

Auditoría 27001



Tipos de Hallazgos



Desliza →

No Conformidades

NO CONFORMIDAD MAYOR

NCM



Incumplimiento grave del estándar.

Afecta la capacidad del SGSI para cumplir objetivos.

Ejemplo: no realizar evaluación de riesgos, o no definir controles clave del SGSI.

Impacto: pone en duda la eficacia del sistema completo.

Consecuencia: suspensión o no otorgamiento de la certificación hasta corregir.

Ingrid Mora

No Conformidades

NO CONFORMIDAD MENOR

NCm



Incumplimiento puntual o aislado.

Desviación sin comprometer todo el SGSI.

Ejemplo: falta de evidencia en la capacitación de un colaborador, o registros incompletos de revisiones.

Impacto: no compromete todo el sistema, pero muestra debilidad.

Consecuencia: debe corregirse en un plazo definido (plan de acción).

Ingrid Mora

No Conformidades

OBSERVACIÓN (OBS) Hallazgo



OBS

No es un incumplimiento directo.

Señala oportunidades de mejora o riesgos potenciales. Indican que algo no cumple del todo y podría evolucionar en no conformidad.

Ejemplo: documentación que podría volverse confusa o procesos sin responsables claros.

Impacto: si no se atiende, puede convertirse en no conformidad en el futuro.

Ingrid Mora

No Conformidades

OPORTUNIDAD DE MEJORA

OM



No son obligatorias, dependen del criterio del auditor.

No implican incumplimiento.

Son recomendaciones para optimizar el SGSI.

Ejemplo: implementar un dashboard de indicadores más visual.

Ingrid Mora

EN RESUMEN



Oficialmente en ISO 27001 solo se reconocen conformidades y no conformidades.

Los auditores clasifican las no conformidades en mayores o menores.

Observaciones, oportunidades de mejora o comentarios dependen de la práctica de cada organismo, pero son comunes en la entrega del informe.

Si quieres ISO27001 o certificar tu empresa, contáctame para asesorarte.

Email: imora@wafratransformation.com



Ingrid Mora