Referencia: GUID 5100 Guidance on Audit of Information Systems, aprobada en el XXIII INCOSAI, 09/2019

Documento elaborado por la Comisión Técnica de los OCEX el 23/10/2020
aprobado por la Conferencia de Presidentes de ASOCEX el 03/12/2020

1. Introducción

1.1 Esta GPF-OCEX 5300 proporciona el marco general para llevar a cabo auditorías de sistemas de información dentro de la metodología de los OCEX.

1.2 El marco establecido en esta guía es coherente con los *Principios fundamentales de la fiscalización del sector público* (ISSAI-ES 100), *los Principios fundamentales de la fiscalización o auditoría financiera* (ISSAI-ES 200), los *Principios fundamentales de la fiscalización operativa* (ISSAI-ES 300), los *Principios fundamentales de la fiscalización de cumplimiento* (ISSAI-ES 400) y las NIA-ES-SP.

1.3 Los Órganos de Control Externo (OCEX) tienen el mandato legal de auditar a las administraciones públicas y sus entidades dentro de su ámbito de actuación. A través de sus actividades, los OCEX tienen como objetivo promover la eficiencia, la rendición de cuentas, la eficacia y la transparencia de las administraciones públicas.

1.4 Las administraciones y otras entidades del sector público han adoptado continuamente innovaciones en tecnología de la información (TI) en sus sistemas de información, con el fin de mejorar la eficiencia y la eficacia en su funcionamiento y en la prestación de los servicios públicos. Las TI han hecho posible capturar, almacenar, procesar, recuperar y proporcionar información electrónicamente. Además, el modo de prestación de servicios públicos ha pasado de lo físico a lo electrónico, dando lugar a que las administraciones públicas tengan que funcionar como plataformas digitales que proporcionan servicios, así como infraestructura para otros sistemas de información basados en TI.

1.5 Esta transición a sistemas de información automatizados y al procesamiento electrónico por parte de las entidades auditadas del sector público ha provocado un **cambio significativo en el entorno en el que trabajan los OCEX.** Es necesario garantizar que las entidades del sector público adoptan controles internos informatizados para mantener la confidencialidad, integridad, autenticidad, disponibilidad y trazabilidad de los datos[1]. En este entorno es imperativo que los OCEX **desarrollen las capacidades adecuadas** para llevar a cabo exámenes exhaustivos de los controles relacionados con los sistemas de información y las comunicaciones.

[1] Véase el Esquema Nacional de Seguridad.

2. Objetivo de esta guía

2.1 Las ISSAI-ES 100, 200, 300 y 400 establecen los principios básicos de fiscalización relacionados con la auditoría financiera, la auditoría operativa y la auditoría de cumplimiento. Estas ISSAI-ES hacen referencia a los principios generales, procedimientos, normas y expectativas de un auditor público y también son aplicables a las auditorías de los sistemas de información.

2.2 El objetivo de esta guía es **proporcionar orientación a los auditores sobre cómo llevar a cabo auditorías operativas y/o de cumplimiento relacionadas específicamente con materias relativas a los sistemas de información y las comunicaciones** o cuando la auditoría de los sistemas de información forme parte de un trabajo de auditoría más grande que puede ser auditoría financiera, de cumplimiento u operativa.

2.3 El contenido de esta guía será aplicado por los auditores en las distintas etapas del proceso de auditoría: planificación, ejecución, informe y seguimiento.

3. Definiciones

3.1 **Sistemas de información**. Un sistema de información es un conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. Los elementos de un sistema de información son: hardware, software, soportes de información, comunicaciones, instalaciones, personal y servicios provisionados por terceros.

3.2 **Auditoría de sistemas de información**. Puede definirse como el examen de los controles relacionados con los sistemas de información y comunicaciones, a fin de identificar los casos de desviación de los criterios, que a su vez se han identificado en función del tipo de auditoría (auditoría financiera, auditoría de cumplimiento o auditoría operativa).

4. Alcance

4.1 Esta guía puede ser utilizada por los auditores para llevar a cabo auditorías operativas y/o cumplimiento sobre los sistemas de información, así como cuando la auditoría de los sistemas de información forme parte de un trabajo de auditoría mayor que puede ser financiera, de cumplimiento y/o operativa.

5. Planificación de la auditoría de sistemas de información

5.1 Los OCEX adoptarán la planificación de auditoría basada en el análisis de riesgos para las auditorías de sistemas de información, de acuerdo con el proceso descrito en las ISSAI-ES 100/200/300/400, dependiendo de los objetivos de la auditoría.

Alcance de la auditoría

5.2 El trabajo de auditoría de sistemas de información estará determinado por el objetivo y el alcance de la auditoría. Algunos ejemplos podrían ser:

1. Evaluar los controles generales TI[2] y controles de aplicación[3] que influyen en la fiabilidad de los datos de los sistemas de información que tienen un impacto en los estados financieros de la entidad auditada.
2. Proporcionar seguridad sobre el cumplimiento con las leyes, las políticas y normas aplicables a la entidad auditada en los procesos de gestión de los sistemas de información.

[2] Ver la GPF-OCEX 5330.

[3] Ver la GPF-OCEX 5340.

3. Proporcionar seguridad de que los recursos de TI permiten alcanzar los objetivos de la organización de manera eficiente y eficaz, y que los controles generales y los controles de aplicación pertinentes son eficaces en la prevención, detección y corrección de casos de abuso, despilfarro e ineficiencia en el uso y gestión de los sistemas de información.
4. Evaluar el nivel de ciberseguridad de la entidad[4].

5.3 Sobre la base de la valoración del riesgo, el alcance de una auditoría de sistemas de información podrá referirse a cualquiera de, o a todos, los siguientes dominios o áreas de la entidad auditada:

A. Marco organizativo
   A.1 Cumplimiento de legalidad
   A.2 Estrategia de seguridad
   A.3 Organización y personal de TI
   A.4 Marco normativo y procedimental de seguridad
B. Gestión de cambios en aplicaciones y sistemas
   B.1 Adquisición de aplicaciones y sistemas
   B.2 Desarrollo de aplicaciones
   B.3 Gestión de cambios
C. Operaciones de los sistemas de información
   C.1 Inventario de hardware y software
   C.2 Gestión de vulnerabilidades
   C.3 Configuraciones seguras
   C.4 Registro de la actividad de los usuarios
   C.5 Servicios externos
   C.6 Protección frente a malware
   C.7 Protección de las instalaciones e infraestructuras
   C.8 Gestión de incidentes
   C.9 Monitorización
D. Controles de acceso a datos y programas
   D.1 Uso controlado de privilegios administrativos
   D.2 Mecanismos de identificación y autenticación
   D.3 Gestión de derechos de acceso
   D.4 Gestión de usuarios
   D.5 Protección de las redes y comunicaciones
E. Continuidad del servicio
F. Gestión de controles de aplicaciones

5.4 Los OCEX al definir el alcance de la auditoría de sistemas de información pueden seleccionar el período de tiempo para el análisis de la auditoría (por ejemplo, un año, tres años, etc.). Se seleccionará un período de tiempo adecuado, que sea relevante para los objetivos definidos para la auditoría.

Equipos integrados

5.5 Cuando una auditoría de sistemas de información forma parte de una auditoría financiera, operativa o de cumplimiento, el OCEX **debe garantizar que el equipo de auditoría en su conjunto trabaje de manera integrada para alcanzar el objetivo general de auditoría.** Para lograr una integración efectiva, los OCEX deberán documentar detalladamente en las directrices técnicas/memoria de planificación de la auditoría:

[4] Ver las GPF-OCEX 5313 y 5314.

1. El trabajo que deben realizar los auditores de sistemas de información;
2. La forma de intercambio de información entre los auditores de sistemas de información y los otros auditores;
3. Identificar qué sistemas de información y objetivos de control están dentro del alcance de la auditoría;

5.6 Los OCEX deben garantizar que **el equipo de auditoría esté compuesto por miembros que colectivamente tienen la competencia** para llevar a cabo las auditorías de sistemas de información y para alcanzar los objetivos de auditoría previstos.

5.7 Los **conocimientos, habilidades y competencias** necesarios pueden adquirirse mediante una combinación de formación, incorporación de personal, y participación de expertos externos.

5.8 Los OCEX deben garantizarán que **los equipos de auditoría de sistemas de información tengan colectivamente** la capacidad de:

1. Comprender los elementos técnicos de un sistema de información, incluidos todos los elementos relevantes de las aplicaciones revisadas, a fin de poder acceder y utilizar la infraestructura de TI para el proceso de auditoría.
2. Comprender las normas, procedimientos y el entorno en el que operan los sistemas de información y comunicaciones de la entidad auditada.
3. Comprender la integración de los procesos de gestión en el diseño y en la lógica de programación del sistema de información de la entidad auditada.
4. Aplicar tanto el conocimiento de los procedimientos de gestión como el tecnológico para evaluar el riesgo de burlar manualmente la configuración de un control del sistema para permitir un procesamiento excepcional de transacciones.
5. Evaluar el diseño y probar la eficacia operativa de los controles de aplicación en los sistemas de información relevantes.
6. Comprender la metodología de auditoría, incluidas las NIA-ES-SP y las guías prácticas de fiscalización de los OCEX.
7. Comprender los criterios de cumplimiento o de rendimiento de TI con los que se van a comparar los resultados de la auditoría, incluidos los marcos para la gestión de sistemas de información y comunicaciones, como COBIT[5], ITIL y TOGAF[6]; y del marco de seguridad establecido por el ENS.
8. Comprender las técnicas de auditoría de sistemas de información para recopilar evidencia electrónica de auditoría[7].
9. Comprender las herramientas de auditoría de sistemas de información para recopilar, analizar y reproducir los resultados de dicho análisis o volver a realizar las funciones auditadas[8].
10. Acceder y utilizar la infraestructura de sistemas de información para obtener y retener evidencias de auditoría.

[5] https://www.isaca.org/resources/cobit

[6] https://www.opengroup.org/togaf

[7] Ver GPF-OCEX 1503.

[8] Ver GPF-OCEX 5370.

11. Acceder y utilizar las herramientas de auditoría de sistemas de información para analizar las evidencias obtenidas.

5.9 Los OCEX pueden considerar **diferentes opciones** para asignar recursos humanos para las auditorías de sistemas de información. Se podría hacer estableciendo un grupo central con especialistas en TI que ayudan a otros equipos de auditoría de la OCEX a llevar a cabo estas auditorías o desplegando especialistas en TI según se requieran. A medida que aumenta el número de trabajos de auditoría de sistemas de información realizados, los OCEX pueden considerar la posibilidad de establecer un grupo especializado de auditoría de sistemas de información. A este grupo se le puede confiar la responsabilidad de llevar a cabo todas las auditorías de sistemas de información para el OCEX, e interactuar con otros equipos del OCEX que tengan conocimientos "históricos" de la entidad auditada, con el fin de obtener rápidamente una comprensión de las funciones de la entidad y de los procesos de gestión relacionados.

A medida que la tecnología se extiende e integra más en los sistemas de información, los OCEX garantizarán que todos los auditores adquieran las habilidades, de carácter general, de auditoría de sistemas de información.

5.10 Los OCEX pueden contratar **recursos externos**, especialistas para llevar a cabo las auditorías sistemas de información, en caso de no poder disponer de personal propio.

Los OCEX garantizarán que dichos recursos externos estén adecuadamente capacitados y familiarizados con las normas aplicables al OCEX, que su trabajo se supervise adecuadamente a través de un contrato o un acuerdo de nivel de servicio y la participación adecuada del personal de la OCEX en las etapas de planificación, ejecución, informe y seguimiento de la auditoría, que supervise el trabajo de los expertos externos y haga cumplir las directrices y los acuerdos de nivel de servicio.

Valoración de riesgos

5.11 Para llevar a cabo la **valoración de riesgos** en las auditorías de sistemas de información, los auditores pueden utilizar los principios establecidos en las ISSAI-ES 100, 200, 300, 400 y en la GPF-OCEX 1315, además de los utilizados en la realización de la materia específica de la auditoría de sistemas de información, tal como se indica a continuación:

1. El riesgo inherente consiste en la probabilidad de que ciertas características de los sistemas de información y comunicaciones de una entidad auditada, por su propia naturaleza, puedan tener un impacto adverso en la ejecución de la función que debe ser llevada a cabo por la entidad. Por ejemplo, un sistema de información de una entidad auditada que está obligado a poner a disposición pública información conlleva el riesgo operativo inherente que más allá de un límite de usuarios máximo previsto, el sistema de información puede no responder y la información no estaría disponible para ningún usuario.

   Si bien la entidad auditada puede adoptar controles para mitigar los riesgos inherentes, en muchos casos, la entidad puede simplemente tolerar la existencia de tales riesgos, dentro de un nivel de riesgo aceptable. El riesgo inherente puede valorarse antes de que los auditores consideren la influencia del riesgo de control o detección.

2. El riesgo de control para un sistema de información y comunicaciones consistiría en la probabilidad de que los controles de TI que han sido adoptados por la entidad auditada no puedan mitigar el impacto adverso para el que fueron diseñados.

   Por ejemplo, un sistema de información de una entidad auditada al que se requiera garantizar que el acceso a los datos confidenciales se limite al personal autorizado puede

adoptar el control de exigir la presentación de un nombre de usuario y contraseña por parte del personal que intente obtener acceso. El riesgo de control en esta situación es que el nombre de usuario y la contraseña no son adecuadamente seguros y pueden ser adivinados por personal no autorizado a través de intentos repetidos, lo que resulta en la pérdida de confidencialidad y un posible impacto adverso en la entidad. Una entidad que insiste en el uso de contraseñas seguras y no triviales que tengan una combinación de letras, números y símbolos especiales, e impide que el sistema de información conceda el acceso al nombre de usuario más allá de un cierto número de intentos fallidos tienen un riesgo de control menor que uno que no tiene estas características.

3. El riesgo de detección consistiría en la probabilidad de que el auditor no detecte la ausencia, fallo o insuficiencia de los controles de TI adoptados por una entidad, que pueden tener un impacto potencialmente adverso en la entidad.

5.12 Para llevar a cabo valoraciones del riesgo de los sistemas basados en TI, los OCEX pueden seleccionar una metodología adecuada para ese propósito. Tales metodologías pueden ir desde clasificaciones simples del perfil de riesgo del entorno de TI de la entidad auditada como alta, media y baja basada en el conocimiento de la entidad y su entorno y en el juicio profesional del equipo de auditoría de sistemas de información de un OCEX, a cálculos más complejos y numéricos que cuantifiquen la calificación de riesgo basada en datos objetivos recopilados de la entidad auditada.

Materialidad

5.13 La **materialidad** en la auditoría de sistemas de información puede decidirse en el marco general para decidir la materialidad en una OCEX. La perspectiva de la materialidad puede variar dependiendo de la naturaleza de la participación de la auditoría sistemas de información.

6. Realización de la auditoría de sistemas de información

6.1 Los OCEX pueden llevar a cabo auditorías de sistemas de información de acuerdo con el proceso descrito para las auditorías financieras (ISSAI-ES 200), auditorías de operativas (ISSAI-ES 300) y auditorías de cumplimiento (ISSAI-ES 400), según sea el caso, en función de la naturaleza del trabajo.

6.2 Específicamente para una auditoría de sistemas de información, los auditores solicitarán la debida cooperación y apoyo de la entidad auditada para completar la auditoría, incluido el acceso a registros electrónicos e información. Los auditores pueden identificar el modo de acceso a los datos electrónicos en el formato necesario para permitir el análisis, de acuerdo con la entidad auditada. El modo de acceso a los datos dependerá de cada tipo de auditoría y de las características de la entidad auditada.

6.3 Antes de iniciar la evaluación de los controles en un sistema de información, los auditores deben adquirir una comprensión de la arquitectura del sistema, de los datos subyacentes (modelo de datos) y sus fuentes, con el fin de identificar las herramientas y técnicas de auditoría necesarias.

6.4 Al recibir paquetes de datos de la entidad auditada, los auditores deben asegurarse de que cada paquete de datos vaya acompañado de una carta de la entidad auditada que especifique:

1. El origen (con referencia a la marca temporal de generación del volcado de datos o número hash para el volcado de datos) de los datos con el fin de garantizar su integridad, autenticación y el no repudio.

2. Los parámetros de extracción utilizados para crear el volcado de datos, es decir, las consultas utilizadas o los informes de ejecución.

3. Si no se recibe esa carta de la entidad auditada, los auditores podrán generar documentos internos señalando información importante, como la fecha en que se entregaron los datos, de qué archivo se creó el volcado de datos y si los datos fueron del entorno de producción o de algún otro entorno, etc.

6.5 Los auditores podrán realizar una evaluación de los controles de TI (controles generales y de aplicación) implantados por la entidad auditada, a fin de examinar su fiabilidad y suficiencia. La evaluación se puede llevar a cabo utilizando una combinación adecuada de las siguientes técnicas: entrevista, cuestionario, observación, prueba paso a paso, flujograma, captura y análisis de datos, verificación, recálculo, reprocesamiento y confirmación de terceros. El alcance de la evaluación de los controles de TI puede incluir un examen que:

1. La política de seguridad de los sistemas de información ha sido definida, adoptada y comunicada.
2. La estructura de gobierno de SI se aplica y está operando.
3. El inventario de los activos de sistemas de información se mantiene actualizado y se han identificado los requisitos de incorporación, sustitución y eliminación.
4. Existen procedimientos para compartir infraestructuras y servicios comunes de sistemas de información con otras entidades públicas.
5. Se han definido, adoptado y comunicado procedimientos de desarrollo, adquisición y mantenimiento de sistemas de información (incluida la gestión del cambio).
6. Los procedimientos para las operaciones de TI (on-premises, out-sourcing, acuerdos de servicio) se han definido, adoptado y comunicado
7. Se han adoptado medidas para garantizar la seguridad física y las condiciones de trabajo físicas previstas.
8. Se han adoptado medidas de formación y sensibilización de los recursos humanos para garantizar la confidencialidad, integridad y disponibilidad de la información, así como el cumplimiento de los requisitos de la estructura de la política y la gobernanza de SI.
9. Se han adoptado medidas para garantizar la confidencialidad, integridad y disponibilidad de diversos modos y canales de comunicación.
10. Se han adoptado medidas para la gestión de la seguridad de la información.
11. Se han adoptado medidas para la gestión del cumplimiento legal.
12. Se han adoptado medidas para la continuidad del servicio y la gestión de la recuperación ante desastres.
13. Los controles de aplicación adoptados en cada sistema de información son adecuados y fiables. Dicha evaluación incluirá la identificación de componentes significativos de la aplicación, la identificación de la criticidad de la aplicación para la entidad, la revisión de la documentación disponible, la entrevista del personal, la comprensión de los riesgos de control de la aplicación y su impacto en la entidad, y el desarrollo de pruebas para examinar la adecuación y fiabilidad de dichos controles de aplicación.

6.6 La evaluación de los controles generales TI y de aplicación puede abarcar las políticas, procedimientos, personas y sistemas de la entidad auditada, de acuerdo con los objetivos de auditoría de sistemas de información.

6.7 Dependiendo del objetivo de la auditoría, los auditores pueden ocuparse del diseño, la implementación y la eficacia operativa de los controles.

Cuando el auditor se ocupa del diseño del control, una entrevista o revisión de las reglas de gestión documentadas puede ser suficiente.

Cuando el auditor se ocupa de la implementación de los controles, la entrevista puede no ser suficiente y puede ser necesario llevar a cabo una prueba de recorrido o paso a paso, o realizar un análisis de datos para constatar que se ha aplicado el control tal como se diseñó.

Por último, si el auditor se ocupa de la eficacia operativa del control, puede estar obligado a revisar una muestra de transacciones para demostrar que el control ha funcionado eficazmente durante todo el período auditado.

6.8 Los auditores también deben considerar cómo las pruebas sobre los **controles generales TI** afectan a la naturaleza, el momento de realización y extensión de las pruebas necesarias para obtener garantías sobre el funcionamiento de los controles de aplicación. Si el auditor ha obtenido evidencia de auditoría suficiente y apropiada sobre la eficacia de los controles generales que respaldan el acceso lógico del personal a los sistemas informáticos y la gestión del cambio en el entorno de producción, puede ser capaz de concluir sobre la eficacia operativa de los procedimientos automatizados de control de aplicaciones. Esto se puede hacer revisando una muestra más pequeña de transacciones porque la eficacia del entorno de TI general proporciona evidencia al auditor sobre la eficacia del control de la aplicación en el período pertinente. En el caso de los procedimientos manuales de controles de aplicación, los auditores pueden tener que revisar un tamaño de muestra adecuado al nivel de confianza seleccionado.

Técnicas de análisis de datos

6.9 Sobre la base de la evaluación de los controles informáticos, los auditores pueden identificar áreas prioritarias para realizar pruebas sustantivas, que implican pruebas detalladas de los controles de TI mediante el empleo de diversas técnicas de auditoría asistida por ordenador (CAAT) para la consulta, extracción y el análisis de datos. Los auditores pueden diseñar y ejecutar pruebas sustantivas para fundamentar los objetivos de auditoría. Los auditores seleccionarán los CAAT apropiados, en función de sus necesidades.

6.10 Los auditores utilizarán CAAT para ejecutar técnicas de auditoría de sistemas de información, como análisis de logs de usuarios, informes de excepciones, comparación de archivos, estratificación, muestreo, comprobaciones duplicados, detección de brechas, análisis de antigüedad, cálculos de campos virtuales, etc. Las ventajas del uso de CAAT incluyen el análisis de grandes volúmenes de datos, la repetibilidad de las pruebas en diferentes conjuntos de datos y con diferentes criterios y la documentación automatizada de las pruebas de auditoría y los resultados con marcas de tiempo.

6.11 Es posible que los auditores no siempre estén en condiciones de examinar todas las instancias, transacciones, módulos o sistemas de TI, dadas las limitaciones de recursos y las relaciones coste-beneficio del ejercicio de auditoría. En tal situación, los OCEX pueden adoptar, sobre la base de consideraciones de materialidad, muestreos de auditoría para un examen detallado y extraer conclusiones razonables de auditoría. Los OCEX pueden utilizar CAAT apropiadas para llevar a cabo diferentes tipos de muestreo y determinar un tamaño de muestra adecuado, dependiendo de los riesgos inherentes y de control subyacentes. Se obtienen muestras de auditoría con el fin de proporcionar al auditor una base razonable sobre la que extraer conclusiones sobre toda la población de datos, sobre la base de conclusiones extraídas de la aplicación de procedimientos de auditoría y análisis a la muestra de auditoría. Los auditores podrán considerar la finalidad del procedimiento de auditoría y las características de la población de la que se extraerá la muestra, y determinar un tamaño de muestra suficiente para reducir el riesgo de muestreo dentro de un nivel aceptable.

La auditoría en un entorno de TI puede facilitar el análisis del 100 por ciento de la población, especialmente en la etapa de evaluación preliminar. Sin embargo, para llevar a cabo pruebas sustantivas, pueden ser necesarias muestras. Al realizar un muestreo dentro del ámbito de una auditoría financiera, los auditores de sistemas de información pueden aplicar NIA-ES-SP 1530 para la selección de muestras.

6.12 Los auditores deben garantizar que la **evidencia electrónica** recopilada y documentada sea suficiente, fiable y precisa para sostener los hallazgos y las conclusiones de auditoría. Dicha evidencia electrónica puede consistir en archivos de datos, registros de usuarios, modelos analíticos, informes de gestión de sistemas de información, etc. y deben recopilarse y almacenarse adecuadamente de manera que estén disponibles para garantizar la exactitud y validez del proceso de auditoría. Las evidencias recopiladas durante una auditoría de sistemas de información pueden tener sellos de tiempo y detalles que contienen los pasos detallados del análisis de datos llevado a cabo, de modo que haya trazabilidad sobre cuándo se creó, almacenó y modificó por última vez la evidencia, para mitigar el riesgo de cambios posteriores.

6.13 La **documentación** de la auditoría de sistemas de información debe conservarse y protegerse de cualquier modificación y eliminación no autorizada. Los OCEX pueden desarrollar nuevas normas para la conservación de la documentación de la auditoría de sistemas de información o adaptar las existentes. El período de conservación dependerá del mandato legal de cada OCEX. Se puede prestar especial atención a los medios de soporte, al formato, su esperanza de vida y los requisitos de almacenamiento de estos datos, para garantizar que los datos sean legibles dentro del plazo definido en la política de conservación y archivado de datos de cada OCEX. Esto puede requerir la conversión de datos de un formato a otro para mantenerse al día con los avances tecnológicos y la obsolescencia.

Auditores externos

6.14 En caso de examen de los informes preparados por **auditores externos**, los auditores adoptarán procedimientos adecuados para garantizar la confianza en dichos informes. Si, como resultado de tales procedimientos, se confía del contenido de dichos informes, dicha confianza debe divulgarse adecuadamente.

Comunicación con el auditado

6.15 Las ISSAI-ES señalan que los auditores deben establecer una **comunicación** eficaz durante todo el proceso de auditoría y mantener informada a la entidad auditada de todos los asuntos relacionados con la auditoría (*ISSAI-ES 100 párrafo 31*). En las auditorías que implican el trabajo de auditoría de sistemas de información, el resultado de la auditoría de sistemas de información puede, en algunos casos, comunicarse a la entidad a través de una carta separada. En estos casos, puede ser importante explicar cómo el resultado del trabajo de auditoría se relaciona con otras comunicaciones que forman parte de la misma auditoría financiera, de rendimiento o de cumplimiento y cómo los resultados del trabajo de auditoría de sistemas de información pueden ser relevantes para el informe de auditoría resultante.

7. Informes sobre la auditoría de sistemas de información

7.1 Dado que una auditoría de sistemas de información puede formar parte de una auditoría financiera, una auditoría operativa o una auditoría de cumplimiento, los auditores pueden considerar los requisitos de presentación de ese tipo de informes.

Por otra parte, cada OCEX puede tener sus propios criterios de presentación de informes basados en la importancia relativa de los hallazgos de auditoría. Asimismo, al informar en una auditoría de SI, se deben considerar las limitaciones legales e internas para la divulgación de información financiera y técnica.

7.2 Los auditores deben ser conscientes de la necesidad de limitar el uso de la jerga técnica. A pesar de la naturaleza técnica de una auditoría sistemas de información, los auditores deben asegurarse de que el informe sea plenamente comprensible por la dirección de la entidad auditada, las partes interesadas y el público en general. Los auditores pueden incorporar un glosario de términos utilizados en los informes, definiciones de acrónimos o de términos con una explicación basada en el contexto.

7.3 Los auditores deben considerar el posible impacto negativo del informe una vez que se publique y de la sensibilidad y confidencialidad de la información presentada en el informe.

Por ejemplo, si el informe de auditoría de sistemas de información detecta algunos riesgos de seguridad en el sistema de información de la entidad auditada y se publican antes de que se hayan adoptado los controles necesarios para mitigar los riesgos, la vulnerabilidad del sistema de información puede estar expuesta al público. En tal escenario, los auditores pueden considerar opciones como la presentación de informes sólo después de que se hayan adoptado los controles necesarios, o no informar del riesgo exacto de seguridad en su totalidad, a fin de evitar posibles impactos adversos en la entidad auditada. Hay que tener cuidado en no divulgar información como contraseñas, nombres de usuario, identificadores e información personal.

8. Seguimiento

8.1 Deberá efectuarse un seguimiento posterior de las deficiencias de control y de las recomendaciones señaladas en el informe de auditoría.