos completados.	Respaldo incompleto o dañado.	Validación de integridad del backup.	Actividades de Control
Bitácora de restauraciones realizadas.	Imposibilidad de restaurar la información.	Pruebas periódicas de restauración.	Actividades de Control
Calendario o cronograma de backups programados.	Ausencia de respaldo por mala planificación.	Backups automáticos programados.	Información y Comunicación
Actas de auditoría interna.	Incumplimiento de procedimientos.	Auditoría interna anual del proceso.	Monitoreo
Informe mensual del estado de los respaldos.	Falta de supervisión del proceso.	Revisión y firma del jefe TI.	Monitoreo
Listado de servidores/equipos incluidos en el plan.	Omisión de equipos críticos.	Actualización del procedimiento de backup.	Entorno de Control
Política de Backup y Recuperación.	Procedimientos inconsistentes.	Actualización del procedimiento de backup.	Entorno de Control
Procedimiento documentado para realizar y restaurar backup.	Errores humanos por falta de guía.	Actualización del procedimiento de backup.	Entorno de Control

4. Matriz RACI mínima (quién ejecuta, aprueba, consulta, informa).

Roles:

- ✓ RTI: Responsable de TI
- ✓ AI: Administrador de Infraestructura
- ✓ AUD: Auditor Interno
- ✓ USR: Usuario Final

Leyenda:

- ✓ R: Responsable (Hace el trabajo)
- ✓ A: Aprobador (Toma decisiones, autoridad)
- ✓ C: Consultado (Da información o criterio)
- ✓ I: Informado (Debe saber el resultado)

Tarea/Actividad	RTI	AI	AUD	USR
1. Configurar la programación de backups	R	A	C	I
2. Ejecutar los respaldos diarios	A	R	I	I
3. Verificar logs y alertas	R	A	C	I
4. Realizar pruebas de restauración	A	R	C	I
5. Documentar procesos y evidencias	R	A	C	I
6. Controlar accesos a respaldos	A	R	C	I
7. Auditar cumplimiento del proceso	I	I	R	I
8. Reportar fallos o incidentes	R	A	C	I

5. **Concluye con 3 mejoras propuestas (rápidas, medibles y asignables).**

El proceso de Gestión de Backups es crítico para la continuidad y resiliencia organizacional. La aplicación del marco COSO permite estructurar un sistema de control interno robusto que abarca desde la cultura organizacional hasta el monitoreo continuo.
A continuación, se presentan 3 mejoras priorizadas, rápidas de implementar, medibles y con responsables asignados:

1. **Implementación de Backups Inmutables**

Esta mejora consiste en configurar Backups inmutables que no puedan ser modificados o eliminados durante un periodo definido, protegiéndolos contra ransomware y eliminaciones accidentales.

Recursos necesarios:

- Tiempo: 1-2 semanas
- Presupuesto: Posiblemente $0 si el software actual lo soporta; hasta $5,000 si requiere upgrade

Responsable: Administrador de Backups

2. **Automatización de Pruebas de Restauración Mensual**

Podríamos considerar en implementar proceso automatizado que ejecute restauraciones completas de sistemas críticos mensualmente y genere reporte automático de éxito/fallo.

Recursos necesarios:

- Tiempo: 2-3 semanas desarrollo + validación

- Presupuesto: $0 (usando recursos existentes)

Responsable: Administrador de Backups

3. **Dashboard de Métricas en Tiempo Real con Alertas Proactivas**

Consiste en implementar dashboard centralizado que muestre en tiempo real el estado de todos los backups, con alertas proactivas basadas en tendencias (no solo fallos).

Recursos necesarios:

- Tiempo: 2 semanas
- Presupuesto: $0 - $2,000 (dependiendo si requiere licencia de herramienta de visualización)

Responsable: Administrador de Backups

Diagrama (mapa visual) ilustrado.

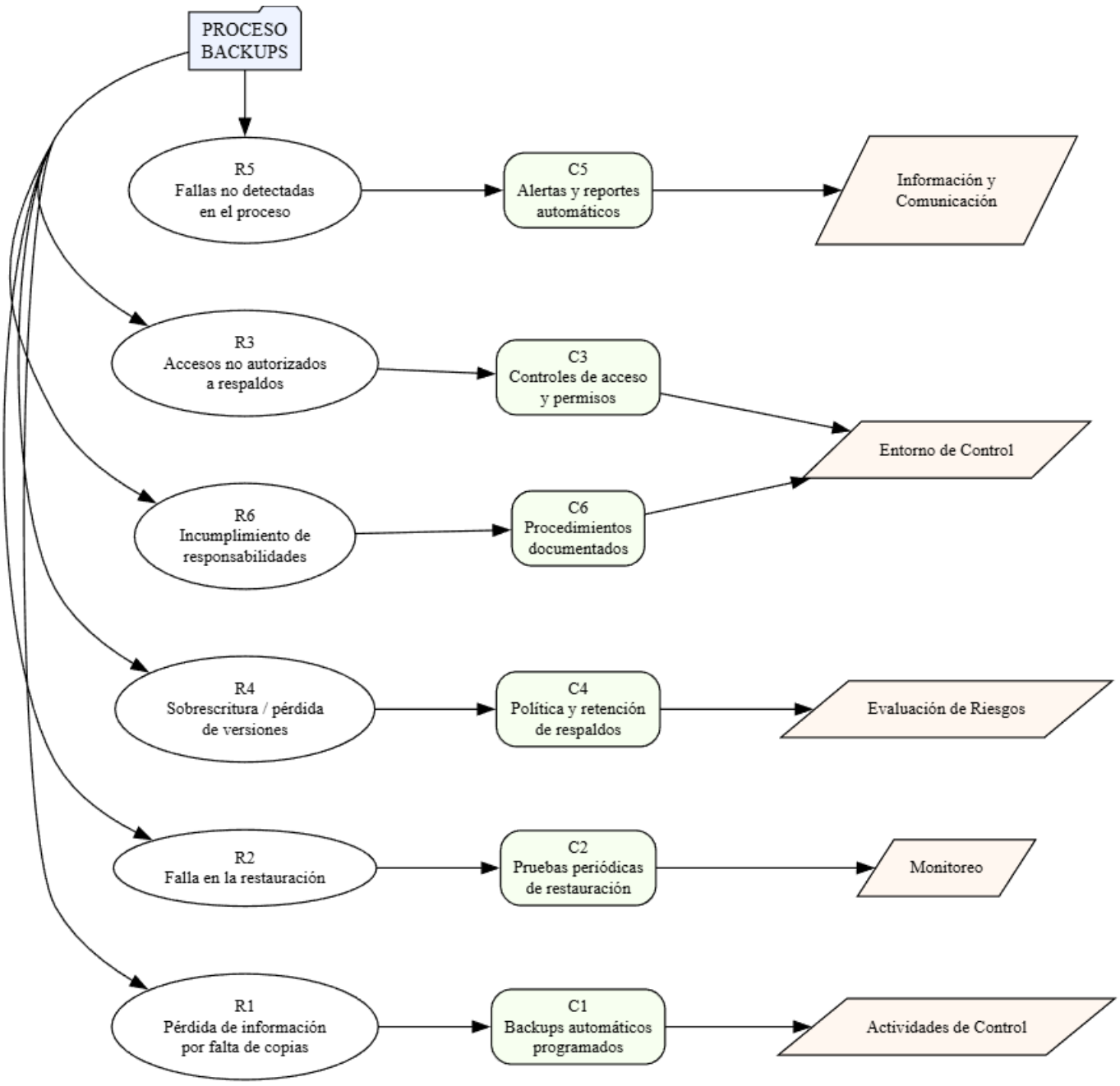

Diagrama: Proceso → Riesgos clave → Controles → Componente COSO

BIBLIOGRAFÍA

Marín, M. S. C. (2014). El control interno basado en el modelo COSO. *Revista de Investigación Valor Contable*, *1*(1). https://doi.org/10.17162/rivc.v1i1.832