ISO 27006-27007-27008

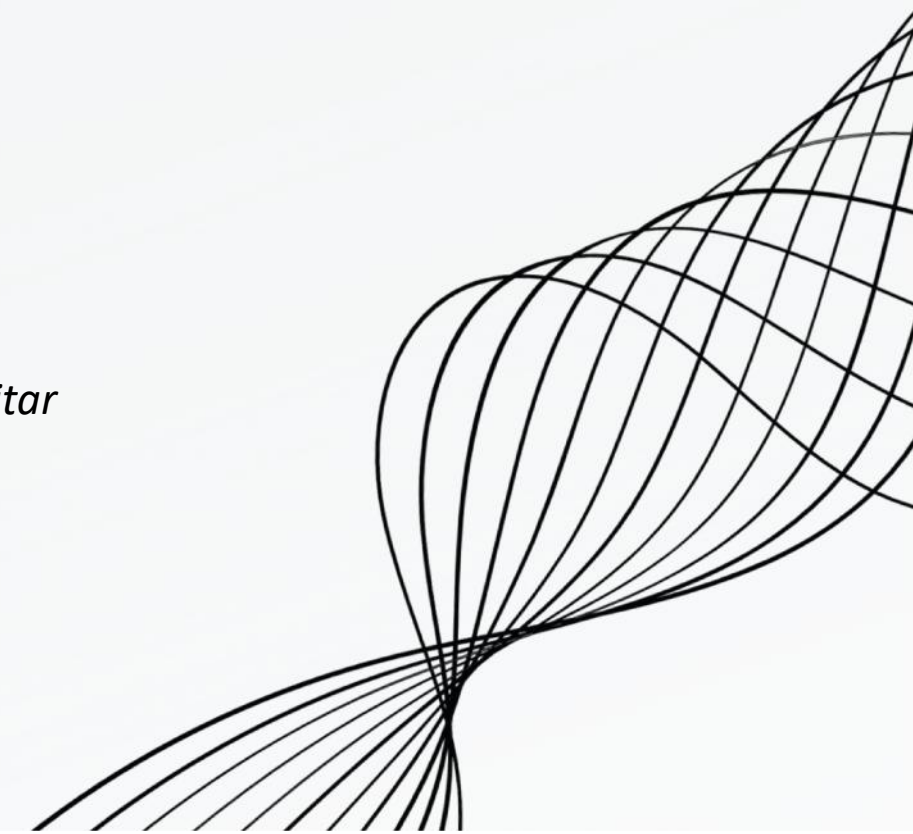
AUDITORÍA, CERTIFICACIÓN Y EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

EXPOSITOR: CARLOS OSMAR VICTORIA AVILA

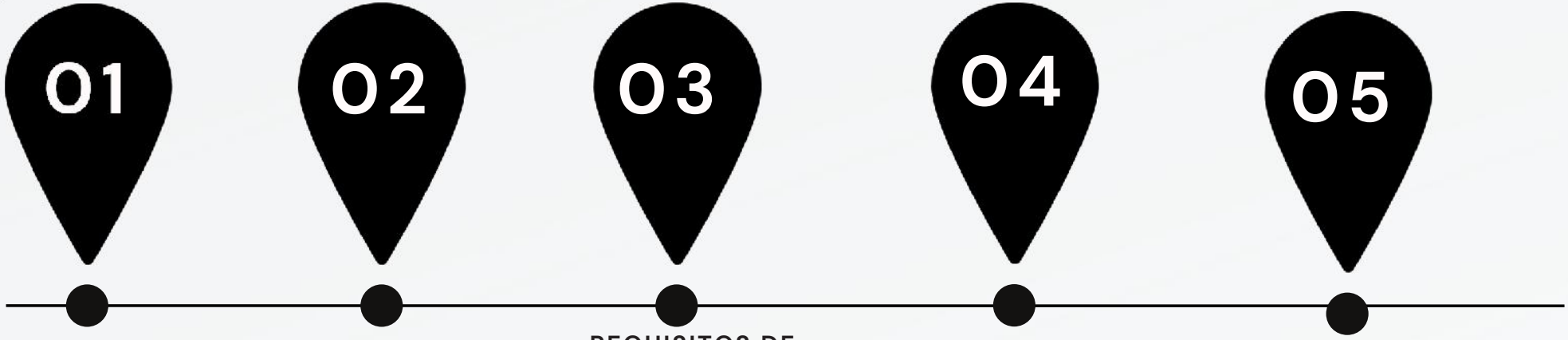
ISO 27006

REQUISITOS PARA LOS ORGANISMOS QUE PROPORCIONAN AUDITORÍA Y CERTIFICACIÓN DE SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

- *Competencia de los auditores*
- *Imparcialidad*
- *Transparencia y consistencia*
- *Requisitos específicos para auditar*



ELEMENTOS QUE LA COMPONEN



REQUISITOS GENERALES

- Imparcialidad
- Conflictos de interés
- Cubrir los riesgos

REQUISITOS ESTRUCTURALES

- ISO/IEC 17021-1
- Requisitos para el personal involucrado en el proceso de certificación

REQUISITOS DE RECURSOS

- Competencia del personal
- Uso de auditores y expertos técnicos externos
- Subcontratación

REQUISITOS DE INFORMACIÓN

- Información pública de los procesos de certificacion
- Proteger Información obtenida en los procesos

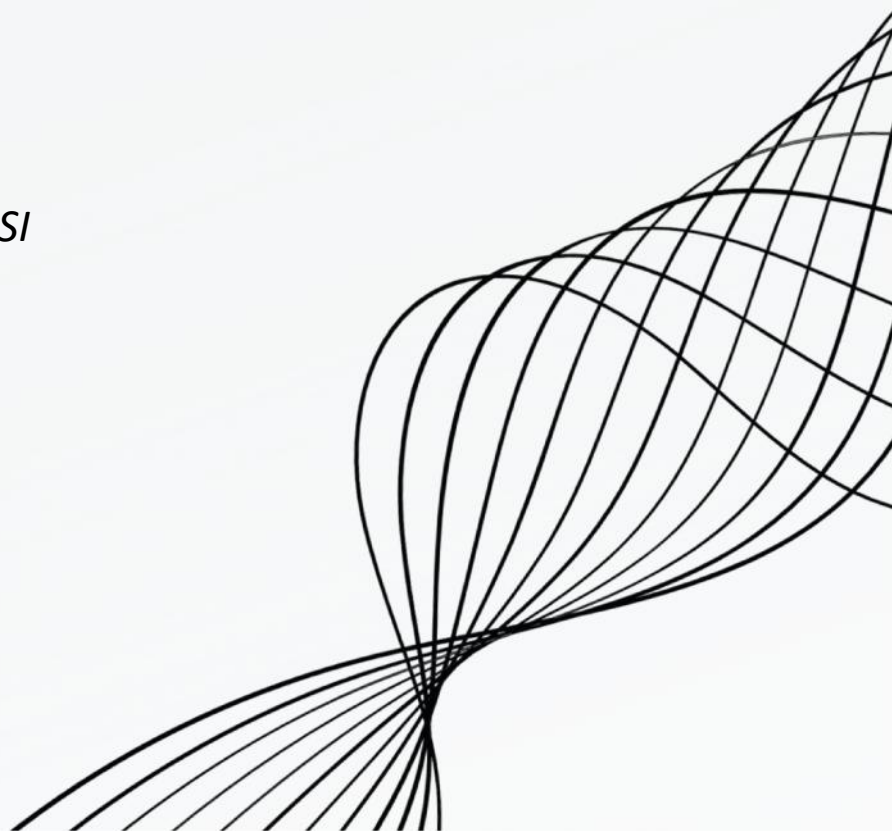
REQUISITOS DE PROCESO

- Actividades previas a la certificación
- Revisión de la solicitud y programa de auditoría
- Auditorías iniciales y mantenimiento de la certificación

ISO 27007

DIRECTRICES PARA LA AUDITORÍA DE SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

- *Directrices para la auditoría de SGSI*
- *Enfoque basado en riesgos*
- *Independencia del auditor*
- *Competencia del auditor*



ELEMENTOS QUE LA COMPONEN

Realización de una auditoría

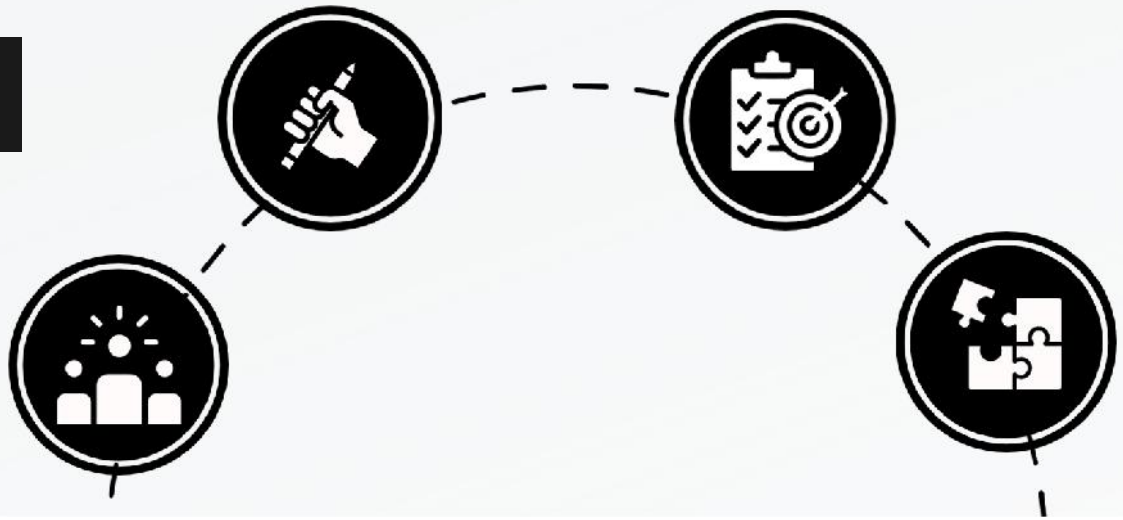
- Planificación
- Ejecución
- Reporte de hallazgos

Informe de los resultados de la auditoría

- Informe claro y conciso
- Recomendaciones
- Efectividad del SGSI

Gestión de un programa de auditoría

- Planificación auditorías internas y externas
- Definición de objetivos
- Selección de los auditores
- Monitoreo continuo



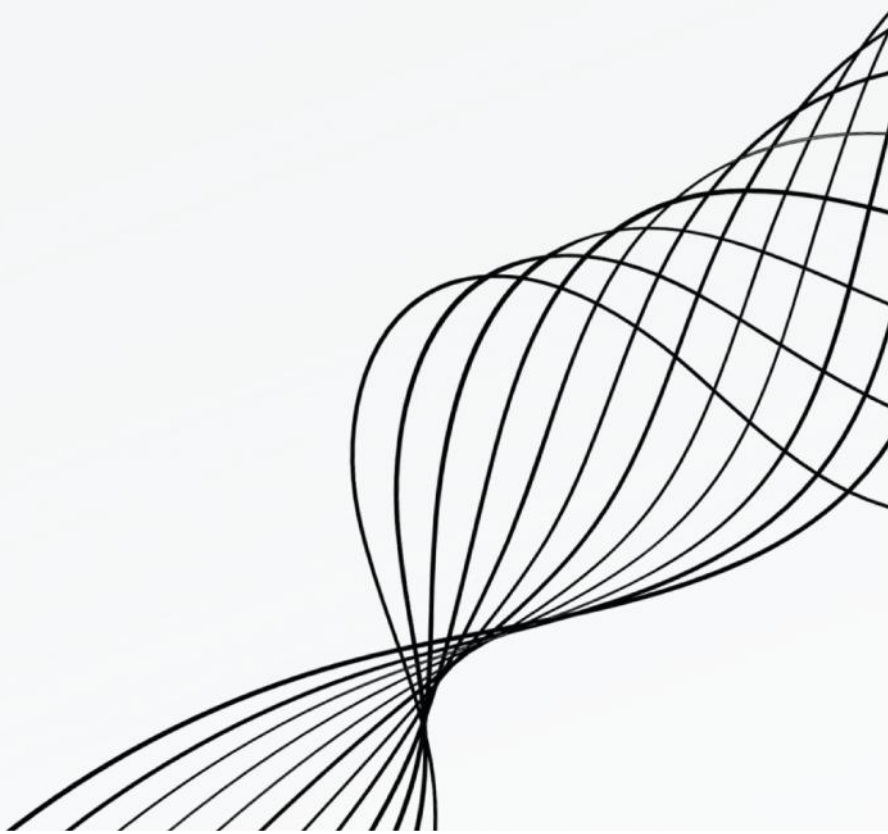
Competencia y evaluación de los auditores

- Conocimientos técnicos
- Experiencia en evaluar controles implementados

ISO 27008

DIRECTRICES PARA LA EVALUACIÓN DE LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN.

- *Evaluación de controles*
- *Independencia y objetividad*
- *Revisión basada en riesgos*
- *Métodos de evaluación*



ELEMENTOS QUE LA COMPONEN

- Recopilación de la información
- Coordinación con los gerentes
- Ajustar el alcance según los riesgos

PANORAMA GENERAL DE LAS REVISIONES DE LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

- Examinar
- Entrevistar
- Probar

MÉTODOS DE REVISIÓN

ACTIVIDADES

ACTIVIDADES

- Políticas entendidas
- Implementación de controles completas
- Estudiar la arquitectura del sistema

PREPARATIVOS

- Tipo de control
- Procedimientos a utilizar
- Objetivos de la revisión

DESARROLLO DE UN PLAN

Ejecución de la revisión

CONDUCCIÓN DE LA REVISIÓN

- Análisis de los resultados de la revisión
- informe con los hallazgos

ANÁLISIS Y REPORTE DE RESULTADOS

GRACIAS