Determinar si las evidencias constatados por el auditor constituyen un hallazgo. En caso afirmativo determinar si se obtiene una conclusión. Realizar recomendaciones si el auditor lo estima oportuno.

Referente: ISO/IEC 27001 Seguridad de los Sistemas de Información

El referente está formado por criterios o controles

Nº	Evidencia	Pert. (S/N)	Suf. (S/N)	Criterio	Hallazgo (S/N)	Objetivo de auditoría	Conclusión	Recomendación
1	Documento de Política de Seguridad no está actualizado	S	S	5.1.1	S	Seguridad de los Sistemas de Información	Mala gestión del documento	Actualizar el documento
2	Método de realizar salvaguardias de las bases de datos explicados por el administrador	S	N	12.3.1	N	Seguridad física		Es necesario tener constancia de qué se hace o donde se hace
3	En la cámara frigorífica del restaurante de la empresa se han constatado 20 yogures caducados	N	N		N	Seguridad de los Sistemas de Información		No tener yogures caducados
4	En una conversación de pasillo el auditor escucha que suelen haber puertas abiertas en los racks de los servidores	S	N	16.1.3	N	Seguridad de los Sistemas de Información		Asegurarse siempre de que las puertas están cerradas
5	El auditor constata visualmente puertas abiertas en los racks de los servidores. Solicita autorización y obtiene evidencia documental fotográfica de ello	S	S	16.1.3	S	Seguridad de los Sistemas de Información	Punto débil en la seguridad	Tener siempre las puertas cerradas
6	El auditor constata visualmente puertas abiertas en los racks de los servidores. Solicita autorización y obtiene evidencia documental fotográfica de ello	N	N		N	Cumplimento legal		Mantener siempre los racks cerrados
7	Robustez débil de las contraseñas: Documento sobre la calidad de las contraseñas	S	S	9.4.3	S	Seguridad de los Sistemas de Información	Punto débil en la seguridad	Obligar siempre a poner contraseñas seguras
8	Aunque se supera el número de trabajadores no hay un servicio médico disponible	N	N		N	Seguridad de los Sistemas de Información		Tener un servicio medico disponible
9	Puertas abiertas en los racks de los servidores	N	N		N	Cumplimento legal		
10	Robustez débil de las contraseñas: Prueba de obtención de contraseñas	S	N	9.4.3	N	Seguridad física		Obligar a cambiar las contraseñas para poner unas más seguras
11	El operador opina que se ha realizado la última revisión de los sistemas de refrigeración de la sala de ordenadores	N	N		N	Seguridad de los Sistemas de Información		
12	El informe sobre la calidad de la comida en el restaurante de la empresa indica que no se revisan las caducidades de los alimentos	N	N		N	Seguridad de los Sistemas de Información		Revisar la fecha de caducidad
13	Robustez débil de las contraseñas: Prueba de obtención de contraseñas	S	S	9.4.3	S	Seguridad de los Sistemas de Información	Punto débil en la seguridad de los sistemas	Obligar a cambiar las contraseñas para poner unas más seguras
14	El auditor cree que no hay un comité de seguridad	S	N	12.1	N	Seguridad de los Sistemas de Información		Si efectivamente no existe un comité es obligatorio crearlo
15	El procedimiento de gestión de personas recoge que se entrega un manual de bienvenida al personal de nueva incorporación	S	N	7.2.2	N	Seguridad de los Sistemas de Información		Hay que asegurarse siempre de que el manual de bienvenida es entregado y revisado por el empleados

16	Falta de definición de responsabilidades y recursos necesarios para la consecución de objetivos	N	N		N	Seguridad de los Sistemas de Información		

Determinar si las evidencias constatados por el auditor constituyen un hallazgo. En caso afirmativo determinar si se obtiene una conclusión. Realizar recomendaciones si el auditor lo estima oportuno.

Referente: ISO/IEC 27001 Seguridad de los Sistemas de Información

El referente está formado por criterios o controles

Nº	Evidencia	Pert. (S/N)	Suf. (S/N)	Criterio	Hallazgo (S/N)	Objetivo de auditoría	Conclusión	Recomendación
17	Ausencia de responsabilidades definidas en el sistema de gestión de seguridad	S	S	6.1.1	S	Seguridad de los Sistemas de Información	Falta definir roles	Es importante definir los roles para que cuando algo pase se sepa quien se tiene que encargar
18	El procedimiento de gestión de personas recoge que se entrega un manual de bienvenida al personal de nueva incorporación	N	N		N	Seguridad de las :omu nicaciones		
19	No disponer de evidencias de la educación, formación, habilidades y experiencia Normalmente anotadas en ficha de empleado o curriculum vitae	S	S	7.2.2	S	Seguridad de los Sistemas de Información	Es necesario que la gente este formada para su propósito para evitar negligencias o intentar prevenirlas	Solicitar y almacenar los datos necesarios antes de contratar
20	El responsable de formación indica que se imparte cursos y seminarios sobre seguridad de la información y concienciación de manera frecuente	S	N	7.2.2	N	Seguridad de los Sistemas de Información		Pedir que se muestren informes de los cursos y seminarios sobre seguridad
21	No hay implementado una herramienta de gestión de versiones en el departamento de desarrollo	N	N		N	Seguridad de los Sistemas de Información		
22	Un usuario ha comentado al auditor que los puertos USB están activos	S	N	9.4.1/12.2	N	Seguridad de los Sistemas de Información		Deshabilitar los puertos USB
23	No hay implementado una herramienta de gestión de versiones en el departamento de desarrollo	N	N		N	Cumplimento legal		
24	Ausencia de responsabilidades definidas en el sistema de gestión de seguridad	S	S	6.1.1	S	Sistema de gestión de calidad	Necesaria la definición de roles	Es imprescindible asignar roles a las tareas
25	El responsable de formación indica que se imparte cursos y seminarios sobre seguridad de la información y concienciación de manera frecuente	N	N		N	Seguridad física		