INTOSAI
IDI
DEVELOPMENT INITIATIVE

INTOSAI
Working Group on IT Audit

WGITA – MANUAL DE LA IDI SOBRE AUDITORÍA DE TI PARA ENTIDADES FISCALIZADORAS SUPERIORES

(REVISIÓN 2022)

WGITA – MANUAL DE LA IDI SOBRE AUDITORÍA DE TI PARA ENTIDADES FISCALIZADORAS SUPERIORES (REVISIÓN 2022)

DECLARACIÓN DE CALIDAD CORRESPONDIENTE AL MANUAL DE LA IDI - WGITA SOBRE AUDITORÍA DE TI PARA ENTIDADES FISCALIZADORAS SUPERIORES (REVISIÓN 2022), VERSIÓN 1 (19 DE DICIEMBRE DE 2022)

En el documento elaborado conjuntamente por las Presidencias de Objetivos de la INTOSAI y la IDI titulado *Aseguramiento de la calidad de los bienes públicos de la INTOSAI que se elaboran y publican fuera del debido proceso*, se enuncian los tres niveles de aseguramiento de la calidad que se exponen a continuación:

ASEGURAMIENTO DE LA CALIDAD DE LOS BIENES PÚBLICOS DE LA INTOSAI QUE SE ELABORAN Y PUBLICAN FUERA DEL DEBIDO PROCESO - Niveles de Aseguramiento de la Calidad

Nivel 1: Productos que se han sometido a procesos de aseguramiento de la calidad equivalentes al debido proceso de la INTOSAI, incluido un período prolongado y transparente de exposición pública (90 días).

Nivel 2: Productos que se han sometido a procesos de aseguramiento de la calidad más limitados en los que intervienen partes interesadas externas al organismo o grupo de trabajo responsable de la elaboración inicial de tales productos. Los procesos de aseguramiento de la calidad incluyen, por ejemplo, aplicaciones piloto, pruebas, y la invitación a partes interesadas clave a formular comentarios, aunque sin la rigurosidad de una exposición pública plena durante un período de 90 días.

Nivel 3: Productos que se han sometido a rigurosas medidas de control de calidad dentro del organismo o grupo de trabajo responsable de su elaboración.

Es posible que para los distintos BPG se requieran diferentes niveles de aseguramiento de la calidad. Este BPG se ha elaborado de acuerdo con el Nivel 2 de aseguramiento de la calidad.

Protocolo de Aseguramiento de la Calidad: Versión 2.0

El Protocolo de la IDI para el Aseguramiento de la Calidad (AC) de los Bienes Públicos Globales de la IDI define medidas destinadas a garantizar la calidad sobre la base de los tres niveles de aseguramiento mencionados anteriormente. Para el Nivel 2 de aseguramiento de la calidad, estas medidas incluyen: la aprobación del Consejo Directivo de la IDI para crear el BPG; la conformación de un equipo competente para el desarrollo de productos; la revisión entre pares por parte de expertos externos al equipo de desarrollo; la modificación basada en revisiones; la corrección, edición y traducción del documento por personas competentes; la exposición pública ante partes interesadas relevantes; y las aprobaciones correspondientes de la Versión 1 del BPG.

Actualizaciones de este BPG

Para asegurarse de que esté BPG conserve su relevancia, la IDI y el grupo de trabajo sobre auditoría de TI (WGITA) de la INTOSAI realizarán revisiones menores de este manual con una periodicidad bienal. Si resultase necesario realizar cambios substanciales, es posible que la IDI y el WGITA decidan elaborar una versión modificada del manual. Tales decisiones se tomarán en función de la revisión bienal efectuada. Las revisiones importantes tendrán lugar de acuerdo con el Protocolo de aseguramiento de la calidad de la IDI. Las revisiones menores normalmente no estarán sujetas a este Protocolo.

Tanto la IDI (el eje de trabajo EFS Relevantes de la IDI) como el WGITA son propietarios de forma conjunta de este BPG, siendo además responsables por su mantenimiento.

Proceso de revisión de aseguramiento de la calidad

Shourjo Chatterjee (Unidad de Apoyo Estratégico, IDI) ha llevado a cabo una revisión de AC del proceso seguido para la elaboración de este BPG, en función del Protocolo de AC, Versión 2.0. El revisor de AC está familiarizado con el protocolo de la IDI para el AC de BPG y no participó en la elaboración del BPG. Este proceso de revisión de AC está diseñado para brindar a todas las partes interesadas la seguridad de que la IDI ha aplicado las medidas de control de calidad indicadas anteriormente, diseñadas para cumplir con el Nivel 2 de aseguramiento de la calidad.

Resultados de la revisión de aseguramiento de la calidad

De la revisión de AC seguida para la elaboración de este BPG surge que se ha seguido el Protocolo según las exigencias de aseguramiento de la calidad del Nivel 2 en todos sus aspectos.

Conclusión

Sobre la base de la revisión de AC practicada, la IDI y el WGITA aseguran a los usuarios de este Bien Público Global (BPG) que el presente documento ha sido sometido a un proceso de aseguramiento de la calidad equivalente al debido Proceso del Marco de Pronunciamientos Profesionales de la INTOSAI (IFPP, por sus siglas en inglés).

E J Gørrissen
Einar Gørrissen (Feb 22, 2023 10:45 GMT+1)

Einar Gørrissen
Director General
Iniciativa de Desarrollo de la INTOSAI
19 de diciembre de 2022

Girish Chandra Murmu
Chair
Grupo de Trabajo sobre Auditoría de TI (WGITA) de la INTOSAI

TABLA DE CONTENIDOS

FIGURAS

PREFACIO

La auditoría de los procesos, controles y sistemas de la tecnología de la información, también denominada auditoría de TI, se ha convertido en uno de los temas medulares de las auditorías realizadas por las Entidades Fiscalizadoras Superiores (EFS) en todo el mundo. Esto constituye una respuesta natural a la crítica dependencia de dichos sistemas que experimentan los gobiernos y organizaciones del sector público. Los sistemas de TI utilizados deben proteger los datos y activos de la organización, además de apoyar su misión, objetivos financieros y demás objetivos específicos.

Aunque la creciente aplicación de la TI ha derivado en una mayor eficiencia de los negocios o actividades que se llevan a cabo, y una prestación más eficaz de servicios, sin embargo, ello ha traído consigo riesgos y vulnerabilidades vinculados con, por ejemplo, la digitalización de servicios y la mayor conectividad con otros sistemas y redes internas y externas. El rol de la auditoría de TI en cuanto a la certeza de que se dispone de los procesos para gestionar los riesgos y vulnerabilidades relevantes en materia de TI es esencial cuando lo que la EFS se propone es brindar información significativa acerca de la eficiencia y eficacia de las operaciones del gobierno y el sector público.

En 2014, el Grupo de Trabajo sobre Auditoría de TI (WGITA) de la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI) y la Iniciativa de Desarrollo de la INTOSAI (IDI), trabajaron en conjunto para elaborar el primer Manual sobre Auditoría de TI, cuyo objetivo era brindar a los auditores de las EFS normas y prácticas adecuadas reconocidas universalmente en materia de TI. La versión 2022 de dicho documento contiene una actualización de las explicaciones relativas a aquellas áreas principales en las que posiblemente los auditores de TI deban enfocarse al realizar auditorías de TI.

El manual elaborado por el WGITA/IDI sigue los principios generales de auditoría establecidos de conformidad con las Normas Internacionales de las Entidades Fiscalizadoras Superiores (ISSAI).[1] Este manual también se basa en marcos de TI reconocidos internacionalmente, como el marco COBIT de la ISACA, la Organización Internacional para la Normalización (ISO), y la guías y manuales de algunas EFS, en un intento por brindar a los usuarios información esencial y preguntas que han de formularse para la planificación y ejecución eficaces de auditorías de TI.

El proyecto de actualización este manual fue liderado la dirección del WGITA, a saber, la EFS de India, la EFS de los Estados Unidos de América y la IDI. El WGITA y la IDI desean agradecer a los integrantes del equipo, quienes trabajaron con denuedo en la elaboración de este documento orientativo. Los auditores de las EFS de Australia, Brasil, Fiji, India, Kuwait, Filipinas, Tanzania y los Estados unidos de América han realizado una valiosa contribución mediante el aporte de ejemplos de informes de auditoría de TI. Muchas gracias también a aquellas EFS que contribuyeron con sus valiosos comentarios y sugerencias acerca del manual.

[1] www.issai.org.

LISTA DE ABREVIATURAS

BCP	Plan de Continuidad del Negocio
CMMI	Integración del Modelo de Madurez de Capacidad®
DRP	Plan de Recuperación de Desastres
FISCAM	Federal Information Systems Controls Audit Manual
GAO	Oficina de Rendición de Cuentas de los Estados Unidos de América
GUID	Guía de la INTOSAI
IDI	Iniciativa de Desarrollo de la INTOSAI
IEC	International Electrotechnical Commission
INTOSAI	Organización Internacional de las Entidades Fiscalizadoras Superiores
ISCP	Plan de Contingencia de Sistema de Información
ISO	Organización Internacional de Normalización
ISSAI	Normas Internacionales de las Entidades Fiscalizadoras Superiores (en documentos más antiguos mencionadas ocasionalmente como Normas de la INTOASAI)
ITIL	Biblioteca de Infraestructura de Tecnología de la Información
KPI	Indicador Clave de Desempeño
NIST	Instituto Nacional de Normas y Tecnología, Departamento de Comercio de los EE. UU.
OLA	Acuerdo de Nivel Operativo
EFS	Entidad Fiscalizadora Superior
SDLC	Ciclo de Vida de Desarrollo de un Sistema
SLA	Acuerdo de Nivel de Servicio
WGITA	Grupo de Trabajo sobre Auditoría de TI

INTRODUCCIÓN

El carácter universal de las TI han modificado el modo en que todos trabajamos, en muchos aspectos, y la auditoría, en tanto profesión, no constituye una excepción a este fenómeno. Con el avance de la tecnología, los gobiernos y otras organizaciones del sector público han incorporado de un modo continuo innovaciones en materia de TI a sus sistemas de información, con el propósito de incrementarr la eficiencia y mejorar la prestación de los diversos servicios públicos.[2] La modalidad de prestación de los servicios públicos también ha transitado del ámbito físico al electrónico. Esta transformación condujo a que las organizaciones gubernamentales tengan que funcionar como plataformas digitales para la prestación de servicios al público, además de como proveedoras de infraestructura para los sistemas de TI en los que se apoyan. La digitalización de la información en curso, o el pasaje desde un formato analógico o manual hacia uno digital de los registros y datos, también ha reforzado la dependencia general de los sistemas de TI.

El ritmo al que la tecnología avanza es más acelerado que nunca, lo cual también acarrea consecuencias para las auditorías de TI. Los sistemas de TI son cada vez más complejos, tecnológicamente diversos, y dispersos en términos geográficos. Estos sistemas se encuentran interconectados con otros sistemas y redes internos y externos, lo que incluye Internet, acrecentándose así su complejidad. Las organizaciones gubernamentales están almacenando una mayor proporción de su información en sistemas basados en la nube,[3] con el propósito de adquirir servicios con mayor prontitud y reducir sus costos. No caben dudas de que la tenencia hacia una computación ubicua y un acceso más sencillo a la información continuará su marcha.

Sin embargo, los avances tecnológicos, han traído aparejados mayores riesgos y vulnerabilidades. Vale destacar que el crecimiento de sistemas y redes de TI basados en la Web ha aumentado los riesgos en materia de seguridad a los que las organizaciones gubernamentales se exponen. Estas organizaciones recopilan y procesan grandes cantidades de información personalmente identificable,[4] lo cual puede plantear desafíos para garantizar su privacidad. La pandemia de COVID-19 también acarreó desafíos sin precedentes para las organizaciones gubernamentales que necesitaban seguir adelante con sus tareas, debiendo asegurarse, al mismo tiempo, de que sus empleados realizaran su labor de manera segura y eficaz.

Estas tendencias, sumadas a la creciente sofisticación con la que actúan los *hackers* y otros sujetos que obran maliciosamente, aumentan el riesgo de que datos sensibles se vean comprometidos. La falta de eficacia en cuanto a la protección de sistemas y redes de una organización también puede afectar la prestación de servicios esenciales. En ese sentido, es necesario detectar cada vulnerabilidad nueva, evaluar el riesgo en términos de probabilidad e impacto, mitigarlo de acuerdo con la tolerancia al riesgo de la organización, y controlarlo en la medida en que sea posible.

---

[2]Los sistemas de información pueden definirse como una combinación de actividades estratégicas, operativas y gerenciales relacionadas con la recopilación, el procesamiento, el almacenamiento, la distribución y la utilización de la información y sus tecnologías relacionadas, mientras que la TI abarca el hardware, el software, las comunicaciones y demás instrumentos utilizados en relación con la entrada, el almacenamiento, el procesamiento, la transmisión y la salida de datos.

[3]La computación en la nube es un medio que permite el acceso a petición a conjuntos compartidos de recursos informáticos configurables (por ejemplo, redes, servidores, aplicaciones de almacenamiento y servicios) que pueden proveerse y ponerse en funcionamiento rápidamente.

[4]Información personalmente identificable es toda información que pueda utilizarse para distinguir o rastrear la identidad de una persona humana, como el nombre, la fecha y lugar de nacimiento, y otros tipos de información personal que puedan vincularse con esa persona, como, por ejemplo, aquella de índole médica, educativa, financiera y laboral.

Con el incremento de la inversión en sistemas de TI por parte de las organizaciones auditadas, y la creciente dependencia de ellos, es imperativo que el auditor de TI adopte una metodología y un enfoque adecuados. Esto puede contribuir a garantizar que la auditoría posibilite la detección de riesgos vinculados con la integridad de los datos, su disponibilidad, validez, potencial abuso, y privacidad, además de corroborar que se dispone de los controles que permiten mitigar tales riesgos. En un entorno de auditoría de TI, los controles son los procesos, herramientas y demás mecanismos de supervisión implementados para gestionar las funciones de TI y evitar riesgos y vulnerabilidades.

En un típico sistema de TI, especialmente cuando éste se implementa en un entorno en el que los controles son inadecuados, la organización auditada enfrenta numerosos riesgos que un auditor de TI debería estar en condiciones de identificar. E incluso en el caso de que la organización auditada hubiese implementado algunas medidas de reducción de riesgos, será necesario efectuar una auditoría independiente para asegurarse de que se dispone de los controles adecuados en materia de sistemas de información. Una auditoría como la señalada debería incluir la corroboración de que se han concebido los controles generales de TI[5] y los controles de aplicación[6] necesarios para minimizar la exposición a diversos riesgos, y que tales controles funcionan de manera eficaz y eficiente.

En síntesis, la transición hacia sistemas de TI y procesamiento digital por parte de las organizaciones auditadas del sector público, ha dado lugar a la necesidad de que las organizaciones de auditoría desarrollen las capacidades idóneas para realizar un examen minucioso de los controles relacionados con los sistemas de TI, que a su vez les permitan cumplir con sus mandatos de auditoría globales. Específicamente, existe la necesidad de asegurarse de que las organizaciones gubernamentales hayan adoptado los controles internos de TI relacionados con la confidencialidad, integridad, validez y disponibilidad de los datos.

Contenido y estructura del Manual

El propósito de este manual es brindar a los auditores de TI una orientación descriptiva sobre diferentes dominios de la auditoría de TI y se elaboró de acuerdo con los requisitos del Protocolo de la IDI para el Aseguramiento de la Calidad de los Bienes Públicos Globales. V2.0.[7]

En el Capítulo 1 de esta guía, los lectores encontrarán una reseña de la definición de auditoría de TI, los mandatos de las EFS, y el alcance y objetivos de las auditorías de TI. También contiene una explicación acerca de los controles generales de TI y los controles de aplicación, y la relación entre ambos tipos de controles. Estos dominios relacionados con el control se explican con mayor detalle en capítulos posteriores. El Capítulo 1 también describe el proceso de auditoría de TI y la metodología de la evaluación basada en riesgos para la selección de auditorías de TI. La descripción del proceso de auditoría de TI tienen un carácter genérico, y se basa en métodos de auditoría estándar[8] seguidos al realizar auditorías de sistemas de TI. Las tablas y diagramas que acompañan la descripción del proceso de auditoría tienen como fin brindar ejemplos ilustrativos y deberían adaptarse a los encargos de auditoría individuales. Los

[5]Los controles generales de TI no corresponden específicamente a una aplicación o a una serie de transacciones individuales; son controles aplicados a una implementación de TI y apoyan el desarrollo, instrumentación y operación de un sistema de TI. Tales controles habitualmente abarcan la gobernanza de TI, la organización y estructura de sistemas de información, el entorno y los aspectos físicos, la seguridad de dichos sistemas, la continuidad del negocio o actividad, y la gestión del acceso y la realización de cambios.

[6]Los controles de aplicación corresponden específicamente a un sistema de TI, y suponen el mapeo de las reglas del negocio o actividad en la aplicación, previéndose así la existencia de controles de entrada, procesamiento, salida y datos maestros.

[7] Este protocolo se encuentra disponible en http://www.idi.no/en/idi-library/global-public-goods

[8]Remítase, por ejemplo, a los siguientes documentos de la, Organización Internacional de las Entidades Fiscalizadores, *Normas Internacionales de las Entidades Fiscalizadoras Superiores (ISSAI) 100: Principios Fundamentales de la Auditoría del Sector Público* (2019) e ISSAI 5100 *Directrices sobre la Auditoría de Sistemas de Información* (2019).

usuarios del manual deben de considerar el proceso de auditoría en el contexto de la información relacionada contenida en las ISSAI y otros marcos y normas internacionales, además de remitirse a los manuales y directrices sobre procedimientos de auditoría de sus respectivas EFS para planificar y efectuar auditorías específicas.

Los Capítulos 2-8 contienen una descripción detallada de diferentes dominios de TI que ayudarán a los auditores de TI a detectar posibles áreas y procesos auditables. Al concluir cada capítulo se enumera una serie de riegos a nivel organizacional relacionados con el dominio de la TI, lo que ayudará a los auditores a detectar áreas de alto a riesgo potencialmente sujetas a auditoría. La orientación brindada acerca de cada dominio también ayudará a los auditores de TI a realizar la planificación correspondiente, ya sea que se trate de un dominio específico o una combinación de ellos, según el alcance y el objetivo de la auditoría de TI (por ejemplo, auditoría de desempeño o financiera). Por ejemplo, la orientación relacionada con la auditoría de la gobernanza de TI puede utilizarse para planificar una auditoría del mecanismo de gobernanza de TI de una organización, o una auditoría del entorno de controles generales, del cual la gobernanza de la TI constituye una parte importante.

El Apéndice I de este manual incluye una reseña de áreas emergentes en el ámbito de la auditoría de TI y brinda referencias para una lectura adicional a los usuarios interesados. El Apéndice II contiene enlaces a informes de auditoría identificados por diferentes EFS de todo el mundo, donde se ofrecen ejemplos valiosos del amplio conjunto de áreas de auditoría de TI analizadas en los Capítulos 2-8 de este manual.

La versión 2014 del Manual de Auditoría de TI incluía una serie de apéndices adicionales con orientación paso a paso sobre la elaboración de una matriz de auditoría. Estos apéndices con matrices de auditoría abordaban cuestiones de auditoría clave, criterios, información necesaria y métodos de análisis. Para acceder al Manual 2014 sobre Auditoría de TI y los apéndices que contienen matrices de auditoría, ingrese en: https://www.intosaicommunity.net/wgita/wp-content/uploads/2018/04/it-audit-handbook-english-version.pdf

Asimismo, la orientación sobre el uso de Técnicas de Auditoría Asistidas por Computadora excede el alcance de este manual. Se insta a las EFS a organizar capacitaciones separadas sobre las Técnicas de Auditoría Asistidas por Computadora dirigidas a su personal. Las EFS también han de considerar la posibilidad postular personal para el Programa de desarrollo de capacidades sobre auditoría de TI ofrecido por la IDI.

Visite los sitios web del WGITA y la IDI para acceder a más información sobre recursos y los próximos programas de capacitación.

WGITA: https://www.intosaicommunity.net/wgita/

IDI: http://www.idi.no

Esperamos que las EFS y su personal de TI encuentren en este manual una herramienta útil para acrecentar sus conocimientos y comprensión de cuestiones vinculadas con la auditoría de TI, y que les ayude a planificar y poner en práctica auditorías de esta especialidad.

Asimismo, también es posible que los destinatarios de este manual deseen remitirse a otros productos globales de la IDI, complementarios de este documento. Ellos son: el *Performance Audit ISSAI Implementation Handbook* [Manual de Implementación de las ISSAI sobre Auditoría de Desempeño],[9] el *Financial Audit ISSAI Implementation Handbook* [Manual de Implementación de las ISSAI sobre Auditoría

[9]International Organization of Supreme Audit Institutions Development Initiative, *IDI Performance Audit ISSAI Implementation Handbook*, version 1 (August 2021), https://www.idi.no/work-streams/professional-sais/work-stream-library/performance-audit-issai-implementation-handbook.

Financiera],[10] y el *Compliance Audit ISSAI Implementation Handbook* [Manual de Implementación de las ISSAI sobre Auditoría de Cumplimento], todos publicados por la IDI.[11]

[10]International Organization of Supreme Audit Institutions Development Initiative, *Financial Audit ISSAI Implementation Handbook*, version 1 (Dec. 8, 2020), https://www.idi.no/news/professional-sais/financial-audit-issai-implementation-handbook-version-1-english-light-touch-review-2020.

[11]International Organization of Supreme Audit Institutions Development Initiative, *Compliance Audit ISSAI Implementation Handbook*, draft version 0 (Jan. 8, 2018), https://www.idi.no/elibrary/professional-sais/issai-implementation-handbooks/handbooks-english/803-compliance-audit-issai-implementation-handbook-version-0-english.

CAPÍTULO 1: AUDITORÍA DE TI

Como señalamos anteriormente, la transición de las organizaciones gubernamentales hacia sistemas de TI y procesamiento digital ha generado la necesidad de que, para cumplir con sus mandatos de auditoría globales, las organizaciones de auditoría desarrollen las capacidades adecuadas para examinar detenidamente los controles relacionados con sistemas de TI. Específicamente, es necesario que las organizaciones de auditoría se aseguren de que las organizaciones gubernamentales hayan adoptado los controles internos de TI relacionados con la confidencialidad, integridad, validez y disponibilidad de los datos que administran.

Este capítulo contiene una reseña del proceso de auditoría de los sistemas de TI, también conocido como auditoría de TI. Asimismo, constituye tanto una introducción a los Capítulos 2-8 como un resumen de ellos. En tal sentido, este capítulo difiere de todos los demás en cuanto a su diseño y destalles.

Previamente, la descripción del proceso de auditoría de TI que se presenta en este capítulo es genérica, basándose en métodos de auditoría estándar, y refleja la metodología de auditoría seguida por las EFS. Por lo tanto, los usuarios deberían considerar el proceso de auditoría descrito en este capítulo en el contexto de la información relacionada contenida en la ISSAI y otras normas internacionales.

I. ¿Qué es una Auditoría de TI?

a. Requisito para la realización de auditorías de TI

El mandato de las Entidades Fiscalizadoras Superiores (EFS) de realizar auditorías de sistemas de TI se establece en la ISSAI 1 – Declaración de Lima.[12] Por extensión, dicho mandato deriva de su mandato general de realizar auditorías de desempeño, financieras y de cumplimiento, o una combinación de estas especialidades.[13]

- Una **auditoría de desempeño** se centra en determinar si las intervenciones, programas e instituciones tienen un desempeño acorde a los principios de economía, eficiencia y eficacia, y si cabe la posibilidad de realizar mejoras.
    - **Auditar la economía** supone centrarse en el modo en que las entidades auditadas lograron minimizar los costos de los recursos utilizados, considerando la adecuada calidad de tales recursos.
    - **Auditar la eficiencia** supone preguntarse si los insumos se han utilizado de una forma óptima o satisfactoria, o si con menos recursos podrían haberse obtenido los mismos productos o productos similares.
    - **Auditar la eficacia** supone observar los resultados. Al evaluar la eficacia, las EFS consideran si una política, programa o actividad de carácter público están logrando las metas previstas, y el modo en que lo hacen.

  En las auditorías de desempeño, se examina el desempeño de una organización en función de criterios relevantes mediante los que se identifica la situación que se pretende o desea lograr respecto a un tema de auditoría, además de la observancia de normas de desempeño razonables y asequibles. También se analizan las causas de las desviaciones de tales criterios u otros problemas. Las auditorías de desempeño habitualmente sirven para verificar si un gobierno utiliza debidamente sus recursos para cumplir los objetivos que sus políticas persiguen. Mediante tales auditorías a menudo se examina

[12]Organización Internacional de las Entidades Fiscalizadoras Superiores, *Declaración de Lima*, Parte VII, Artículo 22.

[13]Organización Internacional de las Entidades Fiscalizadores*, Normas Internacionales de las Entidades Fiscalizadoras Superiores (ISSAI) 100: Principios Fundamentales de la Auditoría del Sector Público*.

la implementación de una o más políticas.

- Una **auditoría financiera** se centra en determinar si la información financiera de una entidad se expone de acuerdo con el marco regulatorio aplicable y las normas pertinentes en materia de presentación de dicha información, además de verificar la exactitud de los informes financieros. El propósito de una auditoría financiera es acrecentar el grado de confianza que los usuarios previstos pueden tener en los estados financieros. Para lograr este cometido, el auditor deberá dictaminar si los estados financieros han sido confeccionados, en todos sus aspectos substanciales, de acuerdo con el marco para la exposición de información financiera pertinente. Una auditoría financiera incluye un examen substancial y detallado de información de carácter financiero.
- Una **auditoría de cumplimiento** es una evaluación independiente concebida para determinar si una materia objeto de auditoría cumple con determinadas pautas aplicables identificadas como criterios. El auditor de cumplimiento evalúa si las actividades, transacciones financieras e información cumplen, en todos sus aspectos substanciales, con las pautas que rigen la organización auditada. Las auditorías de cumplimiento añaden valor al proporcionar una corroboración independiente del cumplimiento normativo de la entidad auditada, sobre la base de un juicio profesional independiente y un análisis sólido y substanciado.
- Una **auditoría integrada** combina diferentes tipos de auditoría para evaluar la interacción de procesos financieros, operativos y tecnológicos en relación con el logro de objetivos de control.[14] Por ejemplo, es posible que una auditoría integrada de los estados financieros de una entidad incluya un análisis de deficiencias en los controles de los sistemas de información.[15]

Las auditorías de TI suelen formar parte de una auditoría más amplia (por ejemplo, de desempeño, cumplimiento, o financiera). Es posible realizar una auditoría de TI que no forme parte de ninguna de las tres especialidades; sin embargo, los principios generales, procedimientos, normas y expectativas aplicables a las auditorías de desempeño, cumplimiento y financieras, también son aplicables a las auditorías de TI.

b. Definición de una auditoría de TI

Las auditorías de TI constituyen un examen de aspectos relacionados con el uso de tecnologías de la información por parte de una organización, lo que incluye infraestructura, políticas y procedimientos, aplicaciones, y la utilización de datos. Las auditorías de TI incorporan regularmente el análisis de sistemas y controles para asegurarse de que ellos satisfagan las necesidades vinculadas con el negocio o actividad de la organización sin comprometer la seguridad, la privacidad, y otros elementos críticos del negocio o actividad en cuestión. Las auditorías de TI también suponen asegurarse de que el desarrollo, la implementación y el mantenimiento de los sistemas de TI satisfagan los objetivos de negocio, salvaguarden los activos relacionados con la información, y mantengan la integridad de los datos. Las auditorías de TI a menudo consisten en detectar casos de apartamiento de los criterios, identificados a su vez en función del tipo de auditoría de que se trate (es decir, de desempeño, cumplimiento o financiera).

Las auditorías de TI varían de acuerdo con los tipos de auditoría de las que ellas forman parte. Por ejemplo:

- En el contexto de una auditoría financiera, una modalidad de auditoría de TI podría consistir en un examen de los controles generales por los que se garantiza el funcionamiento de los sistemas de

[14]Harvard University, “What Is an Integrated Audit?,” https://rmas.fad.harvard.edu/faq/what-integrated-audit.

[15]Para acceder a un ejemplo, remítase a: U.S. Government Accountability Office, *Management Report: Improvements Are Needed in the Bureau of the Fiscal Service’s Information Systems Controls,* GAO-14-693R, (July 18, 2014), https://www.gao.gov/products/GAO-14-693R.

información subyacentes a los procesos financieros de una entidad, según lo reflejado por sus estados financieros.[16]

- En el contexto de una auditoría de desempeño, una auditoría de TI consistiría en la determinación del grado en que la adopción de ciertas tecnologías por parte de un organismo ha generado beneficios mensurables y ahorros de costos para todo el sector gubernamental.[17]
- En el contexto de una auditoría de cumplimiento, una auditoría de TI consistiría en un examen de la eficacia de los sistemas de información para la elaboración de informes de cumplimiento, que permitan a los empleados llevar a cabo las operaciones de una entidad y controlarlas.[18]

Las auditorías de TI pueden abarcar una diversidad de áreas, como la gobernanza de TI; adquisición de activos tecnológicos vinculadas con TI en áreas tales como telecomunicaciones, si existiesen controles suficientes para proteger los datos administrados por determinados entes, como los gobiernos locales; el análisis de la aplicación de nuevas tecnologías, como la inteligencia artificial; o el desarrollo, adquisición y operación de sistemas de TI. Las auditorías de TI también se ocupan de aspectos tales como la seguridad de la información y la ciberseguridad, que se relacionan estrechamente.

- La **seguridad de la información** puede definirse como la capacidad de un entorno de TI[19] de proteger la información y los recursos del sistema, sean ellos digitales o analógicos, en términos de confidencialidad, disponibilidad e integridad.[20] La seguridad de la información incluye aquellas medidas necesarias para gestionar, prevenir, detectar, documentar y contrarrestar dichas amenazas. Asimismo, la seguridad de la información posibilita a una organización proteger su infraestructura de sistemas de información de intrusiones por parte de usuarios no autorizados.
- La **ciberseguridad** es el proceso que consiste en proteger la información digital mediante la prevención y detección de ciberataques y la respuesta frente a ellos.[21] La ciberseguridad abarca las estrategias, políticas y normas relativas a la seguridad en el ciberespacio y las operaciones que en él tienen lugar. También incluye, entre otros factores, la reducción de amenazas y vulnerabilidades, la respuesta a incidentes, la resiliencia frente a fallas y recuperación de ellas, y el aseguramiento de la información.[22]

Una diferencia clave entre la seguridad de la información y la ciberseguridad es que esta última se centraliza más en la protección de la información digital, mientras que la primera se enfoca más ampliamente en la protección de todos los recursos que componen los sistemas de información. Entre

---

[16]Para acceder a un ejemplo, remítase a: U.S. Government Accountability Office, *Management Report: Improvements Needed in the Bureau of the Fiscal Service's Information System Controls Related to the Schedule of Federal Debt,* GAO-22-105569, (Mar. 17, 2022), https://www.gao.gov/products/GAO-22-105569.

[17]Para acceder a un ejemplo, remítase a: U.S. Government Accountability Office, *Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked*, GAO-19-58, (Apr 4, 2019.), https://www.gao.gov/products/gao-19-58.

[18]Para acceder a un ejemplo, remítase a: U.S. Government Accountability Office, *Improper Payments: Additional Guidance Needed to Improve Oversight of Agencies with Noncompliant Programs*, GAO-19-14, (Dec. 7, 2018), https://www.gao.gov/products/gao-19-14.

[19]El entorno de TI está integrado por las aplicaciones de TI, la infraestructura de apoyo y los procesos que una entidad utiliza para respaldar sus operaciones y formular las estrategias de su negocio o actividad.

[20]National Institute of Standards and Technology, *Glossary,* (2021), https://csrc.nist.gov/glossary.

[21]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, version 1.1* (2018).

[22]National Initiative for Cybersecurity Careers and Studies, *Cybersecurity Glossary,* (Gaithersburg, MD: March 10, 2022), https://niccs.cisa.gov/about-niccs/cybersecurity-glossary.

ambas áreas, este manual se ocupa principalmente de la seguridad de la información, aunque muchos elementos clave de la seguridad de la información también son aplicables a la ciberseguridad. Como parte de otro proyecto del WGTIA de la INTOSAI, se está elaborando un documento orientativo de auditoría aparte, en el que se aborda la ciberseguridad y la protección de datos.

b. Etapas de una auditoría de TI

Las etapas principales de una auditoría de TI son: la determinación del alcance, la planificación, el diseño y la realización, y la elaboración de informes sobre los resultados de la auditoría. Cada una de estas etapas se expone con mayor detalle a continuación. La Sección II se centra en la planificación de auditorías, la Sección III, en el diseño de auditorías, la Sección IV, en la realización de auditorías, y la Sección V, en la elaboración de informes sobre los resultados de las auditorías.

Figura 1: b. Etapas comunes de una auditoría de TI

Fuente: Unknown

Nota: Esta figura contiene un ejemplo ilustrativo que debería adaptarse a las actividades encomendadas de auditoría individuales.

II. Paso 1: Planificación de una auditoría de TI

La planificación es una parte esencial de cualquier auditoría, incluidas las auditorías de TI. En la mayor parte de las EFS, la planificación de auditorías se realiza a tres niveles: planificación estratégica; planificación macro, o anual; y planificación micro, o a nivel organizacional. Debería considerarse a la planificación como un proceso continuo que abarca la totalidad de la auditoría, dada la posibilidad del hallazgo de información adicional con impacto en el plan original. Una auditoría que se base en los resultados de una auditoría anterior como parte de un enfoque continuo, exige una planificación similar. Sin embargo, al adoptarse un enfoque de auditoría basado en la continuidad, algunos pasos, como el que consiste en comprender la organización, se abreviarían a resultados de la información ya recabada.

a. Planificación estratégica

El plan estratégico de una EFS consiste en una proyección a largo plazo (3 a 5 años) de las metas y objetivos de auditoría, lo que abarca los sistemas de TI y las organizaciones respectivas dentro del ámbito de competencia de una EFS. Para algunas EFS, tal vez sea posible incluir solamente una lista de áreas nuevas y emergentes de TI en sus planes estratégicos. Esto abarcaría la observación de nuevos métodos para el desarrollo de sistemas (por ejemplo, la programación ágil), las adquisiciones o el uso de la computación en la nube en el sector público, o la adopción de nuevas tecnologías, como aquellas basadas en inteligencia artificial o el uso de *blockchain*. El proceso de planificación estratégica y el plan estratégico de la EFS determinan la tónica y dirección de los objetivos de auditoría de TI de la EFS de cara al futuro. Por ejemplo, como se explica en el Capítulo 3, dedicado al desarrollo y adquisición de TI, una organización que se encuentre planificando una modificación de las metodologías asociadas al ciclo de vida del desarrollo de sistemas, podría proyectar la realización de auditorías destinadas a verificar la situación y el avance de tal modificación.

b. Planificación macro y enfoque basado en riesgos

El nivel macro de la planificación de auditoría habitualmente tiene lugar en función de un ciclo anual a nivel

de EFS para la selección de las áreas de auditoría y, según la EFS de que se trate, la formulación de un proceso para decidir qué áreas se auditarán anualmente.[23] Dada la rápida proliferación de sistemas de TI modernos en todos los gobiernos, y la limitación de los recursos a disposición de las EFS, sería conveniente adoptar un **enfoque basado en riesgos** para priorizar y seleccionar temas relevantes. Además de las consideraciones relacionadas con la selección de los sistemas de TI que se auditarán, las organizaciones también deben tener en cuenta información tal como los gastos globales en TI, la conectividad con otras entidades externas, y la madurez de los procesos de TI y su gobernanza. Asimismo, las EFS también habrán de incorporar auditorías obligatorias, como aquellas exigidas por ley o solicitadas por el Parlamento, el Congreso, u otros organismos dotados de facultades de supervisión.

Las EFS habitualmente fiscalizan numerosas organizaciones que utilizan diferentes sistemas de información. Es posible que haya aplicaciones diferentes para distintas funciones y actividades, y también que exista un conjunto de instalaciones informáticas localizadas en diversas regiones geográficas.

Las consideraciones relacionadas con los sistemas de información que han de auditarse y el modo de hacerlo, se basan en parte en la comprensión del riesgo inherente de una organización. El **riesgo inherente** consiste en la probabilidad de que ciertas características de los sistemas de TI de una organización auditada, por su propia naturaleza, impacten negativamente en la función prevista por el mandato de la organización. Por ejemplo, un sistema de TI cuyo propósito es poner a disposición del público en general determinada información, conlleva el riesgo inherente asociado a su rendimiento de que, superado un límite máximo de usuarios previstos, el sistema no responda y la información no resulte accesible a ningún usuario (denegación de servicio). Aunque la organización puede adoptar controles para mitigar los riesgos inherentes, en muchos casos tal vez deba simplemente tolerar su existencia dentro de un nivel aceptable.

Y aunque todos los sistemas de información presentan riesgos que les son inherentes, ellos inciden de formas diferentes en los distintos sistemas. Por ejemplo, el riesgo de indisponibilidad, tan siquiera durante una hora, puede revestir gravedad para un sistema de facturación de una tienda minorista muy activa, mientras que el riesgo de que se produzcan modificaciones no autorizadas puede derivar en la comisión de fraude y potenciales pérdidas para un sistema de banca electrónica. Los entornos técnicos en los que los sistemas operan, también pueden afectar el riesgo asociado con tales sistemas.[24] Un enfoque basado en riesgos para la selección de los sistemas de TI que se auditarán ayuda al auditor a decidir la prioridad de las auditorías.

[23]La organización de las EFS se estructura de maneras diversas en los diferentes países del mundo. En este caso, la etapa uno prevé una típica configuración de EFS integrada por oficina principal/campo, en la que la planificación a nivel global se realiza o aprueba en la oficina principal de la entidad, mientras que la auditoría se realiza efectivamente a nivel de campo.

[24]S. Anantha Sayana, ISACA.

Para utilizar un marco de evaluación de riesgos, es necesario que una EFS disponga de un mínimo de información de diferentes organismos, habitualmente recabada mediante una encuesta o una autoevaluación de control. El recuadro de la derecha contiene un ejemplo del proceso relativo al modo de evaluar los riesgos para la determinación de los sistemas de TI potencialmente auditables.[25] Para aquellas organizaciones que poseen mandatos más amplios, será necesario acotar el alcance de auditoría potencial, por ejemplo, a determinadas organizaciones o temas de TI, antes de realizar estos pasos.

Ejemplo: pasos de un enfoque basado en riesgos

1. Identificar el universo de auditoría que integraría la lista de todas las organizaciones sujetas a auditoría sobre las que la EFS tiene competencia.
2. Confeccionar una lista de los sistemas de información en uso en las organizaciones/unidades auditables.
3. Identificar aquellos factores que inciden en la criticidad del sistema para que la organización realice sus funciones y preste sus servicios.
4. Asignar ponderaciones a los factores críticos. Esto podría realizarse en consulta con la organización auditada.
5. Recopilar información correspondiente a todos los sistemas de todas las organizaciones, y, sobre la base de puntuaciones acumulativas, asignar a los sistemas/las organizaciones un orden de prioridad para su auditoría.
6. Elaborar un plan de auditoría anual en el que se expongan la prioridad, el enfoque y el cronograma de las auditorías de TI. Este ejercicio podría realizarse a intervalos anuales y, por lo tanto, tratarse de un plan recurrente.

Para realizar evaluaciones basadas en riesgos de sistemas de TI, es conveniente que las EFS seleccionen una metodología adecuada para su propósito. Las metodologías aplicadas pueden variar desde clasificaciones simples del perfil de riesgo del entorno de TI en alto, medio y bajo, a cálculos más complejos y numéricos por los que se cuantifica la calificación de los riesgos sobre la base datos objetivos recabados de la organización auditada. La clasificación se basará en la compresión por parte de la EFS de la organización y su entorno, y del juicio profesional del equipo de auditoría de TI de la EFS. Por ejemplo, como se explica con mayor detalle en el Capítulo 4, al decidir qué sistemas de TI fiscalizar, una EFS puede seleccionarlos teniendo en cuenta en cuáles de ellos se han implementado los cambios más substanciales y agregar criterios vinculados con la gestión de cambios a su lista de áreas de riesgo potenciales.

Aunque un proceso de evaluación de riesgos es una forma de seleccionar la organización a la que se le practicará una auditoría de TI, las EFS también escogen las organizaciones auditables con un criterio cíclico, sobre la base de las auditorías previstas por sus mandatos o en función de solicitudes específicas emanadas de organismos con facultades de supervisión (por ejemplo, el Congreso, el Parlamento o la Legislatura).

c. Planificación micro

La planificación micro consiste en desarrollar un plan de auditoría detallado de la organización seleccionada, que se inicia con una definición de los objetivos de la auditoría. El plan de auditoría ayudará a los auditores a elaborar un programa de auditoría de TI. El paso previo a la elaboración de un programa de auditoría será lograr comprender claramente la organización y sus sistemas de TI. Este manual apunta a ayudar al auditor a que, una vez elaborado el plan, pueda completar la matriz de auditoría con objetivos específicos para cada área (por ejemplo, gobernanza y seguridad de la información) sujeta a investigación. La planificación a nivel micro supone una comprensión de la organización, una evaluación preliminar de los controles aplicados para facilitar una planificación de auditoría detallada, y consideraciones relacionadas con la asignación de recursos y personal para asegurarse de que el equipo de auditoría esté

[25] A continuación, presentamos un ejemplo adicional de una metodología de evaluación de riesgos para sistemas de información, y una guía para auditores sobre el modo de evaluar los riesgos al planificar la labor de auditoría: Internal Audit Community of Practice, *Risk Assessment in Audit Planning* (April 2014), https://www.pempal.org/sites/pempal/files/event/attachments/cross_day-2_4_pempal-iacop-risk-assessment-in-audit-planning_eng.pdf.

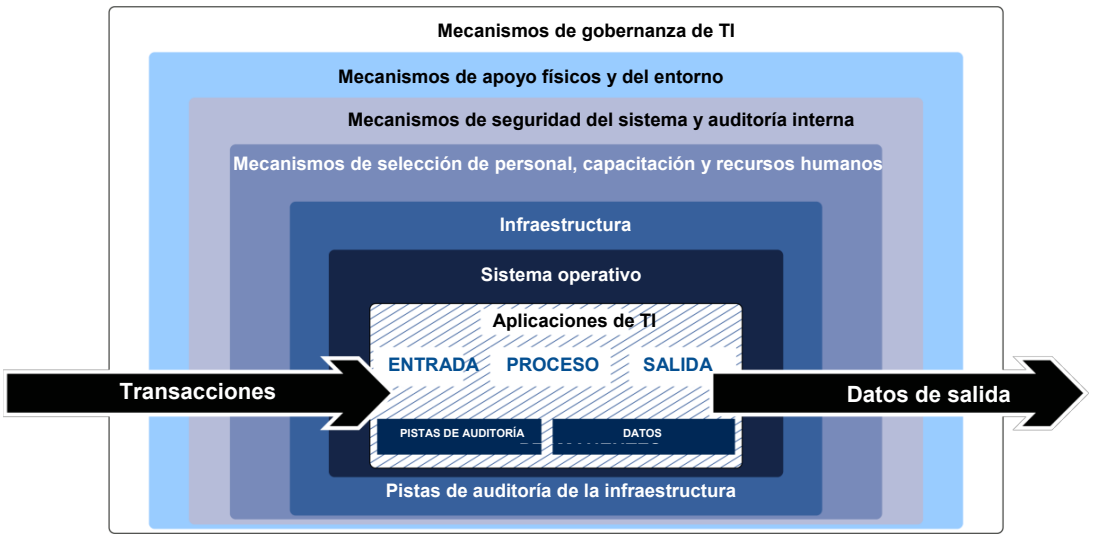
compuesto por miembros que, en su conjunto, dispongan de las competencias para llevar adelante los requerimientos de auditoría de TI de modo tal de lograr los objetivos propuestos. Por ejemplo, como se explica en el Capítulo 6, que versa sobre la gestión de la continuidad del negocio o actividad, es posible que una organización se proponga auditar criterios adicionales correspondientes al área de planificación de recuperación de desastres en sistemas que son esenciales para las operaciones de todos los sectores de la organización.

i. Comprensión de la organización

El grado de conocimiento de la organización y sus procesos, que un auditor de TI precisa tener, depende en gran medida del tipo de organización y del nivel de detalle con el que se realiza la labor de auditoría. Por ejemplo, las auditorías de TI diferirán en función del alcance de lo que se pretende auditar: desde un sistema de TI individual hasta una institución en particular, un área de gobierno, o incluso la totalidad de un país. El conocimiento de la organización debería abarcar los riesgos para el negocio, financieros e inherentes afrontados por la organización y sus sistemas de TI. También debería tenerse en cuenta en qué medida la organización depende de la externalización para cumplir con sus objetivos, y en qué medida sus procesos de negocios se han mapeado en un entorno de TI.[26] El auditor de TI debería utilizar esta información para identificar problemas potenciales, establecer los objetivos y el alcance de su labor, y considerar aquellas acciones de la dirección respecto a las que debería estar alerta. La Figura 2 contiene una disposición típica de un sistema de TI en una organización.

[26]Aquellas organizaciones que pasan de un entorno manual a uno electrónico normalmente realizan un ejercicio de reingeniería de los procesos del negocio o actividad. Es posible que algunos de tales procesos se ejecuten de forma manual, juntamente con los sistemas de TI, o que la organización haya desarrollado procesos automatizados que carentes de eficiencia o eficacia al replicar sus procesos manuales. Estos escenarios particulares se asociarían a áreas de interés específicas para los auditores de TI.

Figura 2: Disposición típica de un sistema de TI en una organización



Fuente: Unknown

Una típica aplicación constitutiva del núcleo de un sistema de TI de una organización está compuesta por un conjunto tecnológico, es decir, una combinación de lenguajes de programación, marcos y herramientas que los desarrolladores utilizan para crear aplicaciones. Este conjunto tecnológico puede abarcar un sistema de gestión de bases de datos constituido por bases de datos específicas, uno o más softwares mediante los que se indentifican las reglas del negocio o actividad en el sistema a través de módulos específicos, y una o más interfaces *front-end* del usuario respaldadas por un software de aplicación de red, si existiese un entorno conectado en red. Las bases de datos y softwares de aplicación se alojan en servidores, que esencialmente son componentes de hardware o software de alta capacidad, en condiciones de alojar bases de datos y aplicaciones amplias y múltiples. Los servidores podrían encontrarse específicamente diseñados para satisfacer diferentes necesidades del usuario, habiendo para ello servidores de datos, servidores de aplicaciones, servidores de Internet, y servidores proxy, entre otros.

Antes de iniciar la evaluación de los controles de un sistema de información, los auditores deberían comprender la arquitectura del sistema, además de los datos subyacentes y sus fuentes, para, de ese modo, identificar las herramientas y técnicas de auditoría que han de aplicarse. Sobre la base de la comprensión del sistema de información y la organización auditada, los auditores de TI podrán decidir el enfoque que adoptarán para la realización de una auditoría de esta especialidad.

Otras actividades de auditoría potencialmente útiles para comprender la organización auditada son:

- realizar un levantamiento de información de las operaciones del negocio o actividad de la entidad auditada,
- realizar una identificación de la interacción de la entidad auditada con sus pares o el entorno externo,
- confeccionar una lista de las actividades del negocio o la actividad de la entidad auditada que son críticas para el logro de sus objetivos, y
- confeccionar una lista de todas las soluciones de TI que la entidad auditada está utilizando.

ii. Materialidad

La materialidad (o relevancia e importancia) de las cuestiones sujetas a una auditoría de TI, debería determinarse conforme al marco general de la EFS para formular la política de materialidad de un informe de auditoría. La perspectiva de la materialidad puede variar en función de

la naturaleza del objetivo de auditoría de TI.[27] El auditor debería considerar la materialidad del asunto en el contexto de, por ejemplo, los estados financieros o la naturaleza de la organización o actividad. La materialidad en un contexto de TI también puede definirse en términos no financieros.

El auditor de TI debería determinar si cualquier deficiencia en esta área podría adquirir la condición de material. La importancia de que los controles generales de TI sean deficientes debería evaluarse en relación con su efecto en los controles de aplicación (es decir, si los controles de aplicación asociados también son deficientes). Si la deficiencia en la aplicación obedece al control general de TI, entonces es material. Por ejemplo, si un cálculo tributario realizado mediante una aplicación es substancialmente erróneo, y ello obedece a deficiencias en los controles a las modificaciones de tablas impositivas, la decisión de la dirección de no corregir una deficiencia general en el control de TI y su correlativo impacto en el entorno de control podría, tornarse relevante al sumarse a otras deficiencias que afectan el entorno de control.[28]

iii. Asignación de recursos y conformación del equipo de auditoria

La auditoría de TI requiere una asignación específica de recursos, en especial, de personal bien familiarizado con los sistemas, procesos y mecanismos de TI que posibilitan una implementación exitosa en esta materia. Además de recursos humanos idóneos,[29] también debería preverse una asignación adecuada de presupuesto e infraestructura, y la cobertura de cualesquiera otras necesidades identificadas. La cronología de una auditoría debería decidirse, de ser posible, en consulta con la organización auditada.

La entidad fiscalizadora debe asegurarse de que el equipo de auditoría esté conformado por miembros que, en su conjunto, dispongan de las competencias para ocuparse de encargos de auditoría de TI con miras a lograr los objetivos propuestos. Los conocimientos, habilidades y competencias necesarios pueden adquirirse a través de una combinación de actividades de desarrollo de capacidades, como la capacitación o la ampliación de la experiencia en el ámbito laboral; la incorporación de personal; o la contratación de recursos externos, de acuerdo con el plan estratégico de la EFS.

Las EFS tienen diferentes opciones al momento de asignar recursos humanos para abordar los encargos de auditoría, entre ellos:

- constituir un grupo central de especialistas en TI que brinden asistencia a otros equipos de auditoría en la EFS para realizar este tipo de auditoría, o designar especialistas en TI.
- Constituir un grupo o función específicamente dedicados al área de TI a cargo de la realización de todas las auditorías de esta especialidad para la EFS, que además interactúe con otros equipos que tengan conocimientos previos de la organización auditada.
- Utilizar una combinación de auditores con un conocimiento amplio en materia de TI y auditores especializados con una experiencia más enfocada en una algunas áreas específicas de TI.
- Incluir otros recursos humanos de la propia EFS como miembros transitorios del equipo de auditoría de TI.

Las EFS pueden contratar recursos externos, por ejemplo, consultores en materia de TI, contratistas,

[27]En el Párrafo 41 de la *ISSAI 100* se expresa lo siguiente: “la materialidad a menudo se considera en función del valor, pero también presenta otros aspectos de carácter cuantitativo y cualitativo. Las características intrínsecas de un elemento o grupo de elementos pueden otorgar materialidad a un asunto por su propia naturaleza. Un asunto también puede poseer materialidad debido al contexto en el que acontece”.

[28]*Materiality Concepts for Auditing Information,* ISACA Guidelines (G6).

[29]Recursos humanos idóneos significa personal que comprenda los sistemas de información y pueda extraer y analizar datos, si fuese necesario, dado que las auditorías de TI invariablemente requieren el uso de aptitudes relacionadas con esta especialidad para su realización. La EFS debería remitirse al Párrafo 39 de la ISSAI 100 sobre la debida capacitación del personal antes de la realización de una auditoría de TI.

especialistas y expertos para realizar auditorías de TI, si existiesen limitaciones en términos de recursos internos, o si los recursos externos se considerasen más adecuados o eficaces en función de los costos. Las EFS deberían asegurarse de que esos recursos externos se encuentren debidamente capacitados e informadosrespecto a las directrices sobre conducta profesional, así como también respecto a los procesos y productos de auditoría de TI aplicables a la EFS en cuestión. Este trabajo debería monitorearse adecuadamente mediante un contrato documentado, un acuerdo de nivel de servicio, o un acuerdo de confidencialidad. Tal vez se precise tener un cuidado especial respecto al mantenimiento de la confidencialidad por parte de los recursos externos, especialmente en lo relativo a la información de la entidad auditada.

Al auditar sistemas de TI, es conveniente que las EFS se aseguren de que los equipos de auditoría correspondientes tengan en su conjunto la capacidad de:

- Comprender los elementos técnicos de un sistema de TI, lo que incluye todas las instancias relevantes de la aplicación en uso, de modo tal de estar en condiciones de acceder a la infraestructura de TI y utilizarla para el proceso de auditoría.
- Comprender el mapeo de los procesos del negocio o actividad en la lógica de programación de los sistemas de TI.
- Comprender la metodología de auditoría, lo que incluye las normas y directrices de auditoría aplicables a la EFS.
- Comprender las técnicas de TI para recopilar evidencia de auditoría de sistemas automatizados.
- Comprender las herramientas de auditoría de TI para recabar, analizar y reproducir los resultados de dicho análisis o volver a ejecutar las funciones auditadas.
- Comprender el modo de evaluar y comparar los costos, como los relacionados con los esfuerzos y recursos, y los beneficios derivados de la implementación de un sistema de TI.
- Determinar las ventajas, desventajas y los riegos para el negocio o actividad de las prácticas y estrategias de adquisición y externalización de TI.
- Determinar si los objetivos del proyecto de TI se lograron, considerando debidamente la calidad y el alcance, y en consonancia con los costos presupuestados y cronogramas previstos.
- Comprender los servicios, requisitos y especificaciones para garantizar una selección de proveedores confiable y basada en la eficacia en función de los costos, y verificar la existencia de los contenidos esenciales en los contratos con proveedores.

Además, cuando se trate de auditorías financieras, las EFS también deberían asegurarse de que los equipos de auditoría dispongan en general de la experiencia suficiente para la realización de auditorías de estados financieros y puedan comprenderlos.

III. Paso 2: Diseño de una auditoría de TI

a. Objetivos de una auditoría de TI

Los objetivos de una auditoría pueden variar en función de una diversidad de factores, entre ellos, el tipo general de auditoría (por ejemplo, de desempeño, financiera o de cumplimiento), la organización u organizaciones sujetas a auditoría, el tipo de operaciones de TI sujetas a auditoría, los riesgos clave para la organización u organizaciones, y otros factores.

Algunos ejemplos de objetivos de auditoría son:

- respecto a las auditorías de desempeño, asegurarse de que los recursos de TI permitan la consecución de metas organizacionales de manera eficaz y eficiente, y que los controles pertinentes resulten eficaces para la prevención, detección y corrección de casos de excesos, así como también de derroche y falta de eficiencia en cuanto al uso y la gestión de los sistemas de información;
- respecto a las auditorías financieras, evaluar los controles pertinentes que tienen impacto en la

confiabilidad de los datos originados en los sistemas de información, que a su vez tienen impacto en los estados financieros de la organización auditada; o evaluar los procesos relacionados con las operaciones en una determinada área, como cuando se trata de sistemas de administración de nóminas salariales o sistemas contables; y

- respecto a las auditorías de cumplimiento, garantizar la observancia de los procesos asociados a los sistemas de información en cuanto a la leyes, políticas y normas aplicables a la organización auditada.

El alcance de las auditorías de TI puede abarcar áreas específicas de la implementación de TI, por ejemplo:

- la adquisición, desarrollo e implementación de sistema de TI,
- operaciones y mantenimiento,
- gestión de cambios,
- gestión de acceso,
- seguridad de la información y continuidad del negocio o actividad,
- relación precio/prestación brindada a través de los sistemas de TI, y
- planificación de los recursos de la organización u otros sistemas de TI complejos/especializados.

Si una auditoría de TI formase parte de un objetivo de auditoría más amplio, la EFS debería asegurarse de que el equipo de auditoría en su conjunto trabaje de manera integrada para lograr el objetivo general de la auditoría. Por ejemplo, para lograr una integración eficaz, las EFS pueden considerar las siguientes acciones:

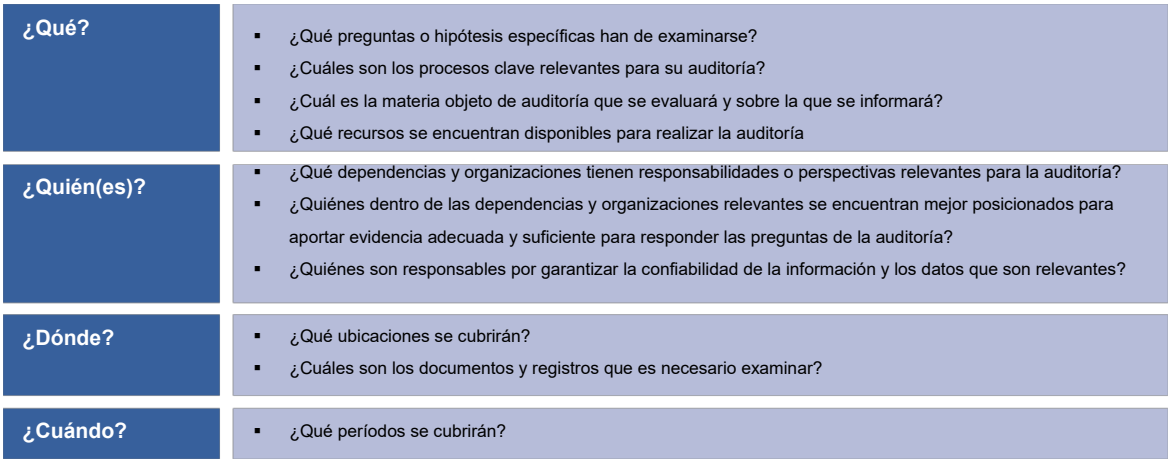
- documentar de forma integral la labor llevada a cabo por los auditores de TI,
- formular un protocolo para el intercambio de información entre los auditores de TI y otros auditores, e
- identificar qué sistemas de información y objetivos de control se encuentran dentro del alcance de la auditoría.

Tras desarrollar lo objetivos y el enfoque de su auditoría, los auditores de TI suelen formular preguntas específicas que orientarán su labor. Las preguntas de auditoría deberían derivar de los objetivos globales de la auditoría, y habitualmente son más específicas en tanto abordan los temas que se describirán o evaluarán durante la auditoría. El propósito es que las preguntas de auditoría abarquen todos los aspectos de los objetivos planteados en la auditoría. Las preguntas de auditoría son o bien **descriptivas** (lo que significa que describen una condición) o **evaluativas** (lo que significa que sirven para evaluar una condición en función de determinados criterios y pueden tener un carácter normativo o analítico).

b. Alcance y metodología de la auditoría de TI

Los auditores de TI disponen de muchas opciones al determinar el alcance de una auditoría. La Figura 3 contiene preguntas típicas relacionadas con el alcance.

Figura 3: Consideraciones sobre el alcance en una auditoría de TI



Fuente: IDI/Equipo de Desarrollo del Subcomité de Auditoría de Desempeño

Nota: Esta figura contiene un ejemplo ilustrativo que debería adaptarse a encargos de auditoría individuales.

Muy a menudo el auditor debe evaluar las políticas y procedimientos que rigen el entorno general de TI de la organización auditada, asegurándose de que existen los mecanismos de control y aplicación correspondientes. La determinación del alcance de la auditoría de TI supone decidir la amplitud del examen de auditoría; la cobertura de los sistemas de TI y sus funcionalidades; los procesos de TI a auditar; las ubicaciones de los sistemas de TI a cubrir, incluidos aquellos en ubicaciones de propiedad de terceros, como prestadores en la nube o externalizados, cuyos propios entornos de control forman parte del entorno de control de la entidad auditada; y el período que la auditoría ha de abarcar.[30]

Las EFS pueden seleccionar el período que el análisis de auditoría abarcará (por ejemplo, un año, tres años, etc.) en la definición del alcance del encargo de auditoría de TI. También podría exigirse que una auditoría concluya en una fecha determinada. Debería seleccionarse un período que sea adecuado para los propósitos definidos para el objetivo de la auditoría.

Una vez establecido el alcance de una auditoría, los equipos de auditoría de TI definen la metodología o los pasos específicos que se proponen aplicar o llevar a cabo para cumplir con los objetivos de la auditoría, de acuerdo con el alcance de ésta. Al definir los detalles metodológicos, es conveniente que los equipos de auditoría se aseguren de que los pasos que pretenden dar son posibles en relación con los datos que se proponen recopilar, que no se den pasos superfluos, y que el resultado de los pasos de auditoría permita al equipo abordar los objetivos de ésta.

Debería informarse a la organización auditada acerca del alcance y los objetivos de la auditoría y, en la medida de lo necesario, deberían discutirse con ella los criterios de evaluación correspondientes. Asimismo, la EFS puede, de ser necesario, redactar la carta de compromiso dirigida a la organización auditada, donde también puede dejar constancia de los términos del objetivoo en cuestión.

c. Controles generales de TI y controles de aplicación

Como se explicó anteriormente, las auditorías de TI se definen como el examen de los controles relacionados con sistemas de TI, con el propósito de determinar casos de apartamiento de los criterios. Los **controles** son los procesos, herramientas y demás mecanismos de supervisión instrumentados para

[30]La ubicación incluye los servidores *back-end* (aplicaciones o datos), las ubicaciones de propiedad de usuarios, y las redes en términos genéricos, y también determina los lugares físicos a cubrir en una red distribuida entre edificios, ciudades o países, si fuese el caso.

gestionar las funciones de TI y evitar riesgos y vulnerabilidades. Los controles que han de evaluarse mediante una auditoría de TI se determinarán en función del objetivo y alcance de la auditoría.

Los controles se utilizan para mitigar los riesgos afrontados por la organización. Específicamente, existen varios tipos de riesgos relevantes para los controles de auditoría de TI:

- El **riesgo de control** consiste en la probabilidad de que los controles de TI adoptados por la organización auditada no puedan mitigar el impacto adverso para el que fueron diseñados. Por ejemplo, un sistema de información en el que debe garantizarse que el acceso a información confidencial se restrinja a personal autorizado, tal vez adopte el control que consiste en que el personal que pretende acceder al sistema disponga de una contraseña y nombre de usuario. En esta situación, el riesgo de control se asocia a la posibilidad de que el nombre de usuario y la contraseña no ofrezcan el nivel de seguridad suficiente y puedan ser deducidos por personal no autorizado mediante la reiteración de intentos, lo que derivaría en una pérdida de confidencialidad y causaría un efecto potencialmente adverso para la organización. Una organización que insista en la utilización de contraseñas no superfluas, integradas por una combinación de símbolos alfabéticos, numéricos y especiales, garantizando que el sistema de información impida el acceso al nombre de usuario tras un número determinado de intentos fallidos, ofrecería un riesgo de control menor que aquella que no adopte tales medidas. Para reducir el riesgo de control en tal situación, también podría recurrirse a una autenticación multifactorial.
- El **riesgo de detección** consiste en la probabilidad de que la ausencia, falla, o falta de eficacia de los controles de TI adoptados por una organización no sean detectados por el auditor, con el consiguiente impacto negativo en ella.
- El **riesgo residual** es el nivel de riesgo remanente luego de haberse aplicado los controles correspondientes, y puede reducirse mediante la identificación de aquellas áreas en las que es menester intensificar los controles. La dirección puede establecer lo que se considera una meta aceptable en términos de nivel de riesgo (tolerancia al riesgo).

En un contexto de TI, los controles se dividen en dos categorías, exhibidas en la Figura 4: controles generales y controles de aplicación. Las categorías dependen del margen de influencia del control, y de si éste está vinculado con una aplicación específica.

Figura 4: Controles generales y de aplicación

Fuente: Unknown

Los **controles generales de TI** constituyen la base de la estructura de control de TI. Ellos se vinculan con el entorno general en el que los sistemas de TI se desarrollan, operan, gestionan y mantienen. Los controles generales son procedimientos manuales o automatizados cuyo propósito es garantizar la confidencialidad, integridad y disponibilidad de la información en el entorno físico dentro del cual los sistemas de información se desarrollan, mantienen y operan. Los controles generales determinan un marco de control global para las actividades de TI y brindan seguridad acerca del cumplimiento de los objetivos de control generales.

Los controles generales se implementan mediante un conjunto de herramientas, como políticas, directrices y procedimientos, además de posibilitar la instrumentación de una estructura de gestión adecuada, lo que incluye aquella utilizada para la gestión de los sistemas de TI de la organización. Algunos ejemplos de controles generales son el desarrollo y la implementación de una estrategia y una política de seguridad de TI, la conformación de un comité rector de TI, la organización del personal de TI para separar funciones incompatibles, el establecimiento de roles y privilegios del sistema adecuados para el rol de una persona, y la planificación para la prevención y recuperación de desastres.

Los controles generales de TI no se aplican específicamente a flujos de transacciones individuales, o a paquetes de contabilidad o aplicaciones financieras específicos. El objetivo de los controles generales de TI es garantizar el desarrollo y la implementación adecuados de aplicaciones, archivos de programas y datos, y operaciones informáticas.

Los **controles de aplicación** son controles específicos exclusivos de los sistemas de información en cada aplicación. Los controles de aplicación son procedimientos automatizados o manuales dependientes de TI dentro de un sistema de información, que inciden en el procesamiento de operaciones y pueden relacionarse con la validación de datos de entrada, el procesamiento exacto de datos, la producción de datos de salida, y los controles relacionados con la integridad de datos maestros. Ellos se utilizan con los segmentos de una aplicación y se relacionan con las transacciones y los datos existentes. Por ejemplo, en una aplicación de pagos en línea, un control de datos de entrada podría consistir en que la fecha de vencimiento de la tarjeta de crédito usada sea posterior a la fecha de la transacción, y que la información ingresada se encuentre encriptada.

El diseño y la implementación de los controles generales de TI pueden tener un impacto significativo en la eficacia de los controles de aplicación. Los controles generales suministran a las aplicaciones los recursos que necesitan para operar y garantizar que no se puedan efectuar consultas y modificaciones sin autorización previa, ya sea en las aplicaciones (es decir, que se las proteja de maniobras de reprogramación) o en datos subyacentes (por ejemplo, en el amplio conjunto de datos vinculados con transacciones).

Son elementos críticos para los controles generales a nivel de aplicación[31]:

- la gestión de la seguridad,
- el control de acceso / la segregación del acceso por parte de usuarios,
- la gestión de la configuración / la gestión de los cambios,
- la gestión de las operaciones, y
- la planificación de contingencias.

Los controles de aplicación operan sobre transacciones individuales o grupos de transacciones, y su propósito es asegurarse de que las transacciones se ingresen, procesen, y produzcan datos de salida de la forma correcta. El diseño y la eficacia operativa de los controles generales de TI influyen substancialmente en el grado en que la dirección depende de los controles de aplicación para gestionar los riesgos.

d. ¿Por qué los controles de TI son importantes para el auditor de esta especialidad?

En general, al auditor de TI se lo convoca para examinar los controles relacionados con cuestiones tecnológicas. A medida que crece el número de organizaciones que dependen del área de TI para automatizar sus operaciones, la línea que divide el rol de un auditor de TI y uno ajeno a esta especialidad, también se desdibuja con rapidez. Como mínimo, todos los auditores deben comprender el entorno de control de la organización auditada de modo tal de brindar un grado de seguridad respecto a los controles internos que en ella operan. Según los Principios Fundamentales de la Auditoría del Sector Público, contenidos en las ISSAI, “los auditores deben comprender la naturaleza de la entidad / el programa que ha de auditarse”.[32] Esto incluye la comprensión de los controles internos, además de los objetivos, las operaciones, el entorno normativo, los sistemas, y los procesos del negocio o actividad involucrados.

Toda área de control se basa en un conjunto de objetivos de control que una organización instrumenta para mitigar un riesgo de control, lo que incluye los requisitos técnicos vigentes para los sistemas de una

[31]U.S. Government Accountability Office, *Federal Information System Controls Audit Manual (FISCAM),* GAO-09-232G, (Feb. 2, 2009), https://www.gao.gov/products/gao-09-232g.

[32]Organización internacional de las Entidades Fiscalizadoras Superiores, *ISSAI 100,* Párrafo 45.

organización. El rol del auditor es comprender los riesgos potenciales relativos al negocio o actividad y al área de TI que la organización auditada afronta y, a su vez, evaluar si los controles aplicados resultan adecuados para cumplir con el objetivo de control. Cuando se trata de controles generales de TI, es importante que el auditor comprenda las categorías amplias y el alcance de los controles generales en operación, evaluar la supervisión por parte de la dirección y el grado de conocimiento de dichos controles del personal de la organización, además de determinar su eficacia a los efectos de ofrecer seguridad. Si los controles generales fuesen endebles, disminuirían substancialmente la confiabilidad de los controles asociados con las aplicaciones de TI individuales.

En capítulos posteriores, como el Capítulo 8, en el que se tratan los controles de aplicación, se analizan en detalle algunas de las áreas clave de los controles generales de TI y dichos controles.

IV. Paso 3: Realización de una auditoría de TI

La realización de una auditoría de TI incluye pasos clave, como la recopilación de evidencia de auditoría que sea suficiente, adecuada, relevante, y confiable; la realización de una evaluación preliminar de los controles, por ejemplo, en lo relativo a políticas y procedimientos, para evaluar su confiabilidad; y exámenes substanciales detallados de áreas prioritarias para determinar el grado en el que un control está funcionando de forma adecuada.

a. Recopilación de evidencia de auditoría

i. Evidencia

Los hallazgos de auditoría deben sustentarse en evidencia, de modo tal que la cantidad y calidad de la evidencia obtenida tienen relevancia. Esto significa que un auditor de TI debe considerar y evaluar continuamente la evidencia que planea obtener, o que ha obtenido, en lo relativo a su suficiencia e idoneidad. La suficiencia se refiere a la cantidad de evidencia recopilada. La idoneidad se refiere a la calidad de la evidencia, y si ella es confiable y relevante. Los auditores pueden evaluar si la evidencia es relevante y confiable al considerar, entre otras cosas, la naturaleza de la fuente y su reputación, los controles operados por la entidad auditada, la presencia de evidencia contradictoria o confirmatoria, y los métodos, modelos y supuestos a los que se recurrió para preparar la información extraída de la evidencia.

Una herramienta útil para evaluar la evidencia obtenida y formular conclusiones y recomendaciones es una matriz de hallazgos de auditoría. Esta herramienta permite a los auditores determinar si los hallazgos y recomendaciones se basan en evidencia suficiente e idónea, cuando ello corresponda. La Figura 5 contiene un ejemplo de una matriz de hallazgos de auditoría.[33]

[33]La página 174 de la Versión 1 (agosto de 2021) del *Manual de Implementación de las ISSAI sobre Auditoría de Desempeño*, publicado por Iniciativa de Desarrollo de las Entidades Fiscalizadoras Superiores, contiene una ilustración de una matriz de auditoría de desempeño completada, https://www.idi.no/work-streams/professional-sais/work-stream-library/performance-audit-issai-implementation-handbook.

Figura 5: Plantilla de una matriz de hallazgos de auditoría

Objetivo de la auditoría: Expresar clara y objetivamente de qué se trata la auditoría.
Pregunta de la auditoría (la misma formulada en la matriz de diseño de la auditoría): Para cada pregunta (o supbregunta) de auditoría, repita cada uno de los elementos mencionados en la tabla.

Hallazgo	**Declaración de hallazgo (situación hallada)**	Incidencias más relevantes detectadas durante el trabajo de campo.
	Criterios	La información utilizada para determinar si el desempeño esperado de aquello que se audita es satisfactorio, supera las expectativas, o es insatisfactorio.
	Evidencia y análisis	Resultado de aplicar métodos de análisis de datos o evaluar su evidencia. Pueden indicarse las técnicas utilizadas para administrar la información recopilada durante el trabajo de campo y los resultados logrados.
	Causas	Motivos de la situación hallada. Puede relacionarse con la operación o el diseño del proyecto de auditoría. Puede encontrarse fuera del control del directivo. Las recomendaciones deberían relacionarse con las causas.
	Efectos	Consecuencias relacionadas con las causas y la evidencia correspondiente. Pueden ser una medida de la importancia de los hallazgos.
¿Es la evidencia suficiente (S/N) y, de no ser así, qué trabajo será necesario realizar para resolver cualquier deficiencia en la evidencia?		Considere la evidencia de la que dispone para cada elemento del hallazgo y si ella es suficiente e idónea. ¿Si la evidencia de la que se dispone para cada elemento no fuese suficiente, qué trabajo será necesario realizar para abordar cualquier falencia de dicha evidencia?
Buenas prácticas		Se identifican acciones que conducen a un buen desempeño. Pueden respaldar las recomendaciones.
Recomendaciones		Propuestas para abordar las causas (o deficiencias) identificadas.

Fuente: Adaptado de la GAO de los EE.UU. y la EFS de Brasil.

Nota: Esta figura contiene un ejemplo ilustrativo que debería adaptarse a encargos de auditoría individuales.

ii. Etapa 1 - evaluación preliminar de los controles de TI

El auditor de TI debería realizar una evaluación preliminar de los controles de TI –tanto los generales como los de aplicación– en el sistema para corroborar que son confiables y suficientes para el logro de los resultados de la auditoría.

El alcance de la evaluación de los controles de TI puede abarcar la determinación de si

- se ha definido, adoptado y comunicado una política de TI;
- existe una estructura de gobernanza de TI en condiciones operativas;
- los controles reflejan de forma exacta los requisitos técnicos correspondientes a los sistemas de información subyacentes;
- se ha realizado periódicamente un inventario de activos relacionados con sistemas de información, y se han identificado las necesidades vinculadas con la expansión, substitución y retiro de tales sistemas;
- existen procesos en estado operativo que permiten compartir infraestructuras y servicios comunes

asociados a sistemas de información con otras organizaciones públicas;

- se han adoptado, definido y comunicado procesos para el desarrollo, la adquisición y el mantenimiento de TI (lo que incluye aquellos procesos relacionados con la gestión de cambios);
- se han definido, adoptado y comunicado procesos relativos a las operaciones de TI (autoaprovisionamiento, externalización y acuerdos de prestación de servicios);
- se han adoptado medidas para garantizar la seguridad y condiciones de trabajo físicas pretendidas;
- se han adoptado medidas para la capacitación y concienciación de los recursos humanos destinadas a garantizar la confidencialidad, integridad y disponibilidad de la información, además de la observancia de la política de TI y los requisitos de la estructura de gobernanza;
- se han adoptado medidas para garantizar la confidencialidad, integridad y disponibilidad de diversas modalidades y canales de comunicación;
- se han adoptado medidas para la gestión del cumplimiento normativo;
- se han adoptado medidas tanto para la gestión de la continuidad del negocio como para la gestión de la recuperación de desastres;
- se han adoptado medidas para garantizar la integridad, exactitud, validez y confidencialidad de las transacciones realizadas y los datos utilizados como parte de los procesos del negocio o actividad; y
- se han adoptado medidas para garantizar el procesamiento oportuno, exacto y completo de la información entre componentes del sistema, por ejemplo, entre aplicaciones.

En función del objetivo de la auditoría, es posible que a los auditores les preocupe el diseño, la implementación y la eficacia operativa de los controles. Si a un auditor le preocupase el diseño de los controles, una entrevista o una inspección de las reglas documentadas del negocio o actividad puede resultar suficiente. Si lo que le preocupase a un auditor es la implementación de tales controles, posiblemente una consulta no sea suficiente, y tal vez sea necesario realizar un examen paso a paso o *walkthrough* (una técnica de auditoría para confirmar la comprensión de los controles), o realizar un análisis de datos para verificar la implementación de los controles correspondientes. Por último, es posible que un auditor al que le preocupa la eficacia operativa de un control deba examinar una muestra de transacciones para corroborar que el control ha funcionado efectivamente durante la totalidad del período abarcado.

También es posible que los auditores consideren el modo en que la evidencia relativa a los controles generales incide en la naturaleza, oportunidad y amplitud de los procedimientos, y en la evidencia que se precisa para corroborar la operación de los controles de aplicación. Por ejemplo, los auditores también deberían considerar la evidencia vinculada con el acceso lógico del personal a los sistemas de TI y la gestión de cambios dentro del entorno de producción. Si los auditores hubiesen obtenido evidencia de auditoría suficiente y adecuada respecto a la eficacia de los controles generales, tal vez estén en condiciones de extraer conclusiones acerca de la eficacia operativa de los procedimientos de control de aplicación automatizados. Para ello puede realizarse un examen de una muestra más reducida de transacciones, debido a que la eficacia del entorno general de TI brinda a los auditores evidencia acerca la eficacia del control de aplicación durante el período correspondiente. Cuando se trate de procedimientos de control de aplicación manuales, es posible que los auditores deban examinar un tamaño de muestra acorde al nivel de confianza seleccionado.

iii. Etapa 2 - pruebas sustantivas

A partir de la evaluación de los controles de TI, los auditores pueden identificar áreas prioritarias para la realización de pruebas substantivas, lo que supone un examen detallado de los controles de TI mediante el empleo de diversas técnicas para la consulta, extracción y análisis de datos. Cuando se trata de pruebas substantivas, las comprobaciones están concebidas para corroborar las aseveraciones formuladas según los objetivos de auditoría.

Entre las técnicas utilizadas para el análisis de datos por los auditores de TI se encuentran los informes de excepción, mediante los que se documentan las desviaciones respecto al desempeño esperado; la

comparación de archivos; la estratificación, es decir, la clasificación de datos en grupos diferenciados; el muestreo; y las comprobaciones de duplicados. Otra opción para examinar un sistema es el enfoque del "hilo y los nudos" (*thread and knots*), por el que se avanza de a un proceso del negocio o actividad a la vez para identificar puntos de actividad significativos y si en cada punto de actividad existen controles de TI adecuados. Los auditores de TI deberían conocer estas opciones y utilizar las herramientas de análisis adecuadas. Asimismo, para realizar el análisis de la información, pueden utilizar software de auditoría general o especializado.

Al realizar pruebas sustantivas, los auditores de TI deberían asegurarse de que la evidencia en formato electrónico recopilada y documentada sea suficiente, confiable y precisa para sustentar las observaciones de auditoría. Dicha evidencia puede consistir en archivos de datos, registros de usuarios, modelos analíticos e informes de sistemas informáticos de gestión, y debería recabarse y almacenarse adecuadamente de modo tal de que se encuentre disponible para corroborar la exactitud y validez del proceso de auditoría.

Un auditor de TI también debería seleccionar una evaluación de riesgos adecuada y utilizar técnicas de muestreo que permitan extraer conclusiones apropiadas derivadas de comprobaciones estadísticamente suficientes basadas en datos limitados. En general, es una buena práctica recurrir a los servicios de un experto o especialista en estadística que forme parte de la organización para seleccionar y determinar el método de muestreo.

En aquellos casos en los que el volumen y transferencia de datos, su forma de almacenamiento y su capacidad de procesamiento lo permitan, también puede realizarse una evaluación de riesgos de alta calidad que abarque la totalidad de la población, de modo tal de identificar tendencias correlacionadas con la comprensión que el auditor tiene del negocio o actividad. Por ejemplo, un auditor podría obtener una lista de todos los usuarios y las fechas en las ingresaron al sistema por última vez, y compararla con una lista oficial de fechas de salida, para obtener un análisis de un 100 por ciento. Esto permitiría a un auditor identificar transacciones o puntos de datos anómalos pertenecientes a la muestra de un modo más centrado en el riesgo.

b. Interacción con la organización auditada

En las ISSAI se recomienda que los auditores entablen una comunicación eficaz durante todo el proceso de auditoría y mantengan a la organización auditada informada acerca de todos los asuntos relacionados con la auditoría que se lleva a cabo.[34] Para realizar una auditoría de TI, los auditores pueden solicitar a la organización auditada la prestación de la cooperación y el apoyo debidos, lo que incluye el acceso a registros e información. Corresponde a los auditores señalar el modo de acceso a datos electrónicos en el formato necesario para permitir su análisis, en consulta con la organización auditada. El modo de acceso es específico de cada EFS.

c. Documentación de una auditoría de TI

La documentación de la auditoría de los sistemas de información es el registro de la tarea de auditoría llevada a cabo y le evidencia que sustenta los hallazgos y conclusiones. Los auditores de TI deben velar por la preservación de los resultados y la evidencia, para, de ese modo, cumplir con los requisitos de confiabilidad, completitud, suficiencia y corrección. También es importante que los auditores de TI garanticen la preservación del proceso de auditoría, de modo tal de posibilitar una posterior verificación de los procedimientos de análisis. Esto supone la aplicación de técnicas de documentación adecuadas.

La documentación incluye registros de

- la planificación y preparación del alcance y los objetivos de la auditoría;
- los programas de auditoría;

[34]Organización internacional de las Entidades Fiscalizadoras Superiores, ISSAI 100.

- la evidencia recabada sobre la base de las conclusiones extraídas;
- toda la documentación de trabajo, lo que abarca archivos generales pertenecientes a la organización y el sistema;
- puntos discutidos durante las entrevistas, indicándose claramente el tema de discusión, la persona entrevistada, su puesto y designación, y la hora y lugar de realización de las entrevistas;
- observaciones efectuadas por el auditor al realizar su labor:
  - las observaciones deberían incluir, por lo menos, el lugar y la hora correspondientes, el motivo de cada una de ellas, y las personas involucradas;
- los informes y datos obtenidos del sistema directamente por el auditor o provistos por el personal auditado:
  - el auditor de TI debería asegurarse de que estos informes contengan la fuente del informe, la fecha y hora correspondientes, y las condiciones examinadas;
  - una opción para el registro de estos detalles es utilizar capturas de pantalla; y
- cualquier comentario y aclaración agregados por los auditores en diversos puntos de la documentación con relación a inquietudes, dudas y la necesidad de información adicional:
  - el auditor debería regresar a estos comentarios con posterioridad y agregar comentarios y referencias acerca del modo y el lugar en que se resolvieron.

La evidencia recopilada durante una auditoría de TI tal vez contenga los indicadores de fecha y hora y los detalles acerca de los pasos de análisis de datos llevados a cabo, lo cual permite conocer claramente el momento en que la evidencia fue creada, almacenada, y modificada por última vez, para mitigar el riesgo de que se produzcan cambios posteriores. La Figura 6 contiene ejemplos de aquello que un auditor debería estar en condiciones de comprender a partir de la documentación de auditoría.

Figura 6: Comprensión de la documentación de auditoría de TI

¿Qué debería un auditor experimentado estar en condiciones de comprender a partir de la	
✓ La naturaleza, el momento y la amplitud de la labor realizada. ✓ Los hallazgos de la labor de auditoría y la evidencia obtenida. ✓ Cuestiones significativas surgidas durante la auditoría (por ejemplo, modificaciones del alcance o el enfoque de la auditoría, decisiones relativas a un nuevo factor de riesgo identificado durante la auditoría, medidas tomadas a raíz de discordancias entre la entidad auditada y el equipo, etc.).	✓ Las conclusiones alcanzadas a raíz de las cuestiones significativas previamente mencionadas. ✓ Decisiones significativas o claves tomada

Fuente: IDI/Equipo de Desarrollo del Subcomité de Auditoría de Desempeño

Nota: Esta figura contiene un ejemplo ilustrativo que debería adaptarse a encargos de auditoría individuales.

Tal como sucede con toda documentación de auditoría, la documentación de auditoría de TI debería conservarse y protegerse de cualquier modificación y eliminación no autorizadas. Las EFS pueden desarrollar nuevas normas para la conservación de documentación de auditoría, o adaptar las normas existentes para satisfacer los requisitos relativos a la conservación de la documentación relacionada con auditorías de TI. El período de conservación debería establecerse en función del mandato de la EFS en cuestión y de las normas legales que rigen sus actividades. Conviene prestar especial atención a los medios, el formato, duración esperada y las condiciones de almacenamiento de estos datos, para asegurarse de que sean legibles dentro del plazo definido en la política de conservación de datos y archivado de cada EFS. Para esto, tal vez sea necesario convertir datos de un formato a otro, de modo tal de mantenerse al día con los avances tecnológicos y evitar la obsolescencia.

Cuando se trate del examen de informes técnicos sobre cuestiones tecnológicas específicas elaborados por auditores externos, los auditores deberán adoptar procedimientos adecuados para garantizar la confiabilidad de determinados aspectos relacionados con cuestiones financieras, el cumplimiento normativo o el desempeño. Si se recurriese al contenido de los informes derivados de tales procedimientos, debería dejarse debida constancia de esa circunstancia.

Para la conservación de datos electrónicos, las EFS deberían prever la realización de copias de seguridad de los datos recibidos de la organización auditada y de los resultados de consultas y análisis. La documentación de auditoría debería mantenerse en confidencialidad y conservase durante un período decidido por la EFS o dispuesto por ley. El borrador y los informes finales de la auditoría también deberían formar parte de la documentación de esta. Cuando la labor de auditoría sea revisada por un par o un superior, las observaciones surgidas de la revisión también deberían formar parte de la documentación.

d. Revisión a cargo de un supervisor

Durante la auditoría, la labor realizada por el personal a cargo de ella debería supervisarse adecuadamente, y la documentación de esa labor, examinada por un miembro superior del personal de auditoría.[35] Ese miembro superior también debería desempeñar el rol de orientador, capacitador y asesor, necesario al realizarse la auditoría.

V. Paso 4: Elaboración de informes sobre los resultados de una auditoría de TI

Una auditoría de TI debería seguir el esquema general del sistema de elaboración de informes seguido por la EFS. En los informes de auditoría de TI deberían medirse las cuestiones técnicas informadas sobre la base del nivel de detalle que el público destinatario requiere.

El auditor de TI debe informar acerca de los hallazgos de forma oportuna, y tales hallazgos deberían plantearse de un modo constructivo y útil para la organización auditada, además de ser significativos para otras partes interesadas. El informe podría presentarse a las autoridades competentes en función del mandato de la EFS y la auditoría de TI.

Los auditores deberían ser conscientes de la necesidad de limitar el uso de argot técnico y de la sensibilidad de la información contenida (por ejemplo, contraseñas, nombres de usuario e información personal) en el informe. A pesar de la naturaleza técnica de una auditoría de TI, los auditores deberían asegurarse de que el informe pueda ser íntegramente comprendido por la dirección superior de la organización auditada, las partes interesadas y el público en general. Como parte de este proceso, los auditores de TI deben saber que los destinatarios de sus informes incluyen tanto a otros expertos en TI como el público en general, y que será necesario que el contenido técnico sea interpretado para este grupo.

Asimismo, es necesario que los auditores consideren el potencial impacto negativo del informe de auditoría de TI una vez publicado. Por ejemplo, si en el informe de auditoría de TI se señalasen algunos riesgos en materia de seguridad detectados en el sistema de una organización auditada, y estos se diesen a conocer antes de la adopción de los controles necesarios, la vulnerabilidad de dicho sistema podría verse expuesta al público. En este caso, los auditores podrían considerar diferentes opciones, por ejemplo, presentar el informe únicamente después de haberse adoptado los controles necesarios, sin informar exactamente el riesgo de seguridad para, de ese modo, evitar el potencial efecto adverso en la organización auditada, o elaborar un informe confidencial separado/anexado cuyo propósito no sea darle una circulación generalizada.

[35]Organización Internacional de las Entidades Fiscalizadoras Superiores, *ISSAI 100,* Párrafos 38, 39, 38.

El Apéndice II contiene enlaces a informes de auditoría señalados por EFS de diferentes partes del mundo relacionados con los capítulos de este manual. Estos informes de auditoría pueden proporcionar ejemplos valiosos del amplio conjunto de áreas de auditoría de TI analizados en este manual.

A. Etapas de la elaboración de informes

La elaboración de informes de auditoría de TI depende de las tradiciones de cada EFS y sus entornos jurídicos. Con frecuencia, la confección de informes sobre el proceso de auditoría comprende las siguientes etapas:

i. Borrador del informe

El proceso de elaboración de informes comienza con el análisis del primer borrador de un informe. Este borrador, tras ser acordado y aprobado en el seno de la EFS, se envía a la dirección de la organización auditada antes de la reunión de cierre. Seguidamente, el borrador se incluye como tema de análisis en dicha reunión. Esto permite identificar, corregir o eliminar tempranamente errores fácticos, expresiones desmesuradas, y/o incongruencias. Una vez que la organización auditada y el auditor hayan conversado acerca de los contenidos del borrador, éste se ocupará de realizar las modificaciones necesarias y enviará a la organización un borrador formal.

ii. Carta a la dirección

La carta a la dirección es el borrador formal entregado a la organización auditada, de forma tal que ella pueda responder a las observaciones formuladas. Esto permite a la dirección de la organización concentrarse en los hallazgos, conclusiones y recomendaciones que contiene el borrador formal recibido. En este punto, es el deber de la dirección redactar formalmente los comentarios/respuestas al auditor y abordar todos los hallazgos.

iii. Informe de auditoría final

Tras recibir los comentarios de la organización auditada, el auditor elaborará una respuesta donde se reflejará la posición de la auditoría. Esto se realiza mediante la combinación de los comentarios del auditor con la respuesta de la organización en un informe, que es el informe de auditoría (en su versión final).

Al informar sobre irregularidades o casos de incumplimiento de leyes o reglamentos, los auditores deben ser conscientes de enfocar sus hallazgos desde una perspectiva correcta. Los informes sobre irregularidades pueden confeccionarse independientemente de las salvedades contenidas en la opinión del auditor.

Por su naturaleza, los informes de auditoría tienden a contener críticas importantes, pero, a los efectos de ser constructivas, también deberían abordar futuras acciones correctivas mediante la incorporación de manifestaciones formuladas por la organización auditada o el auditor, lo que incluye conclusiones o recomendaciones.[36] Según la EFS de que se trate, los destinatarios finales del informe a la dirección pueden ser las personas responsables de la gestión de las operaciones de la organización, o quienes tienen la responsabilidad de supervisar la dirección estratégica de dicha organización y las obligaciones relacionadas con la rendición de cuentas por parte de ella.

Cuando se trate de auditorías que incluyan tareas relacionadas con el área de TI, en algunos casos, el resultado obtenido a raíz de dichas tareas puede comunicarse a la organización mediante una carta separada. En estos casos, quizá sea importante explicar cómo el resultado de la labor de auditoría de TI se relaciona con otras comunicaciones que forman parte de la auditoría de desempeño, financiera o de cumplimiento, y el modo en que los resultados de dicha labor pueden ser relevantes para el informe

[36]Organización Internacional de las Entidades Fiscalizadoras Superiores, *ISSAI 100,* Párrafo 51.

confeccionado por la EFS.

iv. Formulación de conclusiones y recomendaciones

Los hallazgos, conclusiones y recomendaciones de auditoría deben sustentarse en evidencia. Al formular las conclusiones, el auditor de TI debería prestar atención a la materialidad del asunto, considerando la naturaleza de la auditoría o la organización auditada.[37] Para que los informes elaborados sean equilibrados, también debería darse cuenta de los logros dignos de mención que corresponden al mandato de la EFS.

Los auditores de TI deberían extraer conclusiones sobre los hallazgos sobre la base de los objetivos establecidos. Las conclusiones deberían ser relevantes, lógicas e imparciales. Asimismo, deberían evitarse las conclusiones generalizadas acerca de la ausencia de controles y la existencia de riesgos toda vez que ellas no se respalden en exámenes sustantivos, como las pruebas de control.

Los auditores de TI deberían formular recomendaciones cuando de los hallazgos surja la posibilidad de lograr mejoras significativas en las operaciones y el desempeño. También deberían informar acerca de la situación de hallazgos y recomendaciones significativos resultantes de auditorías anteriores y que inciden en los objetivos de la auditoría actual. Las recomendaciones constructivas pueden promover la realización de mejoras. Ellas son más constructivas cuando apuntan a resolver la causa de los problemas identificados, se orientan a la acción y son específicas, se dirigen a las personas que tienen la autoridad para actuar, son factibles, y revisten eficacia en función de los costos.

v. Limitaciones y restricciones de la auditoría de TI

En el informe también deberían señalarse las limitaciones de la auditoría de TI. Las limitaciones típicas son un acceso inadecuado a datos e información, la falta de documentación adecuada del proceso de TI, y el hecho de que el auditor se vea obligado a formular sus propios métodos de investigación y análisis para la extracción de conclusiones. Cualquier otra limitación o restricción afrontadas por el auditor de TI y que afecten el alcance y la ejecución de la auditoría deberían señalarse adecuadamente en el informe.

vi. Respuesta de la dirección

Cuando se trata de informes de auditoría de TI, es extremadamente importante obtener una respuesta a las observaciones de auditoría. Los auditores de TI deberían organizar reuniones con la alta dirección del organismo auditado, y documentar su respuesta. Si tales esfuerzos fracasasen, debería conservarse evidencia suficiente de que fueron realizados, y darse cuenta de ello en el informe.

VI. Referencias y lecturas adicionales

Internal Audit Community of Practice. *Risk Assessment in Audit Planning.* https://www.pempal.org/sites/pempal/files/event/attachments/cross_day-2_4_pempal-iacop-risk-assessment-in-audit-planning_eng.pdf. April 2014.

International Organization of Supreme Audit Institutions Development Initiative. *INTOSAI Development Initiative (IDI) AFROSAI/E-IT Audit Courseware.*

International Organization of Supreme Audit Institutions Development Initiative. *Performance Audit ISSAI Implementation Handbook,* version 1. *https://www.idi.no/work-streams/professional-sais/work-stream-library/performance-audit-issai-implementation-handbook.* August 2021.

Organización internacional de las Entidades Fiscalizadoras Superiores (ISSAI) 100: Principios

[37]Organización Internacional de las Entidades Fiscalizadoras Superiores, *ISSAI 100,* Párrafo 50.

Fundamentales de la Auditoría del Sector Público. 2019.

Organización Internacional de Entidades Fiscalizadoras Superiores. *Organización internacional de las Entidades Fiscalizadoras Superiores (ISSAI) 200: Principios Fundamentales de la Auditoría Financiera.* 2019.

Organización Internacional de Entidades Fiscalizadoras Superiores. *Organización internacional de las Entidades Fiscalizadoras Superiores (ISSAI) 300: Principios Fundamentales de la Auditoría del Desempeño.* 2019.

Organización Internacional de Entidades Fiscalizadoras Superiores. *Organización internacional de las Entidades Fiscalizadoras Superiores (ISSAI) 400: Principios Fundamentales de la Auditoría del Cumplimiento.* 2019.

Organización Internacional de Entidades Fiscalizadoras Superiores. *GUID 5100: Guía sobre Auditoría de los Sistemas de Información.* 2019.

ISACA. *CISA Review Manual,* 27th ed.

ISACA. *COBIT 2019 Framework: Governance and Management Objectives. https://www.isaca.org/resources/cobit.* November 2018.

ISACA. *IT Audit Framework (ITAF): A Professional Practices Framework for IT Audit,* 4th ed. October 22, 2020.

U.S. Government Accountability Office. *Federal Information System Controls Audit Manual* (FISCAM). https://www.gao.gov/products/gao-09-232g. February 2, 2009.

CAPÍTULO 2: GOBERNANZA Y GESTIÓN DE TI

I. ¿Qué son la gobernanza y gestión de TI?

La gobernanza de TI podría considerarse como el marco general que guía las operaciones de TI de una organización para asegurarse de que se satisfagan las necesidades actuales de su negocio o actividad y se incorporen planes para sus necesidades y crecimiento futuros. Asimismo, constituye una parte integral de la gobernanza de una organización y abarca el liderazgo organizacional, sus estructuras y procesos institucionales, y otros mecanismos (relacionados con la elaboración de informes y formulación de comentarios y sugerencias, la observancia de normas, y los recursos de los que dispone, entre otros) que garantizan que los sistemas de TI apuntalen los objetivos y la estrategia de la organización mientras se equilibran los riesgos y se gestionan eficazmente los recursos.

Es importante comprender que, según el marco COBIT de ISACA, existe una distinción clara entre la gobernanza y la gestión:[38]

- La **gobernanza** garantiza que se evalúen la necesidades, condiciones y opciones de las partes interesadas para establecer objetivos organizacionales equilibrados y consensuados; se establezca una dirección mediante la priorización y toma de decisiones; y se monitoreen el desempeño y cumplimiento en función de la dirección y objetivos acordados.
- Mediante los planes de **gestión** se conciben, llevan adelante y monitorean las actividades en concordancia con la dirección establecida por el órgano de gobernanza para lograr los objetivos de la organización.

La gobernanza de TI desempeña un rol fundamental en la determinación del entorno de control y sienta las bases para la instrumentación de prácticas adecuadas de control y elaboración de informes a niveles funcionales para su supervisión y revisión por parte de la dirección. Es esencial asegurarse de que

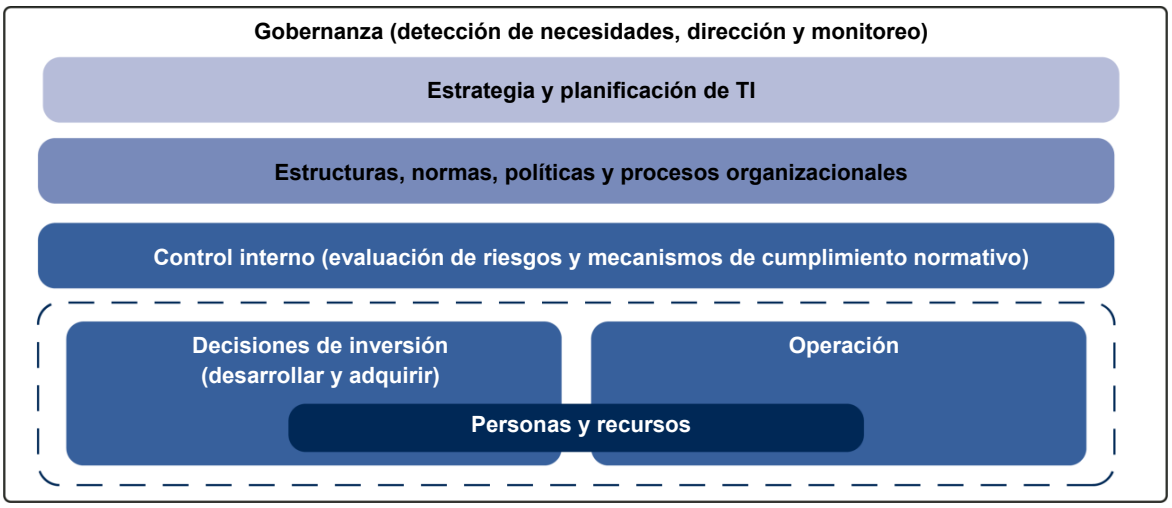
- se evalúen las necesidades, condiciones y opciones de las partes interesadas para establecer objetivos organizacionales equilibrados y consensuados;
- se establezca una dirección basada en la priorización y toma de decisiones; y
- se monitoree el desempeño y cumplimiento normativo en función de la dirección y los objetivos acordados.

En muchas organizaciones, la gobernanza está a cargo de un directorio, bajo la conducción de un presidente. Las responsabilidades de gobernanza específicas pueden delegarse a estructuras organizacionales especiales, a un nivel adecuado, particularmente cuando se trata de organizaciones más grandes y complejas.

La Figura 7 contiene un marco de gobernanza de TI de carácter genérico.

[38] *Remítase a la Sección IV: Referencias y lecturas adicionales* de este capítulo para acceder a referencia y recursos adicionales relacionados con las mejores prácticas y marcos vinculados con la gobernanza y gestión de TI.

Figura 7: Marco genérico de gobernanza de TI



Fuente: Unknown

A. Detección de necesidades, dirección y monitoreo

La gobernanza de TI es un componente clave de la gobernanza institucional general. La gobernanza de TI debería considerarse como la forma en que la tecnología de la información genera valor que se integra a la estrategia de gobernanza organizacional en su conjunto, nunca como una disciplina en sí misma. Al adoptar este enfoque, se requiere que todas las partes interesadas participen en el proceso de toma de decisiones vinculado con la gobernanza de TI. Esto conduce a una aceptación compartida de la responsabilidad por sistemas críticos y garantiza que las decisiones en materia de TI se tomen en función de las necesidades del negocio o actividad, y se sustenten en ellas.

Para que la gobernanza de TI permita garantizar que las inversiones en esta área generen valor para el negocio, y que se mitiguen los riesgos relacionados con ella, es necesario instrumentar una estructura organizacional con roles bien definidos en cuanto a las responsabilidades relativas a la información, procesos del negocio o actividad, aplicaciones e infraestructura.

El órgano de gobierno evalúa las opciones estratégicas, orienta a la dirección superior respecto a las opciones estratégicas seleccionadas, y monitorea los logros alcanzados. La dirección se ocupa de

- la organización general, la estrategia, y las actividades de apoyo relativas a la TI;
- la definición, adquisición e implementación de soluciones de TI y su integración a los procesos del negocio o actividad;
- prestaciones operativas y de apoyo de los servicios de TI; lo que incluye seguridad; y
- monitoreo del desempeño y cumplimiento de los sistemas de TI con las metas de desempeño interno, los objetivos de control interno y los requisitos externos.

También es esencial incorporar la gobernanza de TI al proceso para detectar necesidades nuevas o actualizadas y luego brindar las soluciones de TI (y otras soluciones) adecuadas al usuario. Durante el proceso de desarrollo o adquisición de las soluciones para satisfacer las necesidades del negocio o actividad, la gobernanza de TI garantiza que la solución seleccionada responda a tales necesidades, y que se disponga de la capacitación y los recursos necesarios para implementarla (por ejemplo, hardware, herramientas y capacidad de red). Las actividades de monitoreo pueden ser llevadas adelante por la auditoría interna o por el grupo de aseguramiento de la calidad, informando periódicamente los resultados a la dirección.

II. Elementos clave de la gobernanza y gestión de TI[39]

a. Estrategia y planificación de TI

La estrategia de TI importa una alineación recíproca entre la estrategia de TI y los objetivos estratégicos del negocio o actividad. Entre los objetivos estratégicos de TI deberían considerarse las necesidades actuales y futuras del negocio o actividad, la capacidad actual de prestar servicios de TI, y las necesidades en materia de recursos.[40] La estrategia debería abarcar la infraestructura y arquitectura de TI actuales, las inversiones, el modelo de prestación, y la obtención de recursos (incluidos los recursos humanos), además de delinearse en ella el plan de integración de estos elementos en un enfoque común para respaldar los objetivos del negocio o actividad.

Es importante que un auditor de TI examine la estrategia de una organización en este campo, no solamente para lograr comprender suficientemente a esa organización, sino también para evaluar en qué medida la gobernanza de TI ha sido parte de la toma de decisiones en el ámbito organizacional.

Sin una estrategia de TI, existe un mayor riesgo de que las organizaciones no identifiquen cómo este recurso puede satisfacer las necesidades actuales y futuras del negocio o actividad desarrolladas. Asimismo, sin un plan estratégico de TI actualizado –vinculado con el plan estratégico general de la organización, que incluye los objetivos, medidas de desempeño, estrategias, e interdependencia entre proyectos– las organizaciones corren el riesgo de carecer de una definición clara de lo que desean lograr con la TI y las estrategias para el logro de tales resultados

B. Estructuras, normas, políticas y procesos organizacionales

Las estructuras organizacionales son un elemento fundamental de la gobernanza de TI respecto a la articulación de los roles de diversos organismos de dirección y gobernanza tanto para el negocio o actividad como para la toma de decisiones. Mediante ellas deberían asignarse responsabilidades claramente definidas para la toma de decisiones y el monitoreo del desempeño. Las estructuras organizacionales deben sostenerse en normas, políticas y procedimientos adecuados, capaces de mejorar la capacidad de toma de decisiones.

Las **partes interesadas** (es decir, todos los grupos, organizaciones, miembros o sistemas que pueden afectar o verse afectados por las acciones de la organización) influyen en las estructuras organizacionales de una entidad del sector público. Algunos ejemplos de partes interesadas externas importantes son el Parlamento, el Congreso, y/u otras entidades gubernamentales, además de los ciudadanos. También influyen en las estructuras organizacionales los **usuarios**, tanto internos como externos.

Los usuarios internos son los ejecutivos y departamentos funcionales propietarios de los procesos del negocio o actividad, además de las personas dentro de la organización que interactúan con tales procesos. Los usuarios externos son los organismos, las personas y el público que utilizan los productos o servicios provistos por una organización (por ejemplo, otros departamentos y los ciudadanos). Otra influencia en las estructuras organizacionales es ejercida por los **proveedores**: una compañía, unidad o persona, interna o externa, que provee un servicio.

La necesidad de disponer de funcionalidades de TI surge de los usuarios y las partes interesadas. En todos los casos, el organismo gubernamental competente debería establecer las estructuras, roles y responsabilidades de gobernanza adecuados, con miras a lograr una clara asunción de propiedad y rendición de cuentas respecto a las decisiones y tareas importantes. Esto debería incluir relaciones con

[39]Los elementos clave presentados en este capítulo sobre gobernanza de TI son respaldados por el *Marco COBIT 5, COBIT 2019*, y la norma *ISO 38500*, recurriéndose ampliamente a sus definiciones y ejemplos.

[40]Organización Internacional de Normalización, *ISO 38500*.

proveedores externos de servicios clave de TI.[41]

La estructura organizacional de TI habitualmente incluye un **comité rector de TI**, que es la piedra angular de la estructura organizacional. El comité rector de TI está integrado por miembros de los niveles directivos superiores y tiene la responsabilidad de examinar, autorizar y comprometer el aporte de fondos para la realización de inversiones de TI, además de garantizar el logro de las metas y objetivos principales asignados a la organización. El comité rector debería cumplir una función esencial en la formulación de decisiones relacionadas con el negocio o actividad para las que se requiera tecnología que respalde las inversiones correspondientes, además de aprobar el modo de adquisición de dicha tecnología. Las decisiones de inversión que implican soluciones vinculadas con "construir o comprar" habitualmente recaen en el comité rector de TI, en general, luego de haber recibido las recomendaciones correspondientes de grupos o comités designados a tal efecto.

El comité rector desempeña un papel fundamental en la promoción de la aceptación necesaria y la prestación de apoyo para la instrumentación de programas que implican cambios para la organización. En muchas organizaciones del sector público, las funciones del comité rector de TI son parte de la función directiva. Es importante destacar que la gobernanza de TI es compleja y multifacética. Diferentes estructuras directivas, como el comité rector, servirán a distintos propósitos y desempeñarán y ejercerán roles y responsabilidades diferentes en función de una diversidad de factores, incluidos aquellos que se relacionan con las necesidades, el sector y el entorno de la organización. Aunque los roles y responsabilidades que comprenden la función directiva pueden variar entre países y sectores (por ejemplo, entre organizaciones del sector público y privado), podemos enumerar algunos ejemplos:

- El **Director General Ejecutivo**, es el funcionario de mayor jerarquía, responsable por la gestión global de la organización.
- El **Director General Financiero** es el funcionario de mayor jerarquía responsable por todos los aspectos de la gestión financiera, incluidos los riesgos y controles financieros.
- El **Director General Operativo**, es el funcionario de mayor jerarquía responsable por la operación de la organización.
- El **Director General de Riesgos**, es el funcionario de mayor jerarquía, responsable por la gestión de los riesgos en todos los sectores de la organización. Un Director General de Riesgos puede ejercer funciones relacionadas con los riesgos asociados al área de TI para supervisarlos.
- El **Director General de Privacidad** es la persona responsable por monitorear los riesgos e impactos en el negocio o actividad de las leyes en materia de privacidad y por guiar y coordinar la implementación de políticas y actividades por las que se pretende garantizar el cumplimiento de las directivas en la materia.
- El **Director General de Información** es un funcionario jerárquico responsable por la gestión y operación de las capacidades en materia de TI de una organización. En muchas organizaciones del sector público, las funciones desempeñadas por el Director General de Información pueden ser llevadas a cabo por un grupo o departamento que tenga las responsabilidades, autoridad y recursos necesarios.
- El **Director General de Tecnología** es un funcionario jerárquico cuyas responsabilidades incluyen, entre otras, asegurarse de que la organización utilice la tecnología de forma eficaz y eficiente, mediante la incorporación de las mejores prácticas y procedimientos a la implementación de las capacidades de TI, y la provisión de conocimientos específicos para la adopción de tecnologías emergentes en la organización.
- El **Director General de Seguridad Informática**, es el funcionario de mayor jerarquía responsable por la seguridad de la información de la organización en todos sus formatos.
- El **Director General de Capital Humano** es el funcionario de mayor jerarquía responsable de coordinar las políticas y procedimientos de recursos humanos con la misión y objetivos de la organización.

[41]ISACA, *COBIT 2019*.

- El **Director General de Conocimientos**, es el funcionario de mayor jerarquía responsable por la gestión de todas las formas de conocimiento dentro de la organización.

Sin una estructura organizacional bien definida, lo que incluye un comité rector de TI, es posible que la organización carezca de un órgano responsable de tomar decisiones vinculadas con su negocio o actividad y la provisión de tecnología para respaldar las inversiones correspondientes, además de aprobar el modo de adquirir esa tecnología. Asimismo, las organizaciones pueden carecer del apoyo necesario para la instrumentación de programas. A raíz de ello, es posible que estas actividades se lleven a cabo de una manera incongruente y desorganizada, y no conduzcan al logro de buenas relaciones precio/prestación o la consecución de los objetivos del programa o inversión.

c. Normas, políticas y procesos

Las normas y políticas son adoptadas por la organización y aprobadas por la dirección superior. Las políticas determinan el marco de alto nivel para las operaciones diarias, teniendo en mira el cumplimiento de los objetivos establecidos por el órgano rector. Las normas establecen medidas cuantificables del cumplimiento de las políticas. Las normas y políticas son respaldadas por procesos que definen el modo en que el trabajo o las medidas deben llevarse a cabo o controlarse. La dirección superior establece estos objetivos para dar cumplimiento a la misión de la organización y, al mismo tiempo, cumplir con los requisitos legales y reglamentarios pertinentes.

Es necesario revisar y ajustar regularmente las normas, políticas y procesos correspondientes que, además, deben comunicarse con periodicidad a todos los usuarios pertinentes de la organización. También es necesario brindar a los empleados del departamento de TI capacitación acerca del modo de aplicar y utilizar estas políticas, normas y procesos en sus operaciones diarias. Las políticas y normas y los procesos correspondientes deberían reflejar las actualizaciones concernientes a nuevas tecnologías y amenazas, los cambios significativos en procesos y los nuevos requisitos asociados el entorno y el marco normativo. Habitualmente, serán las normas de una organización lo que una auditoría de TI utilizará como materia objeto de examen, dado que se trata de medidas que pueden auditarse.

Es necesario revisar y ajustar las políticas y los procesos correspondientes de acuerdo con las necesidades. Dichas políticas y procesos deberían comunicarse periódicamente a todos los usuarios pertinentes de la organización. Las políticas deberían reflejar las actualizaciones relativas a nuevas tecnologías y amenazas, los cambios significativos en procesos y los nuevos requisitos asociados con el entorno y el marco normativo. Algunas políticas clave que orientan la gobernanza de TI son:

- **La política de recursos humanos:** La política de recursos humanos se ocupa de la contratación, la capacitación, el cese de relaciones laborales, y otras funciones de la organización. También se ocupa de los roles y responsabilidades de diversos integrantes del personal que la compone, además de las habilidades o capacitación que tales integrantes deben poseer para desempeñarse en sus tareas. La política de recursos humanos también se relaciona con la asignación de roles y responsabilidades y la segregación de tareas. Sin embargo, en organizaciones grandes y complejas, esta función puede delegarse en un departamento exclusivamente dedicado a ella.
- **Políticas de documentación y conservación de documentos:** la documentación de los sistemas de información, las aplicaciones, los roles laborales, los sistemas de elaboración de informes, y la periodicidad de su realización, constituye un punto de referencia importante para alinear las operaciones de TI con los objetivos del negocio o actividad. Las políticas adecuadas en materia de conservación de documentación permiten gestionar cambios iterativos en la arquitectura de información de una organización y realizar un seguimiento de ellos.
- **Política de externalización:** Con suma frecuencia, la externalización de TI tiene por fin permitir a la dirección de la organización concentrar sus esfuerzos en las actividades centrales que lleva adelante. El hecho de recurrir a la externalización puede obedecer a la necesidad de reducir gastos corrientes. Mediante la política de externalización se garantiza que las propuestas de externalización de operaciones y funciones se desarrollen e implementen de un modo beneficioso para la organización. Uno de los ejemplos más comunes de servicios de TI externalizados en la actualidad es lo que se conoce como “computación en la nube”, que permite el acceso a través de una red, a petición, a un

conjunto de recursos informáticos configurables (por ejemplo, redes, servidores, dispositivos de almacenamiento y otros servicios). Remítase al Capítulo 5 para acceder a información sobre externalización y computación en la nube.

- **Política de teletrabajo:** las organizaciones deberían formular políticas de teletrabajo y brindar orientación para asegurarse de que sus empleados estén listos para esta modalidad laboral. Una práctica esencial para facilitar el teletrabajo es redactar convenios de teletrabajo para ser utilizados por empleados y directivos. Los convenios de teletrabajo deberían contener las disposiciones laborales básicas consensuadas por directivos y empleados previamente al inicio de esta modalidad laboral. En estos convenios deberían consignarse las funciones y expectativas laborales, los estándares de desempeño, y resultados y prestaciones mensurables.
- **Política de seguridad y privacidad de TI:** mediante esta política se establecen los requisitos para la protección de activos vinculados con información, y puede referirse a otros procedimientos o herramientas relativos a su modalidad de protección. Esta política debería estar al alcance de todos los empleados responsables por la seguridad de la información, incluidos aquellos usuarios de sistemas organizacionales que cumplen un rol asociado al resguardo de la información (por ejemplo, cuando se trata de registros personales y datos de carácter financiero). Remítase al Capítulo 7 para acceder a información sobre la política de privacidad y seguridad de TI.
- **Política de gestión de datos:** las organizaciones recopilan datos de numerosas fuentes, como los sistemas transaccionales, escáneres, sensores, redes sociales y dispositivos inteligentes, entre otros. Por lo tanto, es necesario que definan políticas y procedimientos relativos al modo en que administrarán los datos durante la totalidad de su ciclo de vida, lo que incluye la recopilación, almacenamiento, seguridad y eliminación de los datos. Remítase al Capítulo 4 para acceder a información sobre la gestión de datos.

Las organizaciones que carecen de políticas y normas relativas a sus operaciones diarias se exponen a un mayor riesgo de incumplir los objetivos en materia de TI. Por ejemplo, una política de recursos humanos es importante para la gestión de las contrataciones y capacitación, y una política de seguridad de TI es importante para garantizar la protección de los activos de información.

d. Control interno

Como se expuso previamente, el control interno es el proceso que consiste instrumentar un sistema de medidas y procedimientos para determinar si las actividades de la organización son congruentes con las políticas, normas y planes aprobados. Si fuese preciso, deberán tomarse las medidas correctivas necesarias, de forma tal de que los objetivos de la política formulada puedan lograrse.

El control interno mantiene al sistema de TI en funcionamiento. Los controles internos incluyen la gestión de riesgos, la observancia de procedimientos e instrucciones internos, así como también de leyes y reglamentos externos; informes de gestión periódicos y *ad hoc*; comprobaciones de progreso; y revisión de planes y auditorías, evaluaciones, y monitoreo.[42]

Sin controles internos, las organizaciones afrontan un riesgo mayor de que sus sistemas de TI no cumplan con las políticas internas, las normas, las leyes y los reglamentos.

i. Gestión de riesgos

La gestión de riesgos de TI debería ser una parte integral de la estrategia y políticas de gestión de riesgos de la organización. En este caso, la gestión de riesgos supone la detección de aquellos riesgos que se vinculan con las aplicaciones e infraestructura de TI actuales, además de una gestión continua, lo que incluye la revisión y actualización de tales riesgos por parte de la dirección, además del monitoreo de las estrategias de mitigación correspondientes. La gestión de riesgos de TI debería formar parte de la gestión

[42]"IT Governance in Public Sector: A top priority," *WGITA IntoIT,* Issue no. 25, (August 2007).

general de riesgos dentro de la organización.

La elaboración de un plan de gestión de riesgos ayuda a facilitar el proceso de gestión de riesgos. El plan sirve para documentar el proceso de identificación y evaluación de riesgos. También sirve para documentar los procesos, herramientas y procedimientos para la gestión y control de riesgos durante un proyecto. Remítase al Capítulo 3 sobre desarrollo y adquisición de TI para acceder a más información sobre gestión de riesgos.

ii. Mecanismo de cumplimiento

Es necesario que las organizaciones dispongan de un mecanismo de cumplimiento por el que se garantice la observancia de todas las políticas, y la normas y procedimientos asociados a ellas. Es importante establecer una cultura organizacional en la que los empleados comprendan el impacto de la inobservancia de las políticas, normas y procedimientos formulados. El mecanismo de apoyo al cumplimiento también puede abarcar el grupo de aseguramiento de la calidad, personal de seguridad y herramientas automatizadas. Un informe de incumplimiento debería ser examinado por los directivos competentes, debiéndose abordar aquellas cuestiones vinculadas con incumplimientos serios o reiterados. La dirección puede optar por abordar situaciones de incumplimiento mediante capacitaciones de repaso, la modificación de procedimientos, o incluso la aplicación de procedimientos sancionatorios de agravamiento progresivo, según sea la naturaleza del incumplimiento (por ejemplo, violaciones a la seguridad y ausencia de capacitación obligatoria).

Un aseguramiento independiente, instrumentado mediante auditorías (o revisiones) internas o externas, puede brindar información oportuna acerca del cumplimiento del área de TI con las políticas, normas, procedimientos y objetivos generales de la organización. Estas auditorías deben realizarse con un criterio imparcial y objetivo, de modo tal que los directivos reciban una evaluación ecuánime del proyecto de TI que se está auditando.

Sin la existencia de mecanismos de verificación del cumplimiento normativo, es posible que las organizaciones carezcan de un aseguramiento independiente de que el proceso y los productos seleccionados se implementen de la forma planificada y concuerden con la descripción, las normas y los procedimientos correspondientes al proceso.

e. Decisiones de inversión

La gobernanza de TI debería brindar a los usuarios organizacionales soluciones que respondan a sus requisitos nuevos o modificados. El departamento de TI puede acceder a estas soluciones mediante decisiones de inversión que impliquen ya sea el desarrollo (elaboración) de software o sistemas nuevos, o la adquisición de estas herramientas de proveedores, considerando para ello la eficacia en función de los costos. A los efectos de tomar decisiones de inversión exitosas, las prácticas óptimas habitualmente suponen un enfoque disciplinado para la identificación, análisis, priorización y aprobación de necesidades; la realización de un análisis costo/beneficio entre soluciones competidoras; y la selección de una solución óptima (por ejemplo, una en la que se equilibren el costo y los riesgos, y permita cumplir una cantidad significativa de los objetivos de la organización).

El desarrollo un caso de negocio (u organizacional), en el que se identifiquen las necesidades de los usuarios y se pongan de relieve las oportunidades y beneficios de una solución, es una herramienta valiosa para orientar las decisiones de inversión. El caso de negocio puede comenzar como una estrategia de alto nivel y derivar en una descripción detallada de tareas, hitos, responsabilidades y roles esenciales. Dicho caso de negocio constituye una herramienta dinámica que requiere actualizaciones continuas para reflejar la situación actual y considerar el futuro de la iniciativa. Remítase al Capítulo 3 para acceder a más información sobre el desarrollo y adquisición de TI.

f. Operaciones de TI

Las operaciones de TI habitualmente consisten en el quehacer diario de la infraestructura de TI para

respaldar las necesidades de la organización. Una adecuada gestión de las operaciones de TI posibilita la detección de cuellos de botella y la planificación de modificaciones vinculadas con la capacidad (por ejemplo, de hardware o recursos de red adicionales), así como también la medición del desempeño para asegurarse de que éste satisface las necesidades acordadas de los propietarios del negocio o actividad, y brindar a los usuarios de TI una mesa de ayuda y apoyo para la gestión de incidentes. Remítase al Capítulo 4 para acceder a más información sobre las operaciones de TI.

g. Personas y recursos

Se recomienda que la dirección se asegure, mediante evaluaciones regulares, de que se asignen recursos suficientes en materia de TI para satisfacer las necesidades de la organización, según las prioridades acordadas y las limitaciones presupuestarias. Asimismo, en las políticas, prácticas y decisiones del área de TI debería respetarse el aspecto humano, considerándose las necesidades actuales y futuras de los participantes en el proceso. Mediante la gestión de la gobernanza debería evaluarse regularmente si los recursos se están utilizando y priorizando en función de las exigencias propias de los objetivos de la organización.

Las organizaciones pueden beneficiarse de la gestión y planificación de la fuerza laboral de TI mediante la comprobación de que las necesidades en términos de competencias y dotación de personal resultan satisfechas, y de la inclusión de prácticas de contratación, capacitación, y desarrollo de la fuerza laboral y la gestión de su desempeño. Algunos elementos clave para disponer de una fuerza laboral adecuada son:

- establecer y mantener un proceso de planificación de la fuerza laboral,
- establecer requisitos en materia de competencias y dotación de personal,
- evaluar regularmente las necesidades relacionadas con las competencias y dotación de personal,
- evaluar las deficiencias en materia de competencias y dotación de personal,
- desarrollar estrategias y planes para el abordaje de las deficiencias en materia de habilidades y dotación de personal,
- implementar acciones para resolver deficiencias, monitorear el progreso en la resolución de tales deficiencias, e
- informar a la dirección acerca los progresos relativos al abordaje de las deficiencias.

iii. Riesgos para la organización auditada

Es necesario que los auditores comprendan y evalúen los diferentes componentes de la estructura de gobernanza de TI para determinar si las decisiones, indicaciones, recursos, gestión y monitoreo de esta área respaldan los objetivos y estrategias de la organización. Para realizar la evaluación, es necesario que los auditores conozcan los componentes clave de la gobernanza y gestión de TI, además de los riesgos asociados a la falta de idoneidad de cada componente en una entidad.

El monitoreo, análisis y evaluación constante de los parámetros relacionados con las iniciativas de gobernanza de TI supone la adopción de una visión independiente y equilibrada para facilitar la mejora de los procesos de TI. La auditoría desempeña un rol importante en la implementación exitosa de la gobernanza de TI mediante la formulación de recomendaciones sobre la mitigación de riesgos asociados con los siguientes aspectos de la gestión y gobernanza de TI:

- la alineación de la función de TI con la misión, visión, valores, objetivos y estrategias de la organización;
- el logro de objetivos de desempeño establecidos por la organización y la función de TI;
- los requisitos en materia legal, ambiental, de calidad de la información, fiduciarios, de seguridad y de privacidad;
- el entorno de control de la organización;
- el riesgo inherente dentro del entorno de seguridad de la información; y

- la inversión/el gasto en TI.

Toda organización afronta desafíos particulares, dada la diferencia entre las cuestiones sociales, ambientales, políticas, geográficas y económicas que inciden en ellas. Aunque esta no es una lista pormenorizada, las consecuencias que se presentan a continuación constituyen riesgos comunes que podrían derivar de la falta de una adecuada gobernanza de TI.

a. Sistemas de TI ineficaces e ineficientes

Los sistemas de administración pública cuyo fin de servir a la sociedad y las empresas, o mejorar la funcionalidad de los organismos gubernamentales, a menudo constituyen soluciones extremadamente amplias y complejas. Por lo tanto, deberían diseñarse adecuadamente, adaptarse a las necesidades reales de la organización, coordinarse de forma competente, y operarse de manera eficiente. La falta de asunción de propiedad respecto a los procesos, aplicaciones y datos por parte de la organización podría conducir a una deficiente gobernanza de TI. Una deficiente gobernanza de TI a nivel gubernamental y organizacional puede ser el primer obstáculo para tener sistemas de TI de buena calidad.

b. Percepción de que la TI contribuye escasamente al valor de la organización

Las inversiones en TI que no se encuentren estratégicamente alineadas con los objetivos y recursos de la organización le aportarán poco o ningún valor. Dicha deficiencia en términos de alineación estratégica significa que incluso una TI de buena calidad puede no contribuir de manera eficaz y eficiente al logro de los objetivos generales de la organización. Una forma de garantizar esa alineación es involucrar a los usuarios y otras partes interesadas que comprendan el negocio o actividad de la organización en la toma de decisiones en materia de TI. Estas partes interesadas pueden contribuir al desarrollo del caso de negocio u organizacional para garantizar la alineación con los objetivos y recursos de la organización.

c. Falta de involucramiento del Departamento de TI de la organización

De la investigación surge que las organizaciones líderes adoptan y utilizan un enfoque que abarca la organización en su conjunto para la gestión de TI, lo que incluye, entre otros elementos:

- la responsabilidad por rubros comúnmente asociados al área de TI, por ejemplo, los servicios de correo electrónico y mesa de ayuda, y la adquisición de hardware y software;
- la supervisión de sistemas específicos para la misión de la organización; y
- responsabilidades claramente distribuidas entre el departamento de TI de la organización y cualesquiera unidades de negocio o componentes.

Sin una autoridad y supervisión centralizadas, el grado de seguridad de que las inversiones en TI se están coordinando a nivel de la organización en su conjunto es menor, lo que también se aplica a la provisión de la combinación adecuada de capacidades que respaldan las necesidades asociadas a la misión de la organización mientras se evitan duplicaciones innecesarias.

d. Exposición a riesgos vinculados con la seguridad de la información y la privacidad

Una organización que no disponga de controles, estructuras, procesos y políticas adecuados en lo relativo a la seguridad de la información, afronta un riesgo mayor de sufrir incidentes e infracciones vinculados con la seguridad y la privacidad. Estos riesgos incluyen, entre otros, la apropiación indebida de activos; la divulgación no autorizada de información; el acceso no autorizado; y la vulnerabilidad a ataques lógicos y físicos, ciberataques, alteraciones e indisponibilidad de la información, uso indebido de la información, inobservancia de leyes y reglamentos sobre datos personales, e incapacidad para recuperarse de desastres. La política de seguridad de TI debería definir los activos organizacionales (por ejemplo, datos, equipamiento y procesos de negocio) que precisan protección y los vínculos con los procedimientos, herramientas, y controles de acceso físico que protegen dichos activos.

Las estructuras de gobernanza a nivel ejecutivo de una organización deberían incluir políticas,

procedimientos y procesos para gestionar y monitorear las medidas de protección en materia de seguridad y privacidad de la información de la organización. Estos documentos deberían comunicar las prioridades de la misión, los recursos disponibles, y la tolerancia general a los riesgos para la seguridad de la información. La organización también debería disponer de un proceso para dar apoyo a las actividades de cumplimiento de las leyes, reglamentos y pautas aplicables en materia de seguridad de la información. Entre otras obligaciones, las personas encargadas de la protección de los sistemas y datos deberían mantener informados a los directivos competentes y encontrarse debidamente capacitados.

Las estructuras de gobernanza de seguridad de la información se definen con mayor detalle en otros materiales de referencia. Esta no pretende ser una lista pormenorizada de las diversas estructuras de gobernanza de seguridad de la información. A continuación, presentamos otros materiales clave sobre seguridad de la información y privacidad

- ISACA. *COBIT 2019 Framework: Governance and Management Objectives*. 2019.
- International Organization for Standardization/International Electrotechnical Commission. *ISO/IEC 27001: 2013—Information technology—Security techniques—Information security management systems—Requirements.*
- National Institute of Standards and Technology. *NIST Special Publication* 800-53, *Security and Privacy Controls for Information Systems and Organizations*, rev. 5. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final. September 2020.
- National Institute of Standards and Technology. *NIST Special Publication 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.* https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final. December 2018.

e. Limitaciones para el crecimiento de la organización

Una planificación deficiente en materia de TI, o la inexistencia de tal planificación, pueden conducir a que el crecimiento de la organización se vea refrenado por la falta de recursos de TI o un uso ineficiente de los recursos existentes. Una forma de mitigar este riesgo es desarrollar y actualizar periódicamente una estrategia de TI, lo que permitiría identificar recursos y planes para satisfacer necesidades futuras de la organización.

f. Gestión ineficaz de los recursos

Para lograr resultados óptimos a costos mínimos, una organización debe gestionar sus recursos de TI de manera eficaz y eficiente. Asegurarse de que existan suficientes recursos técnicos, software y hardware, además de los recursos humanos dotados del conocimiento y la experiencia suficientes para prestar los servicios de TI, son factores clave para extraer valor de las inversiones en TI. Por ejemplo, la definición y el monitoreo del uso de los recursos de TI en un contrato de nivel de servicio, [43] permite a la organización conocer de manera objetiva si los requisitos en materia de recursos son adecuados para satisfacer sus necesidades.

Recurrir a la planificación de la fuerza laboral para garantizar la disponibilidad de personal debidamente capacitado ayuda a optimizar la gestión de los recursos humanos. La utilización de las estrategias previamente analizadas para la planificación de la fuerza laboral beneficiará a la organización mediante la instrumentación del proceso y su utilización para la detección de necesidades clave en términos de dotación de personal y habilidades, además de la formulación de estrategias para satisfacer estas necesidades.

g. Toma de decisiones inadecuada

[43]En un contrato de nivel de servicio se definen los requisitos y responsabilidades específicos del prestador del servicio, y se estipulan las expectativas del cliente.

Las deficiencias en las estructuras jerárquicas pueden conducir a una toma de decisiones inadecuada. Es posible que esto afecte la capacidad de la organización de prestar sus servicios, y tal vez le impida cumplir con sus objetivos. Los comités rectores y demás grupos organizacionales con la representación adecuada ayudan a tomar decisiones que inciden en la organización.

h. Proyectos fallidos

Muchas organizaciones no consideran la importancia de la gobernanza de TI. Emprenden proyectos relacionados con el área sin comprender plenamente cuáles son las necesidades de la organización respecto al proyecto y cómo éste se vincula con los objetivos de la organización. Sin esta comprensión, los proyectos de TI son más propensos a fracasar. También es una falla común que las aplicaciones adquiridas o desarrolladas no satisfagan las mínimas normas de seguridad y arquitectura. En estos proyectos es posible que se incurra en costos adicionales para mantener y administrar sistemas y aplicaciones atípicos. Un **ciclo de vida de desarrollo de sistemas** (SDLC) definido, y su uso en desarrollos y adquisiciones, constituye una forma de reducir el riesgo de que determinados proyectos fracasen. Remítase al Capítulo 3 sobre desarrollo y adquisición de TI para acceder a más información acerca de las metodologías relacionadas con el SDLC.

i. Dependencia de un tercero (proveedor) o problemas en la prestación del servicio por parte del prestador de TI externalizado

De no haber controles adecuados de los procesos de subcontratación y externalización, es posible que la organización se vea expuesta a una situación de total dependencia de un proveedor o contratista. Primero, se trata de un marco de alto riesgo, dado que, si el proveedor abandonase el mercado o no prestase los servicios contratados, la organización se hallaría en una situación complicada. Otros riesgos incluyen, por ejemplo, controversias por cuestiones de propiedad intelectual, y el acceso no autorizado a datos personales y bases de datos. Es posible que las organizaciones que recurran a la externalización o contraten regularmente con proveedores externos, precisen disponer de una política de externalización o adquisición en la que se defina aquello que puede externalizarse y aquello que no. También es importante que las organizaciones identifiquen y gestionen los riesgos para la cadena de suministro al desarrollar y adquirir productos y servicios de TI. Remítase al Capítulo 7 para acceder más información sobre la gestión de la cadena de suministro.

La supervisión y el monitoreo eficaces de los contratos ayudará a afrontar los riesgos asociados a la dependencia de un proveedor externo. En los contratos deberían definirse los acuerdos de nivel de servicio y los derechos de acceso de terceros. Un monitoreo minucioso del desempeño de los terceros, lo que incluye actualizaciones regulares de la situación y el examen de las prestaciones brindadas, ayuda a garantizar el cumplimiento de las responsabilidades del proveedor. Cuando mediante las actividades de supervisión y monitoreo se detecten deficiencias en el desempeño de terceros, la organización podrá tomar medidas correctivas.

Los auditores y las organizaciones deberían advertir que los proveedores externos (lo que incluye servicios en la nube y servicios administrativos brindados por dichos proveedores) forman parte del entorno de control de la organización. Por lo tanto, la aplicación y los controles generales operados por el tercero también pueden formar parte del alcance de la auditoría de TI, además de cualesquiera otros controles, como el monitoreo y la supervisión de las actividades del proveedor.

j. Falta de transparencia y rendición de cuentas

La rendición de cuentas y la transparencia son dos elementos importantes de la buena gobernanza. La transparencia es una fuerza poderosa que, al aplicársela de manera constante, puede ayudar a combatir la corrupción, mejorar la gobernanza y promover la rendición de cuentas.[44] En ausencia de estructuras,

[44]Organización Internacional de Entidades Fiscalizadoras Superiores*, INTOSAI-P 20, Principios de transparencia y rendición de cuentas,* p.5.

estrategias, procedimientos y controles de monitoreo organizacionales adecuados, es posible que la institución no sea plenamente capaz de rendir cuentas y actuar con transparencia.

k. Falta de cumplimiento de las declaraciones legales y reglamentarias

Las partes interesadas exigen un nivel de aseguramiento cada vez mayor de que las organizaciones ofrezcan la certeza de que están cumpliendo con las prácticas propias de una buena gobernanza institucional en sus entornos operativos. Además, dado que la TI ha permitido la realización de procesos relacionados con el negocio o actividad de las organizaciones de una manera casi perfecta, también existe una necesidad creciente de ayudar a garantizar que los contratos incluyan requisitos substanciales en materia de TI en áreas tales como las de privacidad, confidencialidad, propiedad intelectual y seguridad.[45] Las diversas políticas instrumentadas por una organización, como aquellas relacionadas con la seguridad de TI, externalización y recursos humanos, deben incorporar los marcos legales y reglamentarios correspondientes.

l. Gastos en TI desconocidos, excesivamente elevados o insuficientes

A menudo, las organizaciones descubren que desconocen la suma total erogada en TI, o que esta erogación es superior a la esperada. Esto puede obedecer a la inexistencia de una organización centralizada o una persona a cargo de todo el gasto destinado a TI, o porque las unidades de negocios (o actividades) dentro de una organización no clasifican adecuadamente los gastos en cuestión. De acuerdo con las prácticas óptimas en la materia, deben existir mecanismos de decisión (por ejemplo, un consejo de gobernanza de TI) para la aprobación del todo el gasto relacionado con el área de TI. Las decisiones de inversión en TI deberían tomarse sobre la base del conjunto de necesidades existentes en la organización. Sin esa supervisión, es posible que la organización no esté en condiciones de asegurarse de que se está actuando de acuerdo con sus prioridades.

Además del riesgo de que una organización desconozca cuál es su gasto total en TI, o que su gasto en TI sea excesivamente elevado, es posible que concluya que su presupuesto resulta insuficiente para satisfacer nuevas necesidades propias de su actividad o amenazas emergentes. Muchas organizaciones caen en la cuenta de que la mayor parte de sus presupuestos se destinan al mantenimiento de sus sistemas e infraestructura actuales. Por ejemplo, las organizaciones suelen gastar porciones significativas de su presupuesto destinado a TI en licencias de software, y el soporte y mantenimiento relacionados. Dado que la identificación de licencias de software y su utilización no son sencillas sin las herramientas y el conocimiento adecuados, existe un riesgo mayor de que se destinen fondos a la adquisición de software que no se utilice.

Para controlar mejor el gasto en TI, es importante que una organización defina sus necesidades y objetivos en materia de TI, identifique aquellos proyectos que no contribuyen a satisfacerlos, y tome decisiones basadas en la cartera de TI en su conjunto. Por ejemplo, a menudo se afirma que la computación en la nube ayuda a reducir los costos operativos, sin embargo, según el servicio de que se trate, la configuración, y el uso del servicio en la nube, esta modalidad puede resultar más onerosa. En aplicación de los principios de buena gobernanza de TI, tales modelos de negocio nuevos deberían evaluarse antes de adoptarse.

m. Falta de implementación de un proceso de software

La falta de implementación de un proceso de software puede dar lugar a situaciones en las que el software desarrollado o adquirido no satisfaga las necesidades y/o normas de la organización. Es posible que se produzcan las siguientes situaciones:

- adquisición/desarrollo de software que no satisfaga las necesidades del área de negocio o actividad de la organización,

[45] *COBIT 5 Framework, Appendix E—Principle 5—Conformance.*

- adquisición/desarrollo de software sin una verificación de calidad,
- desarrollo de software que no se implementa debido a que carece de una calidad estándar,
- desarrollo de software incompleto o no concordante con las especificaciones, e
- interrupción o falta de conclusión de proyectos de desarrollo de software.

IV. Referencias y lecturas adicionales

Federal Court of Accounts of Brazil. *Get.it: Governance Evaluation Techniques for Information Technology: A WGITA Guide for Supreme Audit Institutions*. 2016.

ISACA. Whitepaper—*Privacy in Practice 2021: Data Privacy Trends, Forecasts and Challenges*. https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whppip. 2021.

ISACA. *COBIT 2019 Framework: Governance and Management Objectives.* 2019.

ISACA. *COBIT 5 Framework: A Governance Framework for the Governance and Management of Enterprise IT*. 2012.

ISACA. *CISA Review Manual,* 27th ed.

ISACA. *Vendor Management Using COBIT 5*. 2016.

International Organization for Standardization/International Electrotechnical Commission. *ISO/IEC 38500:2015 Information Technology—Governance of IT for the Organization.* https://www.iso.org/standard/62816.html. February 2015.

National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity,* version 1.1. https://www.nist.gov/cyberframework/framework. April 2018.

Organisation for Economic Co-operation and Development. *G20/OECD Principles of Corporate Governance*. http://www.oecd.org/corporate/principles-corporate-governance. November 30, 2015.

U.S. Government Accountability Office. *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities*. GAO-20-129. https://www.gao.gov/products/gao-20-129. October 30, 2019

U.S. Government Accountability Office. *Library of Congress: Strong Leadership Needed to Address Serious Information Technology Management Weaknesses*. GAO-15-315. https://www.gao.gov/products/gao-15-315. March 31, 2015.

U.S. Government Accountability Office. *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity (Supersedes AIMD-10.1.23)*. GAO-04-394G. https://www.gao.gov/products/gao-04-394g. March 1, 2004.

CAPÍTULO 3: DESARROLLO Y ADQUISICIÓN DE TI

I. ¿En qué consiste el desarrollo y la adquisición de TI?

Dado que el rol de la TI se ha convertido en algo crítico para lograr los objetivos organizacionales y brindar a los usuarios mayores capacidades, las organizaciones han procurado con énfasis creciente modernizar las soluciones existentes y desarrollar y adquirir nuevas soluciones de TI. Es posible acceder a nuevas soluciones de TI mediante su desarrollo interno, o externamente, mediante su contratación o externalización (remítase al Capítulo 5 para acceder a información adicional sobre la externalización). A menudo se recurre a una combinación de enfoques. Las organizaciones deberían decidir si desarrollar internamente o adquirir soluciones de TI considerando cuál es el enfoque que mejor satisface sus necesidades. En ocasiones, las soluciones de TI se adquieren e integran a las soluciones actuales de una organización. Otras veces, se desarrollan internamente soluciones nuevas para compensar una falta de funcionalidad que pueda suplirse recurriendo a lo existente en el mercado.

Independientemente de si una organización adopta un enfoque interno o externo para el desarrollo, adquisición e implementación de soluciones de TI, el proceso debería planificarse de modo tal que puedan gestionarse los riesgos y maximizarse las posibilidades de éxito. Asimismo, deberían identificarse, analizarse, documentarse y priorizarse los requisitos correspondientes a estas soluciones. Las organizaciones también deberían utilizar una función de aseguramiento y examen de la calidad para brindar una mayor seguridad acerca de la calidad de estas soluciones.

Las soluciones son habitualmente desarrolladas o adquiridas por una estructura de equipo de proyecto. Aunque es posible que en ocasiones las organizaciones no formalicen un proyecto, necesitan llevar adelante actividades clave comunes asociadas con la planificación y ejecución de un proceso de desarrollo o adquisición (por ejemplo, identificación de requisitos y gestión de riesgos).

Según la Versión 1.3 del *Capability Maturity Model® Integration (CMMI) for Acquisition*, elaborado por el Software Engineering Institute, las organizaciones están adquiriendo cada vez más capacidades, dada la inmediata disponibilidad de productos y servicios cuya compra o contratación es habitualmente más barata que su desarrollo interno. Sin embargo, el riesgo de adquirir productos que no cumplen con el objetivo de la organización o no satisfacen las necesidades de los usuarios es algo muy real. Es necesario gestionar estos riesgos de modo tal que una adquisición se adecue exitosamente a los objetivos y la misión de la organización. Cuando se las realiza de un modo disciplinado, las adquisiciones de TI pueden mejorar la eficiencia operativa de una organización al aprovechar la capacidad del proveedor de suministrar soluciones de calidad con rapidez, a un costo menor y utilizando las tecnologías más adecuadas.

La adquisición de un producto o solución supone que la organización comprenda las necesidades y requisitos de su negocio o actividad, identificados mediante el proceso de gobernanza de TI (remítase al Capítulo 2 para acceder a más información sobre la gobernanza y gestión de TI). El proceso de identificación de requisitos debería incluir a todas las partes interesadas pertinentes (propietarios del proceso) que participan en los procesos o actividades de la organización, como, por ejemplo, los usuarios finales y el personal técnico, que finalmente será el que tendrá que mantener el sistema y brindarle apoyo. Al adquirir servicios (por ejemplo, de mesa de ayuda y automatización de escritorio), para la identificación de requisitos debería incluirse al departamento de TI que interactuará con el proveedor correspondiente. Los requisitos deben priorizarse, de modo tal que, si el proyecto registrase un déficit de presupuesto, u otras restricciones en materia de costos, la satisfacción de determinados requisitos puede diferirse para futuros desarrollos o adquisiciones, según sea el caso.

El proceso de desarrollo y adquisición de TI trae aparejado un número de responsabilidades de los directivos. A menudo, las organizaciones utilizan la metodología SDLC para brindar una estructura de gestión de proyectos y asistir en el cumplimiento de tales responsabilidades. La metodología SDLC consta habitualmente de cinco etapas: (1) iniciación, (2) desarrollo y adquisición, (3) implementación, (4)

operación y mantenimiento, y (5) eliminación. Las metodologías SDLC se analizan con mayor detalle en la sección posterior.

a. Metodologías de proyecto

Existen varias metodologías SDLC diferentes que pueden utilizarse para desarrollar sistemas de TI, que se extienden desde el modelo de cascada tradicional, pasando por el modelo de espiral, hasta los modelos iterativos, como el Agile (ágil).

- Un **modelo de cascada** comienza con el desarrollo de los requisitos y continúa secuencialmente a lo largo de otras etapas –diseño, construcción y puesta a prueba– utilizando el producto de una etapa como insumo para la siguiente, para así elaborar un producto terminado al final. Este modelo permite identificar y seguir con facilidad el estado de desarrollo de un proyecto sobre la base de la etapa actual de dicho proyecto.
- El **modelo de espiral** utiliza un enfoque basado en riesgos para construir de forma incremental un sistema a lo largo de un ciclo que abarca las cuatro etapas de desarrollo. Al utilizar este modelo, cada espiral o ciclo incremental típicamente comienza mediante la determinación de los objetivos de desarrollo y el alcance del incremento. A continuación, se evalúan soluciones alternativas y se emplean técnicas de gestión de riesgos para identificarlos y reducirlos. Luego, se desarrolla un producto para aquello que ha de incrementarse (por ejemplo, un prototipo). Finalmente, el producto se evalúa para determinar si se han cumplido los objetivos iniciales del incremento.
- El **modelo Agile** se enfoca en etapas de desarrollo de corta duración y alcance reducido que producen segmentos de un producto funcional. Este modelo opera con etapas similares a las del modelo de cascada tradicional –requisitos, diseño, construcción y prueba– pero utiliza un ciclo de desarrollo más breve para lograr iteraciones múltiples en plazos similares. Se ha determinado que los enfoques del desarrollo de TI más breves e incrementales ofrecen la posibilidad de mejorar la forma en que los productos de TI se desarrollan e implementan.[46]

  Existen otros marcos que se relacionan con Agile y utilizan muchos de los mismos principios y prácticas. Dos ejemplos son:

  - el modelo **DevOps**, que hace hincapié en la colaboración entre las áreas de desarrollo, operaciones de TI y aseguramiento de la calidad, con miras a lograr una mayor frecuencia en la producción de versiones de software. Los valores generales de DevOps se alinean con Agile, y se lo considera una expansión de las prácticas de implementación de Agile en todas las áreas del ciclo de vida de un producto.
  - El **desarrollo iterativo** divide el trabajo en porciones más pequeñas conocidas como iteraciones para desarrollar y realizar pruebas de forma cíclica.

Según la Versión 1.3 del *CMMI for Development*, publicado por el Software Engineering Institute, al establecer una metodología de desarrollo organizacional y adquisiciones, la organización debería definir y mantener requisitos y directrices que puedan adaptarse a un proyecto determinado. Estos requisitos y directrices deberían basarse en el modelo de desarrollo escogido y en otras cuestiones, como las necesidades del cliente, costos, cronogramas y dificultad técnica.

Aunque las organizaciones pueden seleccionar de entre una variedad de metodologías de proyecto, existen prácticas óptimas clave que, al adoptárselas, incrementan la probabilidad de éxito en el desarrollo o la adquisición de productos o servicios. Estos incluyen, entre otros, el desarrollo y gestión de requisitos, la gestión de riesgos, la gestión de proyectos, la realización de pruebas, la supervisión de proveedores (tanto durante la adquisición como más adelante, si operan el sistema o le brindan apoyo), y la capacitación interna. Estas áreas se analizan con mayor detalle en la sección posterior.

No obstante, independientemente de la metodología de proyecto escogida, una adecuada documentación

[46]Para más información acerca del modelo Agile, remítase al siguiente documento elaborado por la Oficina de Rendición de Cuentas del Gobierno de los Estados Unidos: *Agile Assessment Guide: Best Practices for Agile Adoption and Implementation,* GAO-20-590g, (Sept. 28, 2020), https://www.gao.gov/products/gao-20-590g.

es un factor importante. Además, debería prestarse atención para asegurarse de que la documentación también se encuentre disponible luego de haberse completado la documentación. En aquellas situaciones en las que una organización depende de una solución provista por un desarrollador para comunicar los requisitos, armonizar los registros de usuarios, y monitorear el desarrollo, es común que la documentación resulte inaccesible luego del fin del desarrollo, dificultándole a la organización rastrear la amplitud y el grado de cumplimiento de lo que se ha producido.

II. Elementos clave de la adquisición y desarrollo de TI

a. Realización de un estudio de factibilidad

Aunque existen interpretaciones relativas a la metodología de proyectos para las que se utilizan diferentes etapas y denominaciones, las organizaciones pueden considerar una etapa de estudio de factibilidad como paso inicial, previo a la definición de los requisitos. Un estudio de factibilidad ayuda a analizar los beneficios y soluciones para el área problemática identificada. Los objetivos del estudio de factibilidad son:

- identificar claramente la necesidad;
- determinar una solución alternativa óptima basada en riesgos (por ejemplo, si desarrollar o adquirir);
- definir el plazo para la implementación de la solución;
- determinar el costo aproximado del desarrollo o la adquisición; y
- determinar si la solución se adecua a la estrategia de la organización.

El resultado del estudio debería ser un informe comparativo en el que se reflejen los resultados de los criterios analizados (por ejemplo, costos, beneficios, riesgos, recursos necesarios e impacto organizacional), recomendándose una de las alternativas/soluciones y un curso de acción (si desarrollar o adquirir un sistema).

b. Desarrollo y gestión de requisitos

Al adquirir o desarrollar software nuevo o modificar sistemas de información existentes, los desarrolladores y equipos de proyecto deben definir los requisitos y también gestionar los cambios asociados a tales requisitos. Mediante estos requisitos se establece aquello que el sistema debe hacer, cuán bien debe hacerlo, y cómo debe interactuar con otros sistemas. Los requisitos bien definidos y gestionados constituyen el basamento de los esfuerzos eficaces orientados al desarrollo y adquisición de sistemas. En la Versión 1.3 del *CMMI for Development*, publicada por el Software Engineering Institute, se identifican las prácticas principales en cuatro áreas relacionadas con el desarrollo y la gestión de requisitos:

- **Desarrollar los requisitos del cliente.** Recopilar información sobre todas las necesidades, expectativas, limitaciones, interfaces y requerimientos de automatización (y o digitalización) gestionados centralmente por el departamento de TI o con una participación significativa del departamento de TI y traducirlas en requisitos del cliente.
- **Desarrollar los requisitos del producto.** Refinar y elaborar los requisitos del cliente para desarrollar productos y los requisitos de componentes de productos.
- **Analizar y validar los requisitos.** Verificar la posibilidad de utilizar los activos de TI existentes (lo que incluye software de aplicación) de haberlos; analizar y validar los requisitos con respecto al entorno previsto por los usuarios finales.
- **Gestionar los requisitos.** Gestionar los requisitos e identificar incongruencias con planes de proyecto y productos de trabajo.

Según el Software Engineering Institute, las organizaciones también deberían formular y mantener planes en los que se delineen los procesos para llevar a cabo y lograr instrumentar estas prácticas innovadoras en materia de requisitos, y por los que se establezcan y refuercen las expectativas relacionadas con las partes interesadas relevantes. El Software Engineering Institute también recomienda disponer de un proceso documentado y disciplinado para desarrollar y gestionar requisitos con el fin de reducir el riesgo

de desarrollar un sistema que no satisfaga las necesidades de los usuarios, no pueda probarse adecuadamente, y no tenga el desempeño o funcionamiento previstos.

c. Gestión de riesgos

El desarrollo y adquisición eficaces supone que toda organización identifique, priorice y gestiones los riesgos durante cada etapa del SDLC. Cuando se identifican problemas, las actividades relacionadas con el manejo de riesgos pueden planificarse y recurrirse a ellas según las necesidades planteadas durante el ciclo de vida de un proyecto para así mitigar los impactos adversos en los objetivos. Una gestión de riesgos eficaz supone una identificación temprana y decidida de tales riesgos mediante la colaboración y el involucramiento de las partes interesadas relevantes. Sobre la base de lo expuesto en el CMMI del Software Engineering Institute, las actividades de gestión de riesgos pueden dividirse en cuatro áreas clave:

- **Preparación para la gestión de riesgos.** La preparación se realiza mediante la formulación y el mantenimiento de una estrategia para la identificación, el análisis y la mitigación de riesgos. La estrategia de gestión de riesgos aborda las acciones específicas y el enfoque de la dirección utilizados para aplicar y controlar el programa de gestión de riesgos. Esto también incluye la identificación y el involucramiento de las partes interesadas relevantes en el proceso de gestión de riesgos. Las actividades asociadas con la preparación para la gestión de riesgos incluyen, por ejemplo, el desarrollo de los requisitos en materia de gestión de riesgos y una estrategia asociada a dicha gestión.
- **Identificación y análisis de riesgos.** Identificación de riesgos originados en fuentes internas y externa para luego evaluar cada riesgo identificado a fin de determinar su probabilidad y consecuencias. El análisis de riesgos incluye su evaluación, categorización y priorización, y se utiliza para determinar en qué momento se precisa una adecuada atención de la dirección. Las actividades relacionadas con la identificación y el análisis de riesgos incluyen, por ejemplo, la elaboración de una lista de los riesgos identificados y la asignación de una categoría, una prioridad y una fuente a cada riesgo.
- **Mitigación de riesgos.** La mitigación de riesgos supone el desarrollo de técnicas y métodos para evitar, reducir y controlar la probabilidad de que acaezcan determinados riesgos. Deberían desarrollarse planes de mitigación para los riesgos más importantes que un proyecto afronta. Asimismo, debería monitorearse con periodicidad el estado de cada riesgo para determinar si se han superado los umbrales establecidos y si deberían implementarse planes de mitigación de riesgos, según corresponda. Las actividades relacionadas con la mitigación de riesgos incluyen, por ejemplo, el desarrollo de planes de mitigación y de contingencia.
- **Supervisión ejecutiva.** Las actividades principales relacionadas con la supervisión ejecutiva consisten en revisiones de la situación de riesgo del proyecto, efectuadas de manera periódica, y sobre la base de acontecimientos, con los niveles directivos adecuados, para otorgar visibilidad a la potencial exposición a riesgos vinculados con el proyecto y tomar las medidas correctivas adecuadas. Remítase al Capítulo 2 para acceder a más información sobre el rol de la supervisión ejecutiva en la orientación de las actividades de TI dentro de las organizaciones.

D. Gestión y control de proyectos

La gestión de proyectos incluye las actividades de planificación y control de proyectos. La gestión de proyectos también incluye la definición de bases de referencia en términos de costos y plazos, la definición de cronogramas de proyecto, y el involucramiento de partes interesadas en actividades clave. El control de proyectos supone la supervisión y la presentación de informes de forma periódica para tomar medidas correctivas cuando el proyecto no concuerde con el plan. Por ejemplo, si el costo del proyecto se elevase substancialmente, la organización podría, luego de consultar con partes interesadas, recortar determinadas funciones para reducir costos.

Una estructura de gestión de proyectos debería exponerse en el enfoque SDLC de la organización, o en su estrategia de adquisiciones, según corresponda. En general, la estructura de gestión de un proyecto está integrada por un director de proyecto, un funcionario de control de riesgos, personal de apoyo para el aseguramiento de la calidad y gestión de la configuración, y personal del grupo de pruebas, si no formase parte del personal de aseguramiento de la calidad. El plan del proyecto sirve como base para orientar

todas las actividades. Los informes periódicos a la dirección superior mantienen a sus integrantes informados acerca del estado del proyecto y el modo en que los riesgos se están gestionando. Además, le permite considerar las compensaciones de factores entre costos, plazos y desempeño, dado que es raro que un proyecto cumpla con todos los objetivos previstos en estas áreas.

e. Diseño/Desarrollo

A partir de los requisitos definidos, el diseño debería contener una base de referencia relativa a las especificaciones de sistemas y subsistemas en las que se describa las partes del sistema, incluidos el modo en que se interconectan y la forma en que el sistema se implementará mediante el hardware, el software y las instalaciones de red escogidos. En general, el diseño también comprende especificaciones relativas a programas y bases de datos y deberá prever cualquier consideración relativa a la seguridad. Posteriormente, durante el desarrollo, las especificaciones de diseño se utilizan para dar inicio a la programación y formalización del apoyo a los procesos operativos del sistema.

A lo largo de los años, el desarrollo de aplicaciones de negocio ha tenido lugar en gran medida utilizando las etapas del SDLC. Dado que la adquisición de paquetes informáticos se ha convertido en una práctica más común, las etapas de diseño/desarrollo del ciclo de vida tradicional están siendo reemplazadas por la adquisición de estos servicios a través de una **licitación**[47]**.**

A resultas de ello, para adquirir soluciones de TI, las organizaciones recurren a una licitación (convocatoria a presentar propuestas). La licitación es el proceso que consiste en documentar los requisitos del negocio o actividad y recopilar otros materiales de referencia que asistirán al proveedor a ofrecer una solución de TI. Esto incluye la generación de un pliego de licitación y su publicación, la recepción de propuestas, y la selección entre diferentes proveedores. El proceso de selección debería ser transparente, objetivo y basarse en criterios que sean adecuados para el sistema o los servicios que se pretende adquirir. Es esencial que el equipo de proyecto dé participación en este proceso a su departamento jurídico. El equipo jurídico está al corriente de las leyes y reglamentos, y puede brindar su ayuda asegurándose de que los criterios de selección de proveedores sean justos, y que puedan sostenerse frente a un tribunal de justicia si los oferentes no seleccionados objetasen la licitación.

f. Aseguramiento de la calidad y pruebas

El aseguramiento de la calidad brinda al personal a cargo del proyecto y la dirección un panorama acerca de la calidad y funcionalidad de los productos provisorios y definitivos de la labor encomendada. Para lograrlo, el personal involucrado en la función de aseguramiento de la calidad debería establecer un marco para dicho aseguramiento, un manual del usuario del sistema bien documentado, y evaluar periódicamente los productos del trabajo encomendado para corroborar el cumplimiento de normas de calidad documentadas por la organización y si el personal ha seguido los procesos necesarios para el desarrollo de los productos. Es necesario que las organizaciones verifiquen que el producto desarrollado o adquirido cumple con los requisitos, satisface los criterios para su aceptación (por ejemplo, que contenga menos de un número determinado de errores no críticos) y haya sido sometido a pruebas (funcionales, de integración del sistema y de aceptación de los usuarios) con la participación de usuarios y partes interesadas.

El personal de aseguramiento de la calidad también debería asegurarse de que se siga la metodología de desarrollo adoptada y acordada y que se efectúe la supervisión requerida. Por ejemplo, debería asegurarse de que se realicen revisiones (formales o informales) y que se envíen los informes de situación necesarios tanto a la dirección como a las partes interesadas pertinentes. Más avanzado el proceso de aseguramiento de la calidad, el personal dedicado a esta tarea y la dirección superior deberían evaluar si el equipo de proyecto está siguiendo la política y los procedimientos establecidos internamente para las gestiones de adquisición o desarrollo. La supervisión por parte del personal superior debería ser manifiesta en las etapas clave del ciclo de adquisición o desarrollo.

[47]También conocida como etapa de selección y adquisición.

g. Gestión de la configuración

La gestión de la configuración se utiliza para asegurarse de que se mantenga la integridad de los documentos, el software y otros materiales que forman parte de sistema que se está desarrollando o adquiriendo. Se gestionan los cambios a estos materiales (también llamados resultados del trabajo) y se establecen bases de referencia (o versiones), de modo tal que la organización esté en condiciones de volver a versiones conocidas y probadas, si fuese necesario.

Las organizaciones pueden recurrir a un panel de control de configuración para asistir con las actividades de gestión de la configuración. Un panel de control de configuración es un grupo integrado por personal calificado en materia de gestión de la configuración, que participa en la aprobación o autorización de software para su instalación en el entorno de producción. Habitualmente esto tiene lugar luego de la realización de pruebas por parte de los usuarios, y de aquellas pruebas adicionales necesarias para asegurarse de que otros sistemas continúan operando como antes luego de la instalación del nuevo software o sistema (por ejemplo, pruebas de integración[48] o pruebas de regresión).[49] En el acuerdo de externalización suscrito con el desarrollador es importante incluir la integración con los sistemas existentes, así como también las pruebas de regresión. También es importante garantizar la gestión de la configuración no solo en el entorno de producción, sino también en el entorno de prueba durante el desarrollo.

III. Riesgos para la organización auditada

Cuando una organización desarrolla software internamente, afronta una serie de riesgos o desafíos para garantizar el éxito del proyecto. Algunos de estos riesgos se relacionan con las habilidades en el dominio del software, la experiencia en la realización de pruebas y gestión de proyectos, la disposición de estimaciones de costos y beneficios razonables, la posibilidad de monitorear y realizar un seguimiento de la situación del proyecto. Por ejemplo, pueden surgir problemas debido a la aplicación errónea de procesos y métodos de desarrollo ágil de software. Tales problemas pueden incluir la falta de definición de roles clave relacionados con esta modalidad de desarrollo, la priorización de requisitos del sistema, o la implementación de capacidades automatizadas.

Asimismo, la recopilación, puesta a prueba y aprobación de requisitos atinentes al software o el sistema deberían incluir a todos los usuarios (por ejemplo, tanto a los usuarios internos como a los externos), y los auditores deberían comprobar si los usuarios fueron consultados en la definición de los requisitos. Los auditores también deberían observar si el personal involucrado en el área de aseguramiento de la calidad actúa de manera independiente y objetiva en su evaluación de la calidad del sistema mientras éste se desarrolla. Como cuando se trata de adquisiciones, es necesario que la dirección se mantenga periódicamente informada acerca de la situación del proyecto, debiendo tomar medidas correctivas cuando ello sea menester.

El foco principal de los auditores al abordar una organización que se propone adquirir un sistema (o producto) es determinar si se está gestionando el proveedor y recibiendo informes periódicos de la situación, y tomándose las medidas correctivas correspondientes. Para hacer esto, es necesario que el contrato especifique hitos clave durante las etapas de desarrollo e implementación, con informes de

[48]Las pruebas de integración constituyen la etapa de pruebas del software en la que los módulos de software individuales se combinan y se prueban como grupo. Habitualmente esto tiene lugar luego de las pruebas unitarias y antes de las pruebas de validación o aceptación.

[49]Las pruebas de regresión son un tipo de prueba de software mediante las que se se verifica que el software desarrollado y probado con anterioridad todavía funciona correctamente luego de haberse modificado o conectado en interfaz con otro software. Estos cambios pueden incluir mejoras en el software, parches, y modificaciones en la configuración. Durante las pruebas de regresión, es posible que se descubran nuevos errores de software o regresiones.

revisión y situación formales que brinden al organismo de que se trate información sobre costos, plazos y desempeño. Será necesario que el auditor se asegure de que la dirección del organismo o el personal designado reciban y examinen informes de situación y actividades contratadas y tomen las medidas correctivas necesarias.

Un auditor de TI también debería comprobar si:

- se está llevando adelante una planificación adecuada del proyecto, lo que incluye estimaciones efectivas de recursos, presupuesto y tiempo;
- la decisión de desarrollar/adquirir fue adecuada;
- se lograron los objetivos y satisficieron los requisitos del sistema;
- los costos y beneficios identificados en el estudio de factibilidad están siendo medidos, analizados e informados a la dirección de forma exacta;
- se controló la desviación del alcance, y
- en cada etapa del proyecto se realizaron revisiones y análisis de riesgos periódicos.

IV. Referencias y lecturas adicionales

Chief Information Officers Council. *Resource Library: Publications, Playbooks, Guidance, and More*. https://www.cio.gov/resources/.

Defense Contract Audit Agency. *DCAA Contract Audit Manual*. https://www.dcaa.mil/Guidance/CAM-Contract-Audit-Manual/.

ISACA. *BAI01-BAI10 Manage—Audit Assurance Program*. 2014.

ISACA. *CISA Review Manual, 27th ed*. 2019.

ISACA. *COBIT 2019 Framework*: *Governance and Management Objectives*. 2019.

ISACA. *System Development and Project Management Audit Program*. 2009.

National Institute of Standards and Technology. *Special Publication 800-39: Managing Information Security Risk: Organization, Mission, and Information System View.* https://csrc.nist.gov/publications/detail/sp/800-39/final. March 2011.

Software Engineering Institute. *CMMI for Acquisition,* version 1.3. http://www.sei.cmu.edu/library/abstracts/reports/10tr032.cfm. 2010.

Software Engineering Institute. *CMMI for Development*, version 1.3. http://www.sei.cmu.edu/library/abstracts/reports/10tr033.cfm. 2010.

Tsui, Frank and Orlando Karam. *Essentials of Software Engineering,* 2nd ed. 2011.

U.S. Government Accountability Office. *Agile Assessment Guide: Best Practices for Agile Adoption and Implementation.* GAO-20-590G. https://www.gao.gov/products/gao-20-590g. September 28, 2020.

U.S. Government Accountability Office. *Census Bureau Needs to Implement Key Management Practices.* GAO-12-915. https://www.gao.gov/products/gao-12-915. September 18, 2012.

CAPÍTULO 4: OPERACIONES DE TI

I. ¿Qué son las operaciones de TI?

Aunque existen muchas interpretaciones o definiciones diferentes de lo que son las operaciones de TI, generalmente se las considera como las tareas diarias vinculadas con la operación y prestación de apoyo a la infraestructura de TI de una organización (por ejemplo, la operación de servidores, la realización de tareas de mantenimiento, el monitoreo de la seguridad, la provisión del almacenamiento necesario y la operación de una mesa de ayuda). Las operaciones se miden y gestionan utilizando **indicadores clave de desempeño** (KPI) para operaciones de TI, por los que se establecen los parámetros en función de los que ha de medirse la eficacia operativa. Estas medidas, o su equivalente, deberían monitorearse y revisarse constantemente. La mayoría de las organizaciones las documentan en un acuerdo entre los usuarios del negocio y la organización de TI. El **acuerdo de nivel de servicio** (SLA) es un acuerdo formal, en el que se documentan dichos parámetros y otras condiciones. Esta cuestión se analiza con mayor detalle a lo largo de este capítulo.

II. Elementos clave de las operaciones de TI

Los elementos de las operaciones de TI que el auditor debería revisar para determinar si la organización está gestionándolas de forma eficaz son, entre otras: la gestión de la continuidad del servicio de TI, la gestión de la seguridad de la información, la gestión de la capacidad, la gestión de la fuerza laboral, los procedimientos de gestión de incidentes y problemas para garantizar la continuidad de las operaciones, las prácticas de gestión de cambios, y la gestión de riesgos (remítase a la Figura 8). Estas y otras áreas se definen en el marco ITIL (IT Infrastructure Library),[50] que es uno de los marcos más ampliamente adoptados para identificar, planificar y prestar los servicios de TI que respaldan el negocio o actividad de la organización, y darles el apoyo correspondiente.

Para determinar si la organización auditada está prestando de forma eficaz los servicios documentados, el auditor debería evaluar si el SLA incluye los parámetros específicos para los diversos servicios. En algunas organizaciones más pequeñas, es posible que lo acordado entre la organización y el grupo de TI conste en un organigrama u otro documento. Independientemente del modo en que este documento se denomine, los parámetros para la

Figura 8: Dominios de las operaciones de TI

Fuente: Unknown

[50]Axelos, "What is ITIL?," https://www.axelos.com/best-practice-solutions/itil/what-is-itil.

prestación de servicios de TI deben documentarse y ser acordados por los grupos de usuarios y la organización de TI.

a. Gestión de la continuidad del servicio de TI

El propósito de la gestión de la continuidad es satisfacer los requisitos necesarios para la continuidad del negocio o actividad, además de reducir los costos por inactividad y los impactos en el negocio o la actividad al ocurrir desastres. La organización de TI logra esto mediante la determinación de las metas relativas al plazo de recuperación (cuánto lleva recuperarse) y el punto de recuperación (desde qué punto anterior al desastre) respecto a los diferentes componentes de TI que apoyan los procesos del negocio o la actividad con el objetivo de mantener la disponibilidad y desempeño del servicio en los niveles más elevados posibles. Además, la gestión de la continuidad incluye revisar y actualizar periódicamente los plazos y puntos de recuperación para asegurarse de que se mantengan alineados con los planes de continuidad y las prioridades del negocio o la actividad. Esta área se aborda con mayor detalle en el Capítulo 6.

b. Gestión de riesgos

La gestión de riesgos es la práctica destinada a asegurar que una organización comprenda y aborde de forma plena cualquier riesgo para la organización, incluidos aquellos relacionados con las operaciones de TI. Se define al riesgo como aquellos problemas que deberían minimizarse o mitigarse para evitar un impacto en la capacidad de la organización para brindar valor a sus partes interesadas. Los riesgos para las operaciones de TI incluyen actividades o comportamientos no autorizados en el sistema, la divulgación no autorizada de información personalmente identificable, y cambios no autorizados, entre otros. Las prácticas y procedimientos de gestión de riesgos que una organización implementa orientarán las decisiones relacionadas con el riesgo de esa organización. Como se analizó previamente, las prácticas y procedimientos para la gestión de riesgos pueden dividirse en cuatro áreas clave: (1) preparación para la gestión de riesgos, (2) identificación y análisis de riesgos, (3) mitigación de riesgos y (4) supervisión ejecutiva. Para acceder a más información acerca de cada una de las cuatro áreas clave, remítase al Capítulo 3.

c. Gestión de la seguridad de la información

La gestión de la seguridad de la información se relaciona con gestionar los riesgos asociados a la seguridad, garantizar la implementación de controles en materia de seguridad de la información, tomar las medidas adecuadas, y asegurarse de que la información se encuentre disponible, sea utilizable, sea completa y mantenga su integridad, cuando se la necesite. También se relaciona con asegurarse de que solamente los usuarios autorizados tengan acceso a la información y ella se encuentre protegida al ser transferida entre destinos y sea confiable al arribar. Esta área se aborda con mayor detalle en el Capítulo 7.

c. Gestión de la capacidad

La gestión de la capacidad incluye los diversos servicios que dan apoyo a la organización de una forma que se ajuste a las demandas de la organización o los usuarios. La optimización del rendimiento de la red, la disponibilidad de recursos, la optimización del almacenamiento y la previsión de la demanda forman parte de la gestión de la capacidad. A los efectos de gestionar la capacidad, es necesario que la organización mida las condiciones y necesidades actuales para tomar aquellas medidas que facilitan el suministro de capacidad adicional a los usuarios, lo cual puede lograrse, por ejemplo, mediante la adquisición de mayor poder de procesamiento cuando se traspasan determinados parámetros (es decir, cuando la utilización de computadoras se ubica en el 75% o es mayor al 60 por ciento de la jornada laboral).

e. Gestión de cambios

En las organizaciones de TI, el proceso de gestión de cambios normalmente se utiliza para gestionar y controlar las modificaciones a los sistemas de TI y sus componentes, como el software, el hardware y la documentación relacionada. Es preciso controlar las modificaciones para asegurarse de todos los cambios

de configuración en sistemas se encuentren autorizados, probados, documentados y controlados de manera tal que los sistemas continúen respaldando las operaciones de la organización del modo proyectado, y que exista un rastro y un registro adecuados de los cambios efectuados.[51]

Al implementar cambios, es importante que exista una segregación de los entornos de desarrollo, prueba y producción, y que no se permita el acceso al entorno de producción a las personas encargadas de desarrollar los cambios. Esto reduce el riesgo de que en el entorno de producción realicen directamente cambios no sometidos a prueba o aprobados.

Un cambio no aprobado o accidental podría acarrear riesgos graves para la continuidad del negocio o actividad, y consecuencias financieras para una organización. Las organizaciones deberían seguir un procedimiento de gestión de cambios definido que requiera la aprobación de un panel previamente a su implementación en el entorno operativo. Mediante el proceso de gestión de cambios debería garantizarse que éstos se registren, evalúen, autoricen, prioricen, planifiquen, pongan a prueba, implementen, documenten y revisen de acuerdo con los procedimientos de gestión de cambios documentados y aprobados.

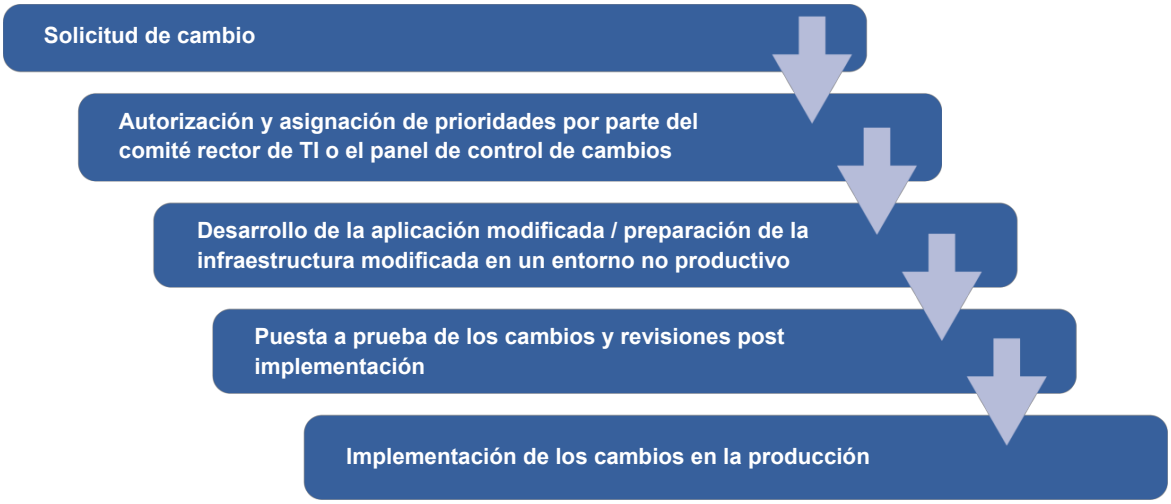
Los cambios pueden ser identificados e iniciados a raíz de, por ejemplo, una variación en el entorno del negocio o actividad, una modificación en el modelo de negocio, necesidades interconectadas, o debido al resultado de un incidente o un análisis de problemas. Los procedimientos de control de cambios deberían incluir procedimientos para:

- autorizaciones de la dirección (por ejemplo, la documentación de un proceso para registrar una solicitud de cambio),
- la realización de pruebas rigurosas y la autorización de la gerencia de operaciones previamente a su utilización en un entorno real,
- revisión por parte de la gerencia de los efectos de cualquier cambio,
- mantenimiento de registros adecuados,
- elaboración de planes de contingencia (en el caso de que algo funcione mal), y
- el establecimiento de procedimientos para cambios de emergencia.

Remítase a la Figura 9 para visualizar los pasos de un proceso de gestión de cambios.

[51]Es posible que determinados cambios en los sistemas de TI no requieran la aplicación de todos los procedimientos expuestos en esta sección. Por ejemplo, los **cambios estándar** habitualmente son nimios y conllevan un bajo riesgo para los sistemas de TI; por consiguiente, es posible que estén sujetos a un menor grado de supervisión (por ejemplo, que no precisen de la aprobación de un panel especial, requiriendo, no obstante, la realización de pruebas y el otorgamiento de aprobaciones operativas).

Figura 9: Pasos en la gestión de cambios



Fuente: Unknown

El costo de los cambios, el impacto en el sistema de TI y los objetivos del negocio o actividad, el impacto de que no se implementen, y los requisitos futuros en términos de recursos, son factores determinantes significativos en cuanto a la autorización y priorización de dichos cambios.

Los **cambios de emergencia** son modificaciones que no pueden esperar para someterse a los procedimientos de control de cambios normales y deben implementarse con una demora mínima. Existe un tiempo acotado para realizar dichos cambios y someterlos a prueba, lo que genera un mayor riesgo de que se cometan equívocos y errores de programación.

Cuando existan procedimientos para los cambios de emergencia, el auditor debería verificar que sean razonables e incluyan alguna forma de control. Esto implica la aprobación de los cambios de emergencia por parte de un integrante del personal con la autoridad adecuada, contar denominaciones y controles de versiones en conjunción con pistas de auditoría adecuados (es decir, el uso de aplicaciones de control de cambios automatizadas), aprobaciones retrospectivas del panel de cambios o el propietario del sistema, la realización de pruebas retrospectivas, y la actualización de documentación.

f. Gestión de la fuerza laboral

La gestión de la fuerza laboral tiene por finalidad asegurarse de que la organización disponga de las personas idóneas, dotadas de las habilidades y los conocimientos adecuados, en los roles correctos para respaldar la organización. Cuando se trata de una organización de TI que presta servicios para el desarrollo de un negocio o actividad, la gestión de la fuerza laboral es eficaz cuando se asigna personal de dicha organización debidamente cualificado y capacitado, se utilizan recursos suficientes y herramientas adecuadas para manejar el monitoreo de la red y las funciones de mesa de ayuda, y el personal asignado se compromete de forma proactiva con la resolución de cuellos de botella mientas conserva su capacidad de respuesta a las necesidades del negocio o actividad de la organización. Como se analiza en el Capítulo 2, las organizaciones deberían evaluar regularmente las necesidades de su fuerza laboral (por ejemplo, aquellas relacionadas con las competencias y dotación de personal), detectar deficiencias, y desarrollar estrategias y planes para subsanar tales deficiencias, entre otras actividades clave.

g. Gestión de incidentes y problemas

La gestión de incidentes abarca los sistemas y prácticas que se utilizan para determinar si los incidentes o errores se registran, analizan y resuelven de forma oportuna. El propósito de la gestión de problemas es resolver determinadas cuestiones mediante la investigación y el análisis en profundidad de incidentes

importantes o recurrentes a los efectos de identificar su causa fundamental. Una vez que un problema se ha identificado y se ha realizado un análisis de su causa fundamental, dicho problema se convierte en un error o ineficiencia conocidos, y puede idearse una solución para abordarlo y evitar futuros incidentes relacionados.

Debería instrumentarse un proceso formal para la documentación de condiciones que pueden conducir a la detección e identificación de un incidente. La sección relativa a las operaciones de TI del SLA debería contener procedimientos documentados para la detección y registro de condiciones anómalas. Para facilitar los análisis de estas condiciones anómalas, las organizaciones a menudo conservan registros de todos los incidentes. Para tener constancia de dichas condiciones, puede utilizarse un registro manual o automatizado dedicado a los servicios de TI. Algunos ejemplos de incidentes son el acceso o intrusión no autorizados por parte de usuarios (seguridad), fallas en las redes (operativos), baja funcionalidad del software (prestación del servicio), o falta de habilidades de los usuarios (capacitación).

En la auditoría de la gestión de incidentes y problemas, el auditor debería examinar los informes sobre ellos, así como también los registros correspondientes, para asegurarse de que se les dé una solución oportuna, y se asignen a las personas o grupos más capacitados para ellos. En algunos casos, puede recurrirse a planes de recuperación de desastres para resolver un incidente. Remítase al Capítulo 6 para acceder a más información sobre los planes de recuperación de desastre y al Capítulo 7 para la gestión de incidentes relacionados con la seguridad de la información.

h. Gestión del nivel de servicio

Como se mencionó previamente, los documentos del SLA contienen diversos parámetros que la organización de TI utiliza para brindar servicios al negocio o actividad. Los parámetros del SLA en general son acordados por los propietarios del negocio o actividad y la organización de TI. El auditor utilizará los parámetros del SLA para corroborar si la organización de TI cumple con los niveles de servicio y si los propietarios del negocio o actividad se encuentran satisfechos y están tomando las medidas adecuadas en el caso de registrarse desviaciones respecto de los parámetros del nivel de servicio acordados. Estos parámetros incluyen medidas cuantificables, como la disponibilidad, utilización o número de errores. En general, también existe un SLA u otro convenio formal entre una organización de TI y sus proveedores. Por ejemplo, es posible que una organización de TI tenga múltiples SLA con los diversos proveedores que brindan servicios externalizados o de computación en la nube.

Es posible que algunas organizaciones también tengan un acuerdo entre la organización de TI y los clientes del negocio o actividad dentro de la organización. A este instrumento se lo conoce como Acuerdo de Nivel Operativo (OLA). El contenido de los OLA es similar al de los SLA descritos previamente, pero aquéllos constituyen convenios internos que un prestador de servicios define para describir el modo en que se dará cumplimiento a los SLA. Un OLA podría contener información tal como el tiempo de respuesta para el abordaje de incidentes o la disponibilidad de servidores. En general, los OLA se utilizan para reflejar las relaciones internas entre un proveedor de servicios de TI y otra parte de la organización.

Un SLA y un OLA contienen, entre otros elementos, los KPI correspondientes a los servicios de TI. La revisión de los KPI le ayudará al auditor a formular preguntas conducentes a determinar

- si los sistemas se están operando según los acuerdos documentados;
- si se dispone de mecanismos para detectar deficiencias en el desempeño o la seguridad, abordar las deficiencias identificadas, y realizar un seguimiento de la implementación de las medidas correctivas tomadas a raíz de la evaluación del desempeño de la organización; y
- detectar cuestiones vinculadas con el control de la organización sujeta a auditoría, para, de ese modo, determinar la naturaleza, oportunidad y alcance de las pruebas.

Por ejemplo, a continuación, se enumeran medidas concernientes a los KPI y las correspondientes definiciones y objetivos para la gestión de cambios:

Proceso	Objetivo (Factor crítico para el éxito)	Indicador Clave de Desempeño (KPI)	Arquitectura de medición
Gestión de cambios	Reducir incidentes provocados por cambios no previstos	Reducción porcentual en el número de incidentes derivados de accesos no autorizados	Seguido a través de la gestión de incidentes, la gestión de cambios, e informado mensualmente

En aquellos casos en los que los KPI no constituyan un medio para que una organización evalúe eficazmente el logro de progresos y la consecución de objetivos, es posible que el auditor desee realizar una evaluación adicional de los KPI. Al evaluar los KPI, un auditor debería determinar si contienen atributos importantes que ayudarán a proporcionarle eficacia en el monitoreo del progreso realizado y la determinación de cuán bien una organización o un proveedor están logrando sus objetivos. A continuación, se presentan algunos ejemplos de estos atributos:

- **Claridad**. La medida se expresa con claridad, y la denominación y definición son congruentes con la metodología utilizada para calcularla.
- **Meta cuantificable**. La medida posee un objetivo numérico; esa medida es cuantificable o posee metas cuantificables, o existen otras medidas que permiten comparar el desempeño esperado con los resultados reales.
- **Objetividad.** La medida se encuentra razonablemente libre de manipulaciones o sesgos significativos que distorsionarían la evaluación precisa del desempeño.
- **Confiabilidad**. La medida produce el mismo resultado bajo condiciones similares.
- **Datos de referencia y tendencia**. A la medida se le asocian datos de referencia y tendencia para identificar, monitorear e informar cambios en el desempeño y ayudar a garantizar que éste se observe en contexto.
- **Vinculación**. La medida es concordante con los objetivos y misiones tanto a nivel de división como de la organización en su conjunto, y se comunica claramente a todos los sectores de la organización.[52]

En algunos casos, la organización de TI externaliza el grueso de sus funciones, designado para ello a un proveedor. En dicha situación, la organización de TI constituye un nexo entre el proveedor y los usuarios, y es responsable por la gestión aquél, de modo tal que debe garantizar que las necesidades del negocio o la actividad se vean satisfechas. Remítase al Capítulo 5 para acceder a información sobre la externalización.

i. Gestión de activos

La gestión de activos es el proceso que consiste en identificar y crear un inventario de activos, de un valor tangible o intangible, que es conveniente proteger, y que incluye a personas, información, infraestructura, finanzas y reputación. Por ejemplo, un activo no puede protegerse o gestionarse de manera eficaz si no se encuentra identificado. Además, la gestión de activos permite que una organización se asegure de que sus activos se mantengan, actualicen, y se eliminen adecuadamente. Antes, los activos eran más sencillos de controlar, dado que a menudo se gestionaban dentro del dominio de la organización, pero hoy en día las organizaciones externalizan servicios y activos. Algunos beneficios de la gestión de activos incluyen la mejora en su utilización, la eliminación del derroche, la facilitación de la productividad y el apoyo a la gestión de la continuidad del negocio o actividad.

j. Gestión de datos

[52]Para más información sobre los atributos clave de los KPI, remítase al siguiente documento publicado por la Oficina de Rendición de Cuentas del Gobierno de los Estados Unidos: *Defense Logistics: Improved Performance Measures and Information Needed for Assessing Asset Visibility Initiatives*, GAO-17-183, (Mar. 16, 2017), https://www.gao.gov/products/gao-17-183.

La gestión de datos es la práctica que consiste en gestionar y proteger los datos en su carácter de recurso valioso para una organización. La gestión de datos supone que una organización recopile, almacene y proteja sus datos, además de acceder a ellos, integrarlos y depurarlos para su análisis. Las organizaciones recopilan datos de muchas fuentes, como los sistemas transaccionales, escáneres, sensores, redes sociales y dispositivos inteligentes, entre otros. La organización puede utilizar los datos recopilados para tomar decisiones y generar valor. La gestión de datos incluye las siguientes actividades, entre otras:

- crear y acceder a datos, y actualizarlos
- almacenar datos en múltiples instalaciones y nubes
- garantizar una alta disponibilidad y la recuperación de desastres
- utilizar datos para brindar apoyo a aplicaciones, análisis y algoritmos
- garantizar la privacidad y seguridad de los datos
- disponer de los datos de acuerdo con las leyes y reglamentos aplicables

Las organizaciones utilizan los sistemas de gestión de datos para gestionar aquellos datos que son necesarios para brindar apoyo a los mecanismos de análisis y algoritmos de la organización. Aunque las organizaciones deberían tener herramientas automatizadas que ayuden a gestionar estos sistemas, será necesaria la presencia de administradores de bases de datos que intervengan de forma manual.

Para gestionar mejor los datos de una organización, ésta podría implementar prácticas de gobernanza de datos. La gobernanza de datos es un marco para gestionar los datos de una organización. Es necesario que las organizaciones definan políticas y procedimientos relativos al modo en que administrarán los datos durante la totalidad del ciclo de vida de esos datos. La gobernanza de datos ayudará a las organizaciones a proteger sus datos mediante la documentación de los activos de datos y los controles de acceso pertinentes, la definición de la propiedad de los datos y las responsabilidades correspondientes, y la formulación de políticas de distribución tanto interna como externamente. Otras funciones de la gestión de datos son:

- **La gestión de la arquitectura de datos**, que define las necesidades en materia de datos de la organización.
- **El desarrollo de datos**, que consiste en el diseño, la implementación y el mantenimiento de soluciones para satisfacer las necesidades en materia de datos de la organización.
- **La gestión de las operaciones con datos**, que consiste en la planificación, el control y la prestación de apoyo para la utilización de datos estructurados durante la totalidad de su ciclo de vida.
- **La gestión de la seguridad de los datos**, que consiste en la implementación de políticas y procedimientos de seguridad concebidos para garantizar la confidencialidad, integridad y disponibilidad de los datos.
- **La gestión del almacenamiento de datos e inteligencia del negocio o actividad**, que se ocupa de los procesos para tomar decisiones que respalden la presentación de informes, la realización de consultas y el análisis de datos.

III. Riesgos para la organización auditada

Como se señaló previamente, las principales herramientas para el auditor son el SLA y el OLA. En estos acuerdos se consignan los parámetros, indicadores de desempeño y requisitos en función de los cuales la organización de TI ha de medirse. Si estos documentos faltasen o no hubiesen sido formalmente revisados y aprobados por los propietarios del negocio (proceso), es posible que los recursos de TI de la organización corran el riesgo de no utilizarse de manera eficaz o eficiente. Luego de obtener el SLA o el OLA, será necesario que el auditor reciba de la organización de TI informes periódicos en los que se mida e informe acerca del estado de los indicadores, además de la revisión realizada por la organización de ellos, y cualesquiera medidas, elementos o indicaciones comunicados a la organización de TI cuando se registren desviaciones significativas de los parámetros acordados.

En el área de la gestión de cambios, el auditor debería corroborar si existen procedimientos de control de cambios para garantizar la integridad del sistema y asegurarse de que en el entorno operativa solo se introduzcan aplicaciones aprobadas, que se hayan sometido a pruebas.

El auditor también debería ocuparse de observar el modo en que el organismo está gestionando la capacidad (por ejemplo, en lo relativo al almacenamiento, CPU, y recursos de red) de un modo proactivo, para estar en condiciones de responder a los usuarios y gestionar incidentes y otras cuestiones de seguridad, de modo tal que no se pongan en riesgo funciones del negocio o actividad.

IV. Referencias y lecturas adicionales

Atlassian. *What Is IT Asset Management (ITAM)?* https://www.atlassian.com/itsm/it-asset-management. 2022.

Axelos. *What is ITIL?* https://www.axelos.com/best-practice-solutions/itil/what-is-itil.

Axelos. *ITIL Foundation: ITIL 4 Edition (ITIL 4 Foundation)*. Norwich: TSO, 2019.

Cichonski, Paul, Thomas Millar, Tim Grance, and Karen Scarone. *NIST Special Publication 800-61, rev. 2: Computer Security Incident Handling Guide*. https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final. 2012.

CISA. *Item Development Guide.* https://www.isaca.org/-/media/files/isacadp/project/isaca/certification/cisa/cisa-item-development-guide_bro_eng_0219.pdf. October 2018.

Cisco. *Service Level Management: Best Practices White Paper.* https://www.cisco.com/c/en/us/support/docs/availability/high-availability/15117-sla.html. October 4, 2005.

DAMA International. *Data Management Body of Knowledge,* 1st ed. https://www.dama.org/cpages/body-of-knowledge. 2010.

ISACA. *Change Management Audit Programme.*

ISACA. CISA Review Manual. 27th ed. https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KokCEAS. ISACA, 2011.

ISACA. *COBIT 2019 Framework*: *Governance and Management Objectives*. 2019.

Knight, Michelle. *What is Data Governance?* https://www.dataversity.net/what-is-data-governance/. December 18, 2017.

Oracle. *What Is Data Management?* https://www.oracle.com/database/what-is-data-management/.

Profisee. *Data Governance—What, Why, How, Who & 15 Best Practices.* https://profisee.com/data-governance-what-why-how-who/.

SAS. *Data Management: What It Is and Why It Matters.* https://www.sas.com/en_us/insights/data-management/data-management.html.

U.S. Government Accountability Office. *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities.* GAO-20-129. https://www.gao.gov/products/gao-20-129. October 30, 2019.

U.S. Government Accountability Office. *Defense Logistics: Improved Performance Measures and Information Needed for Assessing Asset Visibility Initiatives*. GAO-17-183. https://www.gao.gov/products/gao-17-183. March 16, 2017.

CAPÍTULO 5: EXTERNALIZACIÓN

I. ¿Qué es la externalización?

La externalización es un proceso que consiste en contratar la realización de una función o la prestación de un servicio propios del negocio o actividad que anteriormente se realizaban internamente, o de una nueva función o servicio, con una entidad externa. La entidad contratada es responsable de brindar los servicios contractualmente estipulados cambio de una contraprestación acordada. Una organización puede optar por externalizar algunas (o la totalidad de las) partes de su infraestructura, servicios o procesos de TI. La organización debería tener una política o visión respecto a las funciones de su negocio o actividad (típicamente las de TI, pero podrían ser otras) que externalizará, así como también de aquellas que continuará realizando internamente.

A. Ventajas de la externalización

La externalización ofrece algunas ventajas, entre ellas:

i. Flexibilidad en términos de dotación de personal

Si un proyecto requiriese habilidades de las que una organización actualmente carece, es posible que esa organización decida externalizar el proyecto en lugar de capacitar a su personal interno, para, de ese modo, ahorrar tiempo y costos de capacitación. Además, la externalización permitirá que, para aquellas operaciones cuya demanda es estacional o cíclica, se incorporen recursos adicionales cuando una organización los precisa, y los libere una vez finalizadas las operaciones estacionales. Esto puede ser especialmente beneficioso cuando se trata de mercados volátiles, en los que la flexibilidad y escalabilidad de la dotación de personal conllevaría una reducción de los riesgos.

ii. Reducción de costos

La externalización habitualmente deriva en una reducción de costos al desplazar los costos de índole laboral, entre otros, hacia un proveedor cuyos costos laborales son inferiores. Las organizaciones de TI procuran externalizar tareas cuya realización interna sería más onerosa. Por ejemplo, una tarea relacionada con componentes de software que requiera habilidades especializadas. Aquellas organizaciones que no dispongan de empleados aptos para completar esta tarea pueden obtener beneficios financieros de su externalización. La externalización de tareas no básicas también ayuda a la organización a enfocarse en su negocio o actividad central y producir resultados de forma eficiente.

iii. Expertos a disposición

La externalización permite a la organización contar con expertos a disposición, esperando para brindar su asistencia ante cuestiones actuales o emergentes. La organización está en condiciones de responder con rapidez a necesidades cambiantes relacionadas con el negocio o actividad (por ejemplo, nuevas misiones o la asunción de nuevas funciones) con la ayuda del experto. Además, los expertos pueden asistir al personal interno que trabaja junto con el proveedor mediante la provisión de capacitación práctica y la transferencia de conocimientos.

iv. Mitigación de riesgos

Especialmente cuando se trata de mercados volátiles, es posible que las organizaciones procuren mitigar sus riesgos mediante el aumento de sus niveles de externalización. Por ejemplo, pueden reducir su recursos y personal de TI internos y externalizar estas funciones para permitir una mayor flexibilidad y escalabilidad en entornos permanentemente cambiantes. Es posible que las organizaciones de TI decidan

externalizar la totalidad o parte de sus operaciones y, en función de la criticidad del servicio externalizado, una organización puede decidir aumentar o disminuir los controles formales sobre ese servicio. Es esencial recordar que la organización conserva la responsabilidad final por la prestación de tales servicios o la realización de dichas funciones, dado que lo que ha transferido es la función, no la responsabilidad.

b. Ejemplos de externalización

Según ISACA,[53] las organizaciones pueden externalizar diversas áreas del negocio o actividad y su infraestructura de TI. Por ejemplo:

- Infraestructura operativa, como centros de datos y procesos relacionados
- Procesamiento de aplicaciones internas por un proveedor de servicios
- Desarrollo de sistemas o mantenimiento de aplicaciones
- Instalación, mantenimiento y gestión de equipos de computación de escritorio y redes relacionadas

Uno de los servicios de TI más comúnmente externalizados hoy en día es el de la **computación en la nube**. La computación en la nube es un modelo que permite el acceso a petición a un conjunto de recursos informáticos configurables conectados en red (por ejemplo, aplicaciones, redes, servidores, almacenamiento y otros servicios). Entre otros beneficios, la computación en la nube permite a las organizaciones acceder a recursos informáticos basados en un sistema de pago por utilización, y brindan flexibilidad en cuanto a la posibilidad de expandir rápidamente una solución de TI.

A modo de ejemplo, una organización puede externalizar el procesamiento de datos u otros servicios a recursos informáticos de propiedad de un proveedor. El proveedor habitualmente tiene el control físico de los equipos, mientras que la organización conserva el control sobre las aplicaciones y datos. La computación en la nube también incluye la utilización de las computadoras del proveedor para almacenar, realizar copias de respaldo y brindar acceso en línea a los datos de la organización. Si la organización pretende que su personal o usuarios tengan un acceso inmediato a los datos, o incluso a la aplicación que los procesa, será necesario que disponga de un buen acceso a Internet. En el entorno actual, los datos o aplicaciones también se encuentran disponibles desde plataformas móviles (por ejemplo, laptops con conexiones inalámbricas a Internet o celulares/tarjetas móviles, teléfonos inteligentes y tablets).

A menudo, la computación en la nube se categoriza en tres modelos de servicios separados:

- **El software como servicio** – La organización utiliza una aplicación y una infraestructura suministradas por el proveedor.
- **La plataforma como servicio** – La organización utiliza la infraestructura en la nube suministrada por el proveedor para operar aplicaciones cuyo propietario es propio proveedor.
- **La infraestructura como servicio** – La organización externaliza de un proveedor diversos recursos informáticos, por ejemplo, procesamiento, almacenamiento y redes. La organización no gestiona la infraestructura, pero controla la infraestructura, las aplicaciones y los sistemas operativos utilizados.

Además de los diferentes modelos de servicios, existen cuatro modelos separados de instrumentación:

- **Nube privada** – La infraestructura se provee para uso exclusivo de una única organización.
- **Nube comunitaria** – La infraestructura en la nube se provee para una comunidad de consumidores, que a menudo comparten determinadas consideraciones, como una misión, seguridad, y cumplimiento normativo.
- **Nube pública** – La infraestructura se suministra para su utilización abierta por el público en general, y típicamente es operada por una organización empresarial, académica o gubernamental.
- **Nube híbrida** – La infraestructura es una combinación de dos o más de las infraestructuras previamente señaladas, que son interoperables para permitir la portabilidad de datos y aplicaciones.

[53]Outsourced IT Environments Audit /Assurance Programme (2009).

Una adecuada configuración de la nube permite reducir el riesgo de que se presenten problemas de seguridad, y la aplicación de controles de seguridad adicionales permite generar un entorno defendible en dicho medio. Además, los contratos de computación en la nube deberían incluir una cláusula relacionada la prohibición de divulgar información sensible. Asimismo, es necesario que en ellos se defina aquello que constituye una infracción a la seguridad, y se describa el modo en que el proveedor notificará a la organización en el caso de que se produzca tal infracción.

En síntesis, la computación en la nube puede brindar beneficios a una organización, entre ellos, la limitación de costos, el acceso inmediato a recursos, una flexibilidad y escalabilidad dinámicas, y soluciones de respaldo que permitan limitar los tiempos de inactividad. Sin embargo, como suele suceder con todas las instancias de externalización, la computación en la nube presenta riesgos y desafíos vinculados con su implementación. Por ejemplo, la computación en la nube puede generar riesgos adicionales, como los errores de configuración, equívocos vinculados con responsabilidades compartidas, deficiencias en los controles de acceso, el hecho de compartir recursos con otros arrendatarios del proveedor de servicios en la nube, y vulnerabilidades en la cadena de suministro. El modelo de costos flexible que la nube ofrece también puede tornarse muy oneroso si la organización no monitorea y controla su uso.

II. Elementos clave de la externalización

a. Política de externalización

Es necesario que las organizaciones tengan una política que defina qué funciones pueden externalizarse y cuáles de ellas se mantienen en el ámbito interno.[54] Las organizaciones habitualmente externalizan operaciones rutinarias de TI, tareas de mantenimiento, y plataformas de hardware de escritorio. Los registros de recursos humanos y personal son por lo general funciones internas, puesto que precisan de un monitoreo minucioso y se encuentran sujetos a numerosos requisitos en materia de privacidad, dado lo cual, es posible que su externalización les reste eficacia en función de los costos.

Un auditor debería comenzar por examinar la política y procedimientos de externalización de una organización. Es esencial que las organizaciones más grandes, cuyas operaciones de negocios o propias de su actividad a menudo se externalizan en una proporción mayor, tengan una política de externalización aprobada que defina con claridad los procesos asociados a la externalización. Las organizaciones más pequeñas tal vez carezcan de una política formal, pero deberían seguir procedimientos de licitación eficientes y transparentes. Independientemente de su tamaño, las organizaciones deben tener una estrategia de gobernanza clara a los efectos de establecer la dirección y los objetivos vinculados con la externalización.

b. Licitación

La licitación es el proceso que consiste en documentar los requisitos del sistema e incorporar otros materiales de referencia que asistirán al proveedor a construirlo. Esto incluye la generación de un pliego de licitación y su publicación, la recepción de propuestas u ofertas, y la realización de una selección entre los diferentes proveedores potenciales. El proceso de selección debería ser transparente y objetivo y basarse en criterios que sean adecuados para el sistema o los servicios que se pretende adquirir. Antes de tomar la decisión definitiva, la organización debería examinar detenidamente al potencial proveedor para detectar posibles problemas o impedimentos para la prestación del servicio.

c. Gestión de proveedores

[54]International Organization for Standardization/International Electrotechnical Commission, *Information Technology—Cloud Computing—Guidance for Policy Development* (Geneva, Switzerland: International Organization for Standarization, January 2019).

La gestión de proveedores es un elemento clave de la externalización para garantizar que los servicios se presten de acuerdo con las expectativas de la organización. Ésta debería disponer de procesos para garantizar un seguimiento periódico de la situación del proyecto, la calidad del servicio, y la puesta a prueba de los productos generados, antes de su incorporación al entorno operativo. Asimismo, como parte del proceso de monitoreo del proveedor, la organización también puede auditar el proceso interno de aseguramiento de la calidad de dicho proveedor, de forma tal de cerciorarse de que su personal cumple con las políticas y planes contractualmente aprobados al realizar todas sus tareas.

Un componente importante de la gestión de proveedores es el SLA. Como se mencionase anteriormente, el SLA es un acuerdo documentado entre la organización y el proveedor, y una herramienta esencial para la gestión de los proveedores. En el SLA deberían definirse los servicios que se espera que el proveedor brinde, además de los parámetros técnicos correspondientes a esos servicios, dado que se trata de un contrato jurídicamente vinculante entre el proveedor y la organización.

Desde una perspectiva centrada en la gestión de los proveedores, las áreas habitualmente comprendidas por un SLA son:

- los tipos de servicios que el proveedor brindará;
- la distribución de responsabilidades entre la organización y el proveedor;
- los servicios que se medirán, el período de medición, la duración, la ubicación, y los plazos para la presentación de informes (por ejemplo, aquellos vinculados con tasas de defectos, tiempos de respuesta, y horarios de atención del personal a cargo de la mesa de ayuda);
- plazo para implementar la nueva funcionalidad y niveles de reelaboración;
- nivel de derechos de acceso otorgados al proveedor para que preste sus servicios;
- tipo de documentación requerida para las aplicaciones desarrolladas por el proveedor;
- ubicación en la que los servicios deben prestarse;
- frecuencia de copias de respaldo y parámetros de recuperación de datos;
- conclusión, y métodos y formatos de entrega de datos;
- proceso regular de presentación de información e intercambio de información sobre incidentes o problemas; y
- cláusulas de incentivos y penalidades.

Respecto a los SLA relativos a servicios de computación en la nube, una organización puede incorporar a los contratos una serie de prácticas, de modo tal de garantizar que tales servicios se presten de manera eficaz, eficiente y segura.[55] Por ejemplo:

- la definición de medidas de desempeño tales como, nivel de servicio (por ejemplo, duración), nivel de capacidad (por ejemplo, número máximo de usuarios), y tiempo de respuesta (por ejemplo, con qué rapidez se procesa una transacción);
- especificar de qué modo y en qué momento la organización tiene acceso a sus propios datos y redes alojados por el proveedor, especialmente al concluir el contrato;
- especificar el modo en que el proveedor de servicios en la nube monitoreará el desempeño y cuándo la organización lo revisará;
- especificar los parámetros de seguridad, por ejemplo, quién tiene acceso a los datos y protecciones que los rodean; y
- especificar la notificación que se cursará ante un incumplimiento contractual.

[55]International Organization for Standardization/International Electrotechnical Commission, *ISO/IEC 19086-1, Information technology—Cloud Computing—Service Level Agreement (SLA) Framework—Part 1: Overview and Concepts* (Sept. 15, 2016), https://www.iso.org/standard/67545.html and U.S. Government Accountability Office, *Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance,* GAO-16-325, (Apr. 7, 2016), https://www.gao.gov/products/GAO-16-325.

En síntesis, el SLA debe contener la mayoría de los rubros que son críticos para la organización. Es necesario que el auditor de TI solicite el SLA u otro documento (contrato o acuerdo formal) donde estos parámetros se encuentren documentados. Será necesario que el auditor observe si la organización ha determinado sus requisitos relativos a la función externalizada antes de seleccionar el proveedor (por ejemplo, si los requisitos y parámetros operativos específicos se encuentran enunciados en el contrato y en el SLA), si la organización verifica que el proveedor cumple con los requisitos establecidos en el SLA (mediante informes de situación periódicos), y si la organización ha tomado medidas cuando el proveedor no ha cumplido con parámetros estipulados en el SLA (por ejemplo, medidas correctivas o el pago de penalidades).

d. Análisis de costo-beneficio

Uno de los motivos por los que las organizaciones recurren a la externalización es el ahorro de costos. Estos ahorros pueden lograrse cuando el costo de obtener determinados servicios es menor cuando se recurre a un proveedor externo que al utilizar mano de obra o infraestructura internas. Existen otros beneficios que no son directamente mensurables, por ejemplo, el aprovechamiento de la infraestructura del proveedor para ampliar rápidamente el nivel de servicio o utilizar su experiencia para casos especiales. Toda vez que ello sea posible, la organización debería tratar de determinar periódicamente si se logran los ahorros proyectados. Esta determinación es uno de los datos necesarios para decidir si se seguirá externalizando la capacidad en cuestión, o dicha externalización cesará.

e. Seguridad

Al recurrir a la externalización, las organizaciones de TI deben evaluar si los proveedores disponen de prácticas de seguridad lo suficientemente sólidas, y si están en condiciones de satisfacer los requisitos en materia de seguridad interna. Aunque la mayoría de las organizaciones de TI consideran que las prácticas de seguridad de los proveedores son substanciales (y a menudo superan las prácticas internas), el riesgo de que se produzcan infracciones a la seguridad o violaciones a derechos de propiedad intelectual se incrementa intrínsecamente cuando se externalizan datos. También es necesario abordar las preocupaciones relacionadas con la privacidad. Otras preocupaciones relacionadas con la seguridad incluyen el posible mal manejo o la divulgación de datos sensibles, y el acceso no autorizado a datos, aplicaciones y planes de recuperación de desastres. Aunque estas cuestiones rara vez constituyen impedimentos importantes para la externalización, los requisitos deben documentarse.

La utilización de la computación en la nube también conlleva una mayor necesidad de recurrir a prácticas de seguridad sólidas, debido a las características de esta modalidad. En este sentido, algunas de las inquietudes vinculadas con la seguridad son la dependencia de terceros, la mayor complejidad asociada al cumplimiento de leyes y reglamentos (en algunos casos, en una multiplicidad de países), la dependencia de Internet como el canal principal circulación de datos, y el carácter dinámico de la computación en la nube (por ejemplo, la multiplicidad de lugares de procesamiento). Más adelante en este Capítulo se brinda información sobre estas cuestiones y los riesgos relacionados.

Algunos proveedores u organizaciones de servicios se auditan de forma independiente debido a su tamaño y al número de organizaciones vinculadas contractualmente con ellos. Para este tipo de proveedores u organizaciones se elabora un informe de control de la organización de servicios, en el que se enumeran los controles de seguridad de la información y su eficacia. Dichos informes incluyen una evaluación independiente de los controles del proveedor u organización de servicios, que pueden incluir tanto controles internos como controles relacionados con la seguridad, disponibilidad, integridad y confidencialidad. El auditor puede solicitar este informe a través de la organización.

III. Riesgos para la organización auditada

a. Conservación de los conocimientos y la propiedad de los procesos del negocio o actividad

Existe un riesgo inherente vinculado con la pérdida de conocimientos relativos al negocio o actividad, propio de los desarrolladores de aplicaciones. Si el proveedor no estuviese en condiciones de brindar el servicio, las organizaciones de TI deben estar listas para reanudar su prestación. Asimismo, cuando el desarrollo de la aplicación tiene lugar fuera de la organización, ella también corre el riesgo perder la propiedad de los procesos del negocio o actividad desarrollados, en tanto el proveedor del servicio puede reivindicar como suyos los derechos de propiedad intelectual sobre tales procesos. Es necesario que las organizaciones aborden esta cuestión al momento contratar, y se aseguren de disponer de documentación completa acerca del proceso de desarrollo del sistema, además de los diseños de ese sistema. Es esencial que el pliego de licitación enviado al proveedor sea concordante con la planificación estratégica de la organización, contenga definiciones claras y sea detallado, a los efectos de evitar dudas, inexactitudes o ambigüedades en cuanto a los requisitos establecidos. Esto también ayudará a la organización a cambiar de proveedores de servicios, si ello fuese necesario.

b. Incumplimiento del proveedor

Es posible que un proveedor incurra en incumplimiento, ya sea por la entrega de un producto fuera de plazo, o porque dicho producto debe abandonarse debido a que su funcionalidad no es la correcta. Si el proceso de externalización no se implementase correctamente, existe una alta probabilidad de que el sistema o los servicios que se están adquiriendo no satisfagan las necesidades de los usuarios, no alcancen el estándar, sean más caros, precisen de recursos significativos para su mantenimiento u operación, o que su calidad sea tan baja que deban ser reemplazados en el futuro cercano. La deficiencia de los contratos, la existencia de un sistema de selección de proveedores defectuoso, hitos poco claros, y condiciones de mercado desfavorables, son algunas de las razones más comunes de incumplimientos por parte de proveedores.

Es necesario que las organizaciones de TI tengan planes de contingencia para afrontar tales circunstancias. Al considerar la externalización, las organizaciones de TI deberían evaluar las consecuencias de dichos incumplimientos (por ejemplo: ¿el incumplimiento, tiene consecuencias significativas para el desempeño del negocio?). La disponibilidad de documentación detallada sobre el diseño y el desarrollo de sistemas ayudará a la organización a garantizar la continuidad del negocio o actividad a través de otro proveedor de servicios o de sí misma.

c. Falta de personal idóneo para gestionar los contratos de externalización en la organización

La organización debe preparar y mantener personal idóneo en condiciones de llevar a cabo la correcta gestión de los contratos de externalización. Si no se dispusiese de dicho personal durante la totalidad de la ejecución del contrato de que se trate, podría suceder que se realicen sobrepagos al proveedor, o que no se obtengan los resultados esperados, o bien que la externalización no cumpla su cometido en modo alguno. Además, es en el mejor interés de la organización crear un entorno competitivo para contratos en los que los proveedores se evalúen y sus prestaciones se maximicen constantemente. Sin una supervisión adecuada, las organizaciones no estarán en condiciones de maximizar la flexibilidad y el control de sus servicios de TI.

d. Estimaciones inexactas de costos y plazos

Todos los contratos de externalización contienen bases de referencia y supuestos. Si el trabajo real variase respecto a las estimaciones, será el cliente quien deba pagar la diferencia. Esto se ha convertido en un obstáculo substancial para organizaciones de TI sorprendidas por el hecho de que el precio no se “fijó” (por ejemplo, cuando se trata de recursos de computación en la nube), o cuando el proveedor espera ser remunerado por variaciones incrementales en el alcance. Asimismo, a menudo, las organizaciones plantean hipótesis relacionadas con su negocio o actividad que son demasiado optimistas o poco realistas, que pueden derivar en desviaciones significativas respecto al alcance durante la integración de los servicios externalizados.

e. Rotación de personal clave

El rápido crecimiento registrado entre los proveedores externalizados ha dado lugar a un mercado laboral dinámico. Por lo general, existe una gran demanda de personal clave para proyectos nuevos, de alto perfil, incluso corriéndose el riego de que ese personal sea contratado por otros proveedores extraterritoriales. Aunque los proveedores extraterritoriales a menudo citan estadísticas de rotación que parecen relativamente bajas, la estadística más importante a considerar es la rotación de personal clave a cargo de una cuenta. Los niveles de rotación comúnmente se ubican en el orden del 15 al 20 por ciento, y el establecimiento de estipulaciones contractuales en torno a estos niveles constituye un requerimiento razonable.

f. Riesgos externos

La contratación de prestadores de servicios en el exterior es una forma común de externalización, especialmente en un entorno de computación en la nube. En este escenario, los riesgos relativos a tal modalidad comprenden, entre otros, la existencia de normas extranjeras en materia de almacenamiento y transferencia de información que tal vez limiten lo que puede almacenarse, y su modo de procesamiento; que los datos sean utilizados por organismos de seguridad de un país extranjero sin el conocimiento de la organización; que las normas sobre privacidad y seguridad no sean adecuadas; y que no puedan evitarse totalmente controversias relativas a las diferentes jurisdicciones aplicables.

g. Seguridad de la información

La externalización acarrea una diversidad de riesgos para la seguridad de la información, como el mal manejo o la divulgación indebida de datos sensibles, o el acceso no autorizado a los datos, como se mencionó previamente. Asimismo, el impacto en el negocio o actividad y los riesgos asociados con el uso de servicios de computación en la nube incluyen las siguientes áreas y procesos:

- una mayor dependencia de terceros, que puede derivar en un aumento de los riesgos debido a
  - vulnerabilidades en las interfaces externas,
  - agregación de centros de datos,
  - dependencia de procesos de aseguramiento de la independencia y
  - pérdida de la propiedad de los datos o falta de supervisión de los datos utilizados por terceros por parte de las organizaciones;
- una mayor complejidad en cuanto al cumplimiento de leyes y reglamentos, con el consecuente
  - aumento de los riesgos en términos de privacidad,
  - el flujo transfronterizo de información personalmente identificable, y
  - el cumplimiento contractual;
- la dependencia de Internet como canal primario para la transmisión de los datos de la organización, lo que conlleva
  - cuestiones de seguridad relacionadas con el entorno público y
  - problemas asociados a la conectividad y disponibilidad de Internet;
- el carácter dinámico de la computación en la nube, lo que incluye la posibilidad de que
  - la ubicación de las instalaciones de procesamiento cambie según la carga,
  - Que dichas instalaciones se ubiquen traspasando fronteras internacionales,
  - que se compartan instalaciones operativas con competidores, y
  - que cuestiones legales (responsabilidad, propiedad, etc.) vinculadas con las diferentes legislaciones vigentes en los países de alojamiento pongan en riesgos los datos;
- riesgos para la gobernanza de TI, por ejemplo
  - la pérdida de la gobernanza y control de TI por parte de la organización al utilizar servicios en la nube,
  - una menor capacidad de reacción del cliente en comparación con la provisión interna del servicio, y

- falta de apoyo interno debido a la cultura organizacional y la percepción del cliente de que los riesgos asociados con los servicios en la nube son mayores; y

- riesgos relacionados con la actividad de auditoría, por ejemplo
  - la imposibilidad de acceder a sistemas y registros de seguridad de parte de terceros,
  - la pérdida o provisión incompleta de información por parte del proveedor al cliente debido a incidentes de seguridad y cuestiones vinculadas con las pistas de auditoría, y
  - la ausencia de mecanismos de aislamiento de los datos correspondientes a registros de diferentes clientes o fugas de datos.

h. Dependencia exclusiva de un proveedor

La dependencia exclusiva de un proveedor es un problema propio de la externalización, que se plantea en aquellos casos en los que la contratación de un nuevo proveedor o el traslado de las operaciones al ámbito interno se torna algo demasiado oneroso. Esto puede suceder cuando se trata de organizaciones que realizan aportes significativos a un producto o servicio exclusivamente brindados por un proveedor, pudiendo solamente utilizarse ese producto o servicio con el proveedor actual. Dicha situación puede resultar especialmente complicada en un entorno de computación en la nube, en el que el traslado de datos a un tipo de entorno diferente tal vez requiera un reformateo de tales datos. Además, existe la posibilidad de que algunas organizaciones se tornen dependientes del software utilizado con un proveedor específico de servicios en la nube, dado lo cual no les será sencillo cambiar de proveedor. Las organizaciones pueden reducir el riesgo de depender exclusivamente de un proveedor mediante una cuidadosa evaluación de los servicios en la nube, asegurándose de que los datos puedan transferirse con facilidad, realizando copias de respaldo funcionales de los datos, y recurriendo a diferentes servicios en la nube brindados por múltiples proveedores.

IV. Referencias y lecturas adicionales

Federal Court of Accounts, TCU (SAI Brazil). *Report Highlights: Cloud Computing*. https://portal.tcu.gov.br/en_us/biblioteca-digital/report-highlights-cloud-computing.htm. July 15, 2015.

International Organization for Standardization/International Electrotechnical Commission. *ISO/IEC, 19086-1:2016, Information Technology—Cloud Computing—Service Level Agreement (SLA) Framework —Part 1: Overview and Concepts*. https://www.iso.org/standard/67545.html. September 15, 2016.

International Organization for Standardization/International Electrotechnical Commission. ISO/IEC, *19086-2:2018, Cloud computing – Service level agreement (SLA) framework – Part 2: Metric model.* Geneva, Switzerland: International Organization for Standarization, December 2018.

International Organization for Standardization/International Electrotechnical Commission. ISO/IEC, *TR 22678:2019, Information technology – Cloud computing – Guidance for policy development.* Geneva, Switzerland: International Organization for Standarization, January 2019.

International Organization for Standardization/International Electrotechnical Commission. ISO/IEC, *27036-1:2014, Information technology—Security techniques—Information Security for Supplier relationships – Part 1: Overview and concepts.* Geneva, Switzerland: International Organization for Standarization, April 1, 2014.

International Organization for Standardization. *ISO 37500:2014, Guidance on Outsourcing.* Geneva, Switzerland: International Organization for Standarization, November 11, 2014.

National Institute of Standards and Technology. *Special Publication 500-292: Cloud Computing Reference Architecture.* http://www.nist.gov/customcf/get_pdf.cfm?pub%5Fid=909505. September 2011.

National Institute of Standards and Technology. *Special Publication 800-144: Guidelines on Security and Privacy in Public Cloud Computing*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf. December 2011.

National Institute of Standards and Technology. *Special Publication 800-145: The NIST Definition of Cloud Computing.* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf. September 2011.

National Security Agency. *Mitigating Cloud Vulnerabilities.* https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/csi-mitigating-cloud-vulnerabilities_20200121.pdf. January 22, 2020.

Treasury Board of Canada Secretariat. *Guideline on Service Agreements: Essential Elements.* https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=25761&section=html. July 4, 2012.

Oficina de Rendición de Cuentas del Gobierno de los Estados Unidos. *Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance.* GAO-16-325. https://www.gao.gov/products/GAO-16-325. April 7, 2016.

CAPÍTULO 6: GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO O ACTIVIDAD

I. ¿Qué es la gestión de la continuidad del negocio o actividad?

La disponibilidad y correcta operación de los sistemas de TI son requisitos esenciales para que las organizaciones gubernamentales estén en condiciones de cumplir con sus obligaciones legales. Estos sistemas desempeñan un papel importante en actividades tan diversas como el cálculo y recaudación de impuestos y tributos aduaneros; el pago de pensiones estatales y beneficios de seguridad social; y el procesamiento de estadísticas nacionales (por ejemplo, nacimientos, fallecimientos, delitos y enfermedades). De hecho, muchas actividades no pueden llevarse a cabo de manera eficaz, si es que se pueden llevar a cabo, sin el apoyo de sistemas de información. A los efectos de limitar las alteraciones y períodos de inactividad de estos sistemas, las organizaciones deben formular una estrategia de planificación de la continuidad y procedimientos asociados.

Por su naturaleza, los desastres y otras crisis suelen ser acontecimientos inesperados. Aunque no todos estos acontecimientos son evitables, la planificación de la continuidad a menudo disminuye el impacto de estos acontecimientos inesperados. Interrupciones del suministro eléctrico, medidas sindicales, incendios y daños intencionales pueden tener efectos desastrosos en los sistemas de información. De no existir un plan de continuidad viable, a una organización puede demandarle muchas semanas reanudar efectivamente sus operaciones. Además, numerosas operaciones de TI a menudo se externalizan. Si las operaciones de un proveedor de servicios externalizado se viesen alteradas por un desastre, ello podría tener un efecto substancialmente adverso en la organización.

Para prevenir posibles alteraciones originadas en riesgos conocidos, las organizaciones deberían llevar a cabo diversas actividades de gestión de la continuidad del negocio o actividad, y así ayudar a evitar alteraciones del servicio, lo que incluye l**a planificación de la continuidad del negocio o actividad, la planificación de la recuperación de desastres, y la planificación de contingencias relacionadas los sistemas de información**, entre otras. Las expresiones planificación de la continuidad del negocio (o actividad) y planificación de la recuperación de desastres se utilizan en todo momento como sinónimos, sin embargo, se refieren a conceptos diferentes pero complementarios. Ambos son importantes para el auditor de TI, puesto que, combinados, garantizan que la organización está en condiciones de operar con cierta capacidad definida luego de una alteración de orden natural o causada por el ser humano. La planificación de contingencias para sistemas de información es similar a la planificación para la recuperación de desastres, pero se centra en la recuperación de un sistema, independientemente de su ubicación. A continuación, se explican dichas expresiones:

- **La planificación de la continuidad del negocio o actividad** es el proceso que una organización utiliza para planificar y poner a prueba los procesos del negocio o actividad luego de registrarse una alteración. También describe el modo en que una organización continuará funcionando bajo potenciales condiciones adversas (por ejemplo, desastres naturales u otros tipos de desastres, o incluso en ausencia de personal clave). El objetivo final de la planificación de la continuidad del negocio o actividad es que una organización tenga la mayor resiliencia posible en su carácter de tal. Esto incluye la continuidad de funciones críticas para su misión, en momento y frente a cualquier tipo de desastre o alteración.
- **La planificación para la recuperación de desastres** es el proceso que consiste en planificar y realizar pruebas para la recuperación de la infraestructura de TI luego de un desastre natural o de otra índole. Es complementario de la planificación de la continuidad del negocio o actividad. La planificación de la continuidad del negocio o actividad se aplica a las funciones organizacionales, mientras que la planificación de la recuperación de desastres se aplica a la infraestructura de TI que respalda las funciones del negocio o actividad.

- **La planificación de contingencias relacionadas con el sistema de información** es el proceso que consiste en planificar y realizar pruebas para la recuperación de sistemas de información individuales. Esta actividad es complementaria de la planificación de la continuidad del negocio y se vincula con la recuperación de un sistema individual. La planificación de contingencias relacionadas con el sistema de información se concibe como una guía para la recuperación de un sistema y puede activarse para ese sistema independientemente de su ubicación.

Esencialmente, un **plan de continuidad del negocio o actividad (BCP)** se vincula con la capacidad de una organización de continuar funcionando cuando las operaciones normales se ven alteradas. Este instrumento contiene las políticas, procedimientos y prácticas que permiten a una organización recuperarse y reanudar procesos críticos para su misión, tanto manuales como automatizados, luego de una crisis o un desastre. Además de enunciar las prácticas que han de seguirse en el caso de producirse una interrupción, algunos BCP incluyen otros componentes, como la recuperación de desastres, planificación de contingencias, respuesta frente a emergencias, recuperación de usuarios y actividades de gestión de crisis. En tal sentido, en estas organizaciones, la planificación de la continuidad del negocio o actividad se observa como un proceso integral que abarca tanto la recuperación de desastres como la reanudación de las actividades de la organización.

Sin embargo, ya sea como parte del BCP o como un documento separado, en los **planes de recuperación de desastres (DRP)** deberían definirse los recursos, medidas, tareas y datos necesarios para gestionar el proceso de recuperación de una organización en el caso de que se produzca una interrupción del negocio o actividad. Este plan también debería asistir a una organización en la restauración de los procesos afectados de su negocio o actividad, mediante la descripción de los pasos específicos que ella debe dar en su trayecto hacia la recuperación. Específicamente, el DRP se utiliza para la preparación y planificación anticipadas necesarias para minimizar los daños causados por desastres y garantizar la disponibilidad de sistemas de información críticos de la organización. En términos de TI, los DRP abordan la recuperación de activos tecnológicos críticos, lo que incluye sistemas, aplicaciones, bases de datos, dispositivos de almacenamiento y otros recursos de red.[56]

Además del desarrollo de los DRP, la formulación **de planes de contingencia para sistemas de información (ISCP)** constituyen un paso crítico en la implementación de un programa integral de planificación de la continuidad del negocio o actividad. Las organizaciones pueden desarrollar ISCP para cada sistema sobre la base de la criticidad de ese sistema. En general, los ISCP contienen pasos y procedimientos similares a los de los BCP, pero aquéllos se desarrollan independientemente de emplazamientos y ubicaciones específicos. Un ISCP brinda, entre otros elementos, información clave específica del sistema, como roles y responsabilidades, información sobre inventarios, procedimientos de evaluación, y procedimientos de recuperación detallados para ese sistema.

II. Elementos clave de la gestión de la continuidad del negocio o actividad

El auditor de TI debe evaluar los programas de gestión de la continuidad del negocio de la organización, lo que supone examinar sus BCP, DRP e ISCP, entre otros instrumentos. Para ello, es necesario que los auditores comprendan lo que implica el desarrollo de un programa de gestión de la continuidad del negocio actividad y los pasos que deberían dar para evaluar la eficacia de los programas existentes.

[56] Iia.org, *The IT Auditor's Role in Business Continuity Management*, IIA Publication. http://www.theiia.org/intAuditor/itaudit/archives/2008/january/the-it-auditors-role-in-business-continuity-management

Una planificación de la continuidad eficaz tiene varias etapas comunes a todos los sistemas de información. Las etapas genéricas en el proceso son:[57]

- política, plan y organización de la continuidad del negocio o actividad;
- conformación de un equipo a cargo de la gestión de la continuidad del negocio o actividad;
- examen del impacto en el negocio o actividad y evaluación de riesgos;
- controles preventivos y vinculados con el entorno;
- documentación del plan;
- puesta a prueba del plan y capacitación;
- implementación de la seguridad; y
- medidas de respaldo y recuperación de desastres para servicios externalizados.

Estas etapas constituyen elementos esenciales para el logro de una capacidad integral en términos de planificación de la continuidad del negocio o actividad. Los elementos se explican con mayor detalle a continuación.

a. Política, plan y organización de la continuidad del negocio o actividad

Una gestión eficaz de la continuidad del negocio o actividad comienza con la formulación de una política enderezada a dicha gestión. La declaración de política de continuidad del negocio o actividad debería definir los objetivos generales de continuidad de la organización, y en ella establecerse el marco y las responsabilidades organizacionales relativas a la planificación de dicha continuidad. El equipo a cargo de la gestión de la continuidad del negocio o actividad (analizado más adelante), que abarca todas las funciones pertinentes del negocio o actividad, también cumple un rol importante en el éxito del BCP de la organización. La rotación del personal clave puede constituir un desafío para la continuidad del negocio o actividad de cualquier organización y es necesario que se den los pasos necesarios para garantizar la disponibilidad de los recursos adecuados.

i. Prevención y minimización de daños potenciales e interrupciones

Una organización debería tomar una serie de recaudos para impedir o minimizar el daño a las operaciones automatizadas que puede surgir de acontecimientos inesperados. Estos pasos pueden categorizarse como

- la duplicación rutinaria o realización de copias de seguridad de archivos, programas informáticos y documentos críticos con almacenamiento fuera de las instalaciones; y/o la organización de instalaciones remotas de respaldo o para la recuperación de desastres que puedan utilizarse si las instalaciones habituales se encontrasen dañadas al punto de no poder utilizarse;
- la generación de capacidad para que el sistema de información pueda recuperarse y reconstituirse de modo tal que ese sistema de información se restituya a su estado original luego de una alteración o falla;
- la instalación de controles del entorno, por ejemplo, sistemas de extinción de incendios o fuentes de alimentación eléctrica de respaldo;
- asegurarse de que el personal y otros usuarios de sistemas comprendan sus responsabilidades durante emergencias; y
- el mantenimiento efectivo del hardware, gestión de problemas y gestión de cambios.

Adicionalmente, al realizar la externalización, la organización debería cerciorarse de que el proveedor dispone de mecanismos similares y que estos son eficaces.

[57]Para acceder a orientación sobre procesos de planificación de contingencias, remítase a: National Institute of Standards and Technology, *Special Publication 800-34: Contingency Planning Guide for Federal Information Systems*.

ii. Implementación de procedimientos relativos a copias de seguridad de datos y programas

Copiar archivos de datos y software de forma rutinaria y almacenar estos archivos en una ubicación segura y remota suelen ser las medidas más eficaces que una organización puede realizar para mitigar interrupciones del servicio. Aunque el equipamiento a menudo puede reemplazarse de inmediato, el costo asociado a ello podría ser significativo y la reconstrucción de archivos de datos y el reemplazo del software puede ser extremadamente costoso, además de demandar mucho tiempo. En efecto, no siempre los archivos de datos pueden reconstruirse. Además de los costos directos resultantes de la reconstrucción de archivos y la obtención de software, las interrupciones del servicio relacionadas podrían derivar en pérdidas financieras significativas.

iii. Capacitación

El personal debería capacitarse y ser consciente de sus responsabilidades relacionadas con la prevención, mitigación y reacción a situaciones de emergencia. Por ejemplo, el personal de respaldo a cargo de la seguridad de la información debería recibir capacitación periódica sobre procedimientos de emergencia en caso de incendio, inundación y activación de alarmas, así como también sobre sus responsabilidades vinculadas con la puesta en marcha y operación de un centro de procesamiento de datos alternativo. Asimismo, si el rol de los usuarios externos fuese esencial para las operaciones de la organización, ellos deberían estar informados acerca de los pasos que puedan tener que dar como resultado de una emergencia.

iv. Planes para el mantenimiento de hardware, gestión de problemas y gestión de cambios.

Las interrupciones imprevistas del servicio pueden derivar de fallas en el hardware o de cambios en el equipamiento sin la debida advertencia previa a los usuarios del sistema. Para evitar tales hechos, debe instrumentarse un programa eficaz para el mantenimiento, la gestión de problemas y la gestión de cambios en el hardware.

b. Conformación del equipo a cargo de la gestión de la continuidad del negocio o actividad

Para ser exitosos, un equipo de gestión de la continuidad del negocio o actividad debe encontrarse organizado en términos de representar todas las funciones pertinentes del negocio o actividad de que se trate. La dirección superior y otros funcionarios relacionados deben dar apoyo a un programa de continuidad del negocio y asociarse al proceso de formulación de políticas. Los roles y responsabilidades del equipo deberían identificarse y definirse con claridad.

c. Evaluación del impacto en el negocio y evaluación de riesgos

i. Evaluación de la criticidad y sensibilidad de las operaciones de sistemas e identificación de los recursos de respaldo

En cualquier organización, la continuidad de determinadas operaciones es más importante que la de otras, y no es eficaz en función de los costos brindar el mismo nivel de continuidad a todas las operaciones. Por esta razón, es importante que la organización determine qué operaciones son especialmente críticas y qué recursos se precisan para su recuperación y brindarles apoyo. Esta determinación se lleva a cabo mediante la realización de una evaluación de riesgos y una evaluación del impacto en el negocio o actividad,[58] cuyo propósito es identificar probables amenazas y el efecto de ellas en la información de la organización y sus recursos relacionados, por ejemplo, en sus datos y software de aplicación y operaciones. El propósito de una evaluación del impacto en el negocio o actividad es identificar y priorizar los componentes del sistema

[58]Para acceder a un ejemplo de una plantilla de evaluación del impacto en el negocio o actividad, remítase ahttps://csrc.nist.gov/CSRC/media/Publications/sp/800-34/rev-1/final/documents/sp800-34-rev1_bia_template.docx.

mediante su asociación con el proceso de negocios de la organización al que el sistema brinda apoyo. Las evaluaciones de riesgo e impacto en el negocio o actividad deberían abarcar todas las áreas funcionales. Por consiguiente, debería tomarse una decisión sobre el riesgo residual toda vez que el impacto de una posible amenaza sea mínimo, o los sistemas de control resulten adecuados para mitigar tales circunstancias a tiempo.

ii. Identificación y priorización de operaciones y datos críticos

La criticidad y sensibilidad de los diversos datos y operaciones deberían determinarse y priorizarse sobre la base de categorizaciones de seguridad, requisitos en términos de disponibilidad, y una evaluación general de los riesgos para las operaciones de la organización.[59] Tal evaluación de riesgos debería servir como fundamento del plan de seguridad de una organización. Los factores a considerar incluyen la importancia y sensibilidad de los datos y otros activos de la organización, y el costo de no restituir los datos o reanudar las operaciones rápidamente. Por ejemplo, la salida de servicio durante un día de un sistema importante para la recaudación de impuestos o aranceles aduaneros, o la pérdida de datos relacionados, podría ralentizar significativamente o detener la percepción de ingresos, disminuir los controles sobre millones de dólares en fondos recaudados, y reducir la confianza pública. Por el contrario, un sistema que permite monitorear la capacitación de los empleados podría encontrarse fuera de servicio durante varios meses sin consecuencias serias.

En general, las operaciones y datos críticos deberían ser identificados y clasificados por el personal involucrado en el negocio o actividad de la organización o las operaciones del programa. También es importante obtener el acuerdo de la dirección superior respecto a dichas determinaciones, además de la concurrencia de los grupos afectados.

El listado priorizado de operaciones y recursos de información críticos debería revisarse periódicamente para determinar si en él se reflejan las condiciones actuales. Dichas revisiones deberían tener lugar toda vez que se produzca una modificación substancial en la misión y operaciones de la organización o en la ubicación o diseño de los sistemas que respaldan estas operaciones.

iii. Identificación de recursos que respaldan operaciones críticas

Una vez determinados los datos y operaciones críticas, deberían identificarse los recursos mínimos para brindarles apoyo, y analizarse sus roles. Los recursos a considerar incluyen:

- recursos de TI, como el hardware, el software y archivos de datos;
- redes, lo que incluye componentes tales como routers y cortafuegos;
- suministros, lo que incluye papelería y formularios preimpresos;
- servicios de telecomunicaciones; y
- cualesquiera otros recursos necesarios para la operación de la organización, por ejemplo, recursos humanos, instalaciones y suministros de oficina, y registros en papel.

Dado que es probable que los recursos esenciales sean controlados o gestionados por una diversidad de grupos dentro de una organización, es importante que el personal que brinda apoyo al programa y la seguridad de la información cooperen para identificar los recursos que se precisan para realizar operaciones críticas.

iv. Determinación de las prioridades de procesamiento ante emergencias

[59]Para acceder a más información sobre categorizaciones en materia de seguridad, remítase a: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

Además de identificar y clasificar las funciones críticas, la organización debería desarrollar un plan de restablecimiento de esas operaciones críticas. En el plan debería señalarse con claridad el orden en que los diversos aspectos del procesamiento deberían reestablecerse, quiénes son los responsables de ello, y que equipamiento de apoyo u otros recursos serán necesarios. Un plan de restablecimiento del procesamiento desarrollado cuidadosamente puede ayudar a las organizaciones a comenzar el proceso correspondiente de inmediato, y realizar el uso más eficiente de recursos informáticos limitados durante una emergencia. Tanto los usuarios del sistema como el personal de apoyo a la seguridad deberían participar en la determinación de las prioridades de procesamiento de emergencia.

d. Controles preventivos y vinculados con el entorno

Los controles del entorno sirven para prevenir o mitigar potenciales daños a instalaciones e interrupciones del servicio. Algunos ejemplos de controles del entorno son

- los extintores y sistemas de supresión de incendios,
- las alarmas de incendio,
- los detectores de humo,
- los detectores de agua,
- la iluminación de emergencia,
- los sistemas de refrigeración redundantes,
- las fuentes de alimentación eléctrica de respaldo,
- la existencia de válvulas de cierre y procedimientos para el manejo de cualquier sistema hídrico edilicio que pueda poner en peligro las instalaciones de procesamiento,
- la construcción de instalaciones de procesamiento con materiales resistentes al fuego y características ignífugas,
- las políticas que prohíben comer, beber o fumar dentro de instalaciones de TI,
- almacenamiento de respaldo externo a las instalaciones, y
- controles de seguridad técnica, como la gestión de claves criptográficas.

Los controles del entorno pueden disminuir las pérdidas derivadas de algunas interrupciones, como incendios, o prevenir incidentes mediante la detección de problemas anticipadamente, como cuando se trata de fugas de agua o humo, de modo tal que puedan subsanarse. Asimismo, los sistemas de alimentación eléctrica ininterrumpida (UPS) o de respaldo sirven para que una instalación sobrelleve una interrupción breve del suministro eléctrico o se disponga de tiempo para realizar copias de seguridad de los datos y efectuar procedimientos de desactivación ordenados durante interrupciones prolongadas del suministro.

e. Documentación del plan

Los planes de continuidad, como los BCP, DRP e ISCP, deberían documentarse claramente, comunicarse al personal afectado y actualizarse para reflejar las operaciones en curso. Además, debe disponerse de planes listos para su instrumentación que reflejen el entorno actual. Los DRP e ISCP deberían alinearse claramente con el BCP y brindar instrucciones paso a paso relativas a la minimización del impacto de un desastre. A medida que la tecnología cambia, es posible que las estrategias y los planes de recuperación varíen. Tales variaciones conllevan una modificación de la evaluación del impacto en el negocio o actividad, debiéndose documentar con claridad los nuevos requisitos y prioridades asociados a contingencias.

i. BCP

Un BCP se centra en sostener la misión/los procesos relacionados con el negocio o actividad de una organización en el caso de que se produzca un desastre o alteración. Los BCP son críticos para formular procedimientos relacionados con el modo en que una organización seguirá adelante con sus operaciones

durante un desastre o alteración, y una vez transcurridas dichas circunstancias. El BCP puede elaborarse para una única unidad de negocios o para toda una organización. Además, el BCP puede enfocarse en el abordaje de aquellas funciones que, según se ha determinado, son más críticas. El BCP puede coordinarse con otros planes de recuperación para asegurarse de que los procedimientos y expectativas se encuentren alineados.

El BCP debería incluir elementos tales como una evaluación del impacto en el negocio o actividad que ayuden a orientar las prioridades de recuperación reflejadas en este instrumento. Las estrategias de recuperación también deberían documentarse. Tal es el caso de los requisitos en materia de recursos para la aprobación de estrategias de recuperación por parte de la dirección. En el BCP debería documentarse información relativa a los equipos de recuperación y los requisitos en materia de recopilación de datos. Asimismo, el BCP debería incluir requisitos de ejercicio y mantenimiento para asegurarse de que las estrategias de recuperación se mantengan actualizadas y conserven su exactitud. Estos elementos ayudarán a formular un BCP exhaustivo que pueda servir de guía a otros planes, como el DRP.

ii. DRP

El propósito de la elaboración de un DRP es la restauración de aplicaciones críticas; esto incluye mecanismos para instalaciones de procesamiento alternativas en el caso de que las instalaciones habituales se encuentren significativamente dañadas o sea imposible acceder a ellas. Las políticas y procedimientos a nivel organizacional definen los requisitos relativos al proceso de planificación de recuperación y documentación. Asimismo, un plan que abarque la organización en su conjunto debería identificar sistemas críticos, aplicaciones y cualesquiera otros planes subordinados o relacionados.

Los DRP deberían ser acordados por los departamentos a cargo del negocio o actividad y de la seguridad de la información de la organización, y comunicarse al personal adecuado. El plan debería reflejar los riesgos y prioridades operativas que la organización ha identificado. Asimismo, debería diseñarse de modo tal que los costos de la planificación para la recuperación de desastres no superen los costos asociados a los riesgos que se pretende reducir mediante el plan. El plan también debería detallarse y documentarse de manera suficiente, de modo tal que su éxito no dependa de los conocimientos o experiencia de una o dos personas. Debería poder accederse a múltiples copias del DRP, guardándose algunas de ellas en ubicaciones externas al emplazamiento, para asegurarse de que no sean destruidas por los mismos acontecimientos que generaron la indisponibilidad de las instalaciones principales de procesamiento de datos.

Según sea el grado de continuidad del servicio que se precisa, las opciones relativas a emplazamientos o instalaciones alternativos variarán entre un emplazamiento equipado, listo para un servicio de respaldo inmediato, denominado ***hot site***, y un emplazamiento no equipado cuya preparación para la realización de operaciones demandará tiempo, conocido como ***cold site***. Además, es posible concertar previamente diferentes tipos de servicios con los proveedores. Eso incluye la realización de acuerdos con proveedores de hardware de TI y servicios de telecomunicaciones, así como también con proveedores de formularios para el negocio o actividad y de otros insumos de oficina.

iii. ISCP

Las organizaciones deberían desarrollar planes de contingencia para cada sistema de información que pueda verse afectado en el caso de producirse un desastre.[60] El ISCP debería elaborarse en concordancia con otros planes, como el DRP. Los sistemas de información pueden ser muy complejos y respaldar múltiples funciones diferentes del negocio o actividad. Con este fin, es necesario que las organizaciones

[60]Para acceder a orientación acerca de los procesos de planificación para contingencias, remítase a: National Institute of Standards and Technology, *Special Publication 800-34: Contingency Planning Guide for Federal Information Systems*.

trabajen con la dirección al elaborar los ISCP, de forma tal asignar el nivel de criticidad adecuado y que se comprenda el impacto de la alteración o interrupción de un sistema.

Habitualmente, un ISCP contiene cinco componentes principales: información de respaldo, activación y notificación, recuperación, reconstitución y apéndices. La siguiente es una breve descripción de cada uno de estos cinco componentes:

- **Información de respaldo—**Esto incluye el suministro de información esencial sobre antecedentes o de carácter contextual que facilita la comprensión, implementación y mantenimiento del plan.
- **Activación y notificación—**Esto incluye la notificación al personal de recuperación, la realización de una evaluación de la interrupción y la activación del plan.
- **Recuperación—**Esto incluye la implementación de las estrategias de recuperación para restaurar las capacidades del sistema, reparar daños y reanudar las operaciones.
- **Reconstitución—**Esto incluye la validación de una recuperación exitosa y la desactivación del plan. Este componente podría incluir la realización pruebas de funcionalidad para asegurarse de que la funcionalidad del conjunto del sistema ha vuelto a la normalidad.
- **Apéndices—**Esto incluye información valiosa no contenida en el cuerpo del plan.

La inclusión de estos componentes ayudará a cerciorarse de que una organización se encuentre mejor posicionada para afrontar desastres relacionados con sus sistemas.

f. Puesta a prueba del plan y capacitación

i. Puesta a prueba periódica de los planes de continuidad

La puesta a prueba de los planes de continuidad es un paso esencial para determinar si funcionarán de la manera prevista en una situación de emergencia. Las pruebas deberían revelar debilidades importantes en el plan, por ejemplo, instalaciones de respaldo que no podrían replicar adecuadamente operaciones críticas de la manera prevista. Es necesario mejorar substancialmente estos planes mediante los procesos de prueba.

La frecuencia de las pruebas a las que se someterá el plan de continuidad dependerá de la criticidad de las operaciones de la organización. En general, los planes de continuidad relativos a sistemas y funciones altamente críticos deberían someterse a pruebas una vez cada uno o dos años, toda vez que se hubiesen realizado modificaciones significativas al plan, o cuando se hubiese producido una rotación importante de personal clave. Es importante que la dirección superior evalúe los riesgos de que en la ejecución del plan de continuidad surjan problemas, y que formule y documente una política sobre la frecuencia y amplitud de las pruebas que han de realizarse.

ii. Actualización del plan de continuidad sobre la base de los resultados de las pruebas

Los resultados de las pruebas de continuidad brindan una medida importante de la factibilidad de los planes de continuidad. En tal sentido, deberían informarse a la dirección superior de forma tal que pueda determinarse la necesidad realizar modificaciones y pruebas adicionales, y que la dirección superior también esté al corriente de los riesgos de proseguir las operaciones con planes de continuidad inadecuados.

iii. Capacitación

La capacitación del personal que tenga responsabilidades por el plan de continuidad es esencial para que dicho personal se familiarice con sus roles y disponga de las habilidades necesarias para desempeñarlos. Así también se garantiza que el personal se encuentre preparado para participar en la realización de pruebas y en circunstancias reales de interrupción de servicios. Además, el personal debería encontrarse capacitado en la medida necesaria para desempeñar sus roles sin precisar remitirse a la documentación

en la que se describen. Los recorridos documentados de simulación de contingencias con todas las personas clave presentes también pueden ser una herramienta de utilidad.

g. Implementación de la seguridad

La seguridad de los recursos y operaciones debería incorporarse al BCP, dado que, durante cualquier situación de desastre o al tomarse medidas vinculadas con la gestión de la continuidad del negocio o actividad, podrían verse comprometidos datos, software de aplicación, recursos críticos. Por ejemplo, al efectuarse copias de respaldo de los datos, la falta de seguridad podría derivar en duplicaciones y filtraciones de datos importantes. Asimismo, es posible que los datos cuya copia de respaldo se está realizando se vean comprometidos durante el proceso (al guardarse en el servidor de respaldo copias de los datos existentes en el servidor de transacciones).

h. Copias de respaldo y recuperación de desastres para servicios externalizados

Muchas organizaciones externalizan la totalidad o parte de sus operaciones de TI, asignándolas a un proveedor de servicios. Dado que la operación y el control diarios se encuentran a cargo del proveedor de servicios, será esencial que la organización se asegure de que el BCP y el DRP formen parte del contrato. La organización también debería cerciorarse de que el proveedor de servicios garantice la continuidad del negocio o actividad, así como también la preparación para la recuperación de desastres. Esto también incluiría la preparación en materia de seguridad del proveedor de servicios. También es posible que la organización precise asegurarse de que el proveedor de servicios mantenga la confidencialidad de los datos. La organización debería conservar la propiedad del proceso asociado a su negocio o actividad y ocuparse de los riesgos relacionados. Asimismo, debería disponer de un BCP para garantizar la continuidad de sus tareas en el caso de que el proveedor de servicios cese en su actividad. Como se mencionase previamente, a menudo hay disponibles informes de control de la organización de servicios para contar con esta seguridad como parte del contrato con el proveedor.

III. Riesgos para la organización auditada

Los productos o servicios críticos son aquellos que deben ser provistos para asegurar la supervivencia, evitar pérdidas, y dar cumplimiento a las obligaciones legales o de otra índole de una organización. La planificación de la continuidad es un proceso de planificación proactivo por el que se garantiza que los procesos del negocio o actividad y la infraestructura de TI de una organización están en condiciones de respaldar las necesidades relacionadas con su misión luego de un desastre u otra alteración. Las organizaciones gubernamentales atienden muchas necesidades críticas en términos de su misión (como la realización de pagos a los ciudadanos, la atención sanitaria, la educación, la defensa, y otros servicios de los que dependen los ciudadanos). Si estos servicios se viesen alterados durante lapsos prolongados, ello dará lugar a pérdidas financieras y de otra índole. Los auditores deberían asegurarse de que todas las organizaciones gubernamentales dispongan de procesos de planificación de la continuidad de sus quehaceres, por los que se garantice que dichas organizaciones están en condiciones de continuar sirviendo a los ciudadanos.

Al evaluar si los procesos de planificación de la continuidad de una organización están en condiciones de mejorar la confiabilidad y continuidad de la infraestructura y procesos de negocio de TI, los auditores han de centrarse en algunos riesgos de auditoría para determinar la eficacia de la planificación. Estos riesgos de auditoría conllevan determinar si la organización ha desarrollado documentos críticos, como los BCP, DRP e ISCP, que abarcan todas las áreas funcionales críticas. Asimismo, si los roles y responsabilidades no se encuentran claros y son comprendidos por el personal adecuado, un buen BCP puede tornarse ineficaz.

La elaboración de una evaluación del impacto en el negocio o actividad, controles del entorno y preventivos, y la documentación correspondiente; la puesta a prueba del plan de continuidad frente a contingencias; y la capacitación del personal, respaldan la implementación eficaz de un programa de

gestión de la continuidad. Las deficiencias en materia de seguridad relacionadas con la implementación de un BCP y un DRP conllevan el riesgo de que una organización sufra pérdidas de datos, la pérdida de tiempo valioso, y experimente otros costos asociados a una recuperación ineficaz en el caso de producirse un desastre.

La externalización de servicios conlleva riesgos singulares, en tanto la planificación de la continuidad no se encuentra totalmente bajo el control de la organización. Es necesario abordar los riesgos relacionados con la seguridad, la pérdida, el manejo no autorizado y la filtración de datos. Asimismo, las organizaciones afrontan riesgos de continuidad relacionados con la pérdida de conocimientos sobre el negocio o actividad o la propiedad de procesos, además de la incapacidad de cambiar de proveedor de servicios ante un desempeño deficiente de éste o su cierre.

IV. Referencias y lecturas adicionales

IIa. "The IT Auditor's Role in Business Continuity Management," *Internal Auditor*. https://elearn.iia.org.au/mod/resource/view.php?id=10550. January 2008.

International Organization for Standardization/International Electrotechnical Commission. *ISO/IEC 22301:2019—Security and Resilience—Business Continuity Management Systems —Requirements*. https://www.iso.org/obp/ui#iso:std:iso:22301:ed-2:v1:en. 2019.

International Organization for Standardization/International Electrotechnical Commission. *ISO/IEC 22300:2021*—Security and Resilience—Vocabulary. https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en. 2021.

International Organization for Standardization/International Electrotechnical Commission. *ISO/IEC 22313:2020—Security and Resilience—Business Continuity Management Systems—Guidance on the Use of ISO 22301.* https://www.iso.org/standard/75107.html. 2020.

ISACA. *COBIT 2019 Framework: Governance and Management Objectives.* 2019.

National Institute of Standards and Technology. *Special Publication 800-34: Contingency Planning Guide for Federal Information Systems*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf.

National Institute of Standards and Technology. *Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. September 2020.

National Institute of Standards and Technology. *Standards for Security Categorization of Federal Information and Information Systems, FIPS 199.* https://csrc.nist.gov/publications/detail/fips/199/final February 2004.

U.S. Government Accountability Office. *Federal Information Systems Audit Manual (FISCAM).* https://www.gao.gov/products/gao-09-232g. February 2, 2009.

CAPÍTULO 7: SEGURIDAD DE LA INFORMACIÓN

I. ¿Qué es la seguridad de la información?

Como se señaló en el Capítulo 1, la seguridad de la información puede definirse como la protección de información y sistemas de información frente a situaciones de acceso no autorizado, uso, divulgación, alteración, modificación o destrucción, a los efectos de brindar confidencialidad, integridad y disponibilidad.[61] La seguridad de la información incluye aquellas medidas necesarias para gestionar, prevenir, detectar, documentar y contrarrestar dichas amenazas y permite a una organización proteger su infraestructura de sistemas de información de usuarios no autorizados.

La seguridad de la información se relaciona estrechamente con la ciberseguridad, aunque no son lo mismo. Esta última es el proceso que consiste en proteger la información mediante la prevención y detección de ciberataques, a menudo originados en fuentes externas, y la respuesta frente a ellos.[62] La ciberseguridad abarca las estrategias, políticas y normas relativas a la seguridad en el ciberespacio y las operaciones que en él tienen lugar, y comprende, entre otros factores, la reducción de amenazas y vulnerabilidades; la respuesta, resiliencia y recuperación frente a incidentes; y el aseguramiento de la información.[63] Aunque muchos de los elementos clave de la seguridad de la información analizados más adelante en este capítulo son aplicables a la ciberseguridad, su eje principal son las políticas, procedimientos y prácticas de seguridad que las organizaciones deberían implementar. Como parte de otro proyecto del WGTIA de la INTOSAI, se está elaborando otro documento de auditoría de carácter orientativo acerca de la ciberseguridad y protección de datos.

Como se mencionó anteriormente, un aspecto fundamental de la seguridad de la información es la capacidad de garantizar su **confidencialidad**, **integridad** y **disponibilidad** –de lo que depende todo lo demás.

- La **confidencialidad** consiste en preservar las restricciones autorizadas sobre el acceso a la información y su divulgación, lo que incluye la aplicación de medios para la protección de la privacidad personal e información exclusiva. Una pérdida de confidencialidad es la divulgación no autorizada de información.
- La **integridad** consiste en proteger a la información de su modificación o destrucción indebidas, lo que incluye garantizar su no repudio [64] y autenticidad.[65] Una pérdida de integridad consiste en la modificación o destrucción no autorizadas de información.
- La **disponibilidad** consiste en asegurarse de que todos los sistemas de información, lo que incluye el hardware, las redes de comunicaciones, las aplicaciones de software, y los datos que tales elementos

[61]National Institute of Standards and Technology, *Glossary* (2021), https://csrc.nist.gov/glossary.

[62]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity,* version 1.1, 2018.

[63]National Initiative for Cybersecurity Careers and Studies, *Cybersecurity Glossary*, https://niccs.cisa.gov/about-niccs/cybersecurity-glossary.

[64]El **no repudio** consiste en asegurarse de que el emisor de la información reciba una prueba de entrega y que el receptor reciba una prueba de la identidad del emisor, de modo tal que ninguna de las partes pueda, posteriormente, negar haber procesado la información. El no repudio puede no resultar necesario para evaluar la integridad a los efectos de cumplir con un objetivo de auditoría.

[65]La **autenticidad** es la propiedad de un elemento de ser genuino, verificable y fiable; la confianza es la validez de una transmisión, un mensaje, o el originador de un mensaje. La autenticidad puede no resultar necesaria para evaluar la integridad a los efectos de cumplir con un objetivo de auditoría.

contienen, se encuentren a disposición de los usuarios en los momentos necesarios para la realización del negocio o actividad de la organización. También debería garantizarse un acceso oportuno y confiable a la información, así como su utilización. Una pérdida de disponibilidad es la discontinuidad del acceso a la información o un sistema de información, o en el uso de dicha información o sistema.

Es necesario que la seguridad de la información desempeñe muchos roles para la organización y, en última instancia, debe ser una herramienta que facilite la tarea y respalde la consecución de los objetivos de la organización, en lugar de convertirse en un fin en sí mismo. Una forma en que la seguridad de la información puede respaldar los objetivos del negocio o actividad es servir como medio de resguardo de los activos de información de la organización. Esto supone que el programa de seguridad de la información de la organización sirva para proteger sus datos permitiendo al mismo tiempo cumplir con los objetivos propios de su negocio o actividad.

Ello también supone que la organización brinde el cúmulo adecuado de información a los usuarios correspondientes. La aplicación de los principios de la seguridad de la información al uso del hardware, las redes de comunicaciones, las aplicaciones de software y el acceso a datos requerirá una política de control del acceso. El objetivo del **control del acceso** es garantizar que los usuarios utilicen únicamente a aquellos recursos y servicios que están autorizados a utilizar, y que a los usuarios habilitados no se les niegue el acceso a aquellos servicios que legítimamente esperan recibir. La provisión de información a aquellos sujetos que deberían tenerla es tan importante como su protección frente a los que no deberían tenerla.

Esencialmente, la seguridad de la información consiste en minimizar la exposición, recurriendo para ello a la gestión de riesgos en todas las áreas del modelo de gobernanza de TI. La falta de implementación y monitoreo de los procesos de mitigación de riesgos en un área puede causar daños a la organización en su conjunto. Aun cuando se conoce ampliamente que una gestión eficaz de los riesgos para la seguridad de la información es esencial en lo relativo a la seguridad de una organización, a menudo se hace caso omiso de tales riesgos, o las precauciones de seguridad no se actualizan en respuesta a condiciones cambiantes.

a. La necesidad de la seguridad de la información

La seguridad de la información es un factor cada vez más importante para las organizaciones gubernamentales. Dado que la integración de las redes públicas y privadas y el intercambio de recursos de información aumenta la complejidad del control del acceso y la preservación de la confidencialidad, integridad, y disponibilidad de los datos, existe una necesidad creciente de que las organizaciones elaboren programas vinculados con la seguridad de la información.

Los sistemas de información son conjuntos increíblemente complejos integrados por tecnologías, procesos y personas, que actúan colaborativamente para posibilitar el procesamiento, almacenamiento y transmisión de información para respaldar la misión de una organización y las funciones de su negocio o actividad. Por lo tanto, es esencial que toda organización elabore un programa de esa naturaleza.

El objetivo de un programa de seguridad de los sistemas de información es proteger la información de una organización mediante la reducción a un nivel aceptable de los riesgos vinculados con la pérdida de confidencialidad, integridad y disponibilidad de tal información. Si una organización no hubiese concebido un programa de seguridad de la información, aumentarán los riesgos para sus operaciones y el logro de sus objetivos generales y, en última instancia, ello afectará su credibilidad.

Con la ampliación del potencial, la complejidad y el rol de la TI, la seguridad de la información se convierte en un tema cada vez más importante para las auditorías de esta área. De hecho, ella constituye un factor crítico para las actividades de las organizaciones, puesto que las debilidades en cuanto a la seguridad de la información pueden derivar en daños serios. Algunos efectos potenciales asociados a la debilidad en materia de seguridad de la información son:

- infracciones a las exigencias legales y reglamentarias;
- multas, resarcimientos, disminución de las ventas, y generación de costos de reparación o reposición;

- reducción de la eficacia y/o la eficiencia de un proyecto o programa llevados a cabo por la organización o la totalidad de un servicio prestado por ella;
- pérdida o hurto de recursos informáticos, activos y fondos;
- acceso indebido a información sensible relacionada con la seguridad nacional, datos personalmente identificables e información exclusiva de la actividad o negocio de una organización, así como la divulgación, modificación o destrucción de tal información;
- hacking y potenciales exigencias de rescate;
- discontinuidad de operaciones esenciales vinculadas con infraestructura crítica, la defensa nacional o servicios de emergencia;
- deterioro de misiones organizacionales debido a incidentes perjudiciales para su reputación y/o finanzas;
- utilización de recursos informáticos para fines no autorizados o para lanzar ataques sobre otros sistemas; y
- daños a redes y equipos.

Estos daños pueden derivar de:

- **violaciones a la seguridad**–tanto detectables como indetectables;
- **conexiones externas no autorizadas**–con sitios remotos;
- **exposición de información**–divulgación de activos e información sensible de una organización a terceros no autorizados. Un ejemplo del modo en que esto puede producirse se conoce como ingeniería social, que consiste en una técnica de manipulación utilizada por delincuentes, fundada en el instinto básico de la confianza que tienen los seres humanos, para inducir a personas a revelar información confidencial;
- **amenazas internas**–usuarios que utilizan sus puestos dentro de organizaciones para obtener un acceso irrestricto y causar daños; y
- **vulnerabilidades del sistema**–los sistemas y datos a los que se accede de un modo no autorizado son propensos a sufrir una amplia variedad de ataques malintencionados, y pueden abrirse para que se produzcan intrusiones adicionales.

El incremento en el uso de redes sociales por parte de organizaciones gubernamentales también puede convertirse en un área de potenciales auditorías de TI. La utilización de los servicios que ellas proveen –incluso las de mayor difusión, como Facebook, Twitter y YouTube– brinda a los organismos la posibilidad de compartir información de manera inmediata y solicitar el aporte de comentarios y sugerencias del público. Sin embargo, la utilización de estos servicios puede plantear problemas en lo atinente a la protección de información personal, y también en términos de garantizar la seguridad de la información y sistemas, entre otras áreas. Por ejemplo, los atacantes pueden utilizar redes sociales para recopilar información y lanzar ataques contra los sistemas de información de una organización. Asimismo, la privacidad podría verse comprometida si no se estableciesen límites claros respecto al modo en que la organización utiliza la información personal a la que accede a través de los entornos de las redes sociales. Para ayudar a abordar estos desafíos, las organizaciones deberían disponer de políticas y procedimientos para la gestión de riesgos en materia de seguridad y la protección de la privacidad que se ocupen del uso de las redes sociales.[66]

b. Formación de una cultura de la seguridad de la información

[66]Para acceder a más información sobre la auditoría de las políticas y procedimientos de una organización en lo relativo al uso de redes sociales, remítase a la siguiente publicación de la Oficina de Rendición de Cuentas del Gobierno de los Estados Unidos: *Social Media: Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate,* GAO-11-605, (June 28, 2011), https://www.gao.gov/products/GAO-11-605.

Un factor determinante para el éxito de los programas de seguridad de la información de una organización es la gestación de culturas organizacionales que aborden cuestiones de seguridad. Para abordar de manera uniforme estas y otras cuestiones en una organización de grandes dimensiones, debería seguirse un modelo de negocio o actividad basado en la seguridad de la información.[67] Algunos elementos clave para que una cultura de la seguridad de la información sea exitosa son:

- **Concienciación sobre la seguridad.** Esto consiste en la organización de actividades de concienciación general en materia de seguridad de la información y la instrumentación de sesiones educativas dirigidas a empleados. Estas sesiones son una buena oportunidad para comenzar a exponer aquellas responsabilidades que se vinculan con la seguridad de la información. La función de recursos humanos puede encargarse inicialmente de brindar la capacitación orientada a generar conciencia entre los empleados nuevos. Dicha capacitación debería continuar durante el período de empleo y hasta su conclusión, de modo tal de promover en todo momento la conciencia en materia seguridad.
- **Búsqueda del compromiso de la dirección.** El compromiso de la dirección es una condición esencial para la generación de una cultura de la seguridad de la información. La dirección demuestra su compromiso no solamente al elaborar documentación formal de carácter informativo sobre políticas de seguridad, sino además a través de su activa participación. Si la dirección no apoyase genuinamente el programa de seguridad de la información, dicha actitud podría desalentar el sentido de obligación o responsabilidad de los propios empleados respecto al programa. Por lo tanto, es esencial que la dirección asuma la propiedad de la seguridad de la información y respalde íntegramente dicho programa.
- **Creación de una coordinación sólida mediante la conformación de equipos interfuncionales.** Dado que la seguridad de la información abarca muchos aspectos de la organización que requieren de una coordinación, debería considerarse la posibilidad de conformar equipos interfuncionales (por ejemplo, equipos integrados por miembros de múltiples divisiones, lo que incluye el área de TI). La utilización de equipos interfuncionales fomenta la comunicación y la colaboración, y reduce el aislamiento departamental y la duplicación de esfuerzos.

La instauración de una cultura de la seguridad de la información constituye una parte integral de la implementación de la gobernanza dentro de una organización, y se caracteriza por lo siguiente:

- **Alineación entre los objetivos de la seguridad de la información y los del negocio o actividad.** Es necesario alinear los objetivos de la seguridad de la información con los del negocio o actividad, en tanto los primeros posibilitan los segundos y les brindan apoyo. Es necesario que el programa de seguridad de la información se alinee con la organización y prevea controles relacionados con dicha seguridad que sean prácticos y conduzcan a una reducción real y mensurable de los riesgos.
- **Equilibrio entre la organización, las personas, los procesos y la tecnología.** Para lograr eficacia en términos de seguridad de la información se precisa apoyo organizacional, personal competente, procesos eficientes y la selección de la tecnología adecuada. Cada elemento interactúa con otras áreas (teniendo impacto en otros elementos y apoyándolos, a menudo de maneras complejas), por ende, es esencial lograr un equilibrio entre ellos. Si cualquier elemento individual presentase deficiencias, la seguridad de la información se vería disminuida.
- **Gestión de riesgos.** La instrumentación de la seguridad de la información debe sostenerse en la gestión de riesgos. El National Institute of Standards of Technology describe los siguientes cuatro aspectos del proceso de gestión de riesgos en su publicación especial sobre la gestión de riesgos asociados a la seguridad de la información:[68]
    - asignación de responsabilidades relativas a la gestión de riesgos en materia de seguridad a los líderes/ejecutivos superiores;
    - reconocimiento y comprensión constantes por parte de los líderes/ejecutivos superiores de los

[67]ISACA, *Business Model for Information Security,* 2010.

[68]National Institute of Standards and Technology, *Special Publication 800-39: Managing Information Security Risk: Organization, Mission, and Information System View*, 2011.

riesgos a los que están expuestos las operaciones y activos de la organización, las personas y otras organizaciones, derivados de la operación y utilización de sistemas de información;

- Determinación de la tolerancia al riesgo en el plano organizacional, y comunicación de dicha tolerancia a todos los sectores de la organización, lo que incluye impartir orientación acerca del modo en que la tolerancia al riesgo impacta en las actividades de toma de decisiones en curso.
- Rendición de cuentas por parte de los líderes/ejecutivos superiores respecto a sus decisiones asociadas a la gestión de riesgos y la implementación de programas de gestión de riesgos eficaces que abarquen la organización en su conjunto.

II. Elementos clave de la seguridad de la información

El análisis de la seguridad de la información en una organización abarca 12 dominios

- Evaluación de riesgos
- Política de seguridad
- Organización de la seguridad de TI
- Gestión de operaciones y registros
- Gestión de activos
- Seguridad de los recursos humanos
- Seguridad física y del entorno
- Control del acceso
- Desarrollo, adquisición y mantenimiento de sistemas de TI
- Gestión de incidentes de seguridad de TI
- Gestión de la continuidad del negocio
- Cumplimiento normativo

a. Evaluación de riesgos

La evaluación de riesgos es el proceso que consiste en la identificación, el análisis y la evaluación de riesgos en la infraestructura de seguridad de TI. También consiste en evaluar riesgos relacionados con la seguridad originados en amenazas internas y externas a una entidad, sus activos y su personal. El proceso de evaluación de riesgos incluye la identificación y el análisis de

- todos los activos y procesos relacionados con el sistema;
- entornos externalizados relacionados con el sistema;
- amenazas que podrían afectar la confidencialidad, integridad o disponibilidad del sistema;
- vulnerabilidades del sistema y amenazas asociadas;
- impactos y riesgos potenciales originados en la actividad en la que radica la amenaza;
- exigencias en materia de protección para mitigar los riesgos; y
- selección de las medidas de seguridad adecuadas y análisis de las relaciones asociadas a los riesgos.

Una incorrecta evaluación de riesgos puede dar lugar a una subprotección de infraestructura e información sensibles o, en algunos casos, una sobreprotección dispendiosa. El National Institute of Standards of Technology delinea los siguientes cuatro pasos del proceso de evaluación de riesgos en su publicación especial *Guide for Conducting Risk Assessments*:[69]

[69]National Institute of Standards and Technology, Joint Task Force Transformation Initiative, Special Publication 800-30*, Guide for Conducting Risk Assessments*, 2012.

- **Preparación** para la evaluación mediante el desarrollo de un marco de riesgo organizacional.
- **Realización** de la evaluación mediante
  - la identificación de fuentes de amenazas y acontecimientos que las constituyan,
  - la identificación de vulnerabilidad y condiciones predisponentes,
  - la determinación de la probabilidad de acaecimiento,
  - la determinación de la magnitud del impacto en el caso de producirse una violación a la seguridad, y
  - la utilización de la información precedentemente enumerada para determinar el riesgo general.
- **Comunicación** de los resultados de la evaluación.
- **Mantenimiento** de la evaluación.

Las evaluaciones de riesgos no son actividades que se realizan una sola vez y brindan información definitiva a los encargados de tomar decisiones para orientar y sustentar las respuestas a riesgos relacionados con la seguridad de la información. Antes bien, las organizaciones deben realizar evaluaciones de riesgos de forma continua, considerándose que la frecuencia de las evaluaciones de riesgos y los recursos utilizados durante tales evaluaciones deberán ser acordes al propósito expresamente definido y el alcance de ellas.

La aplicación de evaluaciones de riesgos ayudará a la dirección a seleccionar controles adecuados para mitigar tales riesgos de forma eficaz. Para seleccionar los controles de seguridad adecuados, en la *Federal Information Processing Standards Publication 199* se definen tres niveles de impacto potencial –bajo, moderado y alto– en organizaciones y personas si se produjese una violación a la seguridad (es decir, una pérdida de confiabilidad, integridad o disponibilidad).[70] La aplicación de estas definiciones debe tener lugar dentro del contexto de cada organización y del interés nacional en su conjunto.

- El impacto potencial es **bajo** si puede esperarse que la pérdida de confidencialidad, integridad o disponibilidad tenga un efecto adverso **limitado** en las operaciones de la organización, los activos de esta o las personas.
- El impacto potencial es **moderado** si puede esperarse que la pérdida de confidencialidad, integridad o disponibilidad tenga un efecto adverso **serio** en las operaciones de la organización, los activos de esta o las personas.
- El impacto potencial es **alto** si puede esperarse que la pérdida de confidencialidad, integridad o disponibilidad tenga un **efecto grave o catastrófico** en las operaciones de la organización, los activos de esta o las personas.

La categorización del impacto incide en la rigurosidad de las pruebas en muchos dominios relacionados con la seguridad de la información. Por ejemplo, con respecto a los controles de acceso, las evaluaciones de los riesgos organizacionales (y la tolerancia a ellos) son factores importantes para determinar las políticas y procedimientos de control. Las políticas y procedimientos de control del acceso a un recurso determinado deberían ser acordes al nivel de impacto (es decir, la pérdida de confidencialidad, integridad o disponibilidad) que una violación a la seguridad de ese recurso tendría en la organización.

b. Política de seguridad

La política de seguridad de la organización es el conjunto de leyes, reglas y prácticas que rigen el modo en que ella gestiona, protege y distribuye recursos para lograr los objetivos de seguridad especificados. Estas leyes, reglas y prácticas deben identificar los criterios relativos a la autoridad ejercida por determinadas personas, y pueden especificar aquellas condiciones bajo las cuales se les permite ejercer esa autoridad. Para ser significativas, estas leyes, reglas y prácticas, deben otorgar a las personas una

[70]Federal Information Processing Standards 199, *Standards for Security Categorization of Federal Information and Information Systems*, 2004.

capacidad razonable para determinar si sus acciones violan la política en cuestión o concuerdan con ella.

Remítase a la tabla para ver los elementos recomendados de una política de seguridad de TI.

Elementos de una política de seguridad de TI	Definición de la seguridad de la información – objetivos y alcance (incluida la confidencialidad de los datos)
	Principios de seguridad, normas y requisitos de cumplimiento detallados (por ejemplo, el personal del departamento de TI no debería tener responsabilidades operativas o contables)
	Definición de responsabilidades generales y específicas relativas a todos los aspectos de la seguridad de la información
	Uso de activos de información y acceso al correo electrónico e Internet
	Modo y método de acceso (con inclusión de las políticas de control del acceso y autenticación)
	Procedimientos de respaldo
	Procedimientos para hacer frente a software y programas maliciosos (por ejemplo, monitoreo continuo, detección de intrusiones, y un sistema de prevención de intrusiones)
	Elementos de concienciación y capacitación en materia de seguridad
	Procesos para informar presuntos incidentes de seguridad y responder a ellos
	Planes de continuidad del negocio o actividad
	Gestión de parches
	Seguridad física
	Métodos para comunicar al personal la política y procedimientos adoptados en materia de seguridad de la información

c. Organización de la seguridad de TI

La organización de la seguridad de TI a menudo requiere la implementación de una política de seguridad para una entidad. La responsabilidad por la implementación de la política de seguridad puede asignarse a una unidad o una persona, que posteriormente trabaje con la organización para adquirir herramientas y procesos adecuados para implementar la política de manera eficaz. Una vez implementada la política, la organización sería también responsable por brindar capacitación al personal y responder ante incidentes de seguridad. La organización también precisa asegurarse de que sus datos, a los que acceden organizaciones externas, o que se transfieren a ella, se encuentren debidamente protegidos. Será necesario que el auditor se asegure de que las organizaciones externas estén en condiciones de implementar los requisitos en materia de seguridad.

d. Gestión de operaciones y registros

Es necesario que una organización realice un seguimiento de los procesos y procedimientos utilizados para las operaciones de su negocio o actividad. Esto incluye un conjunto de procedimientos y procesos organizacionales que garantizan la existencia de los procedimientos de documentación y procesamiento de datos correctos para el manejo de medios y datos, procedimientos de emergencia, el mantenimiento de registros de seguridad en redes, y procedimientos de respaldo.

e. Gestión de activos

La gestión de activos, definida en términos amplios, se refiere a cualquier sistema por el que aquellos elementos que son valiosos para una organización se monitorean y mantienen. La gestión de activos es un proceso sistemático de operación, mantenimiento, actualización y eliminación de activos de un modo

eficaz en función de los costos.

En el área de TI, la gestión de activos incluye el mantenimiento de un inventario preciso de equipos, la administración de datos, el conocimiento de las licencias necesarias para la utilización del equipamiento asociado, y el mantenimiento y protección de los equipos (por ejemplo, en espacios cerrados y habitaciones controladas). La gestión de activos de TI también incluye la gestión del software y la documentación de procesos que son valiosos para una organización.

Esta gestión es sumamente importante, dado que una organización puede exponerse a riesgos en el caso de no contar con un inventario completo de sus activos. Sin un inventario completo de sus activos de TI, es imposible que una organización sepa si está aplicando los controles de seguridad adecuados a la totalidad de dichos activos. La falta de un inventario completo de tales activos también puede derivar en complicaciones cuando las organizaciones precisan actualizar su software para satisfacer necesidades futuras del negocio o actividad desarrollados.

f. Seguridad de los recursos humanos

Es necesario que los empleados que administran datos personales en una organización reciban capacitación adecuada en materia de concienciación, además de actualizaciones regulares, en un esfuerzo por salvaguardar los datos que les son encomendados. Es necesario que, para cada descripción laboral se asignen roles y responsabilidades adecuados, en línea con la política de seguridad de la organización. Los datos de la organización deben protegerse del acceso, divulgación, modificación, destrucción o interferencia no autorizados. La gestión de los riesgos relacionados con los recursos humanos y la privacidad es una actividad necesaria durante todas las etapas de la relación laboral con la organización.

Las tres áreas vinculadas con la seguridad de los recursos humanos son:

- **La etapa previa al empleo:** Esto incluye la definición de los roles y responsabilidades del puesto, la definición del acceso adecuado a información sensible relacionada con ese puesto, y la determinación de la profundidad de los niveles de examen de los candidatos –todo de acuerdo con la política de seguridad de TI de la organización. Durante esta etapa también deberían estipularse los términos contractuales.
- **La etapa de empleo:** Los empleados de una organización que tengan acceso a información sensible de ésta deberían recibir recordatorios periódicos de sus responsabilidades, y una capacitación continua y actualizada en materia de concienciación sobre cuestiones de seguridad, para cerciorarse de que comprendan las amenazas actuales y prácticas de seguridad correspondientes para mitigarlas.
- **La conclusión del empleo:** Para evitar el acceso no autorizado a información sensible, el acceso debería revocarse de inmediato a partir del cese de la relación laboral con un empleado en condiciones de acceder a dicha información. Esto también incluye la restitución a la organización de cualquier activo que el empleado tenga en su poder. Durante esta etapa, podría prepararse un formulario especial para documentar toda la labor realizada por el empleado, y asegurarse de que se haya revocado toda forma de acceso y se hayan restituido todos los activos.

Debería disponerse de un programa de concienciación en materia de seguridad por el que se le recuerde a todo el personal los posibles riesgos y consecuencias de la exposición, además de sus responsabilidades como custodios de la información de la organización.

g. Seguridad física y del entorno

La seguridad física se refiere a las medidas concebidas para denegar a personal no autorizado (lo que incluye atacantes o incluso intrusos accidentales) el acceso físico a un edificio, instalación, recurso, o información almacenada. Además, incluye orientación sobre el modo de diseñar estructuras para resistir actos potencialmente hostiles. La seguridad física puede ser tan simple como una puerta cerrada con llave o tan compleja como una multiplicidad de barreras, guardias de seguridad armados y casetas de vigilancia.

La seguridad física consiste principalmente en restringir el acceso físico de personas no autorizadas (comúnmente consideradas intrusos) a instalaciones controladas, aunque existen otras consideraciones y situaciones en las que las medidas de seguridad físicas son valiosas (por ejemplo, la limitación del acceso dentro de una instalación o a activos específicos, y controles del entorno para reducir incidentes físicos, como incendios e inundaciones).

La seguridad inevitablemente implica incurrir en costos y nunca será absoluta; mediante ella se pueden reducir, mas no eliminar por completo los riesgos. Dado que los controles son imperfectos, una seguridad física vigorosa supone la aplicación del principio de defensa en profundidad, utilizando combinaciones adecuadas de controles superpuestos y complementarios. Por ejemplo, los controles del acceso físico a instalaciones protegidas en general persiguen como finalidad:

- disuadir a intrusos potenciales (por ejemplo, mediante carteles de advertencia y señalización de perímetros);
- distinguir entre personas autorizadas y no autorizadas (por ejemplo, mediante pases y llaves);
- demorar, frustrar e idealmente impedir intentos de intrusión (por ejemplo, mediante paredes reforzadas, cerraduras y cajas fuertes);
- detectar intrusiones y monitorear/registrar intrusos (por ejemplo, alarmas para intrusos y sistemas de televisión por circuito cerrado); e
- instrumentar respuestas adecuadas frente a incidentes (por ejemplo, mediante guardias de seguridad y agentes de policía).

Los controles del entorno se aplican principalmente a aquellas instalaciones de una organización que contienen concentraciones de recursos asociados a sistemas (por ejemplo, centros de datos, salas de computadoras del tipo mainframe, salas de servidores y salas de comunicaciones). La insuficiencia de este tipo de controles, especialmente cuando se trata de entornos muy desfavorables, puede tener un impacto substancialmente adverso sobre la disponibilidad de sistemas y componentes necesarios para respaldar la misión y funciones asociadas al negocio o actividad de la organización.

h. Control del acceso

El control del acceso se refiere al ejercicio del control de quiénes pueden interactuar con un recurso. A menudo, pero no siempre, ello supone la participación de una autoridad que se ocupa de ejercer el control. El recurso puede ser un edificio, un grupo de edificios, o sistemas de TI. El control del acceso (ya sea físico o lógico) es, en realidad, un fenómeno cotidiano. La cerradura de la puerta de un automóvil es, esencialmente, una forma simple de control del acceso. El PIN del cajero automático de un banco y los dispositivos biométricos son otras modalidades de control del acceso. Disponer del control del acceso cobra especial relevancia cuando lo que se procura es resguardar equipamiento e información importantes, confidenciales o sensibles. Mediante el control del acceso se garantiza que[71]

- se emitan, gestionen, verifiquen, revoquen y auditen identidades y credenciales para dispositivos, usuarios y procesos autorizados;
- se gestione y proteja el acceso físico a activos;
- se gestione el acceso remoto (si es que la organización lo utiliza);
- se gestionen permisos y autorizaciones de acceso, incorporando los principios del menor privilegio y separación de tareas;[72]

[71]U.S. Government Accountability Office, *Federal Information System Controls Audit Manual*, 2009.

[72]El principio del menor privilegio supone que a cada sujeto se le otorgue el conjunto de privilegios más restrictivo posible para la realización de tareas autorizadas. La aplicación de este principio limita el daño que puede derivar de accidentes, errores o el uso no autorizado de un sistema de información. La separación de tareas es un control básico mediante el que se evitan o detectan errores o irregularidades a través de la asignación de responsabilidades por el inicio de transacciones, su registro, y el registro de la custodia de activos a personas diferentes. Este principio se utiliza

- se protege la integridad de la red (por ejemplo, mediante la segregación y segmentación de redes);
- las identidades se comprueban y vinculan con credenciales, y se afirman en las interacciones; y
- se autentican usuarios, dispositivos y otros activos (por ejemplo, factor único, multifactorial) en consonancia con el riesgo de la transacción (por ejemplo, seguridad y riesgos para la seguridad y privacidad de las personas y otros riesgos organizacionales).

Las evaluaciones del riesgo organizacional y la tolerancia al riesgo son factores importantes para determinar las políticas y procedimientos de control del acceso. Las políticas y procedimientos de control del acceso para un recurso determinado deberían ser acordes al nivel de impacto (es decir, la pérdida de confidencialidad, integridad o disponibilidad) que una violación a la seguridad de ese recurso tendría en la organización.

En un entorno gubernamental, el control del acceso es importante porque numerosas entidades gubernamentales procesan datos sensibles y, por cuestiones de privacidad, se establece un límite a las personas que deberían acceder a diversos elementos de esa información. Mediante el control del acceso se garantiza que solamente los usuarios provistos de las credenciales adecuadas accedan a datos sensibles.

i. Desarrollo, adquisición y mantenimiento de sistemas de TI

Es importante que las organizaciones identifiquen y gestionen los riesgos para la cadena de suministro al desarrollar y adquirir productos y servicios. Las cadenas de suministro comienzan con la obtención de productos y servicios y se extienden desde el diseño, desarrollo, fabricación, procesamiento, manipulación y entrega de productos y servicios hasta el usuario final. Dada la existencia de estas relaciones complejas e interconectadas, **la gestión de riesgos de la cadena de suministro** es una función crítica para la organización. Un objetivo primordial de la gestión de riesgos de la cadena de suministro cibernética es identificar, evaluar y mitigar riesgos relacionados con productos y servicios que contienen funcionalidades potencialmente maliciosas, son falsificaciones o presentan vulnerabilidades originadas en prácticas de fabricación y desarrollo dentro de dicha cadena. Las actividades de gestión de riesgos de la cadena de suministro cibernética incluyen:[73]

- determinar los requisitos en materia de ciberseguridad aplicables a los proveedores;
- estipular los requisitos en materia de ciberseguridad mediante acuerdos formales (por ejemplo, contratos);
- comunicar a los proveedores el modo en que tales exigencias de ciberseguridad se verificarán y validarán;
- verificar que las exigencias en materia de ciberseguridad se satisfagan mediante la aplicación de una diversidad de metodologías de evaluación, lo que incluye informes de centros de operaciones de seguridad, si se dispusiese de ellos; y
- administrar y gestionar tales actividades.

Se requiere un mantenimiento constante luego del desarrollo o la adquisición exitosos de un producto o servicio de TI. El mantenimiento de un sistema de TI durante su ciclo de vida incluye cambios y actualizaciones del sistema (por ejemplo, la instalación de parches) producto de la aplicación de nuevos requisitos, la reparación de errores en el sistema y la realización de mejoras como resultado de nuevas interfaces.

---

habitualmente en grandes organizaciones de TI de modo tal que ninguna persona esté en condiciones de introducir código fraudulento o malicioso sin ser detectada.

[73]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity,* version 1.1, 2018.

Para la instalación de parches, las organizaciones deberían emplear la **gestión de parches**. La gestión de parches es el proceso que consiste en identificar, adquirir, instalar y verificar parches de productos y sistemas. Los parches sirven para corregir problemas de seguridad y funcionalidad en software y firmware. Desde una perspectiva centrada en la seguridad, es muy frecuente que los parches susciten interés, puesto que mitigan vulnerabilidades por defectos del software; la aplicación de parches para la eliminación de estas vulnerabilidades reduce significativamente las oportunidades de explotación de tales vulnerabilidades.[74]

j. Gestión de incidentes y acontecimientos relacionados con la seguridad de TI

Como se menciona en el Capítulo 4 sobre operaciones de TI, la gestión de incidentes abarca los sistemas y prácticas utilizados para determinar si los incidentes o errores se registran, analizan y resuelven de forma oportuna. En los campos de seguridad informática y TI, la gestión de incidentes relacionados con la seguridad implica el monitoreo y la detección de acontecimientos asociados a la seguridad en una computadora o red de computadoras, y la ejecución de respuestas adecuadas a esos acontecimientos. La gestión de incidentes relacionados con la seguridad de TI es una forma especializada de gestión de incidentes.

Las organizaciones deberían establecer procesos, planes y políticas formales de respuesta a incidentes. El proceso típico de respuesta a incidentes está integrado por cuatro etapas:

- **Preparación.** Esta etapa consiste en conformar un equipo de respuesta a incidentes y brindarle capacitación; dotar a la organización de la capacidad de responder a incidentes; y prevenirlos, cerciorándose de que los sistemas, redes y aplicaciones sean lo suficientemente seguros, recurriendo para ello a controles de seguridad basados en los riesgos afrontados por los sistemas de información.
- **Detección y análisis**. Esta etapa implica la detección de incidentes utilizando una diversidad de medios con diferentes niveles de detalle y fidelidad. Dichos medios incluyen sistemas de detección y prevención de intrusiones basados en redes y servidores, software antivirus, analizadores de registros, e informes de usuarios. Una vez detectado un incidente, el equipo de respuesta a incidentes de la organización debería trabajar con prontitud para analizarlo y validarlo, siguiendo un proceso predefinido y documentando de cada paso dado.
- **Contención, erradicación y recuperación.** A partir de la detección, las organizaciones deberían esforzarse por contener el incidente. Una parte esencial de la contención es la toma de decisiones (por ejemplo, apagar un sistema, desconectarlo de una red, y deshabilitar determinadas funciones). Tales decisiones son mucho más sencillas de tomar cuando existen estrategias y procedimientos predeterminados para contener el incidente. La contención del incidente le da a la organización tiempo para elaborar una estrategia de corrección a medida.

  Una vez realizada la contención, tal vez sea necesario proceder a la etapa de erradicación para eliminar determinados componentes vinculados con el incidente, por ejemplo, software malicioso, e inhabilitar cuentas de usuarios que hubiesen sufrido violaciones, además de identificar y mitigar todas las vulnerabilidades explotadas.

  Durante la recuperación, los administradores restauran los sistemas a su operación normal, confirman que funcionan normalmente y (si correspondiente) corrigen vulnerabilidades para evitar incidentes similares. La recuperación puede demandar la aplicación de medidas tales como la restauración de sistemas desde copias de respaldo inalteradas, la reconstrucción total de sistemas, la substitución de archivos afectados por versiones limpias, la instalación de parches, el cambio de contraseñas, y el fortalecimiento del perímetro de seguridad de la red (por ejemplo, mediante conjuntos de reglas para cortafuegos y listas de control de acceso para routers perimetrales).
- **Actividad posterior al incidente**. Luego de resolver un incidente, las organizaciones deberían comunicar la experiencia al personal de TI relacionado, y aprovecharla como una oportunidad de aprendizaje y mejora. Las actividades posteriores a los incidentes incluyen la realización de sesiones

[74]National Institute of Standards and Technology, *Special Publication 800-40, rev. 3: Guide to Enterprise Patch Management Technologies*, 2013.

sobre lecciones aprendidas, la recopilación de datos sobre incidentes, la retención de evidencia, y la revisión de procesos de respuesta a incidentes a partir de las lecciones aprendidas.

k. Gestión de la continuidad del negocio o actividad

La planificación de la continuidad del negocio o actividad es el proceso que una organización utiliza para planificar y poner a prueba la recuperación de los procesos subyacentes a su negocio o actividad tras una alteración. También describe el modo en que una organización continuará funcionando bajo posibles condiciones adversas (por ejemplo, desastres naturales). Remítase al Capítulo 4 para acceder a más información sobre la gestión de la continuidad del negocio.

l. Cumplimiento

El auditor de TI debería revisar y evaluar la observancia de la totalidad de los requisitos internos y externos (por ejemplo, los de orden legal, los relacionados con la calidad de la información y el entorno, aquellos de orden fiduciario y relacionados con la seguridad).

III. Riesgos para la organización auditada

Las políticas y procedimientos relacionados con la seguridad de TI, y su observancia, permiten a una organización proteger su infraestructura de TI de usuarios no autorizados. La política de seguridad de TI de una organización determina las exigencias de alto nivel que ella y sus empleados han de seguir para resguardar activos críticos. También prevé la capacitación del personal sobre cuestiones de seguridad y garantiza la adhesión a procedimientos ya establecidos para el acceso a los datos y su control. Asimismo, la política de TI se refiere a leyes y otras normas que la organización debe observar. Las organizaciones enfrentan muchos obstáculos relativos a la implementación de un sistema de seguridad de la información que sea eficaz. Sin una gobernanza eficaz para afrontar estos obstáculos, será mayor el riesgo de que la organización se vea impedida de lograr sus objetivos relacionados con la seguridad de TI.

Toda organización afronta desafíos singulares, dada la diferencia entre sus circunstancias sociales, ambientales, políticas, geográficas y económicas. Cualquiera de estas circunstancias puede presentar obstáculos para la eficacia de la gobernanza de TI, y es la responsabilidad del auditor de esta especialidad señalar a la dirección de la organización los riesgos vinculados con la seguridad de la información.

Los siguientes son ejemplos de riesgos significativos identificados en la mayoría de las organizaciones:

- divulgación no autorizada de información,
- modificación o destrucción no autorizadas de información,
- ataques a los sistemas de información,
- destrucción de la infraestructura de sistemas de información,
- alteración del acceso a la información o un sistema de información y de su uso,
- alteración del procesamiento efectuado por sistemas de información, y
- hurto de información o datos.

Al evaluar la exposición a riesgos de las organizaciones auditadas, debería prestarse especial atención a los siguientes factores:

- estrategias de seguridad de la información no coincidentes con los requisitos del negocio o actividad o en materia de TI;
- falta de aplicación uniforme de políticas con una observancia dispareja;
- falta de cumplimiento de requisitos internos y externos;
- falta de inclusión de la seguridad de la información en los procesos de desarrollo y mantenimiento de la cartera de proyecto;

- un deficiente diseño de arquitectura, lo que da lugar a soluciones ineficientes o erróneas en lo relativo a soluciones de seguridad de la información;
- falta de idoneidad en las medidas de seguridad física y gestión de activos;
- configuración inadecuada de los sistemas de aplicación para hardware;
- organización deficiente de procesos de seguridad de la información y una estructura de responsabilidad en materia de seguridad de la información indefinida o confusa;
- soluciones inadecuadas en materia de recursos humanos;
- utilización ineficaz de los recursos financieros asignados a la seguridad de la información y falta de concordancia de la estructura de valor de la seguridad de la información (costo/beneficio) con las necesidades u objetivos del negocio; y
- falta de monitoreo o un monitoreo deficiente de la seguridad de la información.

Al realizar una auditoría de seguridad de la información, el auditor debería abordar cuestiones relacionadas con los 12 dominios mencionados previamente al abordar esta cuestión.[75] Asimismo, debería comenzar por evaluar la idoneidad de todos los métodos de evaluación de riesgos, y considerar cuestiones de auditoría relacionadas con la implementación de la seguridad de la información. Una matriz de auditoría ayudará al auditor a determinar las preguntas de auditoría, los criterios de evaluación, la documentación que se solicitará y el análisis técnico que se efectuará. Finalmente, será necesario que el auditor elabore un programa de auditoría detallado según las necesidades detectadas y lo desarrollado durante el trabajo de campo de la auditoría.

IV. Referencias y lecturas adicionales

Cichonski, Paul, Thomas Millar, Tim Grance, and Karen Scarone. NIST Special Publication *800-61, rev 2: Computer Security Incident Handling Guide*. https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final. 2012.

ISACA ITAF. *A Professional Practices Framework for IT Assurance.* USA, 2008.

ISACA. *Risk IT Framework.* https://www.isaca.org/bookstore/bookstore-risk-digital/ritf2. 2020.

ISACA. *COBIT 5 Framework*. https://www.isaca.org/bookstore/cobit-5/wcb5. 2012.

ISACA. *Information Security Audit/Assurance Program.* 2010.

ISACA. *IT Risk Management Audit/Assurance Program*. 2012.

International Organization for Standardization/International Electrotechnical Commission. *ISO/IEC 27000: Information Security Management System*. https://www.iso.org/standard/54534.html. 2013.

International Organization for Standardization/International Electrotechnical Commission. *ISO/IEC 27005: Information Security Risk Management*. https://www.iso.org/standard/75281.html. 2018.

National Institute of Standards and Technology. *Federal Information Processing Standards Publication 199: Standards for Security Categorization of Federal Information and Information Systems*. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf. Febrero de 2004.

National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity,* version 1.1. https://www.nist.gov/cyberframework/framework. 2018.

National Institute of Standards and Technology. *Special Publication 800-40, rev. 3: Guide to*

[75]International Organization for Standardization, *ISO 27000 Series Information Security Management System*.

Enterprise Patch Management Technologies. https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final. 2013.

National Institute of Standards and Technology. *Special Publication 800-39: Managing Information Security Risk: Organization, Mission, and Information System View.* https://csrc.nist.gov/publications/detail/sp/800-39/final. 2011.

Oficina de Rendición de Cuentas del Gobierno de los Estados Unidos. *Federal Information System Controls Audit Manual (FISCAM)*. https://www.gao.gov/products/gao-09-232g. February 2, 2009.

U.S. Government Accountability Office. *Information Security: Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies.* https://www.gao.gov/products/gao-15-758t. July 8, 2015.

U.S. Government Accountability Office. *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks.* GAO-21-171. https://www.gao.gov/products/gao-21-171. December 15, 2020.

CAPÍTULO 8: CONTROLES DE APLICACIÓN

I. ¿Qué son los controles de aplicación?

Como se explicó anteriormente, un control interno es un proceso concebido para brindar una seguridad razonable de que

- operaciones tales como el uso de recursos de la organización, son eficaces y eficientes;
- la elaboración de informes financieros, incluidos los informes sobre ejecución presupuestaria, estados financieros, y otros informes para uso interno y externo, son confiables; y
- se observan las leyes y reglamentos correspondientes.

Los controles de los sistemas de información son aquellos controles internos que dependen del procesamiento de sistemas de información e incluyen controles generales (de toda la organización y a nivel de sistemas), controles de aplicación relativos a los procesos del negocio o actividad de la organización, y controles del usuario dependientes de TI (controles realizados por personas que interactúan con sistemas de información).

Los procesos del negocio o actividad son las funciones principales llevadas a cabo por una organización para llevar a cabo su misión. Una aplicación para este tipo de procesos es una combinación de hardware y software que se usa para procesar información del negocio o actividad en apoyo de un proceso específico. Puede incluir tanto procedimientos manuales como informatizados para la creación de transacciones, el procesamiento de datos, el mantenimiento de registros y la elaboración de informes. Cada organización puede disponer de un conjunto de aplicaciones en funcionamiento, que varían en su tamaño desde sistemas que cubren la totalidad de la empresa, a los que acceden todos los empleados, a una aplicación cliente pequeña, a la que accede un único empleado. El software de aplicación puede consistir en un sistema de nóminas salariales, un sistema de facturación, un sistema de gestión de inventarios, o un sistema integrado para la planificación de los recursos de una organización.

Los controles de aplicación de los procesos del negocio o actividad, a los que habitualmente se hace referencia como controles de **aplicación**, son **controles** específicos exclusivos de cada aplicación de TI. Cuando los procesos del negocio o actividad se automatizan en una aplicación de TI, las reglas de ese negocio o actividad se incorporan a la aplicación bajo el formato de controles de aplicación. Ellos operan sobre segmentos de una aplicación y se relacionan tanto con transacciones como con datos existentes. Los controles de aplicación son aquellos que se ocupan de la completitud, exactitud, validez, confiabilidad y disponibilidad de las transacciones y datos durante el procesamiento de aplicaciones.

- Los **controles de completitud** deberían brindar una seguridad razonable de que todas las transacciones ocurridas se ingresan en el sistema, se aceptan para su procesamiento, se procesan una vez y solamente una vez en el sistema, y se incorporan adecuadamente a los datos de salida.
- Los **controles de exactitud** deberían brindar, por ejemplo, una seguridad razonable de que las transacciones se registran debidamente, con las cantidades/datos correctos y de manera oportuna.
- Los **controles de validez** deberían brindar una seguridad razonable de que (1) todas las transacciones registradas efectivamente sucedieron, se relacionan con la organización y se aprobaron debidamente de acuerdo con lo autorizado por la dirección; y (2) solamente se generan datos de salida válidos.
- Los **controles de confidencialidad** deberían brindar una seguridad razonable de que los datos e informes de aplicaciones y otros elementos de salida se encuentran protegidos de accesos no autorizados.
- Los **controles de disponibilidad** deberían brindar una seguridad razonable de que los datos e informes de aplicaciones, y demás información relevante del negocio o actividad, se encuentran inmediatamente a disposición de los usuarios cuando se los precisa.

Una revisión de controles de aplicación permite al auditor ofrecer a la dirección una evaluación

independiente de la eficiencia y eficacia de los controles internos y los procedimientos operativos relacionados con la automatización de un proceso propio del negocio o actividad, e identificar cuestiones relacionadas con aplicaciones que demandan atención. Aunque los controles generales de TI dentro de una organización sientan la pauta del entorno de control general de los sistemas de información, los controles de aplicación se incorporan a determinadas aplicaciones para garantizar y proteger la exactitud, integridad y confidencialidad de la información. Por ejemplo, permiten cerciorarse de que el inicio de transacciones se encuentre debidamente autorizado, y que se procesen, registren completamente e informen de manera exacta datos de entrada válidos. Los controles generales contribuyen a asegurarse de que la labor realizada para implementar un control de aplicación sea proporcional al riesgo de su fracaso; por ejemplo, la probabilidad de que personas no autorizadas accedan a una configuración crítica para un control de aplicación, o que tal configuración sea modificada sin autorización, o sin haberse realizado las pruebas correspondientes.

Dado que los controles de aplicación se relacionan estrechamente con transacciones individuales, el hecho de someterlos a pruebas brinda al auditor seguridad acerca de la exactitud de una funcionalidad determinada, de forma más directa. Por ejemplo, poner a prueba los controles de una aplicación de nóminas salariales brindaría seguridad acerca de las cifras que constan en la nómina correspondiente a las cuentas de un cliente. Debido a la mayor amplitud de su alcance, el hecho de poner a prueba los controles generales de TI del cliente (como los procedimientos de control de cambios) tal vez no brinden un nivel similar de seguridad para el mismo saldo de cuenta.

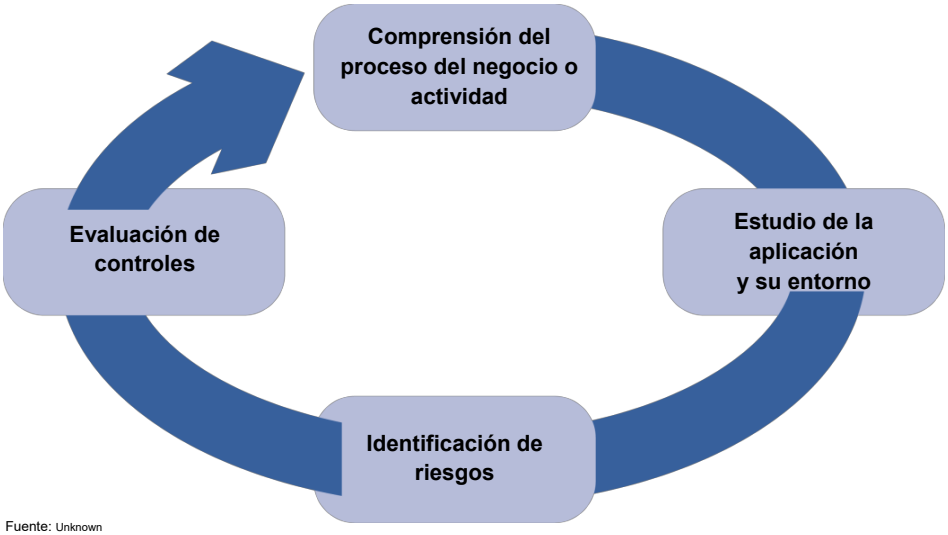
En función de los objetivos específicos de la auditoría, pueden aplicarse diferentes enfoques para la revisión de los controles de aplicación y la realización de pruebas sobre ellos. Por ejemplo, la revisión podría centrarse en la observancia de las leyes y normas correspondientes, en cuyo caso, el objetivo sería verificar si los controles de aplicación ofrecen la ayuda adecuada para abordar estas cuestiones. En su defecto, la revisión de aplicaciones podría formar parte de una auditoría de desempeño, en cuyo caso, sería importante comprobar el modo en que las reglas del negocio o actividad se traducen en la aplicación. Durante un análisis de seguridad de la información, el foco podría centrarse en los controles de aplicación responsables por el aseguramiento de la confidencialidad, integridad y disponibilidad de los datos.

a. Proceso de revisión de los controles de aplicación

Los pasos por seguir para la revisión de controles de aplicación suponen una serie de actividades de carácter cíclico. En la Figura 10 se presentan los pasos comunes del ciclo de revisión de los controles de aplicación. Aunque, como se señala mediante la flecha, lo intuitivo es comenzar por comprender más ampliamente el proceso del negocio o actividad, es importante destacar que no existe un orden jerárquico estricto en estos pasos.

Luego de la figura se presenta una descripción breve de las cuatro etapas.

Figura 10: Ciclo de revisión de la aplicación



Fuente: Unknown

i. Comprensión del proceso del negocio o actividad:

Para explorar cuestiones técnicas vinculadas con la aplicación, es útil contar en primer lugar con una reseña de los procesos del negocio o actividad automatizados por la aplicación: sus reglas, flujos, actores, roles, y requisitos de cumplimiento relacionados. La comprensión de los procesos del negocio o actividad constituye un paso importante para poder verificar la solidez de los controles de aplicación y procesos automatizados. Las actividades que forman parte de este paso variarán de acuerdo con el objetivo de la auditoría. Esto habitualmente se realiza mediante el estudio de los procedimientos operativos y de trabajo, el organigrama de procesos, u otro material de referencia. También podría ser necesario que el equipo de auditoría se reúna con directivos de la organización, ejecutivos de TI y usuarios de aplicaciones clave. Al equipo de auditoría también podría resultarle conveniente elaborar sus propios diagramas de flujo y señalar los procesos, controles, sistemas, interfaces e informes que constituyen el proceso. Los diagramas de flujo generados por el equipo de auditoría pueden ser útiles, puesto que, a menudo, los flujos de proceso propios de los clientes son o bien demasiado complejos y detallados, o no presentan el grado de detalle suficiente como para permitir su comprensión y la identificación de los aspectos y riesgos relevantes del proceso en cuestión.

ii. Estudio de la aplicación y su entorno:

Luego de ponerse al corriente del proceso del negocio o actividad, el auditor debería lograr comprender las redes y sistemas específicos que se utilizan para respaldar aplicaciones clave de dicho proceso. La información obtenida durante este paso es importante para contribuir a la identificación de puntos de control críticos y brindar un sustento que permita comprender dónde se aplican los controles a nivel de aplicación. Las actividades de este paso incluyen una revisión de la documentación (por ejemplo, organigramas, diagramas de flujos de datos y manuales del usuario); entrevistar a personal clave; realizar estudios de funciones clave del software en operación mediante la observación e interacción con el personal mientras se lo utiliza; y a través de discusiones y la realización de recorridas del proceso o aplicación del negocio o actividad desde el ingreso en la fuente hasta los datos de salida y su conciliación para comprobar el modo en que los procesos fluyen efectivamente. Estos pasos también permiten al auditor observar cualesquiera actividades manuales asociadas que pudiesen actuar como controles complementarios.

Los auditores también pueden obtener documentación sobre infraestructura técnica (por ejemplo, sistemas operativos; entornos de red; sistemas de gestión de bases de datos; interfaces con otras aplicaciones creadas internamente o externalizadas; y procesamiento de transacciones en línea, en tiempo real y

mediante ingreso por lotes), que pueden analizar con directivos, operadores y desarrolladores. Estos análisis y la documentación correspondiente pueden ser un indicador útil del modo en que la infraestructura incide en la aplicación.

iii. Identificación de riesgos

Sobre la base de los conocimientos obtenidos por el auditor durante los pasos previos, ese auditor debería evaluar, de forma preliminar, la naturaleza y el grado del riesgo asociado a sistemas de información relacionados con aplicaciones clave. El objetivo de este paso es identificar los riesgos asociados con la actividad/función del negocio o actividad a la que sirve la aplicación, para determinar qué podría funcionar mal, y observar el modo en que estos riesgos se afrontan mediante los controles incorporados al software de aplicación. Tal vez ya se disponga de una evaluación de riesgos del proceso del negocio o aplicación realizada previamente mediante una auditoría o revisión de la dirección. El auditor puede aprovecharla una vez determinada confianza de la evaluación de riesgos existente.

iv. Comprensión y evaluación de los controles:

Dentro de cada aplicación clave del proceso del negocio o actividad, el auditor debería llegar a comprender los tipos específicos de controles a nivel de aplicación que son relevantes para los objetivos de la auditoría. Una vez al tanto del entorno (tanto técnico como del negocio o actividad) que rodea a la aplicación, el auditor estará en mejores condiciones de evaluar los controles utilizados para abordar los riesgos existentes. El auditor deberá recurrir a su juicio al evaluar los controles de aplicación y considerar los costos y beneficios al proponer recomendaciones para la realización de mejoras. Por ejemplo, el exceso de detalles en los registros de transacciones puede derivar en un aumento de los gastos generales, y no proporcionar las pistas deseadas. Esta evaluación supone un examen de los controles de aplicación, en concordancia con lo descrito en la siguiente sección. Además, el auditor puede determinar que existe más de un control mitigando el mismo riesgo, lo que podría dar lugar a una recomendación de mejora del proceso para el cliente.

b. Ilustración

La Figura 11 contiene elementos propios de controles de aplicación, a modo ilustrativo. En una aplicación para pagos en línea, una condición para el ingreso de datos consistiría, por ejemplo, en que la fecha de vencimiento de la tarjeta de crédito sea posterior a la fecha de la transacción. Otra sería que el número de la tarjeta sea válido y coincida tanto con el nombre y apellido de su titular como con el valor de verificación (el número CVV), de acuerdo con los datos que constan en la base de datos del emisor de la tarjeta. Una condición adicional sería que los detalles transmitidos a través de la red sean encriptados. Controles como los incorporados a la aplicación garantizarían la inviolabilidad de las condiciones establecidas y permitirían una mejor validación de las transacciones.

Figura 11: Ejemplo de controles de aplicación

Fuente: Unknown

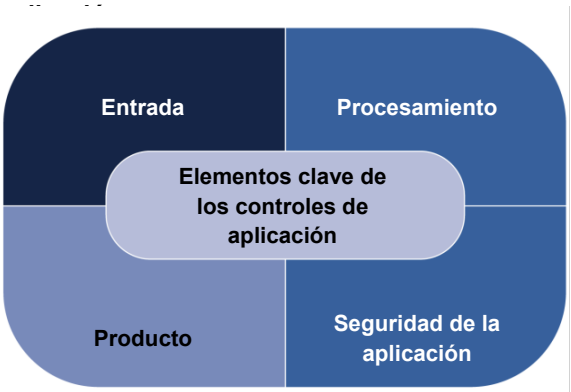
Además de los controles automatizados, como los señalados previamente, los controles de aplicación también incluyen procedimientos manuales que complementan una aplicación. Estos controles no solo forman parte de aplicaciones específicas, sino que además rodean a los procesos del negocio o actividad. Por ejemplo, un empleado de *data entry* puede exigir la firma (aprobación) de un formulario de ingresos de datos antes de su incorporación a la aplicación. La combinación seleccionada de controles manuales y automatizados a menudo responde a consideraciones vinculadas con costos y controles presentes al diseñarse inicialmente una aplicación.

II. Elementos clave de los controles de aplicación

Una aplicación puede dividirse en los siguientes segmentos primarios: entrada de datos (origen e ingreso de datos); procesamiento de transacciones; salida de datos (distribución de resultados) y seguridad (registro, comunicaciones, almacenamiento). Los controles de una aplicación se encuentran incorporados a cada segmento de ella, además de controles que restringen el acceso a la aplicación archivos maestros.

Aunque no es realista brindar pasos de prueba y listas de control detallados para cada permutación posible de una aplicación, un auditor debe estar al corriente de conceptos de control que son comunes para casi todas las aplicaciones y procesos de negocios. La comprensión de estos controles de aplicación comunes puede utilizarse

Figura 12: Elementos clave de los controles de

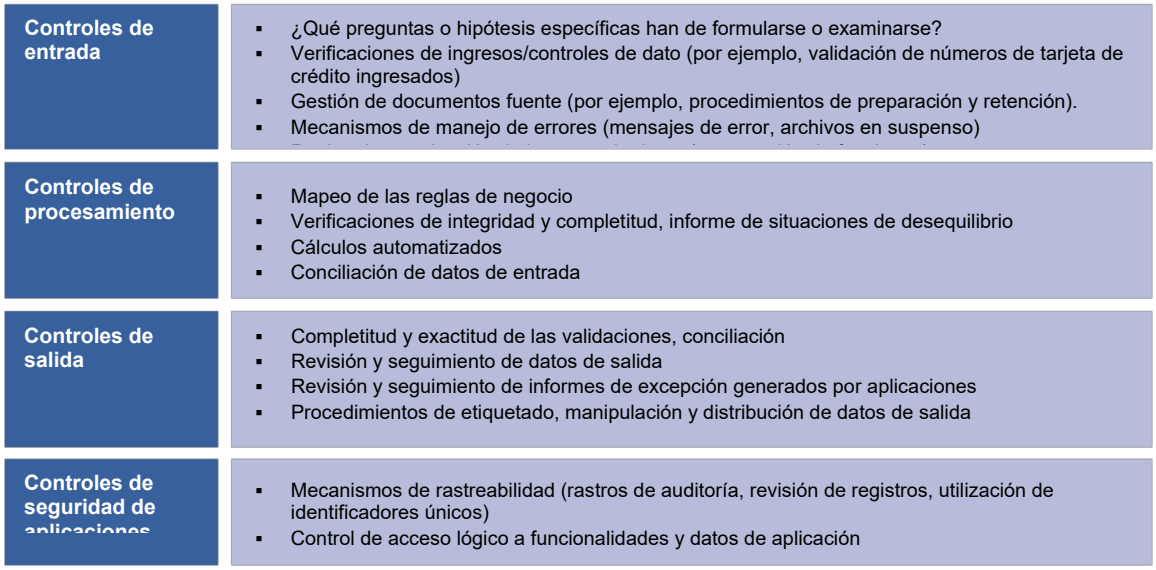


Fuente: Unknown

para generar pensamientos e ideas relacionadas con pasos de prueba de auditoría más específicos para la aplicación que se está auditando.

Algunos de los elementos de control más comunes para cada una de las cuatro áreas clave se muestran en la Figura 13:

Figura 13: Ejemplos de controles de aplicación



Fuente: Unknown

A. Controles de datos de entrada

Los objetivos de los controles de datos de entrada consisten en validad y autenticar los actos de preparación, autorización e ingreso de datos fuente de forma tal que la aplicación acepte de manera puntual datos confiables, exactos y confiables. Mientras que la entrada de datos puede realizar de forma manual o mediante una interfaz, los errores y omisiones pueden minimizarse a través de un buen método de entrada de datos desde el diseño, una adecuada segregación de tareas respecto al origen y aprobación de documentos de entrada, y la instrumentación de controles adecuados de autenticidad, exactitud y completitud (con opciones en un menú o mensajes interactivos). En la siguiente table se enumeran los elementos clave del control datos de entrada.

Elementos del control de entrada de datos	Descripción
Verificaciones del ingreso de datos (validez, completitud, verificación de duplicaciones)	Verificaciones automáticas de la validez respecto a los datos ingresados (por ejemplo, la fecha del viaje excede el período de apertura de reservas); completitud de las verificaciones para asegurarse de que se ha ingresado toda la información clave de la transacción (por ejemplo, las fechas del viaje, los nombres y apellidos de los pasajeros y los números de documentos de identidad son campos obligatorios); comparación entre transacciones nuevas y transacciones previamente para evitar duplicaciones (por ejemplo, verificación de facturas duplicadas); asegurarse de que las entradas de datos que excedan los parámetros determinados por la dirección generen un error.
Gestión de los documentos fuente	Documentación de procedimientos de preparación de documentos fuente, lo que incluye una estrategia definida sobre datos de transacción y procedimientos de retención de documentos; los documentos fuente para las entradas de datos se encuentran registrados y son rastreables; los documentos fuente deberían

	proporcionar códigos de entrada predeterminados para reducir errores e incluir una parte para la autorización de documentos.
Procedimientos de administración de errores	Existen procedimientos para tratar datos de entrada rechazados (por ejemplo, mediante el uso de mensajes de error adecuados, indicaciones que permitan el reingreso de los datos de entrada, y uso de datos en suspenso); los errores se investigan y se toman medidas de corrección posteriores.
Autorización de entrada de datos	En el formulario de ingreso de datos se requiere la aplicación de procedimientos manuales y autorización de un supervisor (por ejemplo, la autorización de una declaración de ingreso otorgada por supervisor antes de su ingreso por un empleado de *data entry* para el procesamiento en solicitudes aduaneras); para la entrada de datos se siguen procedimientos de aprobación.

b. Controles de procesamiento

El objetivo de las medidas de control de procesamiento es procurar la protección de la integridad, validez y confiabilidad de los datos y protegerse de errores de procesamiento durante la totalidad del ciclo de procesamiento de transacciones –desde el momento en que los datos son recibidos desde el subsistema de entrada hasta el momento en que ellos son despachados hasta al subsistema de base de datos, comunicación, o salida. También se pretende asegurar de que los datos de entrada válidos se procesen solamente una vez y que la detección de transacciones erróneas no altere el procesamiento de transacciones válidas. Al actuar de ese modo, lo que se procura es mejorar la confiabilidad de las aplicaciones que ejecutan las instrucciones para satisfacer determinados requisitos de losusuarios.

Los procedimientos de control en esta área también incluyen el establecimiento e implementación de mecanismos para autorizar el inicio del procesamiento de transacciones, cerciorándose de que solamente se utilizan aplicaciones y herramientas adecuadas y autorizadas, y la verificación rutinaria de que el procesamiento se realice de manera completa y precisa, con controles automatizados, cuando corresponda. Los controles pueden incluyen la verificación de errores de secuencia y duplicación o desbordamiento de buffers, monitoreo de transacciones/conteos de registros, realización de verificaciones de integridad y verificaciones de rango referenciales, y comparaciones de totales de control y *hash totals*.

En los sistemas en tiempo real se utilizan otros controles compensatorios, como las verificaciones uno por uno, procesamiento por lotes, reportes de excepciones, y reportes de cuentas en suspenso. En la tabla se enumeran los elementos clave de los controles de procesamiento.

Elementos del control de procesamiento	Descripción
Mapeo de las reglas de negocio	Inspeccionar las configuraciones para asegurarse de que las transacciones se ejecuten de acuerdo con determinados parámetros y tolerancias, específicas de la gestión de riesgos de una organización. Documentar parámetros y tolerancias y hacer que la dirección revise regularmente las restricciones resultantes. Asegúrese de que las transacciones concuerden con las autorizaciones de las autorizaciones de la dirección.
Verificaciones de integridad y completitud	Inspeccionar una selección de registros de sistemas para observar transacciones. Determinar si las aplicaciones realizan los controles de edición y validación adecuados en función de los datos procesados, generan mensajes de error o rechazos, y comunican adecuadamente los errores de procesamiento a los usuarios.
Cálculos automatizados	Determinar en qué medida el procesamiento de aplicación de los datos se encuentra automatizado y estandarizado. Inspeccionar el procesamiento de apoyo de la documentación de diseño y verificar que se están utilizando las versiones adecuadas de las aplicaciones y los datos.

Conciliación de datos de entrada	Inspeccione procedimientos de conciliación periódicos para determinar si las conciliaciones se realizan y documentan, realizando inspecciones adicionales para hallar evidencia de respaldo adecuada. Determinar si el sistema se encuentra configurado para auto equilibrarse, toda vez que ello sea posible.

c. Controles de los datos de salida

Los objetivos de los controles de los datos de salida son medidas incorporadas a la aplicación para garantizar que los datos de salida de la transacción se distribuyan de forma completa, precisa y correcta. Lo que se procura mediante ellos también es proteger datos procesados por una aplicación de su modificación y distribución no autorizadas.

Los procesos de control incluyen una definición adecuadas de datos de salida, reportes deseados en la etapa de diseño y desarrollo del sistema, la documentación adecuada de la lógica de extracción de reportes, controles que limitan el acceso a los datos procesados, revisión de datos de salida, conciliación, y revisión. En la siguiente tabla se enumeran los elementos clave de los controles de los datos de salida.

Elementos del control de los datos de salida	Descripción
Verificaciones de integridad para comprobar la completitud y exactitud	Realización de verificaciones de integridad de datos mediante la conciliación de datos de entrada con datos de salida de procesos para comprobar la exactitud y completitud, según los procedimientos documentados. Revisión de los datos de salida para comprobar su aceptabilidad y completitud incluyendo totales de control y registros de errores. Revisión del volumen, valor y tipo de los datos de salida en relación con las expectativas.
Revisión, seguimiento y rastreo de los datos de salida, incluidos los resultados procesados.	Inspección de los procedimientos de gestión para definir y datos de salida o reportes en relación con las necesidades de los usuarios finales. Inspección de los reportes del rastreo de los resultados de procesamiento, el contenido y oportunidad de las revisiones de los resultados procesados a cargo de la dirección, y el grado en que la dirección monitorea anulaciones aplicadas a transacciones. Revisión y seguimiento de informes de excepción generados por aplicaciones. Examen de los informes de salida para verificar el cumplimiento con las leyes y reglamentos correspondientes.
Etiquetado, administración, distribución y retención de datos de salida	Inspección de procedimientos implementados para monitorear los datos de salida en los informes de la dirección u otras comunicaciones externas e inspección de datos seleccionados de estas comunicaciones. Corroboración de que el acceso de los usuarios a datos de salida se encuentre alineado con su rol.

d. Controles de seguridad de aplicaciones

La seguridad de aplicaciones se relaciona con el mantenimiento de la confidencialidad, la integridad y la disponibilidad de información a nivel de aplicación. A los efectos de una auditoría de la seguridad de aplicaciones, es importante comprender las interfaces (es decir las diferentes fuentes de datos de entrada en la aplicación y los datos de salida de ésta), así como también la forma en que los datos se almacenan.

A la mayoría de las aplicaciones se accede mediante identificaciones de usuario individuales y contraseñas. Sin embargo, otras formas de acceso han alcanzado una gran difusión debido a la magnitud de las aplicaciones utilizadas en un entorno organizacional. Por lo tanto, el diseño de las aplicaciones destinadas a la administración de cuentas y acceso de usuarios debería comprenderse desde un comienzo. Por ejemplo, tal vez sea necesario que un auditor examine las políticas y procedimientos de una organización para la obtención y revocación del acceso de usuarios, de modo tal de comprender las reglas de acceso utilizadas por la aplicación. El acceso de usuarios puede administrarse localmente, a

través de la aplicación, o recurriendo a múltiples sistemas relacionados que abarcan la totalidad de la organización, utilizando un único mecanismo de inicio de sesión.[76]

Para poder comprender los procedimientos de control de seguridad de aplicaciones, también es necesario que el auditor comprenda los actores, roles y responsabilidades que esa aplicación involucra, por ejemplo, administradores, usuarios dotados de determinadas facultades o privilegios, y usuarios regulares. Los métodos de control de acceso a aplicaciones pueden variar, e incluir un modelo estándar de identificación del usuario y contraseña, el uso de certificados digitales para la identificación afirmativa de un usuario,[77] la utilización de tokens o información biométrica,[78] y la aplicación de múltiples métodos de autenticación bifactorial o multifactorial.[79] El acceso puede ser controlado para cada módulo, opción de menú o pantalla en una aplicación, o mediante objetos y roles. El auditor de TI debería revisar el diseño del módulo de control de acceso, teniendo en cuenta la criticidad de las funciones/acciones disponibles.

Algunos ejemplos de cuestiones auditables en relación con los controles de seguridad de aplicaciones son:

- **Examen del monitoreo de auditoría y la gestión de configuración.** Este examen incluye la rastreabilidad de transacciones, como el registro de transacciones y el registro de pistas de auditoría; informes y monitoreo de registros; control de los movimientos de programas, datos y bibliotecas de programas, y el acceso a ellos; y utilización de identificaciones y roles de usuario exclusivos para la realización de cambios. Idealmente, en un registro de rastro de auditoría debería constar qué registros o campos se modificaron, cuándo se modificaron, de qué a qué, y quién realizó la modificación.
- **Examen de controles de acceso**. Este examen incluye una revisión de cuentas del usuarios, permisos y políticas de gestión de contraseñas; uso de cuentas para huésped, de prueba y genéricas; uso de cuentas privilegiadas y del administrador y controles compensatorios; procedimientos para el otorgamiento y revocación del acceso; procedimientos de cese en el puesto y baja del acceso; adopción del principio del menor privilegio; acceso por parte del equipo de TI/desarrollo a bases de datos de producción; procedimientos formales para aprobar y otorgar accesos; uso de contraseñas sólidas; cumplimiento de cambios periódicos y encriptado de contraseñas.
- **Control de la configuración y el mantenimiento de datos maestros.** Los datos maestros constituyen información clave compartida entre múltiples funciones de aplicación. Los controles incluyen la inspección de la configuración de datos correspondiente a campos clave; asegurarse de que las modificaciones de datos existentes se autorizan y llevan a cabo según las reglas relativas a las modificaciones de datos; que los datos permanentes son actualizados y exactos, y congruentes en todos los sectores de la organización; y que se mantiene la integridad y confidencialidad de los datos maestros. Algunos ejemplos de datos permanentes se relacionan con la información sobre proveedores y clientes (nombre y apellido, domicilio, teléfono, número de cuenta); tasas de inflación; datos de administración del sistema, como archivos con contraseñas y permisos de control de acceso.
- **Segregación del acceso de los usuarios.** El acceso por parte de los usuarios debería segregarse cuando se trata de transacciones y actividades que son incompatibles, y dicho acceso monitorearse mediante procedimientos operativos formales, supervisión y revisión.
- **Planificación de contingencias.** Esta planificación incluye evaluar la criticidad y sensibilidad de la aplicación, evaluar los pasos necesarios para prevenir y minimizar daños o interrupciones potenciales de la aplicación, y evaluar la planificación de contingencias de la organización en su conjunto.

---

[76]El inicio de sesión único permite a un usuario utilizar un conjunto de credenciales de registro de inicio de sesión para acceder a múltiples aplicaciones.

[77]Las certificaciones digitales son creadas por una fuente confiable para brindar seguridad sobre la identificación de una persona.

[78]Las aplicaciones biométricas se utilizan para identificar personas sobre la base de características anatómicas, fisiológicas y conductuales mensurables.

[79]La autenticación multifactorial supone la existencia de, por lo menos, dos tipos diferentes de elementos de autenticación para acceder.

III. Sistemas de control de interfaz y gestión de datos

Además de los controles de aplicación de procesos de negocio mencionados, los controles de interfaz y gestión de datos desempeñan un rol suplementario en garantizar que las aplicaciones funcionen adecuadamente.

a. Controles de interfaz

Los controles de interfaz inciden en el modo en que las aplicaciones utilizadas en los procesos del negocio o actividad se interrelacionan mediante interfaces. Se trata de aquellos controles que sobre: a) el procesamiento oportuno, exacto y completo de información entre aplicaciones y otros sistemas de alimentación y recepción de forma continua, y b) la migración completa y exacta de datos limpios durante una conversión. Las interfaces dan como resultado el intercambio estructurado de datos entre dos aplicaciones informáticas. Estas aplicaciones residen en el mismo o en diferentes sistemas informáticos, que a su vez pueden residir en el mismo entorno físico o no. La naturaleza de las interfaces es periódica y recurrente.

Los objetivos de los controles de interfaz son implementar una estrategia y un diseño eficaces, además de procedimientos de procesamiento que garanticen que las interfaces se procesen de forma completa y exacta, los errores se corrijan, que el acceso los datos y procesos de la interfaz se restrinjan adecuadamente, y que los datos sean confiables y se obtengan solamente de fuentes autorizadas. En la medida en que se obtengan datos de entrada de otras aplicaciones, la evaluación de estos datos por parte del auditor debería coordinarse con los controles de datos de entrada enumerados previamente.

b. Controles de gestión de datos

Las aplicaciones que respaldan procesos de negocio habitualmente generan, acumulan, procesan, almacenan, comunican y exhiben datos. Las aplicaciones que administran volúmenes de datos significativos a menudo emplean sistemas de gestión de datos para realizar determinadas funciones de procesamiento de datos dentro de una aplicación. Los sistemas de gestión de datos utilizan software especializado, que puede operar con hardware especializado. Los sistemas de gestión de datos incluyen sistema de gestión de bases de datos, software especializado para transporte/comunicación de datos (a menudo conocido como middleware), criptografía utilizada juntamente con controles de integridad de datos, software de almacenamiento de datos y software para información y extracción de datos. Muchos de los controles de ingreso y procesamiento de datos, como las verificaciones edición, las verificaciones de existencia y los umbrales descritos en secciones anteriores, se implementan en funciones de los sistemas de gestión de datos. A estos tipos de control de datos implementados en los sistemas de gestión de datos a menudo se los denomina reglas del negocio (o actividad).

Al evaluar la eficacia de los controles de aplicación, el auditor debería evaluar las funciones de los sistemas de gestión de datos específicas de los procesos del negocio o actividad bajo examen, además de los controles generales. En la mayoría de las aplicaciones de gran escala y/o alto rendimiento, diversos componentes de los sistemas de gestión de datos se alojan en diferentes servidores, que a menudo utilizan diversos sistemas operativos y tecnologías de hardware. El auditor debería lograr comprender las distintas combinaciones entre tecnologías de gestión de datos y considerar adecuadamente los riesgos relacionados.

La comprensión del diseño lógico y la arquitectura física de los componentes de gestión de datos de la aplicación es un requisito para que el auditor evalúe adecuadamente el riesgo. Además de respaldar las funciones de almacenamiento y recuperación, es habitual que las aplicaciones utilicen sistemas de gestión de datos para respaldar aspectos operativos de la aplicación, como la gestión de los datos de estado transitorio de sesiones de usuarios, registros de auditoría transaccionales y otras funciones que son esenciales para la operación de la aplicación. Los controles asociados con estos tipos de funciones pueden ser críticos para la seguridad de la aplicación.

Los controles en un sistema de gestión de datos deberían incluir consideraciones acerca de rutas de acceso al sistema de gestión de datos. En general el acceso al sistema de gestión de datos puede obtenerse directamente, mediante rutas acceso facilitadas por la aplicación, o a través del sistema operativo subyacente al sistema de gestión de bases de datos.

Los sistemas de gestión de datos poseen cuentas incorporadas privilegiadas que se utilizan para administrar y mantener dichos sistemas. El objetivo del auditor es determinar si se dispone de controles adecuados para proteger estas cuentas privilegiadas. Además de las cuentas privilegiadas, el auditor debería lograr comprender el rol que el sistema de gestión de datos desempeña y las tareas de autenticación y autorización para la aplicación.

IV. Riesgos para la organización auditada

Las consecuencias de las fallas en controles de aplicación habitualmente dependerán de la naturaleza de la aplicación de negocio. Los riesgos pueden variar desde la falta de satisfacción del usuario a desastres reales y pérdida de vidas. Por ejemplo, una organización podría perder participación de mercado si un servicio se encontrase indisponible; o podría perder dinero si sus sistemas de ventas en línea perdiesen órdenes de compra; la confianza de los ciudadanos en los servicios provistos por el gobierno puede descender; la ausencia de cumplimiento con las normas legales puede derivar en acciones judiciales; el suministro eléctrico podría no llegar a los hogares de la gente; y cuentas bancarias podrían verse expuestas a la comisión de fraude.

Específicamente, en ausencia de controles de entrada adecuados, las organizaciones corren el riesgo de que se produzcan casos de procesamiento erróneo o fraudulento, y que la aplicación no cumple con los objetivos del negocio o actividad. Si esto sucediese, los datos procesados por la aplicación podrían resultar incongruentes y los programas generarán datos de salida inadecuados. Asimismo, es posible que, en situaciones muy específicas, se invaliden controles de sistemas. En este caso, debe haber controles compensatorios, como registros y reglas de autorización; caso contrario, el privilegio de invalidación puede utilizarse de manera errónea y conducir al ingreso en la aplicación de datos incongruentes.

La gestión de documentos fuente o la evitación del ingreso de datos inapropiados también son controles de entrada importantes para mitigar los riesgos que una organización afronta. En ausencia de una gestión adecuada de documentos fuente, tal vez resulte imposible rastrear la fuente de la información en el sistema, podría malograrse el cumplimiento normativo, y es posible que se infrinjan las políticas de conservación, lo que conduciría al ingreso de datos no confiables en la aplicación. Por el contrario, de no mediar controles de autorización, los datos no autorizados podrían derivar en errores o fraude.

Las fallas en los controles de procesamiento pueden derivar en errores de procesamiento, y conducir a que la aplicación incumpla los objetivos del negocio o actividad. Estas fallas pueden surgir de un mapeo incorrecto de las reglas del negocio o actividad, pruebas inadecuadas de códigos de programa, o un control inadecuado de diferentes versiones de programas para restaurar la integridad del procesamiento tras la producción de un problema o una interrupción inesperada. En ausencia de las prácticas de control de procesamiento necesarias, podría repetirse transacciones erróneas, lo que afectaría los objetivos y la buena reputación del negocio o actividad.

Algunas de las medidas de control no se encuentran disponibles en sistemas de procesamiento en tiempo real. Por ejemplo, cuando se efectúa la conciliación de lotes totales de entrada y salida, o la retención de determinados documentos de originación de datos para mantener un registro de pistas de auditoría. Sin embargo, los sistemas en tiempo real incluyen otros controles compensatorios dentro de la aplicación, entre ellos, la completitud de datos operativos, peticiones de validación y registro de intentos de acceso.

La falta de controles de salida adecuados conduce al riesgo de modificación o supresión no autorizadas de datos, la creación de informes de gestión erróneamente personalizados, y violaciones de la confidencialidad de los datos. Asimismo, la generación de datos de salida erróneos dependerá en gran medida de la forma en que el negocio utiliza la información.

En el contexto de la seguridad de una aplicación, la insuficiencia de mecanismos de registro puede imposibilitar la atribución de conductas indebidas a sus autores específicos. Asimismo, la conciencia de los usuarios acerca de la existencia de procedimientos de revisión de registros y mecanismos de información puede mitigar el riesgo de uso indebido de los sistemas de información. Los errores relacionados con datos permanentes tienen consecuencias importantes para la aplicación, dado que estos datos podrían utilizarse para una proporción muy grande de las transacciones de la aplicación.

En términos más generales, la utilización insuficiente de controles sobre la seguridad de la información puede derivar en riesgos con diversos grados de seriedad, lo que incluye la pérdida de ingresos, alteraciones del servicio, pérdida de credibilidad, interrupción del negocio, uso indebido de la información, consecuencias legales, acciones judiciales, y uso indebido de elementos sujetos a derechos de propiedad intelectual. Estos riesgos y los controles de mitigación se cubren con mayor detalle en el Capítulo 7 sobre seguridad de la información.

IV. Referencias y lecturas adicionales

Davis, Chris, Mike Schiller and Kevin Wheeler. *IT Auditing: Using Controls to Protect Information Assets*, 2nd ed. January 31, 2011.

ISACA. *IT Audit and Assurance Guideline G38, Access Controls.* 2007.

National Institute of Standards and Technology. *Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations,* rev. 5. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final. September 2020.

Office of the Comptroller & Auditor General of India. *Manual of Information Technology Audit,* vol. I. https://ag.ap.nic.in/GSSA/PDF_Files/ITAM Vol_I.pdf.

U.S. Government Accountability Office. *Federal Information Systems Audit Manual (FISCAM).* https://www.gao.gov/products/gao-09-232g. February 2, 2009.