2024

Metodología común de inspección de auditoría

Programa de trabajo de inspección sobre seguridad de la información y ciberseguridad

Emitido por la Comisión de Órganos Europeos de Supervisión de Auditores (COESA/CEAOB en inglés)

Traducido por:

AUDITORES
INSTITUTO DE CENSORES JURADOS DE CUENTAS DE ESPAÑA

Glosario de abreviaturas empleadas en la traducción

BPC	Plan de Continuidad del Negocio
DORA2	Reglamento sobre Resiliencia Operativa Digital
TI	Plan de Recuperación en caso de Catástrofe
RGPD	Reglamento General de Protección de Datos
ISO	Responsable de Seguridad de la Información
TI	Tecnología de la Información

Traducido por:

AUDITORES
INSTITUTO DE CENSORES JURADOS
DE CUENTAS DE ESPAÑA

Principios clave	
PROGRAMA DE TRABAJO DE INSPECCIÓN SOBRE INFORMACIÓN Y CIBERSEGURIDAD	
	El programa de trabajo de inspección sobre seguridad de la información y ciberseguridad se sustenta en la inspección de **las medidas implementadas por la firma de auditoría («la firma») para proteger la información y, en particular, la documentación de auditoría, lo cual incluye:** • **la documentación producida por el auditor y** • **la documentación del cliente recopilada durante el encargo de auditoría.** Las medidas establecidas deberían asegurar la confidencialidad, disponibilidad y fiabilidad de la información, así como la custodia segura, accesibilidad o recuperabilidad de los datos subyacentes y de la correspondiente tecnología.
Alcance	
	Todos los sistemas y funciones de TI requeridos para la gestión de la calidad y la auditoría legal, incluidos la infraestructura de TI (por ejemplo, los centros de datos, redes y las plataformas de TI), los sistemas (por ejemplo, los sistemas operativos o los sistemas de gestión de bases de datos) y las aplicaciones (por ejemplo, para el análisis de la independencia, documentación de auditoría o el análisis de datos), así como un Sistema de Control Interno adecuado incluidos políticas, orientaciones, procesos, medidas preventivas y controles.
Conclusiones clave	
Al finalizar los procedimientos relativos a esta área, evaluar como conclusión si:	
1	La firma de auditoría ha establecido una organización de TI, ha implementado procesos de TI, así como un entorno de TI que sustenta el Sistema de Control Interno para su trabajo de auditoría.
2	La firma de auditoría estableció un marco de seguridad de la información tanto para la información de la firma como la de sus clientes.
3	La firma de auditoría implementó controles para prevenir y detectar incidentes relacionados con la TI y con la ciberseguridad y reaccionó inmediatamente cuando ocurrió algún incidente.
4	La firma de auditoría evalúa regularmente su marco de seguridad de la información y adopta medidas correctoras oportunamente.
5	La firma de auditoría implementó soluciones actualizadas para asegurar la continuidad de sus actividades.

Definiciones[1]	
COBIT (Control Objectives for Information and Related Technology)	Un marco completo, aceptado internacionalmente para dirigir y gestionar la información de la entidad y la tecnología (TI) que ayuda a los ejecutivos y a la dirección en la definición y logro de los objetivos empresariales y los correspondientes objetivos de TI.
Ciberseguridad	La protección de los activos de información mediante la respuesta a las amenazas al procesamiento, almacenamiento y transporte de la información a través de sistemas de información interconectados.
Gestión de incidentes	Los procesos para la identificación de un hecho o una interrupción del servicio no planificados en el sistema y la respuesta oportuna con objeto de restaurar el servicio a su estado operativo.
Seguridad de la información	Garantiza que, dentro de la empresa, la información se protege contra su divulgación a usuarios no autorizados (confidencialidad), modificación indebida (integridad) y falta de acceso cuando se requiere (disponibilidad).

[1] Las definiciones se basan en el Glosario de ISACA y se han actualizado cuando se ha considerado necesario.

Gobierno de la seguridad de la información	El conjunto de responsabilidades y prácticas llevadas a cabo por el consejo de administración y de dirección con el objetivo de proporcionar dirección estratégica, garantizar que se alcanzan los objetivos, asegurar que el riesgo se gestiona adecuadamente y verificar que los recursos de la empresa se utilizan de manera responsable. También incluye la valoración y evaluación de la eficacia del programa de ciberseguridad.
Tecnología de la Información	El hardware, software, instalaciones de comunicación y otras utilizadas para introducir, almacenar, procesar, transmitir y obtener datos en cualquier forma.
ISO/IEC 27001	Su objetivo es proporcionar la base para la auditoría por terceros y estar armonizada con otras normas de gestión como las. ISO/IEC 9001 y 14001
ITIL (IT Infrastructure Library)	La IT Infrastructure Library de la Oficina Gubernamental de comercio de reino Unido (UK Office of Government Commerce - OGC) Un conjunto de orientaciones sobre la gestión y prestación de servicios de TI.
Seguimiento del sistema de TI	El proceso de revisión de la actividad de un sistema (incluido el procesamiento por lotes) para identificar anomalías que merezcan un seguimiento posterior o investigación adicional.
Prueba de penetración	Comparación los resultados del sistema a otros sistemas equivalentes utilizando referencias bien definidas.
Incidente de seguridad	Una serie de hechos inesperados que implican un ataque o una serie de ataques (que comprometen o violan la seguridad) en uno o más sitios. Un incidente de seguridad normalmente incluye una estimación de su nivel de impacto. Se define un número de niveles de impacto y, para cada uno de ellos, se identifican las actuaciones requeridas y las personas a quienes se debe notificar.
Programas de concienciación sobre seguridad	Un plan clara y formalmente definido, un enfoque estructurado y un conjunto de actividades y procedimientos relacionados que tienen por objeto lograr y mantener una cultura de concienciación sobre seguridad. **Notas sobe el alcance:** Esta definición establece claramente que se refiere a lograr y mantener una cultura de concienciación sobre seguridad, lo que significa alcanzar y mantener la concienciación sobre la seguridad todo el tiempo. Ello implica que un programa de concienciación sobre seguridad no es un esfuerzo puntual, sino un proceso continuo.
Gestión de la vulnerabilidad	El proceso para la identificación de vulnerabilidades (es decir, problemas o debilidades) relativas al entorno de seguridad de una entidad y la implementación de medidas correctoras oportunas para responder a la vulnerabilidad.

Paso	Objetivo de la comprobación	Referencia	Procedimientos de inspección
1	Obtener un conocimiento actualizado del entorno de TI de la firma incluidas, las plataformas de TI, la infraestructura de red relevante, los sistemas operativos y bases de datos, así como los procesos relevantes de TI, que se centran en el sistema de gestión de la firma de auditoría y en la ejecución de auditorías legales.	**NIGC 1 32(f)** **NIGC 1 33(a)** DORA Artículos 5 - 14	1. Conocer y evaluar el IT de la firma incluidos las plataformas de TI subyacentes, la infraestructura de red relevante, los sistemas operativos y las bases de datos, así como los procesos de TI y flujos de datos esenciales.
2	Obtener un conocimiento actualizado del **modelo de gobierno** de la firma acerca de la información y la ciberseguridad.	**NIGC 1 32(f)** DORA Artículo 5 **NIGC 1 33** DORA Artículo 6 DORA Artículos 24-27 **NIGC 1 35** RGPD	1. Conocer y evaluar la organización de la firma, incluidas las funciones y responsabilidades de TI y de la seguridad de la información. 2. Conocer y evaluar las políticas y los procedimientos de la firma sobre información y ciberseguridad. 3. Conocer y evaluar el enfoque de la valoración del riesgo para los riesgos de TI y de seguridad de la información. 4. Conocer y evaluar las actividades de seguimiento internas y externas de la firma relacionadas con la información y la ciberseguridad. 5. Evaluar los cambios clave realizados por la firma desde la última visita de inspección, así como las iniciativas actuales. 6. Evaluar la implementación del RGPD y el modo en el que la firma se asegura del cumplimiento de la normativa.
3	Obtener un conocimiento actualizado del entorno de control de la firma, así como de los procedimientos, las políticas y los procesos relativos a la información y la ciberseguridad.	**NIGC 1 32(f)** **NIGC 1 33(a)** DORA Artículo 9 DORA Artículos 5, 8 11, 12, 26, 28-30	1. Conocer y evaluar las medidas y controles que afectan a la información y la ciberseguridad. 2. Conocer y evaluar los planes de la firma sobre formación y concienciación sobre seguridad de la información y la ciberseguridad. 3. Conocer y evaluar la utilización, el control y seguimiento por la firma de la subcontratación de TI y/o de los servicios de TI prestados por terceros.
4	Obtener un conocimiento actualizado de los procedimientos de la firma para gestionar incidentes de seguridad en la información.	**NIGC 1 33(a)** DORA Artículo 10 DORA Artículos 11-12	1. Conocer y evaluar los procedimientos de la firma para registrar y gestionar incidentes de seguridad en la información. 2. Conocer y evaluar las soluciones de la firma para garantizar la continuidad de las actividades.

5	Evaluar el cumplimiento de los procedimientos de la firma para proteger	**NIGC 1 32(f)**	1. Comprobar los controles de la firma sobre la adquisición, desarrollo, mejora, implementación y funcionamiento del entorno de TI, incluidas las aplicaciones de TI, así como el acceso al entorno de TI, incluidas las aplicaciones de TI, para asegurar la implementación y funcionamiento correctos de los sistemas de TI relevantes.
Paso	**Objetivo de la comprobación**	**Referencia**	**Procedimientos de inspección**
	La información de la firma y de sus clientes.	**NIGC 1 35** DORA Artículo 13	1. Obtener y revisar los resultados de las evaluaciones internas y externas y asegurarse de que la firma tomó medidas correctoras en su caso. 2. Para una muestra de empleados, incluidos los de reciente incorporación, asegurarse de que participaron en sesiones de formación y/o concienciación. 3. Asegurarse de que existe un contrato con terceros, incluidos, en su caso, miembros de la red, y que incluyen cláusulas sobre las funciones y responsabilidades acerca de la protección de la información. 4. Para una muestra de sistemas de TI, revisar las reglas sobre contraseñas implementadas en el sistema y revisar la lista de derechos de acceso de los usuarios para verificar que solo se concede acceso al personal pertinente. 5. Obtener y revisar los resultados de la última revisión de los derechos de acceso de los usuarios para asegurarse de que la firma de auditoría realiza controles posteriores regulares sobre los derechos de acceso.
6	Evaluar el cumplimiento de los procedimientos de la firma en caso de incidentes de seguridad. -	DORA Artículos 17-19 RGPD Datos Incumplimiento Notificación **NIGC 1 32(f)** DORA Artículos 11-12	1. Para una muestra de incidentes de seguridad en la información, revisar la documentación de soporte y asegurarse de que se tomaron medidas oportunamente y en cumplimiento de la normativa nacional. 2. Confirmar que se han llevado a cabo comprobaciones regulares para garantizar que las copias de seguridad pueden ser restauradas y que los PRD/BPC son eficaces y se actualizan si es preciso.

Recursos adicionales	
ISACA	Marco COBIT, Cybersecurity Nexus, conocimiento IT (https://www.isaca.org/)
ISO	Serie ISO/IEC 2700x (https://www.iso.org/)
ITIL	Information Technology Infrastructure Library (ITIL)
BSI	BSI (Oficina Federal de Seguridad de la Información) (https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html)
NIST	NIST (Instituto Nacional de Normas y Tecnología EEUU) (National Institute of Standards and Technology, USA) (https://www.nist.gov/cyberframework)
RGPD	RGPD (Reglamento general de protección de datos (EU) 2016/679) (https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en#legislation)