GUID 5101

Orientaciones sobre la Auditoría de la Seguridad de la Información

INTOSAI

Las Guías INTOSAI (GUID) son emitidas por la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI) como parte del Marco INTOSAI de Pronunciamientos Profesionales. Para más información visite www.issai.org

1) Ratificada en 2025

La GUID 5101 está disponible en todas las lenguas oficiales de la INTOSAI: árabe, inglés, francés, alemán y español.

TABLA DE CONTENIDOS

1

INTRODUCCIÓN

1) La GUID 5101 complementa la GUID 5100 proporcionando orientaciones sobre la auditoría de la seguridad de la información. Las orientaciones establecidas en la presente GUID son coherentes con los Principios Fundamentales de Auditoría del Sector Público (ISSAI 100), así como con los Principios de Auditoría de Cumplimiento (ISSAI 400).

2) La transición a sistemas informatizados y el tratamiento electrónico de la información por parte de las entidades auditadas del sector público obliga a las EFS a desarrollar una capacidad adecuada para auditar los controles relacionados con los sistemas de información. En el marco de la auditoría de los sistemas de información, es necesario garantizar que las entidades auditadas diseñen y apliquen controles para mantener la confidencialidad, integridad y disponibilidad de los sistemas de información y los datos (es decir, la seguridad de la información).

3) Las violaciones de la seguridad de la información pueden dar lugar a graves perjuicios jurídicos, de reputación/credibilidad, financieros, de productividad y de exposición a nuevas intrusiones. Las violaciones de la seguridad pueden deberse a deficiencias y vulnerabilidades que den lugar a una exposición accidental o a la divulgación de información a partes no autorizadas, a la pérdida de disponibilidad o a cambios no autorizados en los sistemas y datos.

2 OBJETIVOS DE LA PRESENTE GUID

4) Las orientaciones aplicables a la auditoría de los sistemas de información se describen en la GUID 5100. El objetivo de esta GUID es proporcionar orientaciones específicas y adicionales para una auditoría de cumplimiento de la seguridad de la información.

5) La auditoría de la seguridad de la información puede considerarse una auditoría de cumplimiento o, en determinadas circunstancias, una auditoría combinada incorporando aspectos financieros, de cumplimiento y/o de desempeño. La presente GUID abarca la auditoría de la seguridad de la información, ya sea como una auditoría de cumplimiento diferenciada o como parte de un encargo de auditoría combinado para comprobar si la gestión informática cumple las normas y requisitos necesarios en materia de seguridad de la información.

6) El contenido de esta GUID podrá ser aplicado por los auditores en las fases de planificación, ejecución, notificación y seguimiento del proceso de auditoría. La GUID enumera posibles asuntos del trabajo de auditoría, factores de riesgo que afectan a la seguridad de la información, fuentes de los criterios de auditoría y preguntas de auditoría de alto nivel. Estas listas son ilustrativas y no exhaustivas.

3

DEFINICIONES

a) **Seguridad de la información: Protección de la información y de los sistemas** de información contra el acceso, la utilización, la divulgación, la interrupción, la modificación o la destrucción no autorizados a fin de proporcionar confidencialidad, integridad y disponibilidad.

b) **Ciberseguridad:** Prevención de daños, protección y restauración respecto de ordenadores, sistemas de comunicaciones electrónicas, servicios de comunicaciones electrónicas, comunicaciones por cable y comunicaciones electrónicas, así como de la información contenida en ellos, a fin de garantizar su disponibilidad, integridad y confidencialidad.

c) **Confidencialidad:** Preservar las restricciones autorizadas sobre el acceso a la información y su divulgación, incluidos los medios para proteger la privacidad personal y la información sujeta a derechos de propiedad, o, de forma alternativa, proteger la información sensible de la divulgación no autorizada. La divulgación no autorizada de información constituye una pérdida de confidencialidad.

d) **Integridad:** Protección de la información para evitar su modificación o destrucción indebida garantizando el no repudio1 y

[1] El no repudio es la protección contra una persona que niega falsamente haber realizado una acción en particular. Brinda la capacidad de determinar si una persona determinada realizó una acción en particular, como crear información, aprobar información o enviar o recibir un mensaje.

la autenticidad de la Información[2]; como alternativa, la exactitud y exhaustividad de la información, así como su validez de acuerdo con los valores y expectativas empresariales. La pérdida de integridad es la modificación o destrucción indebida de información.

d) **Disponibilidad:** El acceso y el uso oportunos y fiables de la información o de un sistema de información para los usuarios autorizados o, alternativamente, posibilidad de disponer de la información cuando así lo requiera el proceso actual y en el futuro, así como la salvaguardia de los recursos necesarios y las capacidades asociadas. Una pérdida de disponibilidad es la interrupción del acceso a la información o a un sistema de información o a la utilización estos.

e) **Evaluación de la vulnerabilidad/pruebas de penetración:** La evaluación de la vulnerabilidad tiene por objeto identificar los problemas de seguridad en las aplicaciones informáticas, las estaciones de trabajo o toda la red organizativa de manera sistemática y organizada, y permite a los auditores clasificar, priorizar y ordenar las vulnerabilidades de seguridad en función de sus niveles de riesgo para su oportuna reparación. La prueba de penetración, similar a la piratería informática ética, es un pirateo o ataque simulado autorizado a un sistema informático, realizado para evaluar la seguridad del sistema.

[2] La autenticidad es la propiedad de ser genuino y poder ser verificado y confiable; confianza en la validez de una transmisión, un mensaje o el emisor del mensaje.

4

EL ASUNTO

7) En la auditoría de la seguridad de la información, el auditor evalúa el cumplimiento del asunto (seguridad de la información o cualquier aspecto o componente específico de la misma) con las autoridades aplicables (leyes, reglamentos, políticas, procedimientos, normas, prácticas, etc.).

8) El trabajo de auditoría de la seguridad de la información estará determinado por los objetivos y el alcance de la auditoría. El alcance de la auditoría podrá incluir diferentes asuntos, tales como:

   a) Cultura de seguridad de la información, incluidos el liderazgo y el compromiso; dirección y políticas de gestión; objetivos de seguridad de la información; funciones, responsabilidades y autoridades organizativas (como el trabajo móvil, el teletrabajo, etc.).

   b) Procesos de gestión de riesgos de seguridad de la información, que consisten en:
      i. Evaluación de los riesgos en materia de seguridad de la información (tales como umbrales de aceptación del riesgo para la seguridad de la información, criterios de aceptación de riesgos, identificación, análisis y priorización) y tratamiento de los riesgos para la seguridad de la información.
      ii. Comunicación (interna y externa) y documentación pertinente para el sistema de gestión de la seguridad de la información
      iii. Revisión y mejora continua de la seguridad de la información y la gestión de riesgos.

c) Seguridad de la información en las relaciones con los proveedores.

d) Seguridad de los recursos humanos en diferentes fases: antes del empleo, durante el empleo y después del empleo.

e) Gestión y control de los activos de información, incluidos el inventario y la clasificación; normas para un uso aceptable; transporte, devolución y eliminación.

f) Autenticación, autorización y control de acceso, así como gestión y autenticación de la identidad, controles criptográficos y controles de autorización y acceso.

g) Seguridad física y del entorno.

h) Gestión de la seguridad y la ciberseguridad de las redes y las comunicaciones

i) Gestión de incidentes relacionados con la seguridad de la información, y control y supervisión de la seguridad.

j) La seguridad en el marco de la adquisición y el desarrollo de sistemas.

k) Seguridad de las operaciones, incluidos los procedimientos operativos y las responsabilidades; protección contra programas maliciosos; copia de seguridad/recuperación de datos y registro y seguimiento.

l) Cumplimiento de los requisitos externos e internos.

m) Leyes nuevas o modificadas

5

PLANIFICACIÓN DE UNA AUDITORÍA DE LA SEGURIDAD DE LA INFORMACIÓN

9) Podrá iniciarse una auditoría de la seguridad de la información a raíz de una evaluación de riesgos. Algunos factores de riesgo relevantes pueden ser:

a) el desarrollo de un nuevo sistema de información o la sustitución o actualización de un sistema de información existente (aplicación o infraestructura) por parte de la entidad auditada, especialmente en un ámbito empresarial crítico;

b) la falta de actualización o de sustitución de un sistema antiguo de información heredado con una infraestructura tecnológica subyacente obsoleta y actualmente no respaldada por parches de seguridad o actualizaciones;

c) la falta de pruebas periódicas de seguridad internas o externas, ni de pruebas de seguridad de los sistemas de información operativa, especialmente cuando se hayan sometido a actualizaciones significativas en las aplicaciones o infraestructuras;

d) el análisis *post mortem* de un incidente o fallo grave de seguridad que haya afectado negativamente al sistema de información en cuestión, o cuando un incidente o fallo de seguridad haya afectado negativamente a sistemas de información en una situación similar en otras entidades auditadas;

e) problemas relacionados con la protección de datos y la privacidad en relación con los sistemas informáticos existentes y necesidad de mejorarlos o actualizarlos para cumplir las últimas regulaciones aplicables en la materia;

detección (a través de otras auditorías, internas o externas/de la EFS) de amenazas significativas para la seguridad de la información con respecto

al sistema de información de la entidad auditada, evaluaciones o valoraciones o deficiencias de control detectadas en anteriores auditorías de seguridad de la información que no se hayan abordado o se hayan abordado solo parcialmente;

f) cambios significativos en las políticas y estructuras organizativas para la gestión y la aplicación de los sistemas de información, así como la seguridad de la información.

10) El auditor podrá evaluar el proceso de gestión de riesgos del auditado (identificación, evaluación y tratamiento de riesgos) y considerar auditorías o evaluaciones internas o externas previas en el proceso de identificación y evaluación de riesgos, si aplica un enfoque de auditoría basado en el riesgo.

11) El auditor podrá examinar la disponibilidad de las políticas y procedimientos pertinentes, y si estos se revisan con la periodicidad adecuada y se actualizan en caso necesario al evaluar las funciones organizativas. El auditor también podrá evaluar si existe entre los usuarios una concienciación y comprensión adecuadas, y una cultura de la seguridad de la información.

12) La materialidad de un problema de auditoría de la seguridad de la información puede decidirse con arreglo al marco general para decidir la materialidad en una EFS, o a orientaciones específicas sobre la materialidad en relación con auditorías de los sistemas de información.

5.1 Fuentes de los criterios de auditoría

13) El auditor podrá utilizar marcos de seguridad de la información aceptados nacional o internacionalmente como fuentes de criterios de auditoría.

14) Los marcos que sirven como fuentes de criterios de auditoría podrían incluir normas como la serie ISO/IEC 27000; el marco de los COBIT preparado/actualizado por la ISACA, las normas y marcos relativos a la información y la ciberseguridad elaborados por el National Institute of Standards and Technology (NIST-CSF) (NIST); los controles del Center for Internet Security (CIS); los marcos y normas sectoriales más acotados/sectoriales, como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, el PCI DSS (Payment Card Industry Data Security Standard), la Ley estadounidense Health Insurance Portability and Accountability Act (HIPAA) para el sector sanitario, etc.

15) La elección de los criterios de auditoría por parte del auditor puede depender de:
- el contexto específico de las EFS y del país (como requisitos legales y reglamentarios, en su caso);
- la entidad o entidades auditadas afectadas;
- el alcance de la auditoría

5.2 Recursos

16) Las consideraciones para asignar recursos humanos a los encargos de auditoría de sistemas de información (entre los que se cuentan las auditorías de seguridad de la información) se analizan en la GUID 5100 y son en general aplicables a las auditorías de la seguridad de la información. Una consideración adicional puede ser que, cuando traten de información sensible y confidencial, las autoridades pertinentes puedan exigir a los auditores que se sometan a una procedimiento especial de control.

6

LLEVAR A CABO UNA AUDITORÍA DE LA SEGURIDAD DE LA INFORMACIÓN

6.1 Finalidad de los procedimientos de auditoría[3]

17) Los procedimientos de auditoría para una auditoría de la seguridad de la información se diseñarán para que se centren en evaluar a) la confidencialidad, b) la integridad (incluido el no repudio) y c) la disponibilidad de datos y sistemas informáticos que entren en el ámbito del encargo de auditoría.

[3] En el anexo figuran, a modo ilustrativo, algunas preguntas de auditoría de alto nivel.

6.2 Procedimientos de auditoría para recabar pruebas de auditoría

18) Los procedimientos de auditoría pueden consistir en una combinación de los siguientes elementos: a) revisión de la documentación, b) observación, pruebas de recorrido, entrevistas, cuestionarios, c) análisis de datos electrónicos, relativos, por ejemplo, a registros de auditoría de diversos tipos, d) evaluación de la vulnerabilidad /pruebas de penetración. En caso de que el auditor vaya a llevar a cabo evaluación de la vulnerabilidad o pruebas de penetración, podrán ser necesarios convenios y acuerdos con la entidad auditada para llevar a cabo tales pruebas intrusivas, así como garantías jurídicas e indemnizaciones cuando sea necesario. Si la evaluación de la vulnerabilidad o pruebas de penetración han sido llevadas a cabo por un tercero, los resultados de dichas pruebas podrán incorporarse como parte de la evidencia de auditoría. En este caso, el auditor obtiene una comprensión suficiente del alcance de la evaluación de la vulnerabilidad /pruebas de penetración, así como de las constataciones y de sus consecuencias.

19) Para evaluar la seguridad física y del entorno, además de la revisión de la documentación, las entrevistas, etc., el auditor podrá considerar una visita física (o inspección conjunta) del centro de datos como un procedimiento de auditoría complementario.

20) El auditor podrá evaluar la adecuación de las normas, directrices y procedimientos diseñados para poner en práctica la política de seguridad de la información y las políticas de notificación y gestión de incidentes y problemas.

21) La auditoría del proceso de gestión de riesgos podrá incluir el examen de la frecuencia de las revisiones periódicas del riesgo y la adecuación de las medidas de seguimiento para mitigar los riesgos detectados y evaluados. La decisión sobre los umbrales de aceptación de riesgos (y la consiguiente aceptación de los riesgos residuales) es una decisión de gestión.

22) Las políticas de identificación, clasificación y control de los activos de información están vinculadas al proceso de gestión de riesgos (en particular, a la identificación y evaluación de riesgos). Entre otros procedimientos de auditoría, puede examinarse si las políticas son comprendidas por los usuarios y si se aplican de manera eficaz.

23) Entre otros procedimientos de auditoría sobre autenticación, autorización y controles de acceso, puede examinarse si se aplica la autenticación multifactor (que normalmente se añade a la autenticación mediante contraseña), si está prevista o prescrita por la política o el contrato.

24) Cuando deban examinarse los archivos de registro para evaluar si el control de acceso se ha aplicado según lo previsto, el análisis de los registros podrá implicar la recepción de volcados de datos o extractos. En caso de recibir volcados de datos de la entidad auditada para su análisis electrónico, los auditores pueden solicitar una carta, tal como se describe en el apartado 6.4 de la GUID 5100, con el fin de garantizar la integridad de los datos, la autenticación y el no repudio.

25) Para la auditoría de la gestión de incidentes de seguridad de la información, además de la revisión de los procesos y la documentación relativos a la identificación y el registro, la evaluación y la resolución de los incidentes, el auditor podrá considerar la posibilidad de llevar a cabo una investigación sobre la adecuación de la resolución a partir de una muestra de usuarios (cuando tales usuarios hayan identificado y registrado los incidentes).

26) Una auditoría de la seguridad de la información puede incluir una evaluación de la planificación y la aplicación de los planes de continuidad del negocio y recuperación tras un desastre con objeto de evaluar el aspecto de «disponibilidad» de los servicios de información, así como la seguridad de la información durante la recuperación tras un desastre. De otro modo, estos aspectos pueden cubrirse en el marco de una auditoría de la gestión de las operaciones de los sistemas de información.

6.3 Consideraciones relativas a los acuerdos de externalización

27) Por lo que se refiere a la seguridad de la información entre proveedores / relaciones externalizadas, la entidad auditada sigue siendo responsable de la seguridad de la información, aunque la responsabilidad de determinadas actividades de los sistemas de información se haya externalizado a un proveedor externo. Además, son significativos aspectos como la separación de funciones contradictorias (por ejemplo, entre los equipos de desarrollo, ensayo y producción), tanto si el desarrollo/la aplicación/las operaciones y el mantenimiento del sistema de información se llevan a cabo internamente como si se realizan a través de un proveedor externo.

7

ELABORACIÓN DE INFORMES RELATIVOS A UNA AUDITORÍA DE LA SEGURIDAD DE LA INFORMACIÓN

28) En el caso de las auditorías de la seguridad de la información, pueden seguirse las orientaciones sobre la evaluación de la evidencia de auditoría y la elaboración de informes con arreglo a la ISSAI 400, así como las orientaciones adicionales con arreglo a la GUID 5100 sobre los informes (sección 7, en la que también se considera aventurado notificar riesgos de seguridad antes de que se adopten los controles necesarios para mitigar los riesgos).

29) La presentación de informes sobre la seguridad de la información por parte de los auditores puede tener en cuenta el posible impacto empresarial de exponer deficiencias técnicas y riesgos para la seguridad en público. En tales casos, el auditor podrá utilizar mecanismos adecuados, como, por ejemplo, ocultación de información delicada o cartas de gestión para compartir con la entidad auditada los detalles y el posible impacto del riesgo.

30) La información puede tener en cuenta, además de la perspectiva de las partes interesadas habituales de las auditorías del sector público, las perspectivas específicas de otros interlocutores, como los proveedores técnicos de apoyo externalizados a las entidades auditadas.

31) El auditor podrá formular recomendaciones para mejorar la seguridad de la información. Al elaborar las recomendaciones, el auditor podrá tener en cuenta cualquier consecuencia práctica para la entidad auditada, incluido el coste de ejecución.

8

SEGUIMIENTO

32) El auditor tiene en cuenta los seguimientos de conformidad con los principios de la auditoría de cumplimiento de la ISSAI 400.

33) Los sistemas informáticos evolucionan constantemente. A modo de ejemplo, cada vez más, los sistemas informáticos están alojados en la web o en la nube. El auditor podrá tener en cuenta estos cambios significativos a la hora de decidir el calendario de las auditorías de seguimiento.

34) Al planificar un seguimiento, el auditor podrá tener en cuenta factores como la tecnología disponible, los costes y la compatibilidad del sistema que puedan afectar a la capacidad de la entidad auditada para abordar las conclusiones de la auditoría y aplicar las recomendaciones.

Preguntas de alto nivel sugeridas para la auditoría

Este anexo contiene preguntas de auditoría de alto nivel sobre el asunto de la auditoría de la seguridad de la información a modo de orientación; solo es indicativo, no exhaustivo. La pertinencia de los objetos dependerá de que la entidad auditada esté obligada por ley u otras obligaciones a cumplir los criterios asumidos en los objetivos. Los cuestionarios de auditoría detallados dependerían del tipo de sistema de información, organización, marco y alcance del encargo de auditoría, etc.

SÍ No	Ámbito de seguridad de la información	Objetivo	Comentarios
1	Política de seguridad de la información	Si dicha política se define, adopta y comunica.	Esta política también debe revisarse periódicamente.
2	Estructura de la organización de la seguridad de la información	Si dicha estructura de gobernanza se ha constituido claramente como responsable de la seguridad de la información.	Los auditores podrán examinar la claridad de las definiciones, la constitución, la composición y el mandato.
		Si se han definido las condiciones del personal en el marco de esta estructura de gobernanza, las funciones individuales y el mecanismo de presentación de informes.	Dentro de la organización debe existir una separación de funciones, con cometidos y responsabilidades distintos, para cada puesto, con una jerarquía de notificación para la elevación de asuntos a órganos superiores.
		Si se han abordado los aspectos de seguridad relativos a los recursos humanos relacionados con los sistemas de información.	Los controles relacionados con los recursos humanos deben aplicarse en todas las fases de la gestión de recursos humanos.
		Si la organización promueve una cultura de seguridad de la información entre el personal de todos los niveles.	La cultura organizativa desempeña un papel importante para determinar el nivel de seguridad de la información en la organización.
3	Gestión de activos de información	Si se ha realizado periódicamente un inventario de los activos de los sistemas de información y si se han determinado los requisitos de seguridad para cada tipo de activo.	Los activos de información deben clasificarse, etiquetarse y gestionarse adecuadamente.
4	Desarrollo, adquisición y mantenimiento de sistemas de información	Si se han definido, adoptado y comunicado los aspectos de seguridad de cada uno de estos procesos.	La seguridad de la información debe ser una consideración primordial durante todo el ciclo de vida.
		Si los proveedores garantizan la seguridad de la información en todas las interacciones.	En función de los riesgos, verificar si la entidad auditada se ha asegurado de que el código y los módulos del sistema de información desarrollado / adquirido haya sido revisado mediante recursos cualificados internos

			o de terceros para garantizar que no existen funcionalidades ocultas que puedan comprometer la confidencialidad, integridad y disponibilidad de los datos.
5	Operaciones informáticas	Si se ha definido, adoptado y comunicado la seguridad de las operaciones informáticas.	Examinar los contratos / acuerdos de nivel de servicio para verificar la incorporación de la no divulgación, la no competencia, la no modificación sin autorización, la no transmisión y otras disposiciones estándar relativas a la garantía de la confidencialidad, la integridad y la disponibilidad de los datos con las partes a las que se externalizan las operaciones informáticas.
6	Seguridad física y del entorno	Si se ha garantizado la seguridad del entorno físico del sistema de información.	Verificar si existen barreras físicas (puertas exteriores, puertas interiores, guardias de seguridad) que requieren la identificación del personal y restringen el acceso al *hardware* de almacenamiento, como servidores, únicamente al personal autorizado. La gestión de infraestructuras y servicios es un aspecto importante del ecosistema global de seguridad.
7	Seguridad de las redes y las comunicaciones	Si se garantiza la seguridad de la información durante la comunicación.	Verificar si los canales de comunicación garantizan el cifrado de los mensajes a fin de evitar la interceptación por terceros y la pérdida de confidencialidad; verificar también el uso de controles criptográficos para las comunicaciones digitales de carácter formal.
		Si la arquitectura de seguridad de la red es adecuada para garantizar la seguridad de la información.	Cuando proceda, los auditores podrán examinar la existencia de controles criptográficos y otros controles de ciberseguridad.
8	Continuidad del negocio y recuperación tras un desastre	Si se han abordado los aspectos de seguridad relacionados con estos procesos y si la seguridad de la información es adecuada para la	Los auditores podrán comprobar si la instalación de seguridad de la información es adecuada durante el proceso de recuperación tras un desastre.

		transición y el funcionamiento de la recuperación tras un desastre.	
9	Cumplimiento de la normativa	Si se han cumplido los requisitos legales relacionados con los aspectos de seguridad de la información.	Los auditores deben realizar controles del cumplimiento de las disposiciones legales y reglamentarias en todos los demás ámbitos, según proceda. La provisión puede requerir una certificación o garantía específica relacionada con la información que deben obtener las entidades. Los auditores también podrán examinar el alcance y la validez de esta certificación.