




## Etapa 7

---

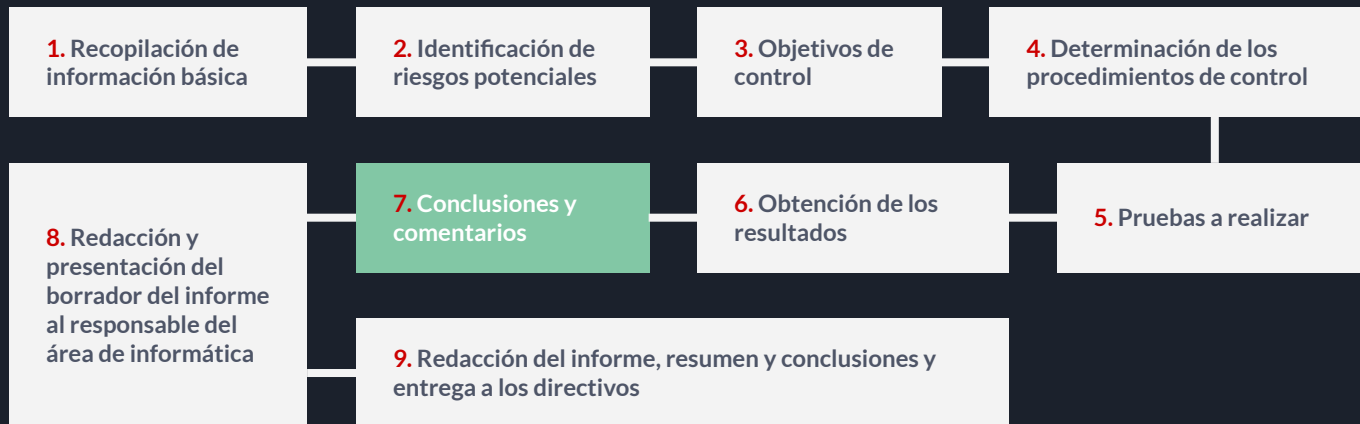
# Conclusiones y comentarios

**Grupos 3 y 4 - Etapa 7**

Ingeniería de Software III - 2021

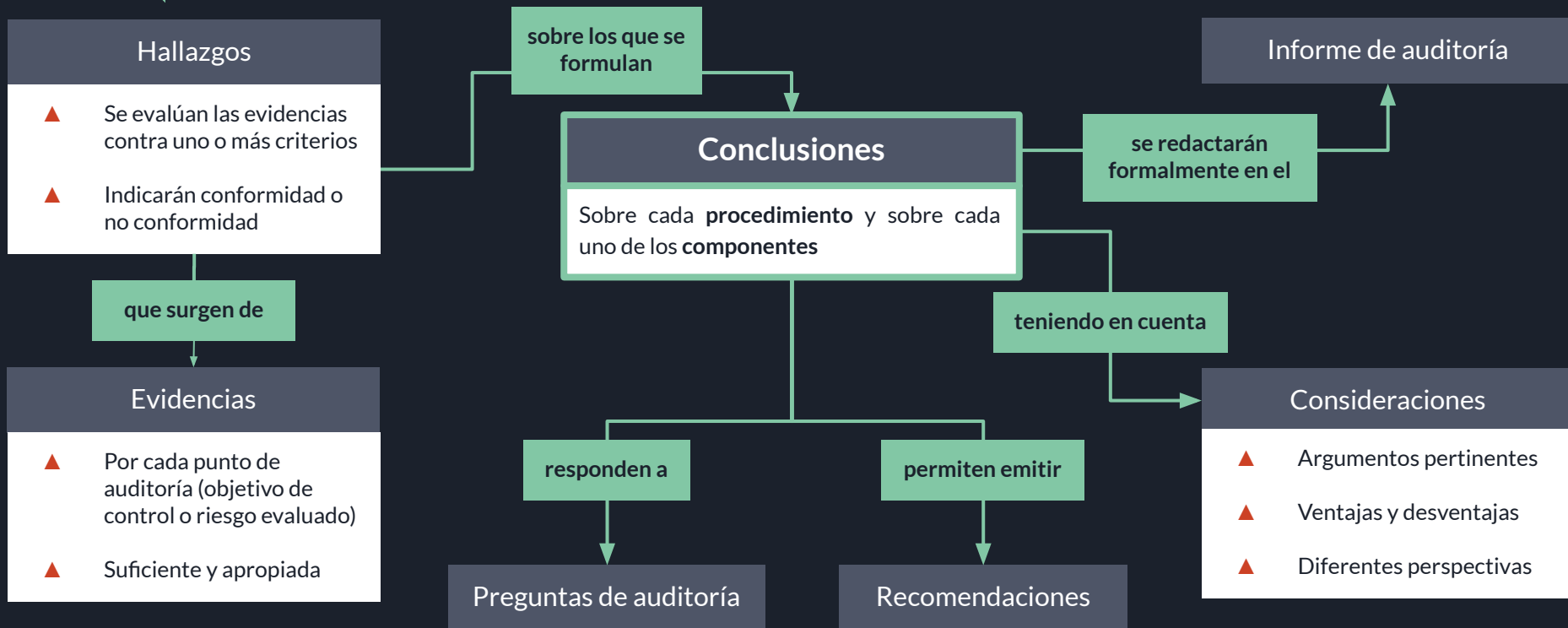


# ¿Dónde se ubica esta **etapa** en el proceso de auditoría?



> Esta etapa está **estrechamente vinculada** con la elaboración del **informe de auditoría**.

# ¿En qué consiste esta **etapa**?



# ¿A qué llamamos **hallazgo**?

(ISO 9000:2015) Un hallazgo de auditoría es el **resultado de evaluar una evidencia frente a un criterio**.

En otras palabras, un hallazgo es cualquier evento, registro, documento, nota, informe obtenido durante la auditoría que nos **permita evaluar si se cumple o no se cumple lo que se está auditando respecto a esos criterios** definidos previamente (decimos que indican conformidad o no conformidad / cumplimiento o no cumplimiento).

Además, pueden conducir a ...

- Identificación de oportunidades para la *mejora*

- Registro de buenas prácticas

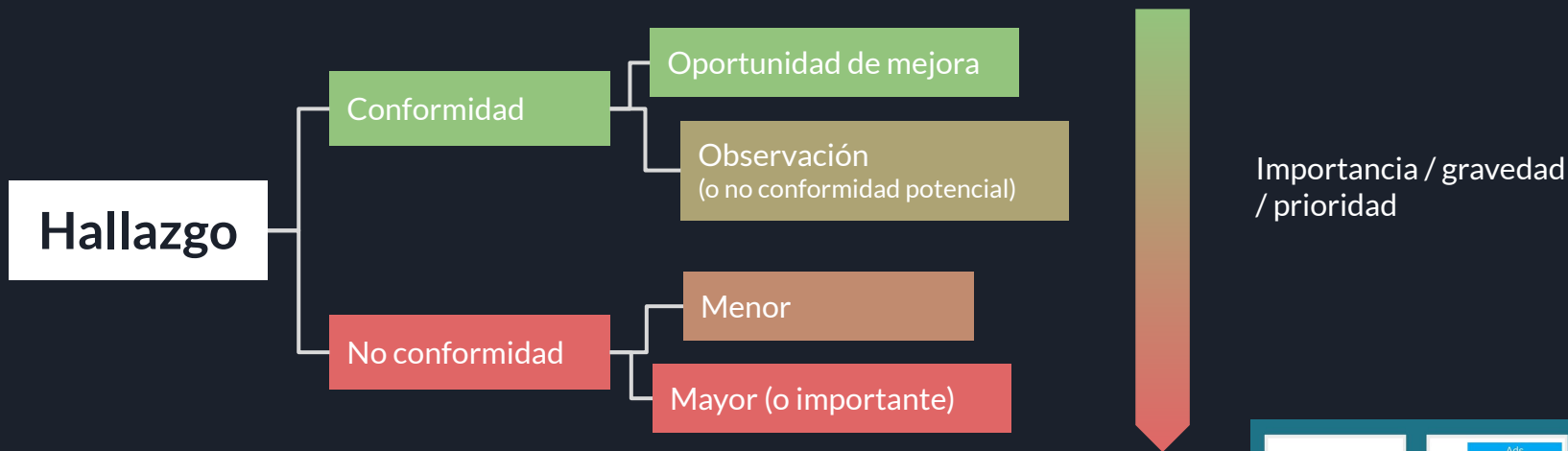
## EJEMPLOS

falta de información sobre la formación de algunos de los empleados

el stock del sistema informático no coincide con el stock físico real



# ¿Cómo podemos **clasificar los hallazgos**?

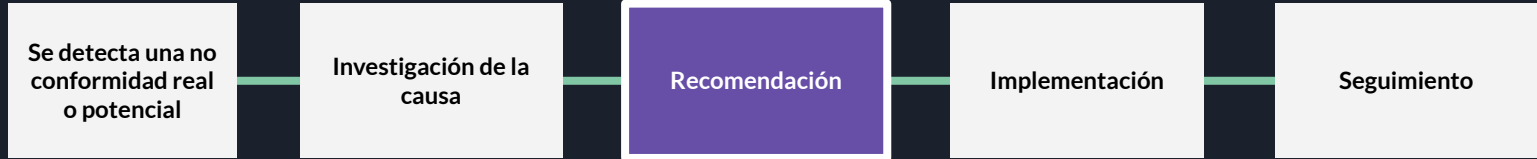


> Dependiendo el tipo de hallazgo, se tomarán **distintos tipos de acciones** o recomendaciones (lo vemos en un ratito)





# Recomendaciones

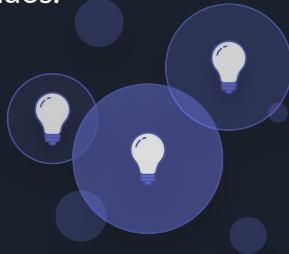


El auditor deberá **emitir la recomendación de los posibles pasos a seguir** para procurar **corregir** las falencias detectadas y así poder **regularizarlas** oportunamente.

Las recomendaciones deben ser formuladas en tono constructivo, teniendo en consideración que las medidas recomendadas sean lo más específicas posibles, factibles de implementar y tengan una relación costo/beneficio apropiada.

Al desarrollar recomendaciones se deben considerar:

- Las circunstancias que ayuden, dificulten o impidan a la empresa alcanzar los criterios especificados.
- Cursos alternativos de acción para la recomendación.
- Efectos positivos y negativos, que pudieran derivarse de la aplicación de la recomendación.
- Factibilidad y costo de implementar la recomendación.
- Impacto en la normatividad vigente.






Según el **tipo de hallazgo**, las recomendaciones pueden ser:

- ▲ preventivas
- ▲ correctivas
- ▲ de mejora

Por ejemplo (y sin especificar mucho ya que se verá en las próximas filminas), en Starship se podría hacer una recomendación acerca de las gestiones de los backups de acuerdo a lo notificado por la etapa anterior, es decir, modificar desde el acceso a los mismos hasta el control de ellos.





# Conclusiones sobre Starship

## 1. Control de la Red

**Evidencia:** registros de reclamos de los empleados relacionados a problemas por conexión de red y/o lentitud en el sistema.

No se requirieron pruebas sustantivas. Se consideraron suficientes los reportes de problemas de conexión.

**Hallazgo:** se cumple el nivel de confianza estimado. El control es correcto.

Se clasifica como “Conformidad”.

**Recomendaciones:**

No se emiten recomendaciones preventivas ni correctivas.

Se considera efectivo el control existente.





# Conclusiones sobre Starship

## 2. Control del acceso físico

**Evidencia:** Se utilizaron las técnicas walk through y entrevistas.

**Hallazgo:**

- Según el personal, el control coincide con lo que debería ser.
- La técnica walk through demostró que se cumple el control (en un intento).
- Se cumple el nivel de confianza estimado. El control es correcto.

Se clasifican estos hallazgos como “Observación”

**Recomendaciones:**

- Revisión periódica del funcionamiento de las cámaras de seguridad, para mejorar su uptime del 99% al 100% (Recomendación preventiva)



# Conclusiones sobre Starship

## 3. Control de backups

### Evidencia:

- Entrevistas a la gerencia
- Entrevistas y análisis exhaustivo con los técnicos a cargo de los backups
- Logs de acceso a backups

### Hallazgo:

- Ambigüedades en las respuestas de la gerencia, a partir de este hallazgo, análisis exhaustivo
- Violaciones a los procedimientos (algunos desarrolladores también acceden a los backups sin conocimiento del equipo de servidores)

### Recomendaciones:

- Aplicación de privilegios en base a las funciones y responsabilidades
- Deben mantenerse los registros de las operaciones administrativas de cualquier usuario para garantizar la rastreabilidad y responsabilidad
- Aplicación de técnicas de autenticación y anti-spoofing



# Conclusiones sobre Starship

## 4. Control del acceso virtual (VPN)

### Evidencia:

- Protocolo de autenticación de la aplicación Cisco AnyConnect Secure Mobility
- Logs de sistema de acceso virtual, que contienen las direcciones IP, usuario, y las horas de conexión y desconexión.

**Hallazgo:** Se cumplen con los requisitos de sistema y de seguridad, por lo tanto se va a clasificar como una “Conformidad”.

**Recomendaciones:** No se emiten recomendaciones correctivas.

Se sugiere una mejora del sistema aplicando una autenticación de 2 factores (2FA).



# Conclusiones sobre Starship

## 5. Control de recursos - Empleados

### Evidencia:

- Análisis de los reportes de medición de progreso del software web utilizado para asignar tareas a los empleados
- Relevamiento de logs físicos sobre dichas tareas

### Hallazgo:

- Varias tareas que no cumplieron el tiempo límite de entrega
- Los logs determinaron que las tareas habían sido cumplidas por empleados que no estaban asignados a ellas
- Se clasifican estos hallazgos como “Observación”

### Recomendaciones:

- Capacitación sobre los empleados respecto al uso del software de medición y asignación de tareas (Recomendación preventiva)



# Conclusiones sobre Starship

## 6. Control de recursos - Gerencia

### Evidencia:

- Análisis de los reportes del área de soporte

### Hallazgo:

- No hay ningún criterio sobre de la asignación de recursos dentro de las gerencias
- Se detectó que varios empleados devolvieron los recursos asignados al serles insuficientes para cumplir su rol
- Se clasifican estos hallazgos como “No conformidad”

### Recomendaciones:

- Sistematizar la gestión de asignación de recursos de las gerencias siguiendo reglas y criterios en base a los roles definidos (Recomendación correctiva)



# Conclusiones sobre Starship

## 7. Control de utilización de recursos

### Evidencia:

- Análisis de inconsistencias de registros del software de trackeo instalados en los dispositivos entregados a los empleados, que se sincronizan periódicamente con el servidor de la empresa.

### Hallazgo:

- Las inconsistencias se deben a problemas de conectividad del empleado, pero no de la empresa, en la cual los registros no eran enviados al servidor. Se clasifican estos hallazgos como “Observación”

### Recomendaciones:

- Se recomienda una mejora en el software de trackeo para que sea tolerante a los problemas conexión, mediante envíos asíncronos de reportes e intentos de reconexión reiterados. (Recomendación correctiva)

# FIN

Muchas gracias!

**Grupos 3 y 4 - Etapa 7**

Ingeniería de Software III - 2021