GTAG

GUÍA DE AUDITORÍA DE TECNOLOGÍA GLOBAL

CONTROLES DE TECNOLOGÍA DE LA INFORMACIÓN

The Institute of Internal Auditors

Guía de Auditoría de Tecnología Global

Controles de tecnología de la información

Autores:

David A. Richards, Presidente, El IIA
Alan S. Oliphant, MIIA, QiCA, MAIR International
Charles H. Le Grand, CIA, CHL Global

Marzo 2005

Copyright © 2005 del Instituto de Auditores Internos, 247 Maitland Avenue, Altamonte Springs, Florida 32701-4201. Todos los derechos reservados. Impreso en Estados Unidos. Ninguna parte de esta publicación puede ser reproducida, guardada en un sistema de recuperación o transmitida en forma alguna ni por ningún medio, sea electrónico, mecánico, fotocopia, grabación, o cualquier otor, sin obtener previamente el permiso por escrito del editor.

El IIA publica este documento con fines de informativos y educativos. Este documento tiene como propósito bindar información, pero no sustituye el asesoramiento legal o contable. El IIA no ofrece ese tipo de asesoramiento y no garantiza ningún resultado legal ni contable por medio de la publicación de este documento. Cuando surgen cuestiones legales o contables, se debe recurrir y obtener asistencia profesional.

Capítulo 1
Resumen ejecutivo 1

Capítulo 2
Introducción 3

Capítulo 3
Evaluación de controles de TI – Una perspectiva 4

Capítulo 4
Comprensión de los controles de TI 5

Capítulo 5
Importancia de los controles de TI 13

Capítulo 6
Funciones de TI en la organización 14

Capítulo 7
Análisis de riesgos 19

Capítulo 8
Supervisión y técnicas 23

Capítulo 9
Evaluación 26

Capítulo 10
Conclusión 29

Capítulo 11
Apéndice A – Elementos de un programa de seguridad de la información 30

Capítulo 12
Apéndice B – Cumplimiento con la legislación 31

Capítulo 13
Apéndice C –Las tres categorías de conocimientos de TI para los auditores internos 35

Capítulo 14
Apéndice D – Esquemas de cumplimiento 37

Capítulo 15
Apéndice E - Evaluación de los controles de TI mediante COSO 45

Capítulo 16
Apéndice F - Objetivos de control de información y tecnologías relacionadas (CobiT) de ITGI 47

Capítulo 17
Apéndice G – Ejemplo de métricas de control de TI 49

Capítulo 18
Apéndice H – Cuestionario del DEA 52

Capítulo 19
Apéndice I – Referencias 54

Capítulo 20
Apéndice J – Glosario 56

Capítulo 21
Apéndice K – Sobre la GTAG 58

Capítulo 22
Apéndice L – Socios y Equipo Global del Proyecto GTAG 59

La guía *Controles de Tecnología de la Información* de la GTAG describe el conocimiento que necesitan los miembros de los órganos de gobierno, los ejecutivos, los profesionales de TI y los auditores internos para tratar los temas de control de la tecnología y su impacto en el negocio. Otros profesionales pueden encontrar orientaciones prácticas y relevantes. Esta guía proporciona información sobre marcos de referencia disponibles para la evaluación de los controles de TI y describe cómo establecer un marco adecuado para una organización. Por otra parte, establece el escenario para futuras GTAG que cubrirán, en mayor detalle, aspectos específicos de TI asociados con las funciones de negocio y las responsabilidades.

Los objetivos de la Guía de Controles de TI son:

- Explicar los controles de TI desde una perspectiva a nivel ejecutivo.
- Explicar la importancia de los controles de TI dentro del sistema global de controles internos.
- Describir las funciones y responsabilidades organizativas para asegurar que se enfoca adecuadamente el tratamiento de los controles de TI dentro del sistema global de controles internos.
- Describir los conceptos de riesgo inherente en uso y la gestión de la tecnología en cualquier organización.
- Describir el conocimiento básico y el entendimiento de los controles de TI, necesarios para el director ejecutivo de auditoría interna para asegurar una evaluación efectiva de los controles de TI, por parte de auditoría interna.
- Describir los elementos relevantes del proceso de evaluación de los controles de TI, producido por la función de auditoría interna.

1.1 Introducción de los Controles de TI

Los controles de TI no existen en forma aislada. Forman una continuidad interdependiente de protección, pero también pueden estar sujetos a una situación comprometida debido a un enlace débil. Están sujetos a errores y a invalidaciones de gestión, pueden abarcar desde simples hasta altamente tecnificados y pueden existir en un entorno dinámico. Los controles tienen dos elementos significativos: la automatización de los controles de negocio y del control de TI. De esta forma, los controles de TI ayudan a la dirección y al gobierno del negocio, a la vez que proporcionan controles generales y técnicos sobre las infraestructuras de TI. La función del auditor interno en los controles de TI comienza con un entendimiento sólido y conceptual y culmina, proporcionando los resultados de evaluaciones de riesgo y control. La realización de auditorías internas implica una interacción significativa con las personas que ocupan puestos de responsabilidad en cuanto a controles y requiere de un aprendizaje continuo y de una reevaluación permanente a medida que surgen nuevas tecnologías y que hay cambios en las oportunidades, usos, dependencias, estrategias, riesgos y requerimientos de la organización.

1.2 Entendimiento y comprensión de los controles de TI

Los controles de TI proporcionan aseguramiento relacionado con la fiabilidad de la información y de los servicios de información. Los controles de TI ayudan a mitigar los riesgos asociados con el uso de la tecnología en una organización. Estos abarcan desde políticas corporativas hasta su implementación física dentro de instrucciones codificadas y desde la protección de acceso físico, a través del seguimiento de acciones y transacciones, hasta las responsabilidades individuales y desde ediciones automáticas hasta análisis de razonabilidad para grandes conjuntos de datos.

Usted no necesita conocer "todo" acerca de los controles de TI, pero recuerde los dos conceptos claves de control:

- El aseguramiento debe ser proporcionado por los controles de TI dentro del sistema global de control interno y debe ser continuo y producir una pista de evidencia fiable y continua.
- El aseguramiento del auditor es una evaluación independiente y objetiva prioritaria. Se basa en el entendimiento, examen y evaluación de los controles claves relacionados con los riesgos que gestionan, así como la ejecución de pruebas suficientes para asegurar que los controles se diseñan adecuadamente y funcionan de forma efectiva y continuada.

Existen muchos marcos de referencia para categorizar los controles de TI y sus objetivos. Esta guía recomienda que cada organización use los componentes aplicables de marcos de referencia existentes para categorizar y evaluar sus controles de TI, a la vez que se proporciona y se documenta el propio marco de referencia para lo siguiente:

- Cumplir con las regulaciones y legislación aplicables.
- Lograr la consistencia con las metas y los objetivos de la organización.
- Evidenciar de forma fiable (aseguramiento razonable) que las actividades cumplen con las políticas de gobierno de la dirección y que son coherentes con el riesgo asumido por la organización.

1.3 Importancia de los Controles de TI

Muchos temas llevan hacia la necesidad de tener controles de TI, ellos abarcan desde la necesidad del control de costes y mantenimiento de la competitividad, hasta la necesidad de cumplimiento con gobiernos internos y externos. Los controles de TI promueven la fiabilidad y la eficiencia y facilitan la adaptación de la organización a entornos de riesgos cambiantes. Cualquier control que mitigue o detecte fraudes o ataques cibernéticos aumenta la resistencia de la organización porque la ayuda a descubrir el riesgo y gestionar su impacto. Esta resistencia es el resultado de un sistema fuerte de controles internos porque una organización adecuadamente controlada tiene la posibilidad de gestionar perfectamente desafíos, retos o trastornos.

Los indicadores clave de controles eficaces de TI son los siguientes:

- Capacidad para ejecutar y planificar trabajos nuevos, tal como la actualización de la infraestructura de TI que se requiere para admitir nuevos productos y servicios.
- Proyectos de desarrollo entregados a tiempo y dentro del presupuesto mediante los cuales se obtienen resultados eficaces en cuanto a costes y mejores ofertas en productos y servicios en comparación con los competidores.
- Capacidad para asignar recursos de forma previsible.
- Consistencia en cuanto a disponibilidad y fiabilidad de la información y de los servicios de TI a través de la organización y sus clientes, los socios de negocio y otras interrelaciones externas.
- Comunicaciones claras a la dirección sobre indicadores clave de controles eficaces.
- Capacidad para proteger contra vulnerabilidades y amenazas y capacidad de recuperación rápida y eficiente desde cualquier perturbación de servicios de TI.
- Eficiencia en el uso de centros de asistencia al cliente o "mesas de ayuda".
- Conciencia en cuanto a seguridad de los usuarios y cultura de concienciación sobre seguridad en toda la organización.

1.4 Funciones y responsabilidades de TI

Dentro de la organización, en los últimos años, han aparecido muchas y diversas funciones para puestos con responsabilidades de control de TI y de propiedad de TI. Cada puesto de trabajo dentro de los niveles de gobierno, de dirección, operativos y técnicos debe tener una descripción clara de funciones, responsabilidades y propiedad con respecto a los controles de TI para asegurar la asignación de responsabilidad en relación con temas específicos. Esta sección está dirigida a las funciones y responsabilidades del control de TI dentro de la organización y las asigna a posiciones específicas dentro de una estructura organizativa hipotética.

1.5 Evaluación de riesgos

Los controles de TI se seleccionan e implementan en función de los riesgos para cuya gestión están diseñados. A medida que se identifican los riesgos, se determinan las respuestas adecuadas y estas abarcan desde no hacer nada y aceptar el riesgo como un coste del negocio, hasta la aplicación de un amplio rango de controles específicos, incluyendo la contratación de seguros. Esta sección explica los conceptos referentes a cuándo aplicar los controles de TI.

1.6 Supervisión y técnicas

La implementación de una estructura formal de control facilita el proceso de identificar y evaluar los controles de TI necesarios para afrontar riesgos específicos. Un esquema de control es un mecanismo sistematizado de categorización de controles, para asegurar que el espectro completo de control esté adecuadamente cubierto. Esta estructura puede ser formal o informal. Un enfoque formal satisfacerá más fácilmente los diversos requerimientos regulatorios o estatutarios para aquellas organizaciones que estén sujetas a ellos. El proceso de seleccionar o construir un esquema de control debe incluir todos los puestos de trabajo de una organización que tengan responsabilidad directa sobre los controles. La estructura de control debería ser aplicada y utilizada por toda la organización y no solamente por auditoría interna.

1.7 Evaluación del control de TI

La evaluación de los controles de TI es un proceso continuo. Los procesos de negocio cambian constantemente y a su vez la tecnología evoluciona de forma permanente. Las amenazas aparecen a medida que se descubren nuevas vulnerabilidades. Los métodos de auditoría mejoran a la par que los auditores adoptan un enfoque en el que los aspectos de control de TI, como soporte de los objetivos de negocio, tienen una alta prioridad en la agenda.

La gerencia proporciona métricas e informes sobre los controles de TI. Los auditores verifican su validez y opinan sobre su valía. El auditor debe trabajar en estrecho contacto con la gerencia en todos los niveles y con el comité de auditoría para ponerse de acuerdo sobre la validez y la efectividad de las métricas y el aseguramiento de los informes.

La tecnología de la información es una parte esencial de todos los procesos que permiten a los negocios y a los gobiernos lograr sus misiones y objetivos. La TI facilita las comunicaciones locales y globales, a la vez que fomenta la cooperación internacional empresarial. Los controles de TI tienen dos componentes significativos: la automatización de los controles de negocio y el control de TI. Estos secundan la gestión y el gobierno empresarial y proporcionan controles generales y técnicos de las políticas, los procesos, los sistemas y el personal que conforman las estructuras de TI.

Los controles de TI no existen aislados. Forman una serie interdependiente de protección, y pueden también verse comprometidos a causa de un punto débil. Están sujetos a errores y negligencia gerencial, pueden variar desde simples a altamente técnicos y pueden existir en un entorno dinámico. Los controles de TI soportan el concepto de "defensa en profundidad", de tal forma que una sola debilidad no siempre da como resultado un solo punto de fallo.

Los controles existen para proteger los intereses de los accionistas:

- El capital del propietario.
- Los intereses de los clientes, tales como privacidad e identidad.
- Las responsabilidades y aptitudes de los empleados para demostrar que hicieron sus tareas de modo correcto.
- La tranquilidad de la gerencia dada la seguridad que proporcionan los procesos automatizados.

El aseguramiento del control de TI se concentra en la capacidad de los controles para proteger a la organización de las amenazas más importantes, a la vez que proporcionan evidencia de que los riesgos residuales muy improbablemente causarán daños significativos a la organización y a sus accionistas. Estos controles también son esenciales para asegurar la fiabilidad de los procesos e informes financieros.

Todo está conectado.

Cuando un administrador de seguridad selecciona las reglas en un archivo de configuración del filtro de seguridad (una tarea técnica que requiere conocimiento y habilidades específicas), implementa una política (que puede o no estar documentada) que, cuando se distribuye, determina los mensajes que serán o no permitidos dentro o fuera de la red de comunicaciones, a la vez que establece los "puertos" a través de los cuales estos pueden circular.
Su organización consigue un elemento de protección con sus filtros de seguridad, que es vital para la protección de la información y de las infraestructuras donde esa información es recogida, procesada, almacenada y comunicada.

Cuando el Director Ejecutivo de Auditoría (DEA) revisa y evalúa los controles de TI, debe preguntarse:

- ¿Qué queremos indicar por controles de TI?
- ¿Por qué necesitamos los controles de TI?
- ¿Quién es responsable de los controles de TI?
- ¿Cuándo es apropiado aplicar controles de TI?
- ¿Dónde se aplican exactamente los controles de TI?
- ¿Cómo realizamos las evaluaciones de los controles de TI?

El proceso de auditoría proporciona una estructura formal para encaminar los controles de TI dentro del sistema global de controles internos. En la Figura 1, *Estructura de auditoría de TI*, expuesta a continuación, se divide la evaluación en una sucesión lógica de pasos.

El papel del auditor interno en relación con los controles de TI comienza con una comprensión conceptual clara de estos y culmina comunicando los resultados de las evaluaciones de los riesgos y de los controles. Los auditores internos interactúan con el personal responsable de los controles y deben perseverar en el aprendizaje y la reevaluación continuos, a medida que emergen nuevas tecnologías y que cambian las oportunidades, los usos, las dependencias, las estrategias, los riesgos y los requerimientos de la organización.

> "Guardo seis hombres honestos y serviciales
> (que me enseñaron todo lo que sé);
> Sus nombres son Qué, Por Qué, Cuándo,
> Cómo, Dónde y Quién"
>
> — Rudyard Kipling,
> de "Elephant's Child"
> en *Just So Stories*.

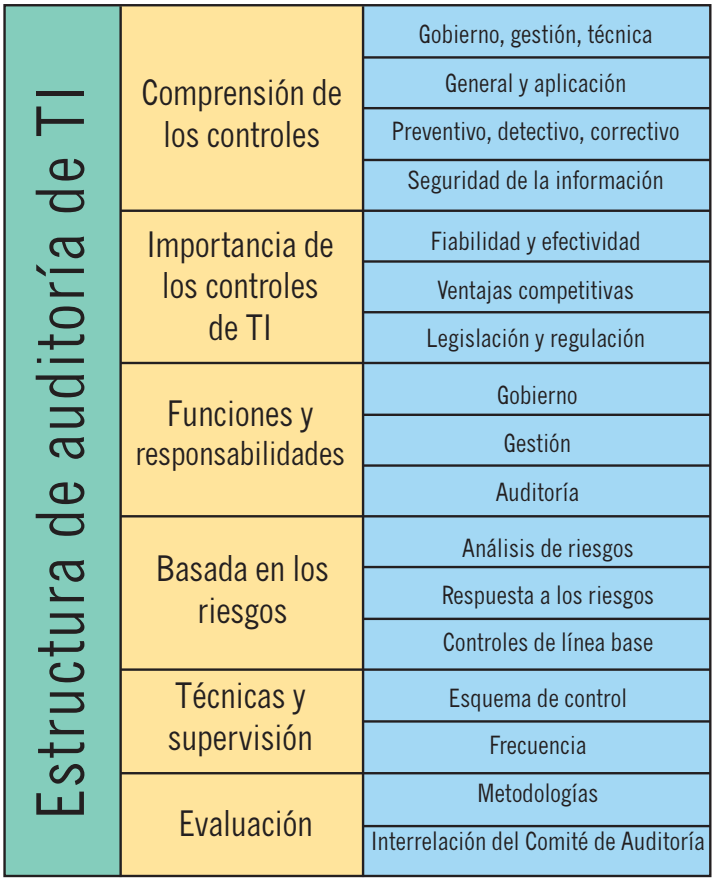

Figura 1 · Estructura de auditoría de TI

COSO[1] define el *control interno* como: "Un proceso, efectuado por el Consejo de Administración, la Dirección y el resto del personal de una organización, diseñado para proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:

- Efectividad y eficiencia de operaciones.
- Fiabilidad de los informes financieros.
- Cumplimiento de las leyes y regulaciones aplicables."

Los controles de TI abarcan estos procesos que proporcionan aseguramiento para la información y los servicios de información y ayudan a mitigar los riesgos asociados con el uso de la tecnología en la organización. Estos controles se extienden desde las políticas corporativas escritas hasta su implementación en instrucciones codificadas, desde la protección del acceso físico hasta la habilidad de rastrear acciones y transacciones de los individuos responsables de estas, y desde ediciones automáticas hasta análisis de racionalidad para grandes volúmenes de datos.

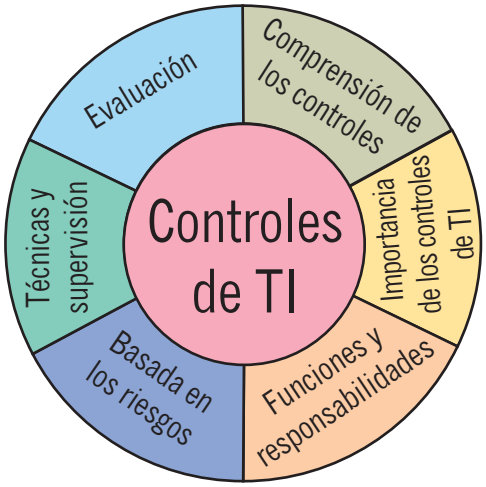

Figura 2

4.1 Clasificaciones de los controles

Los controles se pueden clasificar para ayudar a entender sus propósitos y ver dónde se integran dentro del sistema global de controles internos (Consulte la Figura 3, *Algunas clasificaciones de los controles*). A partir de la clara comprensión de estas clasificaciones, el analista y el auditor del control pueden establecer mejor su situación dentro de la estructura de control y responder preguntas claves como la siguiente: ¿Son los controles de detección adecuados como para identificar errores que pueden burlar los controles preventivos? ¿Son los controles correctivos suficientes a fin de reparar los errores una vez que han sido detectados? Una clasificación común de los controles de TI es controles *generales* versus controles de *aplicación*.

Los controles generales (también conocidos como controles de infraestructura) se aplican a todos los componentes de sistemas, procesos y datos para una determinada organización o entorno de sistemas. Los controles generales incluyen, entre otros: políticas de seguridad de información, administración, acceso y autenticación, separación de funciones claves de TI, gestión de la adquisición e implementación de sistemas, gestión de cambios, respaldo, recuperación y continuidad del negocio.

Los controles de aplicación están relacionados con el ámbito de los procesos individuales de negocio o sistemas de aplicación. Incluyen controles tales como ediciones de datos, separación de funciones del negocio (ej. la iniciación de transacciones versus autorización), cuadre de totales de procesos, registro de transacciones e informes de error. La función de un control es altamente relevante para la evaluación de su diseño y efectividad. Los controles se pueden clasificar como *preventivos*, de *detección*, o *correctivos*.

Los controles preventivos impiden que se cometan errores, omisiones o incidentes de seguridad. Los ejemplos

No es necesario conocer "todo" acerca de los controles de TI.

No se preocupe si no entiende la serie completa o todas las técnicas complejas de los controles de TI. Muchos de estos controles son del dominio de especialistas que manejan riesgos específicos asociados a los componentes individuales de los sistemas y de la infraestructura de la red. Según las buenas prácticas de separación de funciones, puede ocurrir que algunas personas con conocimientos especializados en una tecnología, como la gestión de bases de datos, conozcan poco sobre componentes de red o protocolos de comunicación y viceversa.

Hay dos conceptos claves de control a recordar:

1. *El aseguramiento debe ser proporcionado por los controles de TI dentro del sistema global de control interno, debe ser continuo y producir una pista de evidencia fiable y continua.*
2. *El aseguramiento del auditor es una evaluación independiente y objetiva prioritaria. Se basa en el entendimiento, el examen y la evaluación de los controles clave relacionados con los riesgos que gestionan, así como la ejecución de pruebas suficientes para asegurar que los controles se diseñen apropiadamente y funcionen efectivamente.*

[1] COSO – Comité de Organizaciones Patrocinadoras para la Comisón Treadway sobre informe financiero fraudulento. Consulte www.coso.org.

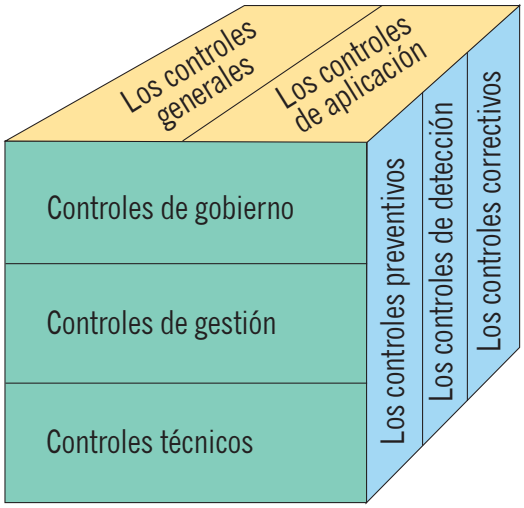

Figura 3 · Algunas clasificaciones de los controles

incluyen ediciones simples de entrada de datos que impiden que se ingresen caracteres alfanuméricos en campos numéricos, controles de acceso que protegen la información sensible o los recursos de sistemas contra el ingreso de personas no autorizadas y controles técnicos dinámicos y complejos tales como software antivirus, filtro de seguridad y sistemas de prevención de intrusos.

Los controles de detección didentifican errores o incidentes que eluden a los controles preventivos. Por ejemplo, un control de detección puede identificar números de cuentas inactivas o de cuentas que han sido marcadas para supervisar y detectar actividades sospechosas. Los controles detectivos pueden también incluir supervisión y análisis para dejar al descubierto actividades o acontecimientos que exceden límites autorizados o violan patrones definidos en datos que pueden indicar una manipulación incorrecta. Para las comunicaciones electrónicas sensibles, los controles de detección pueden indicar que un mensaje se ha corrompido o que la identificación segura del remitente no puede ser autenticada.

Los controles correctivos corrigen errores, omisiones, o incidentes una vez que se han detectado. Van desde la corrección simple de errores de entrada de datos hasta la identificación y eliminación de usuarios o software sin autorización en sistemas o redes, hasta la recuperación ante incidentes, interrupciones o desastres.

Generalmente, es más eficiente prevenir errores o detectarlos tan próximos a su origen como sea posible para simplificar su corrección. Estos procesos correctivos deben también estar sujetos a controles preventivos y de detección, porque representan otra oportunidad de errores, omisiones o falsificación.

Muchas otras clasificaciones de controles descritas en esta guía pueden ser útiles en la evaluación de su efectividad. Por ejemplo, los controles automatizados tienden a ser más fiables que los controles manuales y los controles no discrecionales pueden ser aplicados consistentemente de forma más probable que los controles discrecionales. Otras clasificaciones de control incluyen los siguientes: control obligatorio, voluntario, complementario, compensatorio, redundante, continuo, a pedido, e impulsado por eventos.

4.2 Controles de gobierno, de gestión y técnicos

Otra clasificación común de controles es la que se establece en función del grupo responsable de asegurar su implementación y mantenimiento correctos. A fin de evaluar las funciones y responsabilidades, esta guía categoriza principalmente los controles de TI como controles de gobierno, de gestión y técnicos. Los elementos del programa de seguridad de la información para estas tres categorías se describen en el Apéndice A. Los primeros dos niveles –gobierno y gestión– son los más aplicables según el alcance de la guía, si bien también pueden ser útiles para entender cómo se establecen específicamente los controles de alto nivel dentro de las infraestructuras técnicas de TI. Los controles técnicos serán materia de un tema más específico de las Guías de Auditoría de Tecnología Global (GTAG, en inglés).

4.2.1 Controles de gobierno

La responsabilidad primaria por el control interno reside en el Consejo de Administración en su papel de encargado de la estructura de gobierno. El control de TI a nivel de gobierno implica asegurar la gestión efectiva de la información, garantizar que existan principios de seguridad, políticas, gestión de procesos y métricas de cumplimiento y rendimiento que demuestren un soporte continuado para esa estructura.

Los controles de gobierno son aquellos promulgados o controlados por el Consejo de Administración en su conjunto o por un Comité de Dirección conjuntamente con la dirección ejecutiva de la organización. Estos controles están vinculados a los conceptos de gobierno corporativo, ambos inducidos por las metas y estrategias de la organización y por los grupos exteriores tales como los organismos de control.

Una distinción importante entre el gobierno y los controles de la dirección es el concepto de "narices adentro, dedos afuera". La responsabilidad del Consejo implica supervisión más que ejecución real de las actividades del control. Por ejemplo, el comité de auditoría del Consejo no audita, pero supervisa ambas auditorías de la organización, la auditoría interna y la externa.

4.2.2 Controles de gestión

La responsabilidad de la dirección sobre los controles internos implica típicamente llegar a todas las áreas de la organización con especial atención en los activos críticos, la información sensible y las funciones operativas. Por lo tanto, una colaboración estrecha entre los miembros del Consejo y los gerentes ejecutivos es esencial. La gerencia debe cercio-

El Centro para la Seguridad de Internet (www.cisecurity.org) considera que aplicar controles consistentemente en los sistemas y en la configuración de los componentes de la red protegerá a la organización contra más del 85% de las vulnerabilidades más frecuentes identificadas por el Instituto Nacional de Normas y Tecnología de Estados Unidos (NIST, en inglés), la Oficina Federal de Investigación (FBI, en inglés), el Instituto SANS y el Instituto de Seguridad Informática (CSI, en inglés).

rarse de que los controles de TI necesarios para lograr los objetivos establecidos por la organización se aplican y aseguran que el proceso es fiable y continuo. Estos controles son distribuidos como resultado de acciones deliberadas por la gerencia a fin de lograr lo siguiente:

- Reconocer los riesgos de la organización, sus procesos y activos.
- Promulgar mecanismos y procesos para mitigar y gestionar riesgos (proteger, supervisar y medir resultados)

4.2.3 Controles técnicos

Los controles técnicos forman el fundamento esencial que asegura la confiabilidad de prácticamente todo el resto de los controles de la organización. Por ejemplo, la protección contra accesos no autorizados e intrusiones, estos proporcionan la base para la confianza en la integridad de la información –incluida la evidencia de todos los cambios y su autenticidad. Estos controles son específicos para las tecnologías usadas dentro de las infraestructuras de TI de la organización. La capacidad para automatizar controles técnicos que implementen y demuestren cumplimiento con las políticas planificadas de la dirección, basadas en la información, es un recurso importante para la organización.

4.3 Controles de TI – Qué esperar

Los mecanismos individuales de control que un DEA puede esperar dentro de la organización se definen dentro de la jerarquía de los controles de TI, desde las declaraciones de política de alto nivel emitidas por la dirección y refrendadas por el consejo de administración hasta los mecanismos específicos de control incorporados en los sistemas de aplicación.

La jerarquía en la Figura 4, *Controles de TI*, representa un enfoque lógico de tipo descendente, tanto cuando se consideran controles para implementar como cuando se determinan las áreas en las cuales centrar los recursos de auditoría durante las revisiones del entorno operativo de TI completo. Los diversos elementos de la jerarquía no son mutuamente exclusivos; todos están conectados y pueden mezclarse. Muchos de los tipos del control dentro de los elementos se describen en este capítulo.

4.3.1 Políticas

Todas las organizaciones necesitan definir su metas y objetivos mediante planes estratégicos y declaraciones de políticas. Sin declaraciones claras de políticas y normas para la dirección, las organizaciones se pueden desorientar y funcionar ineficazmente. Las organizaciones con metas y objetivos claramente definidos tienden a ser exitosas.

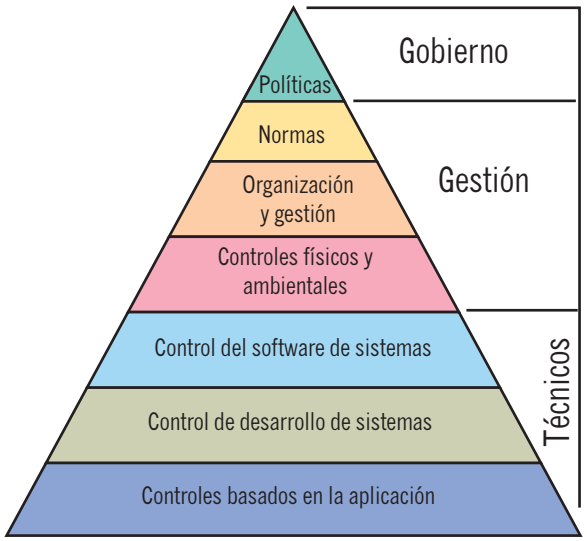

Figura 4 · Controles de TI

Dado que la tecnología es vital para las operaciones de la mayoría de las organizaciones, las declaraciones de políticas claras con respecto a todos los aspectos de TI deben ser diseñadas y aprobadas por la dirección, refrendadas por el consejo de administración y comunicadas a todo el personal. Se pueden necesitar muchas y diferentes declaraciones de políticas, según el tamaño de la organización y el alcance del servicio de TI. Para organizaciones más pequeñas, una sola declaración de política puede ser suficiente, pero debe cubrir todas las áreas relevantes. Las organizaciones más grandes que implementan TI de manera amplia necesitarán políticas más detalladas y específicas.

Las declaraciones de políticas de TI incluyen, entre otras, las siguientes:

- Una política general sobre el nivel de seguridad y privacidad para toda la organización. Esta política debe ser consistente con toda la legislación nacional e internacional relevante y debe especificar el nivel de control y de seguridad requeridos según la sensibilidad del sistema y de los datos procesados.
- Una declaración sobre la clasificación de la información y sobre los derechos de acceso en cada nivel. La

política debe también definir cualquier limitación respecto a uso de la información por parte de las personas con acceso autorizado.
- Una definición de los conceptos de la propiedad de los datos y sistemas, así como de la autoridad necesaria para crear, modificar o eliminar información. Sin estas pautas, frecuentemente es difícil coordinar el cambio en organizaciones grandes porque es posible que no exista alguien designado específicamente que posee la responsabilidad total de los datos y los sistemas.
- Una política general que define el grado en que los usuarios pueden distribuir las estaciones de trabajo inteligentes para crear sus propias aplicaciones.
- Las políticas de personal que definen y aplican condiciones al personal en áreas sensibles. Esto incluye la investigación de los antecedentes del personal nuevo, antes de su incorporación a la organización, realizando además pruebas anuales y haciendo que los empleados firmen acuerdos para aceptar las responsabilidades de los niveles de control, seguridad, y confidencialidad requeridos. Esta política también debería detallar los respectivos procedimientos disciplinarios.
- Definiciones de los requisitos globales de planificación para la continuidad del negocio. Estas políticas deben asegurar de que se consideren todos los aspectos del negocio ante la posible ocurrencia de una interrupción o un desastre, no sólo de los elementos de TI.

Una buena fuente para las políticas y la seguridad de TI, es la página de SANS (http://www.sans.org/ resources/policies/#intro), que proviene de un proyecto de investigación con consenso de la comunidad del Instituto SANS. El proyecto ofrece ayudas gratis para el desarrollo y la implementación rápidos de políticas de seguridad referentes a la información, incluidas plantillas de políticas para 24 requerimientos importantes de seguridad. Si bien las plantillas fueron compiladas para ayudar a las personas que asistían a los programas de entrenamiento de SANS, SANS los pone a disponibilidad de todos porque la seguridad de Internet depende de la vigilancia de todos los participantes.

4.3.2 Normas

Las normas sirven para apoyar los requerimientos de las políticas. Intentan definir formas de trabajo que permitan alcanzar los objetivos requeridos de la organización. La adopción y el cumplimiento de las normas también promueve la eficacia porque no requiere que el personal reinvente la rueda cada vez que se construye una aplicación de negocio nueva o se instala una red nueva. Las normas también permiten que la organización mantenga todo el entorno de operaciones de TI de manera más eficiente.

Las organizaciones grandes y con recursos significativos están en una posición que les permite diseñar sus propias normas. En el sentido opuesto, las organizaciones más pequeñas difícilmente tengan recursos suficientes para ese ejercicio. Hay muchas fuentes de información sobre normas y mejores prácticas, algunas de las cuales se enumeran en el Apéndice I.

A modo de directriz, el DEA esperará encontrar normas adoptadas para los siguientes ítems:
- **Procesos de desarrollo de sistemas.** Cuando las organizaciones desarrollan sus propias aplicaciones, las normas se aplican a los procesos para diseñar, desarrollar, probar, implementar y mantener los sistemas y programas. Si las organizaciones externalizan el desarrollo de aplicaciones o adquieren sistemas a proveedores, el DEA debe comprobar que los acuerdos exijan a los proveedores la aplicación de principios que sean consistentes con las normas de la organización o aceptables para ella.
- **Configuración del software de sistemas.** Dado que el software de sistemas proporciona un importante elemento de control en el entorno de TI, las normas para asegurar las configuraciones del sistema, como las de "benchmark" de CIS están comenzando a ganar amplia aceptación en organizaciones destacadas y en proveedores de tecnología. La forma en que los productos como sistemas operativos, software de interconexión de redes y sistemas gestores de bases de datos son configurados puede aumentar la seguridad o crear debilidades que pueden ser explotadas.
- **Controles de aplicaciones.** Todas las aplicaciones que soportan las actividades del negocio deben ser controladas. Las normas son necesarias para todas las aplicaciones que la organización desarrolla o compra ya que definen los tipos de controles que deben estar presentes en todo el ámbito de las actividades del negocio, así como los controles específicos que se deben aplicar a los procesos e información sensibles.
- **Estructuras de datos.** Disponer de definiciones consistentes de datos a través de toda la variedad de las aplicaciones asegura que diferentes sistemas puedan acceder a los datos perfectamente y que los controles de seguridad para los datos privados y sensibles se apliquen de modo uniforme.
- **Documentación.** Las normas deben especificar el nivel mínimo de la documentación requerida para cada sistema de aplicación o instalación de TI, así como para las diversas clases de aplicaciones, procesos y centros de procesamiento.

De la misma forma que las políticas, las normas deben ser aprobadas por la dirección, deben estar redactadas en un lenguaje claro y comprensible y deben estar disponibles para todos aquellos que las implementen.

4.3.3 Organización y gestión

La organización y la gestión desempeñan un papel importante en todo el sistema de control de TI, como con cada aspecto de las operaciones de una organización. Una estructura apropiada

de organización permite que puedan definir líneas de reporte y responsabilidad y que se puedan implementar sistemas de control efectivos.

4.3.3.1 Separación de funciones

La separación de funciones es un elemento vital para muchos controles. La estructura de una organización no debe asignar la responsabilidad de todos los aspectos del procesamiento de datos a un solo individuo o departamento. Las funciones de iniciar, autorizar, ingresar, procesar y verificar datos se deben separar para garantizar que ningún individuo pueda realizar ambas funciones y crear un error, omisión, u otra irregularidad y autorizarlo y/o ocultar la evidencia. Los controles de separación de funciones en los sistemas de aplicación se proporcionan al otorgar privilegios de acceso sólo en función de los requerimientos del trabajo desempeñado para procesar funciones y ganar acceso a la información sensible.

La separación tradicional de funciones en el entorno de TI se divide entre desarrollo de sistemas y operaciones. El área de Operaciones y Explotación debe ser responsable de ejecutar los sistemas de producción, a excepción de la distribución de los cambios, y debe tener poco o ningún contacto con el proceso de desarrollo. Este control debe incluir restricciones que impidan el acceso de los operadores para modificar programas, sistemas o datos de producción. De igual manera, el personal de desarrollo de sistemas debe tener poco contacto con los sistemas en producción. Durante la implementación y los cambios de procesos, al asignar funciones específicas al personal responsable de los sistemas de aplicación y a los responsables de operaciones, se puede impulsar la correcta separación de funciones. En organizaciones grandes, se deben considerar muchas otras funciones para asegurar la separación apropiada y esos controles pueden ser bastante detallados. Por ejemplo, las cuentas privilegiadas, como el grupo administrador de Windows y de superusuario en UNIX, pueden modificar registros de entrada, obtener acceso a cualquier archivo y en muchos casos actuar como cualquier usuario o función. Es importante restringir al mínimo el número de personas con este privilegio. También hay herramientas de software disponibles que se deben considerar para limitar la capacidad de los usuarios con cuentas privilegiadas y para supervisar sus actividades.

4.3.3.2 Controles financieros

Dado que las organizaciones hacen inversiones considerables en TI, son necesarios los controles presupuestarios y otros controles financieros para asegurar el rendimiento de la tecnología, el retorno de la inversión o los ahorros previstos. Deben existir procesos de gestión para recoger, analizar y brindar información relacionada con esos aspectos. Desafortunadamente, los nuevos desarrollos de TI con frecuencia se ven afectados por estimaciones de costes masivos y no logran producir los ahorros previstos debido a una planificación insuficiente. Los controles presupuestarios pueden ayudar a identificar tempranamente fallos potenciales en el proceso, lo cual le permitirá a la dirección tomar acciones categóricas. Además, esos controles pueden producir datos históricos que luego las organizaciones utilizarán en proyectos futuros.

4.3.3.3 Gestión de cambios

Los procesos de gestión de cambios se consideran elementos de control gerenciales y organizativos. Esos procesos deben asegurar que los cambios de entorno de TI, software de sistemas, sistemas de aplicación y datos se apliquen de modo tal que se cumpla la correcta separación de funciones. Tales procesos garantizan que los cambios se ejecuten según lo requerido, a la vez que se impide que se los utilice con propósitos fraudulentos, también revelan los costes verdaderos de las ineficacias e interrupciones del sistema que se pueden llegar a ocultar como consecuencia de procesos ineficaces de supervisión y reporte. La gestión de cambios es una de las áreas más sensibles de los controles de TI y puede impactar seriamente en la disponibilidad del sistema y del servicio si no se administra con eficacia. El instituto IT Process Institute ha publicado una investigación en la que se demuestra que la gestión eficaz de cambios de TI puede proporcionar ventajas significativas a las organizaciones.

4.3.3.4 Otros controles de gestión

Otros controles típicos de gestión incluyen la tarea de examinar los procedimientos para el personal nuevo, medir el rendimiento, proporcionar entrenamiento especializado al personal de TI y revisar los procedimientos disciplinarios. Estos controle se enumeran en los Elementos del Programa de Seguridad de la Información en el Apéndice A y serán cubiertos en mayor detalle en otras publicaciones de GTAG.

4.3.4 Controles ambientales y físicos

Para muchas organizaciones, el equipo de TI representa una inversión considerable. Debe ser protegido contra daño, pérdida accidental o deliberada. Los controles medio ambientales y físicos, que fueron desarrollados originalmente para grandes centros de datos de alojamiento de ordenadores, computadoras centrales, etc., son igualmente importantes en el mundo moderno de sistemas distribuidos cliente-servidor y sistemas basados en la Web. Si bien el equipo de uso habitual hoy en día se diseña para facilitar su utilización en un entorno normal de oficina, su valor para el negocio, el costo y la sensibilidad de las aplicaciones que ejecutan procesos de negocio pueden ser significativos. Todo el equipo se debe proteger, incluidos los servidores y las estaciones de trabajo que permiten el acceso del personal a las aplicaciones.

Algunos controles típicos ambientales y físicos son los siguientes:

- Ubicar los servidores en salas cerradas con llave con acceso restringido.
- Restringir el acceso al servidor a personas específicas.
- Proporcionar equipos de detección y extinción de incendios.

- Colocar el equipo, las aplicaciones y los datos sensibles lejos de peligros ambientales, como inundaciones en pisos inferiores o almacenamiento de líquidos inflamables.

Cuando se considera la seguridad física y ambiental, es también apropiado considerar la planificación de contingencias –también conocida como planificación de recuperación de desastres– que incluye respuestas a incidentes de seguridad. ¿Qué hará la organización si ocurre un incendio, una inundación o cualquier otra amenaza? ¿Cómo la organización restaurará el negocio, sus instalaciones y servicios relacionados para asegurar la continuidad del procesamiento normal con mínimos efectos en las operaciones regulares? Este tipo de planificación va más allá de proporcionar una mera alternativa disponible para la capacidad de procesamiento de TI y de los habituales respaldos de los datos de producción, debe considerar la logística y coordinación necesarias para el ámbito completo de las actividades del negocio. Finalmente, la historia constantemente demuestra que un plan de recuperación de desastres que no se ha probado satisfactoriamente en una simulación realista no es fiable.

4.3.5 Controles del software de sistemas

Los productos del software de sistemas permiten al equipo de TI que los mismos sean utilizados por los sistemas de aplicación y los usuarios. Estos productos incluyen sistemas operativos tales como Windows, UNIX y Linux; software de red y comunicaciones; software de filtro de seguridad; productos antivirus; y sistemas gestores de base de datos (DBMS) como Oracle y DB2.

El software de sistemas puede ser altamente complejo y se aplica a los componentes y dispositivos dentro del entorno de sistemas y de red. Se configura para ajustarse a necesidades altamente especializadas y normalmente se requiere un alto grado de especialización para su mantenimiento con seguridad. Las técnicas de configuración controlan el acceso lógico a las aplicaciones, aunque algunos sistemas de aplicación contienen sus propios controles de acceso y pueden proporcionar una puerta de entrada para los piratas informáticos que deseen ingresar en un sistema. Además, esas técnicas de configuración también proporcionan los medios para aplicar la separación de funciones, generar pistas de auditoría especializadas y aplicar controles de integridad de datos mediante listas de control de acceso, filtros y registros de actividad.

Se requieren auditores especialistas de TI para evaluar los controles en este área. En las organizaciones pequeñas, es poco probable que se tengan los recursos necesarios como para contratar tales especialistas por lo que se debe considerar la externalización del trabajo. Independientemente del tipo de contratación de auditores de TI, sea directa o por externalización, estos deben poseer conocimientos muy específicos y elevados. Gran parte de ese conocimiento proviene de la experiencia, pero además el profesional se debe actualizar constantemente para mantenerse al día y ser útil. La certificación confirma que un especialista técnico ha adquirido un conjunto específico de conocimientos y experiencia, y que ha aprobado un examen al respecto. En el mundo de auditoría de TI, entre los certificados globales se incluyen los siguientes: Calificación en Auditoría Informática (QiCA, en inglés) del IAI del Reino Unido e Irlanda; Auditor Certificado de Sistemas de Información (CISA, en inglés) disponible a través de la Asociación de Auditoría y Control de Sistemas de Información (ISACA, en inglés); Certificación Global del Aseguramiento de la Información (GIAC, en inglés), Auditor de Sistemas y Redes (GSNA, en inglés), del programa GIAC del Instituto SANS. Otras certificaciones adicionales se centran en la capacidad general y especializada en la seguridad de la información, administración de redes y otras áreas relacionadas estrechamente con la auditoría de TI y son útiles para identificar la aptitud potencial del auditor de TI.

Algunos controles técnicos claves que el DEA debe esperar en un entorno de TI bien gestionado, son los siguientes:

- Derechos de acceso asignados y controlados según la política estipulada por la organización.
- Separación de funciones impulsadas en su cumplimiento por medio del software de sistemas y de otros controles de configuración.
- Existencia de una evaluación del intrusismo y de la vulnerabilidad, prevención, detección y supervisión continuas.
- Pruebas de intrusión realizadas regularmente.
- Servicios de cifrado aplicados allí donde la confidencialidad es un requerimiento establecido.
- Existencia de procesos de gestión de cambios, incluida la gestión de parches, para asegurar un proceso estrictamente controlado de aplicación de cambios y parches en los componentes de software, los sistemas, las redes y los datos.

4.3.6 Controles de desarrollo y adquisición de sistema

Rara vez, las organizaciones adoptan una única metodología para todos los proyectos de desarrollo de sistemas. Las metodologías se suelen elegir para satisfacer las circunstancias particulares de cada proyecto. El auditor de TI debe determinar si la organización desarrolla o adquiere sistemas de aplicación usando, o no, un método controlado que proporcione posteriormente controles eficaces de las aplicaciones y de los datos que procesan. Todos los sistemas de aplicación informáticos deben realizar solamente aquellas funciones que el usuario requiera de manera eficiente. Por el examen de los procedimientos de desarrollo de aplicaciones, el auditor puede obtener aseguramiento de que las aplicaciones funcionan de manera controlada.

Algunas consideraciones de control básico deben ser evidentes en los trabajos de desarrollo y adquisición de sistemas:

- Los requerimientos de usuario deben ser documentados y sus logros deben ser medidos.

- El diseño de sistemas debe seguir un proceso formal para asegurarse de que los requerimientos y las funcionalidades de diseño estén incorporadas dentro del producto terminado.
- El desarrollo de sistemas se debe conducir de manera estructurada para asegurar que los requerimientos y las características del diseño estén incorporados en el producto terminado.
- Las pruebas deben asegurar que los elementos individuales del sistema trabajen según lo requerido, que las interfaces del sistema operen según lo esperado, que los usuarios participen en el proceso de pruebas y que se proporcione la funcionalidad prevista.
- Los procesos de mantenimiento de las aplicaciones deben asegurar que los cambios en los sistemas sigan un patrón coherente de control. La gestión de cambios debe estar sujeta a procesos estructurados de aseguramiento de la validación.

Cuando el desarrollo de los sistemas sea externalizado, los contratos con el que subcontrata o con el mismo proveedor deben requerir controles similares.

Las técnicas y los controles para la gestión de un proyecto necesitan ser parte del proceso de desarrollo, tanto si los desarrollos son realizados "a medida" o son externalizados. La dirección debe saber si los proyectos se están desarrollando según tiempo previsto y presupuesto, y si los recursos se han usado eficientemente. Los procesos de reporte o informes deben asegurar que la dirección comprenda totalmente el estado actual de los proyectos de desarrollo y que no reciba sorpresas cuando se realice la entrega del producto final.

4.3.7 Controles basados en la aplicación

El objetivo de los controles internos sobre los sistemas de aplicación es asegurar lo siguiente:

- Todos los datos de entrada son exactos, completos, autorizados y correctos.
- Todos los datos se procesan según lo previsto.
- Todos los datos almacenados son exactos y completos.
- Toda la salida de datos es exacta y completa.
- Se mantiene un registro de actividad para rastrear el proceso de los datos desde su entrada, almacenamiento y eventual salida.

La revisión de los controles de aplicación ha sido tradicionalmente "el pan y la mantequilla" del auditor de TI. Sin embargo, dado que los controles de aplicación representan un porcentaje importante de los controles de negocio, deben ser la prioridad de cada auditor interno. Todos los auditores internos necesitan poder evaluar un proceso del negocio, entender y evaluar los controles proporcionados por los procesos automatizados.

Hay varios tipos de controles genéricos que el DEA espera ver en cualquier aplicación:

- Controles de entrada. Estos controles se utilizan principalmente para chequear la integridad de los datos ingresados dentro de una aplicación de negocio, independientemente de si el dato de origen es ingresado directamente por el personal,, remotamente por un socio del negocio o a través de una aplicación Web habilitada. La entrada se chequea para verificar que se encuentre dentro de los parámetros especificados.
- Controles de proceso. Estos controles proporcionan un medio automatizado para asegurar que el proceso sea completo, exacto y autorizado.
- Controles de salida. Estos controles se centran en qué se hace con los datos. Deben comparar los resultados con el resultado previsto y verificarlos contra la entrada.
- Controles de integridad. Estos controles supervisan los datos de un proceso y/o del almacenamiento para asegurar que los datos siguen siendo consistentes y correctos.
- Pista de gestión. Los controles del historial del proceso, a menudo se denominan pista de auditoría y permiten a la dirección rastrear las transacciones desde su origen hasta el último resultado, y viceversa, desde los resultados hasta identificar las transacciones y eventos registrados. Estos controles deben ser adecuados para supervisar la efectividad de todos los controles e identificar los errores tan cerca de sus orígenes como sea posible.

4.4 Seguridad de la información

La seguridad de la información es una parte fundamental de todos los controles de TI. La seguridad de la información se aplica desde la infraestructura hasta los datos y es la base para la fiabilidad de la mayoría de los otros controles de TI. Las excepciones son los controles referentes a aspectos financieros de TI (por ejemplo, el retorno de la inversión, los

Riesgo asumido

El "grado de aceptación del riesgo" o la tolerancia al riesgo de una organización define el grado de riesgo que una compañía u otra organización está dispuesta a correr en la búsqueda de sus metas, según lo determinado por la dirección y el gobierno ejecutivo. El "grado de aceptación del riesgo" puede especificar, por ejemplo, si una organización asumirá un papel agresivo en la distribución de tecnologías nuevas y emergentes. El grado de aceptación del riesgo de una organización puede verse afectado por su industria y entorno normativo específicos. Se relaciona estrechamente con el grado de aceptación y la tolerancia al riesgo de una organización, mide qué distancia se está dispuesto a desviar de la medida indicada en tal grado de aceptación del riesgo.

controles presupuestarios) y a algunos controles de la gestión de proyectos.

Los elementos universalmente aceptados de seguridad de la información son:

- **Confidencialidad.** La información confidencial debe solamente divulgarse cuando sea adecuado y debe ser protegida contra la revelación no autorizada o interceptación. La confidencialidad incluye consideraciones de privacidad.
- **Integridad.** La integridad de la información se refiere a que los datos deben ser correctos y completos. Esto incluye específicamente la fiabilidad del proceso y los informes financieros.
- **Disponibilidad.** La información debe estar disponible para el negocio, sus clientes y los socios en el momento, el lugar y de la manera apropiados. La disponibilidad incluye la capacidad de recuperar los servicios de TI ante pérdidas, interrupciones o corrupción de datos, así como ante la ocurrencia de un desastre mayor en el lugar donde la información haya estado localizada.

4.5 Entorno de los controles

Los controles de TI no son automáticos. Durante más de 50 años, las organizaciones han utilizado TI y los controles no han sido siempre condición predeterminada de los nuevos sistemas de hardware o software. Por lo general, el desarrollo y la implementación de controles tienen lugar a continuación del reconocimiento de vulnerabilidades en los sistemas y de amenazas que explotan tales vulnerabilidades. Además, los controles de TI no se definen en ninguna norma reconocida que sea aplicable a todos los sistemas o a las organizaciones que las utilizan.

Existen muchos esquemas para categorizar los controles de TI y sus objetivos. Cada organización debe utilizar los componentes más aplicables de esos esquemas para categorizar o evaluar los controles de TI que le sean útiles, para proporcionar y documentar su propia estructura de control interno a fin de alcanzar lo siguiente:

- Cumplir con las regulaciones y legislación aplicables.
- Ser consistentes con las metas y los objetivos de la organización.
- Dar evidencia confiable (aseguramiento) de que las actividades son coherentes con las políticas de gobierno de la dirección y con el riesgo asumido por la organización.

Muchos temas llevan a la necesidad de controles de TI, incluyendo controles de costes y el mantenimiento de la competitividad, protección contra robos de piratas informáticos y el cumplimiento de la legislación y regulación, como la Ley de 2002 de Sarbanes-Oxley de Estados Unidos*, la directiva de protección de datos de la Unión Europea y legislaciones relacionadas de otros países. Los controles de TI promueven la fiabilidad, la eficiencia y permiten que la organización se adapte a riesgos cambiantes de los entornos. Por ejemplo, cualquier control que mitigue o detecte el fraude o los ataques cibernéticos mejora la "resistencia" de la organización al ayudarla a descubrir el riesgo y gestionar su impacto.

La "resistencia" es el resultado de un fuerte sistema de control interno que otorga a la organización la capacidad de gestionar los trastornos con eficacia. La legislación y las regulaciones de algunos países actualmente requieren que las organizaciones informen sobre la efectividad del control interno e, implícitamente, sobre la efectividad del control de TI. La ley más importante, entre las nuevas leyes, es la Sarbanes-Oxley, que requiere que todas las compañías que cotizan en Estados Unidos y sus subsidiarias en el extranjero, informen sobre su sistema de controles internos en relación con los informes financieros, que se realizan conjuntamente con la auditoría de los estados contables. En el Apéndice B se proporciona una lista de algunas de las legislaciones y regulaciones aplicables a los controles internos.

La necesidad de controles está principalmente dada por la complejidad resultante de la necesidad de que los diversos componentes técnicos trabajen el uno con el otro. Mientras que la resistencia y la adaptabilidad de TI son cruciales para alcanzar las necesidades cambiantes de clientes y empresas asociadas del negocio, como responder a las presiones competitivas, también agregan complejidad al negocio y a las infraestructuras de TI. Adicionalmente, la seguridad de la información ha sido reconocida como un componente clave del control interno con la aparición y amplia aceptación de normas tales como el Código de buenas prácticas para la gestión de seguridad de la información (ISO 17799), de la Organización Internacional de Normalización.

Las organizaciones que implementan controles de TI eficaces experimentan mejoras en la eficacia, fiabilidad de los servicios, resistencia de los sistemas y disponibilidad del aseguramiento de la evidencia, todos ellos añaden valor e incrementan la confianza de los accionistas y del organismo de control de la organización. Algunos indicadores clave de la efectividad de los controles de TI incluyen:

- La capacidad de ejecutar nuevos trabajos planificados, como actualizaciones de infraestructuras de TI requeridas para dar soporte a nuevos productos y servicios.
- La entrega de los proyectos de desarrollo a tiempo y dentro del presupuesto, con el resultado de obtener productos y servicios más eficaces a menor precio en comparación con la competencia.
- La capacidad de asignar los recursos de forma previsible.
- La disponibilidad y fiabilidad uniforme de la información y de los servicios de TI en la organización y para todos los clientes, empresas asociadas del negocio y otros contactos externos.
- Una comunicación clara para gestionar controles eficaces.
- La capacidad de protegerse contra nuevas vulnerabilidades y amenazas de forma rápida y eficiente, y para recuperarse ante cualquier interrupción de los servicios de TI.
- El uso eficiente de un centro de atención al cliente o mesa de ayuda.
- Una cultura de conciencia sobre seguridad entre los usuarios finales a través de toda la organización.

Aunque la función de auditoría interna incluirá probablemente auditores especialistas de TI para enfocar los aspectos de TI en detalle, el DEA(4) también debe entender los temas de control de TI a un alto nivel, en particular, las interacciones de los controles de TI con otros que no sean de TI. Este entendimiento es particularmente importante a la hora de analizar el cumplimiento o las deficiencias del control con la alta dirección, como el presidente, el director financiero (CFO, en inglés), o el director de TI y con los diversos comités de dirección.

El DEA debe ser capaz de analizar las regulaciones y la legislación relevante con el comité de auditoría, el responsable principal de la asesoría legal y con otras personas y comités relevantes. El DEA también debe entender cómo los controles de TI sirven de respaldo a la fiabilidad y la eficiencia, a la vez que ayudan a promover la ventaja competitiva. Más aún, el DEA debe entender a fondo los temas más importantes o críticos que conducen a la necesidad de controles dentro de un sector particular de la organización con el fin de asegurarse de que estén considerados en el alcance de las evaluaciones de auditoría. Sin un conocimiento y entendimiento profundo de los controles de TI, el auditor sería incapaz de comprender su significado o de determinarlo adecuadamente como parte de la revisión global del control interno.

* Ley de 2002 de la Reforma de la contabilidad pública de empresas y protección del inversionista, conocida como Ley Sarbanes-Oxley en honor a sus patrocinadores, el senador Paul Sarbanes y el congresista Michael Oxley de EEUU.

En los últimos años han surgido varias funciones diferentes para los puesto de las organizaciones con responsabilidades y propiedad sobre los controles de TI. Cada función, en los diferentes niveles de gobierno, gestión, operativos y técnicos, debe tener una descripción clara de sus funciones y responsabilidades en relación con los controles de TI, a fin de evitar confusiones y asegurar la asignación de responsabilidad sobre cada asunto en concreto. Esta sección se ocupa de las distintas funciones y responsabilidades sobre los controles de TI dentro de una organización y asignándolas a puestos específicos dentro de una hipotética estructura organizativa.

No existe forma práctica de definir una estructura organizativa para los controles de TI, que sea válida universalmente. El DEA debe identificar dónde recaen las responsabilidades sobre los controles de TI y evaluar si son apropiados respecto a la segregación de funciones, así como las carencias que puedan existir en las responsabilidades asignadas. Una vez hecho esto, el DEA debe saber con quiénes se deben tratar todos los aspectos específicos de TI y de dónde se puede obtener información especifica.

Generalmente, los objetivos del uso de TI dentro de una organización son:

- Entregar información fiable de forma eficiente y servicios de TI seguros, alineados con la estrategia de la organización, las políticas, los requisitos externos y el riesgo asumido.
- Proteger los intereses de los accionistas.
- Potenciar mutuamente relaciones beneficiosas con clientes, socios de negocio y otras partes externas para alcanzar los objetivos de negocio.
- Identificar y responder adecuadamente a las amenazas potenciales de violación de los controles.

Estos objetivos son respaldados por funciones específicas dentro de la organización. La descripción y denominación de los puestos pueden ser diferentes según los países, los sectores y las organizaciones; en organizaciones más pequeñas, algunas de estas funciones pueden estar fusionadas. Sin embargo, siempre deben existir puestos dentro de la organización que sustenten la función del control de TI e interactúen con el DEA y los miembros de auditoría interna.

6.1 Consejo de Administración u órgano de gobierno

Un papel importante del consejo de administración es determinar y aprobar estrategias, fijar objetivos, y asegurar de que se alcancen los objetivos que a su vez respaldan las estrategias. En relación con TI, esto requiere:

- Concienciar sobre temas claves de TI, como las políticas de seguridad de la información y de TI, y los conceptos de riesgo referentes a TI.
- Entender la infraestructura y los componentes estratégicos de TI, así como conocer los proyectos claves de desarrollo y adquisición de sistemas, y sobre cómo ellos respaldan e impactan en la estrategia general, los objetivos y presupuestos (a largo y corto plazo) de la corporación.
- Aprobar la estructura de clasificación de la información y de los respectivos derechos de acceso.

El consejo puede establecer diferentes comités según sea su relación con la organización. Los comités más comunes del consejo son: comité de auditoría, comité de retribuciones y comité de nombramientos; algunos Consejos pueden tener otros comités adicionales, como el comité financiero o el de gestión de riesgos. Estos comités pueden tener nombres diferentes de los que se muestran aquí y sus funciones pueden variar. Lo importante, por lo tanto, son las funciones y no los nombres.

6.1.1 Comité de auditoría

La función del comité de auditoría abarca la vigilancia de cuestiones financieras, la evaluación del control interno, la gestión de riesgos y la ética. Los controles de TI son elementos importantes para cada una de esas obligaciones y requieren:

- Entender la gestión financiera (función de experto financiero) y la dependencia de la organización en relación con TI para el procesamiento y reporte de la información financiera.
- Asegurar que los temas de TI sean incluidos en el orden del día de las reuniones del comité, especialmente el informe del director de TI.
- Asegurar que los controles generales de TI y los controles de los sistemas de aplicación y procesos involucrados en la preparación de los estados contables sean evaluados y probados adecuadamente.
- Supervisar la evaluación global de los controles de TI.
- Revisar los aspectos de negocio y control en relación a los nuevos desarrollos o adquisiciones de sistemas.
- Examinar los planes de auditoría (internos y externos) y procurar asegurar que los aspectos de TI sean cubiertos adecuadamente.
- Revisar los resultados de los trabajos de auditoría y supervisar la solución de los temas presentados.
- Comprender los aspectos de TI que impacten en la supervisión de cuestiones éticas.

6.1.2 Comité de retribuciones

El comité de retribuciones no tiene relación directa con TI. Sin embargo, puede mejorar la supervisión del consejo sobre las TI mediante la inclusión de TI como uno de los elementos de desempeño en cualquier plan de compensación que apruebe.

6.1.3 Comité de nombramientos

El comité de gobierno es responsable de la selección y evaluación de los miembros del consejo, y del liderazgo de las operaciones del consejo. En relación con TI, este comité debe:

- Asegurarse de que los miembros del consejo (potenciales o actuales) tengan el conocimiento o la experiencia adecuados de TI.
- Evaluar el desempeño de los comités del consejo en términos de su supervisión de TI.
- Revisar cualquier evaluación sobre el gobierno por regulación externa en relación con temas de TI.
- Asegurarse de que el consejo revise las políticas de TI periódicamente y que las reuniones del consejo se centren en la TI con una frecuencia adecuada.

6.1.4 Comité de gestión de riesgos

El comité de gestión de riesgos es responsable de la vigilancia de todos los análisis y evaluaciones de riesgos, de las acciones de respuesta y de la supervisión de los riesgos.
Esta función incluye:

- Evaluar en qué medida la dirección ha establecido una gestión de riesgo eficaz de la entidad en la organización.
- Estar al tanto y coincidir con la aceptación y tolerancia al riesgo de la organización.
- Tener conciencia del impacto de los riesgos relacionados con la TI.
- Revisar el conjunto de riesgos de la organización, incluidos los riesgos de TI y contrastarlo con el riesgo asumido por la organización.
- Mantenerse informado sobre los riesgos de TI más significativos y determinar si las respuestas de la dirección a los cambios en los riesgos y amenazas es apropiada.
- Supervisar y evaluar todas las actividades realizadas por la dirección para minimizar todos los riesgos conocidos y documentados.

6.1.5 Comité financiero

El principal papel de un comité financiero es revisar los estados contables, las proyecciones de los flujos de caja y gestionar las inversiones. Los miembros de este comité necesitan entender los elementos de control de TI para asegurar la exactitud de la información utilizada en el proceso de toma de decisiones financieras clave y para generar informes contables. Deben también considerar los beneficios y costes de mantener los sistemas críticos de TI, en comparación con su reemplazo, a través del pedido de informes sobre esto a la gerencia. Los informes de la gerencia deben considerar aspectos relativos a la eficiencia del software, tales como pérdidas o ganancias de productividad debido a mejoras en el uso de TI, los costes del hardware debido a reparaciones y actualizaciones, y los riesgos potenciales a causa de pérdidas o corrupción de datos.

6.2 Gerencia / Dirección

En las grandes organizaciones han aparecido varias funciones específicas en relación al riesgo y control de TI. Como se indicó anteriormente, las organizaciones pequeñas no pueden designar una persona para cada función, sin embargo la función siempre debe existir. Una persona puede realizar varias funciones, pero se debe tener precaución para que al asignar esas funciones, no se atente contra la necesidad de la separación de responsabilidades cuando dos funciones sean incompatibles. Cuando los servicios de TI están externalizados , no desaparece la necesidad de que la organización mantenga muchas de estas funciones supervisando las funciones externalizadas.

6.2.1 Presidente (CEO, en inglés)

Al ser la persona que tiene el control general sobre la estrategia y las operaciones de la organización debe tener en cuenta la TI en la mayoría de los aspectos de su función. En particular, el presidente deberá:

- Definir los objetivos corporativos y las medidas de rendimiento relativas a TI.
- Actuar como custodio de los factores críticos de éxito de la organización en relación con la TI.
- Entender y aprobar la estrategia de TI a corto y largo plazo.
- Aprobar los recursos de TI para la organización, incluidas la estructura y la supervisión.
- Determinar las cuestiones de TI para las deliberaciones periódicas con el consejo de administración, los gerentes y demás personal.
- Operar como propietario de los controles en el más alto nivel teniendo la última responsabilidad por el éxito o fracaso de los controles y por la coordinación de todos los demás gerentes operativos dentro del marco de sus responsabilidades, quienes actúan como propietarios del control en sus áreas específicas.

6.2.2 Director Financiero (CFO, en inglés)

El director financiero tiene la responsabilidad general sobre todas las cuestiones financieras en la organización, debe tener un conocimiento profundo del uso de TI tanto para facilitar la gestión financiera como para respaldar los objetivos corporativos. Esta función debe tener una comprensión general sobre los siguientes temas:

- El coste total de la propiedad de las iniciativas de TI.
- Las estrategias de TI de la entidad para que siga siendo competitiva tecnológicamente.
- Las tecnologías usadas en la implementación de las aplicaciones financieras.
- La operación o explotación o ejecución de aplicaciones financieras específicas.
- Las limitaciones y beneficios de TI.
- La estructura de control de TI para los controles generales que se aplican a todos los sistemas y datos de negocio así como los controles que son específicos para aplicaciones financieras.

El director financiero debe operar como el proprietario de los controles al mas alto nivel para los sistemas y datos financieros.

6.2.3 Director de TI (CIO, en inglés)

El director de sistemas tiene la responsabilidad general del uso de la TI en la organización. En relación con los controles de TI, el director de sistemas debe:

- Entender los requerimientos del negocio que implican la necesidad de implementar TI.
- Trabajar conjuntamente con los gerentes del negocio para:
  - Asegurar que la estrategia de TI esté alineada con la del negocio.
  - Asegurar el cumplimiento (legislativo y normativo).
  - Aprovechar las mejoras de eficiencia en los procesos.
  - Mitigar los riesgos evaluados.
- Diseñar, implementar y mantener un marco de control interno para TI.
- Planificar, proveer y controlar los recursos de TI.
- Explorar, evaluar, seleccionar e implementar avances tecnológicos (por ejemplo, las comunicaciones inalámbricas).
- Fomentar la formación del personal de TI con el fin de asegurar que los niveles de conocimiento y calificación estén permanente actualizados.
- Operar como custodio, al más alto nivel, de los sistemas / datos y como propietario de los controles de TI.
- Medir el rendimiento operativo de TI en relación con el respaldo que le proporciona a los objetivos del negocio; esto se realiza a través de las siguientes acciones:
  - Establecer metas.
  - Evaluar los resultados
- Desarrollar las medidas necesarias para verificar y confirmar que la TI presta los servicios y el respaldo esperados por usuarios y clientes finales, así como por los organismos de control o los auditores externos e internos.

6.2.4 Director de Seguridad (CSO, en inglés)

El director de seguridad es responsable de toda la seguridad a lo largo y ancho de la organización, incluida la seguridad de la información, que también puede ser responsabilidad del director de seguridad de la información cuyas características son las siguientes:

- Tiene la responsabilidad de documentar la política de seguridad de la compañía y asegurar que se han establecido mecanismos para comunicar e impulsar el cumplimiento de dicha política.
- Tiene la responsabilidad general sobre la seguridad lógica y física en la organización, y para todas las conexiones externas a Internet o a otras redes.
- Actúa como nexo entre las funciones de cumplimiento legal, de negocio, dirección de TI y de auditoría.
- Está en primera línea para implementar los principales programas de cumplimiento que afectan a la TI, como la Ley Sarbanes-Oxley y la directiva de protección de datos de la Unión Europea.
- Es responsable de la planificación de continuidad del negocio incluyendo el tratamiento de incidentes y la recuperación de desastres.
- Garantiza que el personal de seguridad proporcione el respaldo necesario para implementar controles en todos los niveles.
- Actúa como líder principal investigando y evaluando nuevas "mejores prácticas" que pueden ser incorporadas a la organización.

6.2.5 Director de Seguridad de la Información (CISO, en inglés)

La seguridad de la información es un subconjunto de la función general de seguridad. El director de seguridad de la información realiza lo siguiente:

- Desarrolla e implementa la política de seguridad de la información de manera coordinada con el director de seguridad.
- Controla y coordina los recursos de seguridad de la información, se asegura que se asignen adecuada-

Controles de TI y ética

Como quedó evidenciado en los casos relacionados con los fondos de inversión en acciones durante los años setenta y en los escándalos que siguen apareciendo hoy día, el uso de la tecnología crea oportunidades significativas para iniciar y perpetuar fraudes y engaños. La capacidad y autoridad para soslayar ciertos controles trae consigo la tentación de iniciar acciones irregulares. Si esas irregularidades no son percibidas, o son tácitamente permitidas, pueden terminar en un fraude rotundo. Por lo tanto, cuando una organización da a un individuo la oportunidad de realizar acciones en nombre de la organización, esta tiene la correspondiente responsabilidad de proporcionar la supervisión adecuada como para detectar y corregir actividades irregulares rápidamente. La organización tiene también la responsabilidad de identificar amenazas de este tipo y establecer salvaguardas como medida preventiva. Las mismas herramientas tecnológicas que pueden crear las oportunidades de fraude se utilizan para identificar actividades, e incluso patrones inusuales en las transacciones u otros datos que podrían indicar una evidencia de fraude o comportamiento cuestionable.

mente para alcanzar los objetivos de seguridad de la organización.
- Asegura la alineación de los objetivos de seguridad de la información y de los objetivos de negocio.
- Gestiona los riesgos operativos de la información en toda la organización.
- Supervisa la seguridad dentro de la organización de TI.
- Proporciona formación y toma de conciencia sobre los asuntos relacionados con la seguridad de la información y con nuevas "mejores prácticas".
- Desarrolla políticas de usuarios finales para el uso de TI conjuntamente con la función de Recursos Humanos.
- Coordina los trabajos de seguridad de la información con el director de riesgos (CRO, en inglés) y el director de TI.
- Asesora al presidente, al director de riesgos, al director de TI y al consejo sobre cuestiones relacionadas con los riesgos de TI.
- Actúa como enlace principal del DEA cuando la auditoría interna realiza auditorías relacionadas con los controles de TI.

6.2.6 Asesoría jurídica

El asesor jurídico puede ser un empleado o directivo de la organización o un asesor externo. Esta función implica lo siguiente:
- Entender y ocuparse de las obligaciones que surgen de la divulgación de información y proporcionar orientación a nivel de políticas para ayudar en la gestión de los riesgos relacionados.
- Asegurar que los informes y las presentaciones financieras cumplan con las leyes y regulaciones.
- Entender los aspectos legales de TI y asesorar sobre los riesgos legales relacionados con la TI.
- Gestionar el buen nombre de la organización en lo referente a cuestiones legales, cumplimiento y relaciones públicas.
- Entender el fraude relacionado con la TI.
- Gestionar los aspectos contractuales de TI.
- Comprender los protocolos de investigación forense en relación con supuestas actividades delictivas.

6.2.7 Director de Riesgos (CRO, en inglés)

Al director de riesgos le incumbe la gestión de los riesgos en todos los niveles de la organización. Dado que los riesgos de TI son parte de esa función, este debe considerarlos con la ayuda del director de seguridad de la información (CISO, en inglés). Esto incluye:
- Análisis y evaluación de las exposiciones a los riesgos de TI, incluyendo aquellas que comprometan a la información, como pérdidas, daños, divulgación no autorizada e interrupción del acceso.
- Evaluación de contingencias de TI como interrupciones, desastres y cambios.
- Análisis y evaluación de los riesgos de negocio y como son afectados por los riesgos de TI.
- Supervisión, soporte, promoción de todas las actividades de TI relacionadas con la minimización de riesgos.

6.3 Auditoría Interna

6.3.1 Auditoría interna, DEA y personal de auditoría

La auditoría interna es una parte esencial del proceso de gobierno corporativo, independientemente de si se utiliza un grupo de auditoría interna específico. Los auditores internos deben tener conocimiento y comprensión general de TI, pero el nivel de tal conocimiento varía según la categoría de las auditorías o el nivel de supervisión (Norma del IIA 1210.A3). El IIA define tres categorías de conocimiento de TI para auditores internos que se describen en el Apéndice C. En relación con la TI, la función de la auditoría interna implica:
- Asesorar al comité de auditoría y a la alta dirección sobre aspectos relacionados con el control interno de TI.
- Asegurar que la TI se incluya en el universo de auditoría y en el plan anual (seleccionar temas).
- Asegurar que los riesgos de TI sean considerados cuando se asignan los recursos y las prioridades en las actividades de auditoría.
- Definir los recursos de TI necesarios para el departamento de auditoría, incluida la formación especializada del personal de auditoría.
- Asegurar que la planificación de auditoría considere los aspectos de TI en cada auditoría.
- Actuar como enlace con los clientes de auditoría para determinar qué desean o qué necesitan saber.
- Realizar análisis de riesgos de TI.
- Determinar qué constituye una evidencia fiable y verificable.
- Realizar auditorías de controles de TI a nivel de empresa.
- Realizar auditorías de los controles generales de TI.
- Realizar auditorías de los controles de aplicación.
- Realizar auditorías especializadas de los controles técnicos de TI.
- Utilizar de manera eficiente y eficaz la TI para contribuir al proceso de auditoría.
- Durante las actividades de desarrollo o análisis de sistemas, debe actuar como experto que conoce cómo se pueden implementar o eludir los controles.
- Ayudar en la supervisión y verificación de la adecuada implementación de actividades que minimicen todos los riesgos de TI conocidos y documentados.

6.3.2 Auditoría Externa

Las auditorías externas independientes son un requisito para la mayoría de las organizaciones y son realizadas normalmente de forma anual. Los temas que deben ser considerados por el departamento de auditoría interna y el comité de auditoría incluyen:

- El alcance de las responsabilidades del auditor externo para entender y evaluar los sistemas y los controles relacionados con TI durante las auditorías financieras.
- El alcance de las responsabilidades del auditor externo en el examen de los sistemas y controles de TI durante un examen formal requerido por los estatutos o por las regulaciones, como los controles internos de la información financiera u otros requisitos legales.

7.1 El riesgo determina la respuesta

Los controles de TI son seleccionados e implementados en función de los riesgos que deben gestionar según su diseño. Una vez que los riesgos son identificados mediante la experiencia o la evaluación formal, se determinan las respuestas convenientes, que podrán variar desde no realizar ninguna acción y aceptar el riesgo como un coste más de funcionamiento del negocio hasta la aplicación de una amplia gama de controles específicos, incluidos los seguros.

Sería una tarea relativamente sencilla crear una lista de controles de TI recomendados a implementar en cada organización. Sin embargo, cada control tiene un coste específico que puede no estar justificado en términos de efectividad cuando se considera el tipo de negocio realizado por la organización. Adicionalmente, ninguna lista de controles es universalmente aplicable a todos los tipos de organizaciones. Aunque existe una gran cantidad de buenas guías disponibles para la elección de controles convenientes, siempre se debe utilizar el propio discernimiento. Los controles deben ser apropiados para el nivel de riesgo al que se enfrenta la organización.

El director ejecutivo de auditoría interna debe poder asesorar al comité de auditoría para determinar si el marco de control interno es fiable y si proporciona un nivel de confianza apropiado conforme al riesgo asumido por la organización. A este respecto, el riesgo asumido por la organización es definido por COSO[3] como:

> "… el grado de riesgo, en sentido amplio, que una compañía u organización esta dispuesta a aceptar en la consecución de sus metas. La dirección considera el "riesgo asumido" de la organización; primero, evalúa las alternativas estratégicas, después establece los objetivos y los alínea con la estrategia escogida para desarrollar los mecanismos y gestionar los riesgos relacionados".

Adicionalmente, el director ejecutivo de auditoría interna debe considerar la tolerancia al riesgo. COSO la define como:

> "… el nivel aceptable de variación en la consecución de los objetivos. Cuando se establezcan tolerancias especificas al riesgo, la dirección debe considerar la importancia relativa de los objetivos correspondientes y alinear las tolerancias en función del riesgo asumido."

Por lo tanto, el director ejecutivo de auditoría interna debe considerar lo siguiente:

- Si el entorno de TI de la organización es coherente con el riesgo asumido por la organización.
- Si el marco de control interno es adecuado para asegurar que el desempeño de la organización se mantenga dentro de la tolerancia al riesgo establecida.

7.2 Consideraciones sobre el riesgo al determinar la adecuación de los controles de TI

La gestión de riesgos es aplicable a todo el espectro de actividad de una organización, no sólo a la función de TI. La TI no se puede considerar de forma aislada, se la debe tratar como parte integrante de los procesos de negocio. Elegir los controles de TI no consiste en implementar las recomendaciones de las "mejores practicas", sino que estos deben añadir valor a la organización reduciendo el riesgo de manera eficiente y aumentando la efectividad.

Cuando se considera la adecuación de los controles de TI en el marco de control interno de la organización, el director ejecutivo de auditoría interna debe considerar los procesos establecidos por la dirección para determinar lo siguiente:

- El valor y la criticidad de la información.
- La aceptación y tolerancia al riesgo para cada función y proceso de negocio.
- Los riesgos de TI a los que se enfrenta la organización y la calidad del servido prestado a sus usuarios.
- La complejidad de la infraestructura de TI.
- Los controles de TI apropiados y los beneficios que aportan.
- Incidentes nocivos en TI en los últimos 24 meses.

La frecuencia del análisis de riesgo es importante y los cambios tecnológicos influyen. En un entorno empresarial y tecnológico estático, la evaluación de los riesgos puede ser poco frecuente (por ejemplo anualmente) o puede ser realizada en consonancia con la implementación de un proyecto importante.

7.2.1 La infraestructura de TI

El análisis y evaluación de riesgos en relación con la TI pueden ser complejos. La infraestructura de TI está formada por el hardware, el software, las comunicaciones, las aplicaciones, los protocolos (reglas) y datos, y su implementación en un entorno físico de la estructura organizativa, y entre la organización y su entorno externo. La infraestructura también incluye a las personas que interactúan con los elementos físicos y lógicos de los sistemas.

El inventario de los componentes de la infraestructura de TI muestra información básica sobre las vulnerabilidades del entorno. Por ejemplo, los sistemas de negocio y las redes conectadas a Internet están expuestos a amenazas que no existen en sistemas o redes aisladas. Dado que la conectividad de Internet es un elemento esencial para la mayoría de los sistemas y redes de negocio, las organizaciones deben asegurar que sus sistemas y arquitecturas de red incluyan controles fundamentales para garantizar una seguridad básica.

El inventario completo de componentes de TI, hardware, software, redes y datos de la organización forma la base para evaluar las vulnerabilidades dentro de las infraestructuras de TI que pueden impactar en los controles internos. Los esque-

[3] Se encuentra estas definiciones en *Enterprise Risk Management – Integrated Framework* (octubre de 2004) de COSO.

mas de la arquitectura de sistemas muestran la implementación de los componentes de la infraestructura y cómo se interconectan con otros componentes dentro y fuera de la organización. Para el experto en seguridad de la información, el inventario y la arquitectura de los componentes de TI, incluida la localización de los controles y tecnologías de seguridad, ofrecen vulnerabilidades potenciales. Desafortunadamente, la información sobre un sistema o una red también ofrece vulnerabilidades para un atacante potencial, por lo tanto el acceso a esa información se debe restringir sólo a las personas que verdaderamente la necesitan. Un sistema y una red debidamente configurados minimizarán el volumen de información a disposición de atacantes potenciales, además, un entorno de aspecto seguro ofrece un objetivo menos atractivo para la mayoría de los atacantes.

7.2.2 Riesgos de TI a los que se enfrenta la organización

El director ejecutivo de auditoría interna analiza los aspectos de riesgo de TI con el director de TI y con los propietarios de los procesos para asegurarse de que todas las partes relacionadas sean conscientes del tema, a la vez que poseen un conocimiento apropiado de los riesgos técnicos a los que se enfrenta la organización por el uso de TI, y sobre sus responsabilidades para aplicar y mantener controles eficaces.

7.2.3 Aceptación y tolerancia al riesgo

Aprovechando el conocimiento de los riesgos de TI, el auditor puede validar la existencia de controles eficaces para alcanzar el grado de aceptación y tolerancia al riesgo de la organización en cuanto a TI. La evaluación del auditor incluirá los debates con los miembros de la dirección y en última instancia con el consejo. El nivel de detalle de esos debates puede ser determinado por el director de riesgos con la información aportada por el director de TI, el director de seguridad de la información, el director de seguridad, el DEA, y por los propietarios de los procesos. La decisión final respecto al grado de aceptación y tolerancia al riesgo debe ser tomada por el comité de riesgo con el asesoramiento del comité de auditoría, y debe ser apoyada por el consejo por completo. Las definiciones de grado de aceptación del riesgo y tolerancia deben ser comunicadas a todos los gestores relevantes para su efectiva implementación.

El objetivo de la gestión de riesgos de la compañía es asegurar que todos estén trabajando con el mismo nivel y comprensión del riesgo y que las decisiones tomadas en todos los niveles de la gerencia sean consistentes con la aceptación de riesgo de la organización.

7.2.4 Realización del análisis de riesgos

La realización del análisis de riesgo no sólo es realizada por el director de riesgos o por el director ejecutivo de auditoría, aún cuando ambos o sus representantes deben estar incluidos, sino también por representantes de TI y de las áreas de negocio.

Existen ocho preguntas básicas asociadas al proceso de evaluación de riesgos. Estas incluyen este primer grupo de cinco:

- ¿Cuáles son los activos en riesgo y cuál es el valor de su confidencialidad, integridad y disponibilidad?
- ¿Qué puede suceder para que el valor de los activos de información se vea afectado negativamente? De forma implícita a esta pregunta está el análisis de vulnerabilidades y la identificación de la relación de vulnerabilidades con las amenazas y con los activos de información potencialmente impactados.
- Si la amenaza se materializa, ¿Cuán negativo podría ser el impacto?
- ¿Con qué frecuencia se espera que se materialicen los eventos negativos (frecuencia de ocurrencia)?
- ¿Cuánta certeza se dispone en las respuestas dadas a las cuatro primeras preguntas (análisis de incertidumbre)?

El segundo grupo de tres preguntas se refiere a la mitigación del riesgo:

- ¿Qué puede hacerse para reducir el riesgo?
- ¿Cuánto costará?
- ¿Es eficiente según la relación costo-beneficio?

7.2.5 El valor de la información

Determinar el valor de la información procesada y almacenada no es tarea fácil debido a la naturaleza multidimensional del valor. Los Principios de seguridad de la información generalmente aceptados (GAISP, en inglés) incluidos en el documento "Pautas para valoración de la información" publicado por la Asociación de Seguridad de Sistemas de Información (ISSA, en inglés, www.ISSA.org) encuadra el valor de la información dentro de los siguientes categorías:

- Bien exclusivo: coste de la pérdida de confidencialidad.
- Utilidad: coste de la pérdida de integridad.
- Coste de la creación y recreación.
- Responsabilidades en caso de litigio.
- Convertibilidad o negociabilidad: representa el valor de mercado.
- Impacto operativo de la indisponibilidad.

7.2.6 Controles de TI apropiados

Finalmente, los controles de TI apropiados deben ser escogidos e implementados para cubrir los riesgos identificados. Existen abundantes consejos al respecto. Consulte Apéndice I.

El director y el grupo de auditoría interna deben estar involucrados en el proceso de analizar y evaluar el riesgo. Al mismo tiempo, deben actuar de forma tal que mantengan la independencia y objetividad de su función, y deben también proporcionar una opinión sobre la efectividad del marco de control interno.

7.3 Estrategias de mitigación de riesgos

Cuando se identifican y analizan los riesgos, no siempre es apropiado implementar controles para contrarrestarlos. Algunos riesgos pueden ser menores y tal vez no sea efectivo (en cuanto a costes) implementar procesos de control para ellos.

En general, existen diversas formas de mitigar el impacto potencial de los riesgos:

- **Aceptar el riesgo.** Una de las funciones de la dirección es gestionar el riesgo. Algunos riesgos son menores debido a que su impacto o probabilidad de ocurrencia son bajos. En ese caso, aceptar conscientemente el riesgo como un coste más del negocio es apropiado, así como revisar periódicamente el riesgo para asegurar que el impacto sigue siendo bajo.
- **Eliminar el riesgo.** Es posible que un riesgo esté asociado al uso de una tecnología, distribuidor o proveedor en particular. El riesgo puede ser eliminado remplazando la tecnología con productos más robustos o buscando proveedores más capaces.
- **Compartir el riesgo.** Los enfoques de mitigación del riesgo pueden ser compartidos con los socios comerciales y los proveedores. Un buen ejemplo de esto es la gestión de una infraestructura externalizada(10). En este caso, el proveedor mitiga los riesgos de la gestión de la infraestructura de TI al ser un especialista y dado que tiene acceso a personal más altamente especializado que la organización primaria. El riesgo también puede ser mitigado transmitiendo el coste de un riesgo materializado a un proveedor de seguros.
- **Controlar o mitigar el riesgo.** Cuando se han eliminado las demás opciones, se deben crear e implementar controles convenientes para prevenir que el riesgo se ponga de manifiesto o para minimizar sus efectos.

7.4 Características a considerar de los controles

Algunos de los aspectos que se deben tener en cuenta durante el proceso de evaluación de los controles de TI son los siguientes:

- ¿Es efectivo el control?
- ¿Alcanza el resultado esperado?
- ¿Es efectivo el conjunto de controles preventivos, de detección y correctivos?
- ¿El control provee evidencia cuando los parámetros de control son rebasados o cuando fallan? ¿Cómo se alerta a la Dirección de los fallos y qué pasos se espera que se den?
- ¿Se conserva la evidencia (pistas de auditoría o de gestión)?

7.5 Controles de línea base de TI

Los controles de TI deben ser aplicados cuando la mitigación del riesgo es la mejor opción. Aunque ellos deben ser aplicados teniendo en cuenta los riesgos relevantes, existe un conjunto de controles a poner en práctica para proporcionar un nivel fundamental: el nivel de higiene de TI. Por ejemplo, el uso de un filtro de seguridad para controlar el tráfico entre la red corporativa y una red pública como Internet, o entre diferentes dominios de la red interna, es un control básico. El nivel de riesgo asociado al valor del negocio y la sensibilidad del trafico de red, los servicios proporcionados y la información almacenada en la infraestructura determina el alcance en el cual los filtro de seguridad deben restringir el tráfico entrante y saliente de las redes de la organización. Los filtros de seguridad son manifestaciones físicas y lógicas de los elementos de la política de seguridad de la información que dictaminan qué cosas pueden entrar y salir de una organización.

Los controles de TI más ampliamente aplicables a todas las infraestructuras de TI son conocidos como controles de línea base y existen diferentes tipos. Dos de ellos que se aplican a la seguridad de TI, uno se denomina "Digital Dozen" y pertenece al Programa para la seguridad de la información de titulares de tarjetas de crédito (CISP, en inglés) de VISA, otro se llama "Fundamental Five" y proviene del Centro para la Seguridad de Internet (CIS, en inglés); ambos controles se complementan.

No es fácil definir los controles de línea base de TI porque las amenazas generales, como el software malicioso y la "piratería informática" cambian y frecuentemente se implantan nuevas tecnologías y aplicaciones en la organización. Las siguientes cuestiones deben ser consideradas cuando se selecciona un conjunto adecuado de controles de línea base:

- ¿Existen políticas que incluyan controles de TI?
- ¿Se han definido, asignado y aceptado las responsabilidades de TI y de controles de TI?
- ¿Se han asegurado lógica y físicamente los equipos y herramientas de la infraestructura de TI?
- ¿Se usan mecanismos de control para el acceso y la autenticación?
- ¿Se ha implementado un software antivirus y se realiza su mantenimiento?
- ¿Se ha implementado una tecnología de filtros de seguridad conforme a la política de la empresa (por ejemplo, en lo lugares de conexiones externas, como Internet, y en los lugares donde se necesita una separación entre redes internas)?
- ¿Se han completado evaluaciones de vulnerabilidades, se han identificado los riesgos y todo se ha resuelto adecuadamente?
- ¿Existen procesos de gestión de configuración, de cambios y de aseguramiento de calidad?
- ¿Existen procesos de supervisión y de medición del servicio?
- ¿Se dispone de especialistas con competencias en auditoría de TI (sea interna o externamente)?

En el Apéndice I, se puede obtener información adicional sobre controles de línea base de TI.

.

"Digital Dozen"

Una de las guías de seguridad más concisa y ampliamente útil es la del centro CISP de VISA, esta ha probado su valor durante dos años de uso por parte de los proveedores de red de tarjetas de crédito VISA, incluidos bancos, procesadores e intermediarios, entre otros. VISA utiliza la denominación "Digital Dozen" para referirse a estos requisitos.

1. *Instalar y mantener un filtro de seguridad para proteger los datos.*
2. *Mantener al día las actualizaciones de seguridad.*
3. *Proteger los datos almacenados.*
4. *Cifrar los datos enviados por redes públicas.*
5. *Usar y actualizar regularmente software antivirus.*
6. *Restringir el acceso a las personas que deben conocer la información.*
7. *Asignar un identificador único (ID) a cada persona con acceso a una computadora.*
8. *No utilizar las contraseñas de acceso y parámetros de seguridad predeterminados por el proveedor.*
9. *Registrar todos los accesos y los datos mediante identificador único (ID).*
10. *Probar regularmente los sistemas y procesos de seguridad.*
11. *Probar regularmente los sistemas y procesos de seguridad.*
12. *Restringir el acceso físico a los datos.*

"Fundamental Five"

Los "benchmark de consenso" del Centro para la Seguridad de Internet (www.cisecurity.org), proporcionan una guía denominada "Fundamental Five" de higiene básica de seguridad. Del uso de esos criterios se obtiene una reducción del 80 y 95% de las vulnerabilidades conocidas.

1. *Gestión de la identidad y del acceso (incluida la asignación de privilegios y autenticación).*
2. *Gestión de cambios (incluida la gestión de actualizaciones).*
3. *Gestión de la configuración.*
4. *Filtro de seguridad (estaciones de trabajo, servidores, sub-redes, perimetral).*
5. *Protección contra software dañino (incluidos gusanos y virus).*

8.1 Elegir la infraestructura de control

La adopción por parte de la organización de un esquema formal de control ayuda sustancialmente al proceso de identificar y evaluar los controles de TI necesarios para tratar riesgos específicos. Este esquema debe aplicarse y ser utilizado en toda la organización, y no sólo por auditoría interna. Aunque existan muchos esquemas, ninguno cubre específicamente cada tipo de negocio o implementación tecnológica.

El marco de control es una manera organizada de categorizar los controles para asegurar que el espectro entero de control esté cubierto adecuadamente. El esquema puede ser informal o formal. Un enfoque formal podrá satisfacer más fácilmente los diferentes requerimientos regulatorios o estatutarios a los que se enfrentan muchas organizaciones.

Cada organización debe examinar los esquemas de control existentes para determinar cuál de ellos, o qué parte de ellos, se ajusta más estrechamente a las necesidades. El proceso de elegir o construir un esquema de control debe involucrar a todos los puestos de trabajo la organización que tengan responsabilidad directa sobre los controles. El director de auditoría interna debería estar involucrado en el proceso de decisión porque la función de auditoría interna determinará la adecuación y uso del esquema como contexto para la planificación y ejecución del trabajo de auditoría.

El director ejecutivo de auditoría interna debe tener conocimiento global de los temas de riesgo de TI para evaluar la efectividad y lo apropiado de los controles de TI. El director ejecutivo de auditoría interna basará el plan de auditoría y asignará los recursos de auditoría según las áreas de TI que merecen atención dado sus niveles inherentes de riesgo. El análisis y evaluación de riesgos no se pueden pensar como procesos de única vez, especialmente cuando son aplicados a TI, porque la tecnología cambia constante y rápidamente, al igual que los riesgos y las amenazas asociadas. Es útil categorizar los controles de TI de acuerdo a su ubicación, propósito y funcionalidad organizativa tanto para la evaluación de su valor y adecuación, como para lo apropiado del sistema de controles internos. El conocimiento del rango de controles disponibles de TI, las fuerzas impulsoras para los controles, y los roles y las responsabilidades organizativas permiten analizar y evaluar exhaustivamente los riesgos. En la evaluación de la efectividad de los controles, es también útil entender si los controles son obligatorios o voluntarios, discrecionales o no, manuales o automatizados, primarios o secundarios, y si pueden ser omitidos o ignorados por la dirección.

Finalmente, la evaluación de los controles de TI implica seleccionar controles claves para realizar pruebas, evaluar los resultados de las pruebas y determinar si existen o no evidencias que indiquen debilidades significativa de control. El cuestionario que se adjunta en esta guía (Apéndice H) puede ayudar al director ejecutivo de auditoría interna en cuanto a asegurar que todos los temas relevantes se han considerado

Modelo COSO para controles de la tecnología

Vigilancia o supervisión:
- Métricas mensuales del rendimiento de la tecnología.
- Análisis del rendimiento del control y costes de la tecnología.
- Evaluaciones periódicas de la gestión de la tecnología.
- Auditoría interna de la tecnología de la empresa.
- Auditoría interna de las áreas de alto riesgo.

Actividades de control:
- Comité examinador de la gestión de cambios.
- Comparación de las iniciativas de tecnología con los planes y el retorno de la inversión.
- Documentación y aprobación de planes de TI y arquitecturas de sistemas.
- Cumplimiento de las normas de seguridad física y de la información.
- Adhesión a la evaluación de riesgos para continuidad del negocio.
- Impulsar el cumplimiento de las normas de tecnología.

Información y comunicación:
- Comunicaciones corporativas periódicas (Intranet, correos electrónicos, reuniones, correos).
- Conocimiento de las mejores prácticas de la tecnología en curso.
- Capacitación en seguridad y TI.
- Mesa de ayuda para consultas y resolución de problemas en curso.

Evaluación de riesgos:
- Riesgos de TI incluidos en la evaluación global de los riesgos corporativos.
- TI integrada en las evaluaciones de riesgo del negocio.
- Diferenciación de los controles de TI para áreas/funciones de alto riesgo del negocio.
- Evaluación de la auditoría interna de TI.
- Evaluación de la seguridad de la TI.

Entorno de control:
- Alinear de manera descendente los controles de TI y seguridad considerados importantes.
- Política global de tecnología y política de seguridad de la información.
- Comité de Gobierno Corporativo de Tecnología.
- Comité de Normas y Arquitectura de Tecnología.
- Representación completa de todas las unidades del negocio.

Figura 5 · Modelo COSO para controles de la tecnología

durante la planificación y dirección de las evaluaciones de auditoría interna y de los controles de TI. Algunos esquemas y enfoques existentes pueden ayudar al director ejecutivo de auditoría interna y a otros gerentes cuando se determinan los requerimientos de control de TI. Sin embargo, las organizaciones deben investigar suficientes esquemas como para determinar cuál es el que mejor se ajusta a sus propias necesidades y cultura. En el Apéndice D se proporciona una lista parcial de esquemas disponibles.

El Enfoque Integrado de Control Interno de COSO (1992) es aceptado por el Consejo Supervisor Contable de Empresas Públicas (PCAOB, en inglés) con el propósito de informar sobre el cumplimiento con las provisiones de información financiera, pero no es específico para todas las áreas de TI. Este esquema se considera un esquema "adecuado y reconocido" que se puede adoptar para el cumplimiento de la Ley Sarbanes-Oxley porque cubre todas las áreas de implementación de TI, aunque a un nivel alto de abstracción.

8.2 Supervisar los controles de TI

No es fácil determinar dónde se debe aplicar la supervisión y evaluación de los controles y su frecuencia. La participación del auditor, en el ejercicio del análisis de riesgos y la implementación de un entorno de control adecuado, pueden ayudar a que el director ejecutivo de auditoría interna tenga información suficiente para crear un plan adecuado de auditoría que contemple los riesgos más importantes de TI.

En última instancia, la dirección es responsable de la supervisión y evaluación de los controles. La supervisión y las evaluaciones del auditor se realizan para corroborar, de forma independiente, las afirmaciones de la dirección en cuanto a la adecuación de los controles. Las actividades de supervisión y evaluación del control realizadas por la dirección, deben ser planificadas y conducidas dentro de diversas categorías, tales como las siguientes:

8.2.1 Supervisión continua

- **Diaria o periódica:** Hay determinada información que se debe verificar diariamente para asegurar que los controles estén funcionando tal como se requiere. La dirección realiza normalmente esta supervisión que tradicionalmente incluye la verificación de los informes de control del proceso de los datos que permiten determinar que las tareas y los trabajos(8) se han completado satisfactoriamente. Estos controles, cuando existen, generalmente están automatizados. El director ejecutivo de auditoría interna se asegurará de que la gestión de supervisión exista y que esté sujeta a la evaluación de la auditoría interna.
- **Orientada a los sucesos:** Las discrepancias, o incluso los fraudes, pueden tener lugar dentro del procesamiento normal, o en circunstancias especiales, como puede suceder cuando existen transacciones por valores considerables. En muchos entornos de TI, es probable que ocurran ataques malintencionados. Consecuentemente, deben existir controles específicos para detectar y reportar actividades inusuales para una unidad dentro de la organización que está facultada específicamente para investigar y determinar si deben aplicarse acciones preventivas o correctivas. Estos controles de supervisión son complementarios a los controles habituales usados y proporcionan aseguramiento(10) sobre la efectividad de aquellos controles o alertas tempranas que pueden indicar que los controles habituales pueden haber sido rotos o infringidos.
- **Continua:** La tecnología proporciona hoy en día, la posibilidad de supervisar y evaluar continuamente ciertos controles sensitivos. Un buen ejemplo de supervisión continua es el uso de software de detección de intrusos, que vigila continuamente el tráfico de red, proporcionando evidencias para otros controles de protección, como filtro de seguridad y protección contra virus, que pueden ser violados.

8.2.2 Revisiones especiales

- **Evaluación del control anual (o trimestral):** La Ley Sarbanes-Oxley en Estados Unidos requiere evaluaciones de control cíclicas. Aún cuando se requiere que el Consejo de Administración haga declaraciones en relación con la efectividad de los controles internos, la dirección es la que realmente debe propor-

Esquema adecuado y reconocido

"…el esquema, en el cual se basa la declaración de la dirección sobre el control interno en relación con los informes contables, debe ser un enfoque de control adecuado y reconocido establecido por un organismo o grupo que ha seguido los procedimientos debidos en estos procesos, incluida la distribución de tal enfoque para su observación pública". Sin duda, el mejor enfoque conocido que alcanza esta definición es el diseñado por el Comité de Organizaciones Patrocinadoras de la Comisión Treadway, más conocido como el informe COSO, que fue publicado en 1992 y traducido al castellano por el Instituto de Auditores Internos de España.

— Scott A. Taub, Contador Subdirector, Comisión del Mercado de Valores de EE. UU. (SEC, en inglés), SEC y Conferencia de Informes Financieros, Pasadena, California, 29 de mayo de 2003

cionar esas "aseveraciones o garantías" al Consejo y tanto los auditores internos como externos deben realizar un trabajo de auditoría suficiente para avalar dichas aseveraciones.

- **Revisiones de Auditoría:** A pesar de la proliferación de nuevos enfoques de auditoría, aún es necesario un programa regular de revisiones de auditoría. Solamente a través de una revisión formal de la infraestructura, procesos e implementación de la tecnología, es que el director ejecutivo de auditoría interna puede evaluar la fiabilidad y fortaleza global del sistema de controles internos. En el pasado estas revisiones eran planificadas cíclicamente. Sin embargo, dada la rapidez de los cambios en el mundo de TI, las revisiones de auditoría deberán ser agendadas según el nivel de riesgo.

9.1 ¿Qué metodología de auditoría utilizar?

La auditoría de TI ha sufrido muchos cambios en los 40 años de su existencia: los componentes de la tecnología se han vuelto más pequeños, más rápidos, más baratos, mientras que el coste global de TI para la organización ha aumentado significativamente. La mayoría de los procesos de negocio se han automatizado, especialmente para proporcionar eficacia, pero también para hacer posible ciertos procesos de negocio que no se pueden realizar manualmente. Las consabidas comunicaciones de red, incluyendo Internet, han eliminado cualquier distinción entre el negocio y el negocio electrónico. De forma similar, el proceso de auditoría ha evolucionado para ponerse al mismo nivel de la automatización de los procesos de negocio. En los primeros tiempos de la automatización, los auditores "auditaban alrededor de la computadora". Ahora utilizan software para probar o analizar datos y controles técnicos dentro de los sistemas.

Un enfoque de auditoría usado mayoritariamente incluye el análisis del procesamiento de transacciones de negocio importantes mediante sistemas automatizados. En tales auditorías, el auditor identifica las actividades y la información que deben estar sujetas a control y evalúa la capacidad de los controles existentes para proporcionar una protección fiable, incluida la suficiencia de la evidencia en relación a la fiabilidad de los controles. Dado que las auditorías operativas de los procesos automatizados de negocio identifican frecuentemente las deficiencias del control interno, los auditores internos pueden a veces transferir su atención a auditorías de los procesos, o hasta incluso implicarse en aquellas actividades de negocio que están automatizadas, tales como diseño, desarrollo y adquisición, implementación y mantenimiento de sistemas.

Los auditores experimentados desarrollan un conocimiento extenso de los controles internos, sus fortalezas y sus debilidades. Por lo tanto, no es raro que los auditores internos proporcionen servicios de consultoría a la dirección para diseñar e implementar controles internos. El alcance y las limitaciones sobre tal actividad de consultoría son prescritas en las *Normas Internacionales para la Práctica Profesional de Auditoría Interna* (consulte http://www.theiia.org/guidance.). Sin embargo, la implicación del auditor interno en actividades de diseño, desarrollo, o implementación no absuelve a la dirección de la responsabilidad de esas actividades.

Hoy en día, no hay metodologías de auditoría específicas que puedan ser consideradas como mejor, actual y única práctica. Los auditores internos adoptan los métodos y prácticas que mejor se adecúen al trabajo específico. Por ejemplo:

- Cuando se realiza la evaluación en función de los requisitos de Sarbanes-Oxley, un enfoque de auditoría basado en sistemas puede ser el mejor método.
- Las investigaciones de fraude tal vez requieran el uso de software de auditoría para analizar datos y buscar evidencia. El software de auditoría proporciona capacidad analítica potente y adicionalmente proporciona la capacidad para examinar todos los registros y archivos relevantes.
- La realización del trabajo anual de auditoría como soporte de los objetivos principales de auditoría interna, seguirá muy probablemente un enfoque basado en el riesgo.

9.2 Prueba de los controles de TI y aseguramiento continuo

Además de evaluar la adecuación de los mecanismos de control de TI, se deben realizar revisiones regulares para asegurarse de que los controles continúan funcionando según lo requerido. Un método tradicional usado por los auditores internos es crear una población de datos de prueba que se procesan a través de los sistemas de negocio para verificar los resultados y asegurar, por ejemplo, que los controles continúan aceptando datos válidos y rechazan elementos incorrectos e inválidos. Sin embargo, dado que los sistemas del negocio de hoy día son muy amplios, de naturaleza compleja, e interactivos, las pruebas de auditoría tienden a centrarse más específicamente en controles automatizados claves y en el análisis de los datos.

Cómo la auditoría contribuye a los controles de TI

Durante las últimas cuatro décadas, ha habido períodos de reflexión cuando la dirección y los auditores convinieron en que los auditores podrían agregar valor a la organización contribuyendo con su experiencia en controles al desarrollo de los procesos para asegurar que fuesen incorporados en los nuevos sistemas, en vez de añadir controles después que una auditoría revelara una deficiencia. Esas actividades coincidieron con los progresos en el diseño e implantación de los controles y la autovaloración de riesgos en los sectores más importantes del mundo de la auditoría. La consultoría de auditoría y la auditoría basada en riesgos se difundieron ampliamente. Los años 90 y posteriores también fueron testigos de una creciente e importante atención a la gestión de seguridad de la información dado que los ataques del ciberespacio aumentaron en número y en severidad. Estos acontecimientos han ayudado a delinear la función del auditor de TI así como al reconocimiento por parte del mundo de los negocios, de la importancia de una gestión efectiva en cuanto a seguridad de la información.

9.2.1 Supervisión continua y automatizada

Las herramientas de auditoría y supervisión continua se han utilizado por muchos años. Anteriorment se denominaban "Software de auditoría integrado", allí el código del programa comprueba los datos que son procesados en los sistemas de negocio según los criterios predeterminados e informa sobre las anomalías que detecta. La ventaja de tal supervisión es obvia: cualquier discrepancia puede ser identificada y se puede actuar inmediatamente sobre ella. Actualmente, muchos productos propietarios de software de negocio proporcionan tal funcionalidad de supervisión continua. El concepto también ha ido más allá de las aplicaciones de negocio. Por ejemplo, la mayoría del software de filtros de seguridad y de los sistemas de detección de intrusos realizan continuas verificaciones para saber si hay escenarios potenciales de ataques y proporcionan alarmas inmediatas cuando se detectan ataques potenciales. Este tipo de supervisión puede causar problemas debido al volumen considerable de datos y errores potenciales que se detecten, no todos de ellos, serán dignos de atención. La tarea de refinar las técnicas de análisis y supervisión de los limites mínimos requiere vigilancia constante para determinar qué alertas que se deben destacar y cuáles se deben aceptar como sucesos normales.

9.2.2 Herramientas automatizadas de análisis de control interno

El software de auditoría puede ser utilizado para analizar datos almacenados y comprobar su validez para así asegurar la ejecución continua y fiable de los controles internos. Originalmente denominados como software de interrogación de auditoría, los productos tales como ACL (www.acl.com) o IDEA de CaseWare (www.caseware.com) proporcionan ahora funcionalidades sofisticadas y específicas de análisis que pueden reducir la carga de trabajo de la evaluación del control mientras se incrementa la efectividad y eficiencia. Los productos tales como Microsoft Excel también contienen herramientas potentes de análisis que los auditores pueden utilizar.

9.2.3 Análisis de riesgos automatizado

También hay disponibles herramientas para automatizar el proceso de análisis de riesgos. Estas herramientas son inestimables para toda la función de auditoría interna, no solo para el auditor de TI o especialista en riesgos. En nuestros días, realizar un análisis apropiado de riesgos en entornos de TI complejos no es fácil sin la ayuda de herramientas automatizadas.

La dirección es responsable de realizar evaluaciones de riesgos para determinar los controles a implementar o para mejorarlos. Los auditores internos realizan análisis similares cuando evalúan la adecuación de los controles para determinar los objetivos del plan de trabajo y el alcance de la auditoría. Las herramientas automatizadas pueden asistir a ambos procesos. La automatización de la gestión de la auditoría interna es un tema importante por derecho propio.

9.3 Interfaces entre la auditoría o el comité de auditoría o la dirección

No es práctico establecer reglas para informar sobre cada situación especial de los controles de TI. El director ejecutivo de auditoría interna debe aplicar un juicio prudente cuando exprese una opinión o emita un informe al comité de auditoría. Esto no es diferente de la forma en que el director ejecutivo de auditoría interna interactúa con el comité de auditoría con respecto a otros temas de control interno.

El director ejecutivo de auditoría interna discutirá con el comité de auditoría los temas de control interno para determinar el nivel óptimo de la información a ser proporcionada para permitir al comité de auditoría cumplir con sus obligaciones de gobierno estatutarias, legales, de políticas, de debido cumplimiento u otras

Las "métricas y el informe" y "los resúmenes de informes de auditoría" son dos áreas donde el director de auditoría interna debe interactuar con el comité de auditoría con respecto a los controles internos. Otras interacciones dependerán de las necesidades específicas del comité de auditoría y de cualquier requisito legislativo o regulatorio.

Métricas e informes . Las métricas y los informes deben presentar información significativa sobre el estado de los controles de TI. Mientras que la dirección proporciona las métricas y los informes, el director ejecutivo de auditoría interna debe poder atestiguar su validez y opinar sobre su valor. Esto se logra a través de una revisión de auditoría de las áreas de control relevantes para producir una evaluación objetiva e independiente. El director ejecutivo de auditoría interna debe comunicarse con la dirección en todos los niveles y con el comité de auditoría para acordar sobre la validez y la efectividad de las métricas y de los aseguramientos elegidos para los informes.

Un conjunto básico de métricas de gobierno y de gestión para la seguridad de la información se incluye en el Apéndice G. Estas métricas no incluyen datos específicos con respecto a la realización de controles técnicos detallados, aunque los controles técnicos pueden proporcionar la información usada en la medición. Las métricas reales usadas dependerán de la organización y de las necesidades del comité de auditoría. El director de auditoría interna puede seleccionar ejemplos de mediciones tomadas en cualquier nivel de la organización para ayudar a ilustrar las materias que pueden impactar materialmente sobre los controles a nivel de gobierno.

Resúmenes de informes de auditoría. Preparados habitualmente para el comité de auditoría, estos informes resumen hallazgos, conclusiones y opiniones sobre el estado de los controles de TI. También pueden informar sobre las acciones acordadas de informes de auditorías anteriores y el estado de esas acciones, probablemente sobre una base de excepciones en cuanto a acciones no implementadas en el marco de tiempo previsto. Los resúmenes de controles de TI

no pueden ser presentados de manera aislada, sino que deben ser presentados en el contexto del marco completo de control interno.

La frecuencia de los informes depende de las necesidades de la organización. En un entorno regulador fuerte, tal como el proporcionado por Sarbanes-Oxley en Estados Unidos, se requiere que los informes sean trimestrales. En otros casos, la frecuencia de los informes se ajustará al esquema de gobierno de la organización, a la filosofía y al alcance de los riesgos de TI.

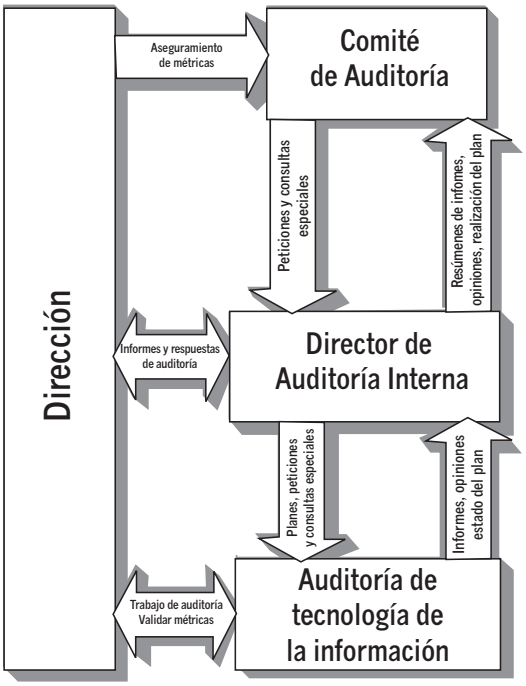

Figura 6 · Interrelaciones de auditoría

La evaluación de los controles de TI es un proceso constante, debido a que los procesos de negocio cambian permanentemente, la tecnología avanza continuamente, las amenazas se desarrollan a la vez que emergen nuevas vulnerabilidades y los métodos de auditoría continúan mejorando. El director ejecutivo de auditoría interna debe mantener las evaluaciones de los controles de TI que respaldan los objetivos de negocio, en el nivel más alto de la agenda de auditoría.

La evaluación de los controles de TI no es un trabajo de sólo determinar si se están empleando las mejores prácticas, dado que los controles son específicos para la misión, objetivos, cultura, tecnología y procesos implementados y riesgos de la organización. La tecnología debe ser adaptada para proporcionar controles eficaces y el director de auditoría interna debe asegurar que la auditoría interna adopte métodos apropiados y eficaces. La auditoría de TI es un proceso de aprendizaje continuo.

El director ejecutivo de auditoría interna my rara vez entiende todas las tecnologías usadas en su entorno y sus implicaciones de control específicas. Por ello, los auditores de TI, adecuadamente certificados y con experiencia son un activo importante para cualquier función de auditoría interna. Sin embargo, el director ejecutivo de auditoría interna debe entender los temas globales de control y poder comunicarlos a la más alta dirección y a los comités apropiados del Consejo de Administración en una forma que pueda ser fácil de entender y de una manera que dé lugar a una respuesta apropiada. La clave para evaluar efectivamente los controles de TI es la comunicación con el personal técnico, la dirección y los miembros del Consejo.

Nota: Este apéndice se extrae del informe del equipo de mejores prácticas y métricas del Grupo de Trabajo de Seguridad de la Información Corporativa (CISWG, en ingés), enviado el 17 de noviembre de 2004, al Subcomité de Política de Tecnología de la Información, Relaciones Intergubernamentales y Censo; Comité de Reforma de Gobierno; Cámara de Representantes de Estados Unidos; enmendado posteriormente el 10 de enero de 2005. Se puede obtener información adicional en la sección "Tecnología" de http://www.theiia.org

11.1 Gobierno (Consejo de Administración)

- Supervisar los programas de gestión de riesgos y cumplimiento relacionados con la seguridad de la información (por ejemplo, Ley Sarbanes-Oxley, Ley de Registro de Seguros Médicos y Ley Gramm-Lixivian-Bliley).Accountability Act, Gramm-Leach-Bliley Act).
- Aprobar y adoptar principios amplios del programa de seguridad de la información y aprobar la designación de gerentes clave responsables de seguridad de la información.
- Procurar la protección de los intereses de todos los accionistas en lo referente a seguridad de la información.
- Revisar las políticas de seguridad de la información con respecto a socios estratégicos de negocio y otras terceras partes.
- Asegurar la continuidad del negocio.
- Revisar las previsiones de auditorías internas y externas del programa de seguridad de la información.
- Colaborar con la dirección en especificar las métricas de seguridad de la información que se comunicarán al Consejo.

11.2 Dirección

- Establecer las políticas de gestión de seguridad de la información, los controles y la supervisión del cumplimiento.
- Asignar las funciones de seguridad de la información, responsabilidades y conocimientos requeridos y hacer cumplir el criterio de privilegios de acceso basado en la necesidad de información de cada función.
- Evaluar los riesgos de la información, establecer umbrales de riesgo y gestionar activamente la mitigación del riesgo.
- Asegurar la implementación de los requisitos de seguridad de la información para los socios estratégicos y otras terceras partes.
- Identificar y clasificar los activos de información.
- Implementar y probar los planes de continuidad del negocio.
- Aprobar la arquitectura de los sistemas de información durante la adquisición, desarrollo, operaciones y mantenimiento.
- Proteger el entorno físico.
- Asegurar la realización de auditorías internas y externas del programa de seguridad de la información, con el oportuno seguimiento.
- Colaborar con el personal de seguridad para especificar las métricas de seguridad de la información que se deben comunicar a la dirección.

11.3 Técnica

Establecer un programa completo de seguridad de la información requiere la atención a los siguientes componentes de programas técnicos:

- Identificación y autenticación de usuarios.
- Gestión de cuentas de usuarios.
- Privilegios de usuarios.
- Gestión de configuraciones.
- Registro y supervisión de eventos y actividades.
- Comunicaciones, correos electrónicos y seguridad en los accesos remotos.
- Protección de códigos malignos, incluyendo virus, gusanos y troyanos.
- Gestión de cambios de software, incluyendo parches.
- Filtro de seguridad.
- Cifrado de datos.
- Copia de respaldo y recuperación.
- Detección de incidentes, vulnerabilidades y respuesta a ellos.
- Colaborar con la dirección para especificar las métricas técnicas que se deben comunicar a la dirección.

Hay un volumen creciente de legislación que afecta de forma estructural al sistema de control interno que las organizaciones eligen implementar. Aunque gran parte de esta legislación ha surgido en años recientes en Estados Unidos como resultado de varios escándalos corporativos, esto también ha afectado a organizaciones en otros países. Las organizaciones deben informarse sobre la legislación, las regulaciones y las prácticas de negocio relevantes en el mundo, en particular, las de los países en los que tienen negocios, con el fin de evaluar los impactos y requerimientos organizativos.

Por ejemplo, la legislación de protección de datos de Europa inhibe la transferencia de información a otros países que no tengan una regulación comparable sobre protección de datos. Esto afecta las relaciones comerciales en las que la información que se debe transferir se refiere a la identificación de las personas. La Ley Sarbanes-Oxley establece requisitos de información del sistema de control interno para todas las organizaciones que coticen en Estados Unidos, así como para sus subsidiarias en el extranjero.

El apéndice proporciona un resumen de requisitos y el impacto de la principal legislación y regulación que debería ser considerada en la evaluación y en la gestión de controles de TI. Aunque esta GTAG está dirigida a una audiencia global cubre la Ley Sarbanes-Oxley con una cierta profundidad porque es una de las legislaciones más significativas de los últimos años. Los Principios de Gobierno Corporativo de la Organización para la Cooperación y el Desarrollo Económicos (OCDE, en inglés) proporciona un marco general para la implementación de controles de negocio. Los acuerdos de Basilea II tienen un impacto importante en el sector financiero internacional y muchos han sugerido que la dirección marcada por Basilea II puede también influir en otros sectores.

12.1 Ley Sarbanes-Oxley de Estados Unidos del año 2002

La ley Sarbanes-Oxley (http://www.theiia.org/iia/guidance/issues/sarbanes-oxley.pdf) fue ideada para reformular las prácticas de la auditoría externa y otros procesos del gobierno corporativo en los mercados de capitales, como consecuencia de los escándalos del caso Enron y del Worldcom. El PCAOB proporciona una conjunto extenso de información y consejos sobre la Ley Sarbanes-Oxley en su sitio Web http: www.sarbanes-oxley.com. Los principales requisitos de la Ley Sarbanes-Oxley, la SEC y las Bolsas de Valores de Estados Unidos se comparan y contrastan en el análisis de la Fundación para la Investigación del IIA, titulado "Assessment Guide for U.S. Legislative, Regulatory, and Listing Exchanges Requirements Affecting Internal Auditing" (www.theiia.org/iia/download.cfm?file=519).

Sin embargo, la Ley Sarbanes-Oxley no trata la aplicación de controles de TI de manera específica. Esto no significa que se pueda ignorar la TI cuando se realizan las revisiones de cumplimiento requeridas por esa ley. La ley es neutral con respecto a la tecnología, pero dadas las implicaciones, está claro que los controles de TI son críticos con respecto al sistema general de control interno de una organización. Como los controles de TI apuntan al desempeño seguro, estable, y fiable del hardware, del software, y del personal, para asegurar la fiabilidad de las aplicaciones, procesos, e informes financieros, éstos deben ser un elemento significativo de las revisiones de cumplimiento.

Se han interpretado ciertas áreas clave de controles de TI como que no han sido incorporadas dentro del alcance de la Ley Sarbanes-Oxley. Éstas incluyen la privacidad, la continuidad de negocios, los sistemas de negocio, la clasificación de los datos, y la información no específica del proceso financiero y su divulgación. Por lo tanto, cualquier revisión limitada específicamente a la conformidad con la Ley Sarbanes-Oxley no cubrirá todos los riesgos de la organización, y se debe complementar para asegurar la cobertura completa por parte de la auditoría en cuanto a gestión de riesgos y control interno de la organización.

12.1.1 Secciones de la Ley Sarbanes-Oxley relevantes para los controles de TI

Los siguiente puntos describen brevemente las secciones de la Ley Sarbanes-Oxley que se relacionan con los auditores y los controles de TI.

12.1.1.1 Secciones 103 y 802

Estas secciones establecen las reglas referidas a la auditoría y al informe de auditoría, para la firma de auditoría externa. En particular, requieren que el Consejo de Administración establezca las normas para el trabajo de la auditoría. También requieren que los auditores prueben los esquemas de control interno y corroboren la fortaleza de esos esquemas. Esta revisión debe incluir un examen cuidadoso de los controles de TI que son fundamentales para el sistema del control interno relacionado con la información financiera.

Hay un requisito específico que está relacionado con la retención de registros "que en razonable detalle y exactitud reflejen las transacciones y las disposiciones de los activos." Una vez más, esto está mayormente influenciado por la forma de registrar y mantener los registros de TI.

12.1.1.2 Sección 201

Esta sección requiere que los auditores externos sean independientes. Esto los imposibilita de realizar trabajo para un cliente en el ámbito de consultoría de TI o la prestación de servicios subcontratados de auditoría interna. Las organizaciones que no desean emplear sus propios auditores de TI no pueden subcontratar el trabajo a sus auditores externos.

12.1.1.3 Sección 301

La sección 301 define la necesidad de que los miembros del Comité de Auditoría sean independientes y los inhabilita de realizar cualquier otro trabajo de consultoría en nombre de la organización. También requiere que los Comités de

Auditoría establezcan procedimientos para manejar el envío anónimo y confidencial, por parte de los empleados, sobre aspectos preocupantes o cuestionables de la contabilidad o aspectos importantes de la auditoría. Esto también se aplicaría con cualquier tema similar al de los controles de TI.

12.1.1.4 Secciones 302 y 404

La sección 302 de la ley requiere que el presidente (CEO, en inglés) y el director financiero (CFO, en inglés), responsables de la información financiera y del sistema de control interno, evalúen el sistema de control interno cada 90 días e informen sus conclusiones y cambios realizados.

Deben poner de manifiesto:

- "Todas las deficiencias significativas en el diseño o en la realización de los controles internos que podrían afectar adversamente la capacidad del emisor de registrar, procesar, resumir y divulgar datos financieros e identificar, para los auditores del emisor, cualquier debilidad material en los controles internos".
- "Cualquier fraude, material o no, que involucre a la dirección o a otros empleados que tienen un papel significativo en los controles internos del emisor".

La sección 404 requiere que el CEO y el CFO generen un informe de auditoría anual que:

- Evalúe la efectividad del esquema de control interno en relación con la información financiera.
- Ponga de manifiesto todas las debilidades conocidas de control interno.
- Ponga de manifiesto todos los fraudes identificados.

Este informe cubrirá todos los controles de TI aplicables, incluidos la programación lógica y los controles de cambios relacionados, los controles de acceso y la protección de los datos. La Norma de Auditoría N.º 2 del PCAOB sugiere el enfoque COSO como base para la sección 404 de gestión del cumplimiento. Las referencias a la Declaración sobre Normas de Auditoría 95 (SAS, en inglés) también acentúan la importancia de TI y de los controles de seguridad de la información para la Ley Sarbanes-Oxley.

12.1.1.5 Sección 409

La sección 409 requiere que las organizaciones pongan de manifiesto cualquier cambio material en las operaciones en tiempo real y en un lenguaje comprensible. Hay quienes afirman que estos requisitos determinan el establecimiento o la necesidad de una continuidad en la supervisión, la auditoría y los procesos del aseguramiento y que se conviertan en parte significativa de los procesos de control interno.

12.2 El acuerdo de Basilea

El acuerdo de Basilea II es un tratado normativo que define las normas globales para las prácticas de gestión de riesgos del mundo empresarial en el sector financiero con la intención de atenuar riesgos de pérdidas en la industria. El foco está en el sector bancario, pero hay un intento claro para armonizar normas a través de todos los segmentos de la industria. Todas las áreas de operaciones bancarias están incluidas, personal, procesos, sistemas, gobierno y gestión de proveedores.

Un banco que desee calificar para el Enfoque de medición avanzada (AMA, en inglés) en función del riesgo operativo debe poder implementar las mejores prácticas en las operaciones y en la gestión de riesgos. Para la gestión de riesgos, esto significa lo siguiente:

- La alta dirección está implicada activamente.
- El banco tiene un sistema de gestión de riesgos operativos, procesos, políticas y procedimientos globales.
- El banco tiene un adecuado gobierno y los recursos suficientes para gestionar los riesgos operativos.
- El banco tiene una función de gestión de riesgo operativo que es responsable de:
  - Diseñar e implementar el esquema de gestión de riesgos operativos.
  - Codificar las políticas, los procedimientos y los controles.
  - Diseñar e implementar una metodología de medición del riesgo operativo.
  - Diseñar e implementar un sistema de gestión de informes de riesgos operativos.
  - Desarrollar estrategias para identificar, medir, supervisar y controlar o atenuar los riesgos operativos.
- El sistema de medición de riesgo operativo está integrado estrechamente en el proceso cotidiano de gestión de riesgos.
- Las exposiciones a riesgos operativos y las experiencias de pérdidas debidas a riesgo operativo se informan regularmente.
- El sistema de gestión de riesgo operativo está documentado.
- Los auditores internos y externos revisan regularmente la gestión de procesos de riegos operativos y el sistema de medición.

La llave de éxito en la gestión de riesgos operativos es un sistema de información que apoye la autoevaluación de la exposición al riesgo operativo, que permita el seguimiento del proceso, consistente en una base de datos de pérdidas por riesgos operativos y funciones de reporte, y presupone una función de la gestión basada en acción-planificación.

El Comité de Basilea no especifica el enfoque o las estimaciones de distribución que se deben utilizar para generar la medición de riesgos operativos con fines regulatorios para el capital. Sin embargo, el marco permite tres enfoques básicos que esencialmente son dependientes de la calidad y la cantidad de datos de la gestión de riesgos. Mientras que usar más datos y mediciones históricas para probar el buen funcionamiento puede permitir que los bancos mantengan menos reservas de capital y que las cuantifiquen según los riesgos operativos, los bancos deben poder demostrar que capturan los acontecimientos potencialmente severos de pérdida de registros (pérdidas inesperadas y severas). Por otra parte, según lo definido por el comité de Basilea, se requiere

la consistencia con el alcance del modelo de riesgos operativos.

Primero, las metodologías globales de organizaciones sobre la evaluación de riesgos de un banco deben considerar los factores del entorno así como los factores de control interno que pueden cambiar el perfil de riesgo operativo. Además, el banco debe tener un proceso para evaluar si su capital total es adecuado.

Luego, el sistema de medición de riesgos debe ser lo suficientemente granular como para capturar la cola de las estimaciones de pérdida. Se espera que los bancos utilicen la opinión de expertos conjuntamente con datos externos en el análisis del escenario para evaluar su exposición a acontecimientos de alta severidad. Dado que un banco no tiene suficientes datos propios en el área de riesgos de alto impacto, riesgos de baja frecuencia, debe adquirir datos de un proveedor externo como Zurich-based ORX, Global Operational Loss Database (GOLD), o MORE Exchange.

Los bancos deben tener un enfoque creíble, transparente, bien documentado y verificable para sopesar estos elementos fundamentales en el sistema global de medición de riesgos operativos. Hay requisitos previos adicionales a calificar para el AMA.

- Las pérdidas internas de datos y fallos de rendimiento, como éxitos, posibles pérdidas y fallos, se deben rastrear y registrar (se deben conciliar con los libros del banco).
- Las pérdidas internas de datos se deben relacionar con las actividades económicas actuales del banco.
- Se requiere un período de observación de cinco años, como mínimo, para aquellos datos internos perdidos, con un mínimo de tres años para calificar para el enfoque AMA.
- De acuerdo con el proceso interno de recopilación de pérdidas:
  – Las pérdidas del modelo de riesgo operativo relacionadas con el riesgo crediticio e incluidas históricamente en las bases de datos de riesgos crediticios de los bancos, deben continuar siendo tratadas como riesgo de crédito, con el fin de calcular el capital mínimo legal según este marco de referencia. Estas pérdidas deben ser marcadas por separado.
  – Las pérdidas del modelo de riesgo operativo relacionadas con el riesgo de mercado se tratan como lo hace el modelo de riesgo operativo para calcular el capital mínimo legal según este marco de referencia y están sujetas al cargo de capital del modelo.
- El sistema de medición del modelo de riesgo operativo debe utilizar datos externos relevantes.

Tercero, el criterio de manifestación de Basilea II requiere que los bancos describan sus objetivos de gestión de riesgos y las políticas en cuanto a riesgos para cada área diferente, se incluyen:

- Estrategias y procesos.
- La estructura y la organización de la función de gestión de riesgos.
- Alcance y naturaleza de la información o informes sobre el riesgo.
- Políticas para la omisión y mitigación de riesgos (incluidas las operaciones).

Nota: La herramienta BITS, Key Risk Measurement Tool for Information Security Operacional Risks, o "BITS Kalculator" (http://www.bitsinfo.org/bitskalculator-july04.pdf), es una herramienta que las instituciones financieras de todo tamaño pueden utilizar para evaluar riesgos críticos de seguridad de la información en sus negocios. Puede ser descargada sin coste alguno del sitio Web de BITS (http:// www.bitsinfo.org/wp.html).

12.3 Protección de datos

El concepto de protección de datos fue desarrollado cuando en las conferencias de Naciones Unidas y la OCDE se plantearon distintos aspectos de la computarización en los últimos años de la década del 60. La primera ley nacional fue promulgada en 1974 en Suecia y la OCDE publicó sus Guías para la Protección de Datos en el año 80 (OCDE C (80) 58 última parte). Los organismos regionales, como el Consejo de Europa (Convención de protección de datos 108/1981, basada en derechos humanos) y la Comisión Europea (EC, en inglés) (Directiva 95/46/EC Orientada a la protección del consumidor) ha aprobado marcos de referencia vinculantes para la implementación en sus estados miembros. Según su sistema legislativo, muchos países del mundo tienen previsiones constitucionales y leyes generales o de amplio espectro con regulaciones para la protección de los datos. Para tender un puente entre las diferentes regulaciones en Estados Unidos y en la Unión Europea (EU), la EC y el Ministerio de Comercio de EE. UU. desarrollaron un marco de seguridad de "puerto seguro" para las compañías de EE. UU. El "puerto seguro" es un acuerdo marco que consiste en siete principios y en una serie de preguntas realizadas frecuentemente. (Véase también: http://www.was4.hewitt.com/hewitt/resource/legislative_updates/europe/eu_data1.htm).

La legislación de la Unión Europea requiere que las organizaciones protejan la información personal. También obliga a que se tomen las medidas técnicas apropiadas para garantizar la seguridad de los datos personales, sean electrónicos o manuales. Se puede encontrar información adicional sobre protección de datos en el Centro de Información sobre Privacidad Electrónica (EPIC, en inglés) (http://www.epic.org); Privacy Internationaln (http://www.privacyinternational.org) y UK Office of the Information Commissioner (http://www.ico.gov.uk).

12.4 Ley Gramm-Leach-Bliley (GLBA) de EE. UU. – La ley de modernización financiera de 1999

La Ley GLBA nació para proteger la privacidad de la información de clientes en el sector financiero, pero

se extiende más allá de las compañías financieras. Cualquier compañía que maneje información financiera no pública de clientes puede ser considerada responsable bajo el imperio de esta ley, dependiendo de las circunstancias. Se puede encontrar más información disponible en EPIC (http://www.epic.org/privacy/glba/) y en U.S. Federal Trade Comisión (http://www.ftc.gov/bcp/conline/pubs/buspubs/glblong.htm-whois).

12.5 Ley HIPAA de 1996 (Ley de Responsabilidad y Portabilidad del Seguro Médico de EE. UU.)

HIPAA contiene los requerimientos para la protección de la información personal y para la seguridad de la información. La ley se aplica a las compañías con sede en EE. UU. del sector médico, pero puede también alcanzar a cualquier compañía que proporcione servicios de protección o cobertura médica a sus empleados, según las circunstancias. Si desea más información, visite http://www.hipaa.org.

12.6 Ley de Infracciones a la Seguridad de la Información de California. Sección 1798.29 y 1798.82 del Código Civil (Habitualmente se la conoce como Bill-CA SB 1386)

La CA SB 1386 del Estado de California enmendó la Ley de Prácticas de la Información de 1977, del Código Civil, para crear una regulación amplia que determina la divulgación pública de las infracciones a la seguridad de las computadoras cuando se pudiera haber visto comprometida la información confidencial de los residentes de California. Las empresas, públicas o privadas, que realizan transacciones comerciales con los residentes de California se ven potencialmente afectadas. La información confidencial cubierta por la ley incluye los números de seguridad social, los números de licencia de conductor de California, los números de cuentas bancarias y los números de tarjetas de crédito o débito. Aunque no se mencionan aquí casos de esta legislación, hay algunas discusiones sobre el tema que han indicado que las cortes pueden no tener una visión favorable de una organización si trata diferente a sus clientes de California que al resto de los clientes

12.7 Regulaciones nacionales a nivel mundial

Muchos países tienen regulaciones nacionales que cubren el control interno, incluidos Alemania (KonTraG, requisitos de la gestión de riesgos) y Francia (LSF, requisitos de información del control interno). Además, se puede requerir que los auditores externos certifiquen la adecuación de los mecanismos y de los controles de los informes financieros. Aunque la mayoría de estas regulaciones no tratan directamente con la TI, ellas implican la necesidad de una infraestructura de TI adecuadamente controlada. Por esta razón muchos organismos nacionales de la Federación Internacional de Contadores (IFAC) proporcionan guías detalladas para la evaluación de los controles de la TI.

13.1 Consideraciones sobre el conocimiento del auditor

Norma 1210: El nivel de competencia sobre las *Normas* del IIA, requiere que la actividad de la auditoría interna, en su conjunto, tenga u obtenga el conocimiento, las aptitudes y otras competencias necesarias para cumplir con sus responsabilidades1. Se necesitan diversos niveles de conocimiento de TI en la organización para proporcionar un enfoque sistemático y disciplinado a fin de evaluar y mejorar la efectividad de los procesos sobre la gestión de riesgos, los controles y del gobierno. El conocimiento de cómo se utiliza la TI, los riesgos relacionados y la capacidad de utilizar la TI como un recurso en el desarrollo del trabajo de auditoría es esencial para la eficacia del auditor en todos los niveles.

El Comité Internacional de Tecnología Avanzada del IIA, ha identificado tres categorías de conocimiento de TI para los auditores internos.

13.1.1 Categoría 1: Todos los auditores

La categoría 1 es el conocimiento de TI necesario para todos los auditores profesionales, desde las nuevas incorporaciones hasta el director de auditoría interna. El conocimiento de TI abarca entender conceptos, como las diferencias en el software usado en aplicaciones, sistemas operativos y software de sistemas y redes. Esto implica entender los componentes básicos de seguridad de TI y de control, tales como seguridad perimetral, detección de intrusismo, autenticación y controles de los sistemas de aplicación. El conocimiento básico incluye entender cómo los controles de negocio y los objetivos de aseguramiento pueden verse afectados por vulnerabilidades en las operaciones de negocio y lo relacionado con los sistemas de soporte y los componentes de redes y datos. Es fundamental asegurar que los auditores tienen suficiente conocimiento para centrarse en el entendimiento de los riesgos de TI, sin necesariamente tener conocimientos técnicos significativos.

13.1.2 Categoría 2: Supervisores de Auditoría

La categoría 2 se aplica al nivel de supervisión de auditoría. Además de tener el conocimiento básico en TI, los supervisores de auditoría deben entender los aspectos y elementos de TI, de forma suficiente para considerarlos en las tareas de auditoría de planificación, pruebas, análisis, informe y seguimiento y en la asignación de las habilidades de los auditores a los proyectos de auditoría. Esencialmente, el supervisor de auditoría debe:

- Entender las amenazas y vulnerabilidades asociadas a procesos automatizados de negocio.
- Entender los controles de negocio y la mitigación del riesgo que debe ser proporcionada por la TI.
- Planificar y supervisar las tareas de auditoría para considerar las vulnerabilidades y los controles relacionados con la TI, así como la eficacia de la TI en la provisión de controles para las aplicaciones y entornos de negocio.
- Asegurar que el equipo de auditoría tiene competencia suficiente, incluidas las habilidades en TI, para las tareas de auditoría.
- Asegurar el uso eficaz de las herramientas de TI en los trabajos de auditoría y en las pruebas.
- Aprobar los planes y las técnicas para probar los controles y la información.
- Evaluar los resultados de las pruebas de auditoría para evidenciar las vulnerabilidades o debilidades de control de la TI.
- Analizar los síntomas detectados y relacionarlos con las causas que pueden tener su origen en el negocio o en la misma TI, como planificación, ejecución, operaciones, gestión de cambios, autenticación, u otras áreas de riesgo.
- Proporcionar recomendaciones de auditoría basadas en los objetivos del aseguramiento del negocio, centrándose en los orígenes de los problemas observados, más que en divulgar simplemente los problemas o los errores detectados.

13.1.3 Categoría 3: Especialista en auditoría técnica de TI

La categoría 3 se aplica al especialista en auditoría técnica de TI. Aunque los auditores de TI pueden funcionar a nivel de supervisión, deben entender la tecnología subyacente que respalda a los componentes del negocio y estar familiarizados con las amenazas y vulnerabilidades asociadas a las tecnologías. Los auditores de TI también pueden especializarse en ciertas áreas de la tecnología.

Los programas y productos del IIA se diseñan sobre todo para resolver las necesidades de información de la categoría 1 y 2 de los auditores. El auditor de la categoría 1 buscará las guías del IIA para relacionar las amenazas, las vulnerabilidades y los controles de TI con los objetivos de aseguramiento del negocio. Los productos del IIA también proporcionan información que puede ser útil para explicar los impactos de los problemas técnicos en el negocio. Además, los productos de IIA pueden ayudar a la categoría 3 de auditores técnicos de TI para ganar competencia en las áreas de tecnología con las que no están familiarizados y en esforzarse para alcanzar competencias de supervisión o gerenciales de auditoría.

El instituto SANS proporciona formación en seguridad de la información y concede la Certificación Global de Aseguramiento de la Información (GIAC, en inglés), una certificación relevante para los profesionales de la seguridad de la información, incluidos los auditores. Las ofertas de cursos y certificaciones que los acompañan coinciden con las demandas crecientes de estudiantes, de nuevas amenazas y de nuevas tecnologías. Las certificaciones GIAC (http://www.giac.org/subject_certs.php) están agrupadas por

[4]Nota: El documento de "Las tres categorías del conocimiento de TI para los auditores internos" no forma parte de las *Normas* del IIA, pero es una orientación práctica proporcionada por el Comité Internacional de Tecnología Avanzada del IIA

tema y por nivel de dificultad. Algunas son certificaciones completas que acompañan cursos de aprendizaje de cinco a seis días, mientras que otros son certificados relacionados con cursos de uno a dos días. Los certificados son menos complicados pero están más centrados que las certificaciones.

También de interés y beneficio para todas las categorías de auditores de TI es el material proporcionado por la Asociación de Auditoría y Control de Sistemas de Información (ISACA, en inglés). ISACA ofrece normas y pautas a los profesionales de auditoría de TI, además de trabajos de investigación técnica centrados en aspectos de auditoría de TI, la certificación de Auditor Certificado de Sistemas de Información (CISA, en inglés) obtenida por más de 35.000 personas en todo el mundo, publicaciones, formación, y conferencias dedicadas a los profesionales de la auditoría de TI.

14.1 COSO

Constituido en 1985, COSO es una iniciativa independiente del sector privado, estudió los factores que pueden dar como resultado información financiera fraudulenta y desarrolló recomendaciones para las compañías que cotizan en bolsa y sus auditores independientes, para el SEC y para otros organismos de control, e instituciones educativas. COSO publicó su "Enfoque integrado de control interno", Apéndice E, traducido al castellano por el Instituto de Auditores Internos de España. Este es una herramienta ampliamente aceptada tanto para la gestión como para los auditores y luego publicó el "Enfoque integrado de gestión de riesgo empresarial" en el otoño de 2004, también traducido al castellano por el IAI. Los detalles de ambos se pueden encontrar en http://www.coso.org.

14.2 CICA y CoCo

El Instituto Canadiense de Contadores Certificados (CICA, en inglés) publicó en 1992 los *Criterios del Esquema de Control* (CoCo) para tratar cuestiones públicas e institucionales que la visión tradicional del control ya no abordaba de manera eficaz en la prevención de quiebras corporativas. La misión de CoCo es mejorar el funcionamiento de la organización y la toma de decisiones mediante la mejor comprensión del control, el riesgo y el gobierno. Más aún, el marco proporciona una base para emitir juicios sobre la eficacia del control.

En 1995 se edita la *Guía de control*, que describe la estructura de CoCo y define el control de una manera que va más allá del control interno tradicional sobre la información financiera. El modelo de CoCo es una manera de centrarse en el futuro de una organización para asegurarse de que esté controlada, teniendo un sentido claro de los propósitos compartidos, el compromiso colectivo para alcanzar ese propósito, los recursos que se necesitan para hacer el trabajo y la capacidad de aprender de la experiencia.

14.3 Guía de control de TI del CICA

La *Guía de control de TI*, publicada por el CICA, es una fuente de referencia para evaluar los controles de TI. Está organizada de una manera fácil de utilizar y está escrita en un lenguaje de negocio directo.

14.4 Objetivos de control de información y tecnologías relacionadas (CobiT) del ITGI

Establecido en 1998, el Instituto de Gobierno de TI (ITGI) proporciona orientación en los aspectos actuales y futuros relacionados con el gobierno, la seguridad y el aseguramiento de la TI. La publicación principal de la dirección del ITGI es el CobiT (consulte el Apéndice F). El CobiT del ITGI proporciona un marco de referencia y un lenguaje común a través del ciclo de vida de los sistemas de información (SI), tanto para el área de los SI como para los responsables del negocio y para los profesionales de auditoría de los SI, control y seguridad. CobiT es uno de los conjuntos de pautas más populares e internacionalmente aceptadas para el gobierno de TI.

14.5 ISO 17799 (Código de práctica para la gestión de seguridad de la información)

ISO/IEC 17799:2000(E) fue emitida por la Organización Internacional para la Estandarización (ISO, en inglés) y la Comisión Internacional Electrotécnica (IEC, en inglés), define los principios de seguridad de la información que, en última instancia, proporcionan una garantía tanto a las partes del negocio como a los organismos de control, que la información de una organización está protegida correctamente. Derivado de la norma británica BS 7799 (Instituto Británico de Normas), el Código de buenas prácticas para la gestión de seguridad de la información, se construye alrededor de los elementos específicos de seguridad requeridos en 10 áreas, incluidas seguridad física y ambiental, comunicación, gestión de operaciones y control de accesos. Aunque como código de práctica, la ISO/IEC 17799:2000 proporciona orientaciones y recomendaciones de actuación, no intenta ser una especificación y se debe tener en cuenta que los reclamos de cumplimiento no deben ser confusos.

La norma original BS 7799 tiene dos partes:

- La parte 1, que es el "Código de Práctica" y es idéntico a la ISO/IEC 17799:2000.
- La parte 2, que es una especificación para implementar un Sistema de Gestión de Seguridad de la Información (ISMS, en inglés).

Para dar conformidad a la parte 2 de la BS 7799 (BS 7799-2:2002) se debe implementar un ISMS en la organización, conforme con los requisitos descritos en la norma, que están en las especificaciones. Terceras partes se han acreditado para certificar, o para registrar a las organizaciones con respecto a la BS 77992:2002.

14.5.1 ¿Qué es la seguridad de la información?

LA BS 7799 trata a la información como un activo, que como otros activos importantes del negocio, tiene valor en una organización y por lo tanto la necesidad de ser protegido. La seguridad de la información protege la información contra una amplia gama de amenazas para asegurar continuidad del negocio, minimizar daños en el negocio y para maximizar el retorno de inversiones y oportunidades de negocio.

La información puede existir en muchas formas: impresa o escrita en el papel, almacenada electrónicamente, transmitida por correo u otros medios electrónicos, exhibida en películas, en las conversaciones. Cualquier forma que la información tome, o medio por el que se comparta o almacene, la BS 7799 indica que siempre se debe proteger apropiadamente.

La seguridad de la información se caracteriza según BS 7799 en preservar lo siguiente:

- **Confidencialidad,** asegurar el acceso a la información

solamente a las personas autorizadas.
- **Integridad,** salvaguardar la exactitud y la totalidad de la información, y los métodos de proceso.
- **Disponibilidad,** asegurar que los usuarios autorizados tengan acceso a la información y a los activos asociados cuando lo requieran.

La seguridad de la información se alcanza implementando un sistema adecuado de controles de la BS 7799, pueden ser políticas, prácticas, procedimientos, estructuras de organización y funciones del software. Se deben establecer los controles para asegurar que se alcancen los objetivos específicos de seguridad de la organización.

14.5.2 Cómo establecer los requisitos de seguridad

La BS 7799 indica que es esencial que una organización identifique sus requisitos de seguridad. Hay tres fuentes principales:
- Evaluación de los riesgos de la organización. La BS 7799 no prescribe una metodología
- Requisitos legales, estatutarios, legales y contractuales que la organización, sus socios, los contratistas y los proveedores de servicios, deben satisfacer.
- Sistema particular de principios, objetivos y requisitos para el tratamiento de la información que la organización ha desarrollado para respaldar sus operaciones.

14.5.3 Evaluar los riesgos de seguridad

La BS 7799 sugiere que los requisitos de seguridad sean identificados por un sistema metódico de evaluación de riesgos de seguridad. El gasto en controles debe estar equilibrado con el valor del posible daño al negocio, debido a fallos en la seguridad. Probablemente sea necesario realizar el proceso de evaluación de riesgos y de selección de controles un número de veces hasta lograr cubrir las diversas áreas de la organización o de los sistemas de información en particular y es importante revisar periódicamente los riesgos de la seguridad y los controles implementados.

14.5.4 Seleccionar los controles

Una vez que se hayan identificado los requisitos de seguridad, los controles de la BS 7799 deben ser seleccionados e implementados para asegurar que los riesgos se reducen a un nivel aceptable. Los controles se deben seleccionar basándose en el coste de su puesta en marcha y en función de los riesgos que reducen, considerando además las pérdidas potenciales que existirían si se produce un fallo en la seguridad. Los factores no monetarios, como pérdida de reputación, también se deben considerar. Para obtener más información, consulte http://www.bs7799-iso17799. com/.

14.5.5 Temas tratados en la BS 7799

1. Alcance.
2. Términos y definiciones.
3. Política de seguridad:
   3.1 Documento de política de seguridad de la información.
   3.2 Revisión y evaluación.
4. Organización de la seguridad:
   4.1 Infraestructura de seguridad de la información.
   4.2 Seguridad del acceso de terceros.
   4.3 Externalización(3).
5. Clasificación y control de activos:
   5.1 Responsabilidad(4) sobre activos.
   5.2 Clasificación de la información.
6. Seguridad del personal:
   6.1 Seguridad en la definición de trabajos y recursos.
   6.2 Formación de usuarios.
   6.3 Respuesta a los incidentes y fallos de seguridad.
7. Seguridad física y ambiental:
   7.1 Áreas seguras.
   7.2 Seguridad de los equipos.
   7.3 Control general.
8. Gestión de comunicaciones y operaciones:
   8.1 Procedimientos operativos y responsabilidades.
   8.2 Planificación y aceptación del sistema.
   8.3 Protección contra software dañino.
   8.4 Mantenimiento interno.
   8.5 Gestión de la red.
   8.6 Manejo y seguridad de medios.
   8.7 Intercambios de información y de software.
9. Control de acceso:
   9.1 Requisitos del negocio para el control de accesos.
   9.2 Gestión del acceso de usuarios.
   9.3 Responsabilidades del usuario.
   9.4 Control de acceso de red.
   9.5 Control de acceso al sistema operativo.
   9.6 Control de acceso de las aplicaciones.
   9.7 Supervisión del acceso y uso de los sistemas.
   9.8 Computación móvil y teletrabajo.
10. Desarrollo y mantenimiento de sistemas:
    10.1 Requisitos de seguridad de los sistemas.
    10.2 Seguridad de los sistemas de aplicación.
    10.3 Controles criptográficos.
    10.4 Seguridad de los archivos del sistema.
    10.5 Seguridad en procesos de desarrollo y soporte.
11. Gestión de la continuidad del negocio:
    11.1 Proceso de gestión de la continuidad del negocio.
12. Cumplimiento:
12.1 Cumplimiento con requisitos legales.
    12.2 Revisiones de la política de seguridad y cumplimiento técnico.
12.3 Consideraciones de la auditoría de sistemas.

14.6 Norma ISF de buenas prácticas para la seguridad de la información

El Foro de Seguridad de la Información (ISF, en inglés) con sus *Normas de Buenas Prácticas de Seguridad de Información* tiene como objetivo gestionar los riesgos asociados a cada aspecto de los sistemas de información, independientemente del sector de mercado, tamaño, o estructura de la empresa. La norma fue desarrollada por los grupos de trabajo del ISF y

es un documento público disponible, que se encuentra dividido en cinco áreas claves: gestión de la seguridad, sistemas críticos del negocio, instalaciones de sistemas, redes y desarrollo de sistemas. Para más información y detalles, consulte http://www.isfsecurity standard.com.

14.7 Principios generalmente aceptados para la seguridad de la información (GAISP)

Los principios generalmente aceptados para la seguridad de la información (GAISP, en inglés) resumen la mejor práctica de un conjunto de esquemas similares. Desarrollados en 1991, estos principios proporcionan una amplia jerarquía de guías para asegurar la información y la tecnología de soporte, entre ellos se incluyen:

- **Principios básicos** – guía a nivel del Consejo
- **Principios generales de funcionamiento** – diseñados para la gestión de la información a nivel ejecutivo (borrador distribuido en septiembre de 1999).
- **Principios detallados** – guía para la gestión de seguridad de la información operativa (en desarrollo).

Estos principios ahora están siendo desarrollado por la Asociación de Seguridad de Sistemas de Información (ISSA, en inglés) (http://www.issa.org), que puede proporcionar detalles de ello.

14.7.1 Principios básicos

Se refieren a la confidencialidad, integridad y disponibilidad de la información. Proporcionan una guía general para establecer y mantener la seguridad de la información y de la tecnología de soporte.

- **Principio de responsabilidad.** La asignación de responsabilidad sobre seguridad de la información y las responsabilidades deben estar claramente definidas y deben ser aceptadas.
  Razonamiento. La responsabilidad caracteriza la capacidad de auditar las acciones de todas las partes y procesos que interactúan con la información. Las funciones y responsabilidades deben estar claramente definidas, identificadas y aprobadas a un nivel adecuado según sensibilidad y criticidad de la información. La relación entre las partes, los procesos y la información se debe definir claramente, se debe documentar y debe ser conocida por todos. Todas las partes deben tener responsabilidades en función de las cuales deberán rendir cuentas.
- **Principio de conocimiento.** Todas las partes que necesariamente deben conocer la información, incluidos, entre otros, los propietarios de la información y los actores de la seguridad de la información, deben tener acceso a los principios, las normas, las convenciones o los mecanismos disponibles para asegurar la información y los sistemas de información, así como también se los debe informar sobre posibles amenazas a la seguridad de la información.
  Razonamiento. Se aplica entre las organizaciones y dentro de ellas. El conocimiento de los principios, las normas, las convenciones y los mecanismos de seguridad de la información aporta valor, genera controles y ayuda a minimizar las amenazas. El conocimiento de las amenazas y de su significación también aumenta la aceptación de los controles por parte del usuario. Sin el conocimiento de la necesidad de controles particulares, los usuarios pueden poner en riesgo la información ignorando, no respetando, o extralimitando los mecanismos existentes de control. El principio del conocimiento se aplica a las partes autorizadas y no autorizadas.
- **Principio de ética**. Se debe utilizar y administrar la información y la seguridad de la información de manera ética.
  Razonamiento. Los sistemas de información forman parte de nuestras sociedades. El desarrollo de reglas y la evolución de las expectativas se relacionan con la disponibilidad, el uso apropiado y la seguridad de los sistemas de información. El uso de la información y de los sistemas de información debe cubrir los requisitos establecidos en las normas y obligaciones sociales.
- **Principio multidisciplinario.** Los principios, las normas, las convenciones, los mecanismos para asegurar la información y los sistemas de información deben tratar las consideraciones y los puntos de vista de todas las partes interesadas.
  Razonamiento. La seguridad de la información se alcanza por el esfuerzo combinado de los propietarios de la información, los usuarios, los que tienen asignada su custodia y el personal de seguridad de la información. Las decisiones tomadas con la debida consideración de todos los puntos de vista relevantes y de las capacidades técnicas pueden realzar la seguridad de la información y recibir mejor aceptación.
- **Principio de la proporcionalidad.** Los controles sobre la seguridad de la información deben ser propor-

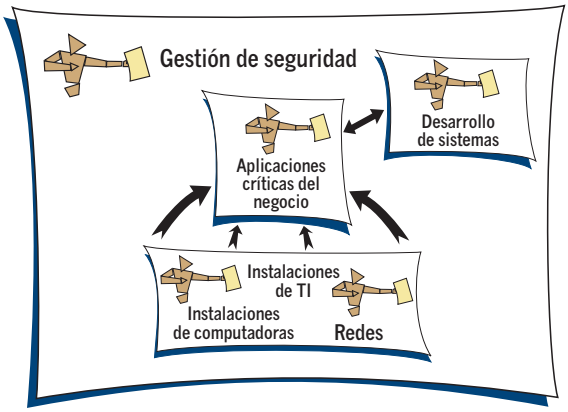

Figura 7 – Gestión de seguridad

cionales a los riesgos de manipulación, negación de uso, o de acceso a la información.

Razonamiento. Los controles de seguridad deben ser adecuados al valor y vulnerabilidad de los activos de la información. Se debe considerar el valor, la sensibilidad y la criticidad de la información, así como la probabilidad, la frecuencia y la severidad del daño o de la pérdida directa e indirecta. Este principio reconoce el valor de la seguridad de la información que se extiende desde la prevención a la aceptación del riesgo.

- **Principio de integración.** Los principios, normas, convenciones y mecanismos de seguridad de la información deben coordinarse e integrarse con las políticas y los procedimientos de la organización para crear y mantener la seguridad a través de un sistema de información.

  Razonamiento. Muchas brechas de seguridad de la información implican que estén comprometidas más de una medida de protección. Las medidas de control más eficaces son componentes de un sistema integrado de controles. La seguridad de la información es más eficiente si está planeada, gestionada y coordinada por medio del sistema de control de la organización y si se considera la vida de la información.
- **Principio de la oportunidad.** Todas las partes responsables deben actuar de manera oportuna y coordinada para prevenir o responder a las brechas y a las amenazas a la seguridad de la información y de los sistemas de información.

  Razonamiento.– Las organizaciones deben poder coordinar y actuar rápidamente para prevenir o atenuar las amenazas. Este principio reconoce la necesidad de los sectores públicos y privados de establecer mecanismos y procedimientos en común para responder de manera rápida y eficaz a amenazas informadas o conocidas. El acceso al historial de amenazas respalda la gestión de respuestas eficaces a los acontecimientos y ayudar a prevenir futuros incidentes.
- **Principio de análisis.** Los riesgos de la información y de los sistemas de información se deben analizar periódicamente.

  Razonamiento. – Los requisitos de la información y de la seguridad varían en el tiempo. Las organizaciones deben analizar periódicamente la información, su valor y la probabilidad, la frecuencia y la severidad del daño posible o de la pérdida directa e indirecta. El análisis periódico identifica y mide las variaciones de las medidas de seguridad establecidas que están activas, tal como se articula en la guía GAISP, así como el riesgo asociado a tales variaciones. También permite a los responsables tomar decisiones, respaldadas en la gestión de riesgos de la información, sobre la aceptación, atenuación, o transferencia de los riesgos con la debida consideración de la relación de coste beneficio.
- **Principio de equidad.** La dirección respetará los derechos y la dignidad de individuos al fijar las políticas y al seleccionar, implementar y hacer cumplir las medidas de seguridad.

  Razonamiento. Las medidas de seguridad de la información implementadas por una organización no deben interferir con las obligaciones, los derechos y las necesidades de los usuarios, los dueños u otras partes afectadas por la información, siempre que tales medidas se ejerzan según los parámetros legítimos de la consecución de objetivos.

14.8 Principios y criterios de servicios confiables del AICPA/CICA.

El Comité Ejecutivo de Servicios de Aseguramiento del Instituto Estadounidense de Contadores Públicos Certificados (AICPA, en inglés) y el Consejo de Desarrollo de Servicios de Aseguramiento de CICA desarrollaron los Principios y criterios de servicios confiables para tratar los riesgos y las oportunidades de la TI. Estos principios precisan una serie de declaraciones de principios e identifican criterios específicos que se deben alcanzar para resolver cada principio. Los principios son declaraciones amplias de objetivos. Los criterios son comparaciones usadas para medir y presentar el tema y contra los que, quienes realizan las evaluaciones, pueden analizar tal tema. En los Principios y criterios de servicios confiables, los criterios son apoyados por una lista de controles ilustrativos y se organizan en cuatro áreas amplias:

- **Políticas.** La organización ha definido y documentado sus políticas1 relevantes en sus Principales Principios
- **Comunicaciones.** La organización ha comunicado sus políticas ya definidas a los usuarios autorizados.
- **Procedimientos**. La organización utiliza procedimientos para alcanzar sus objetivos de acuerdo con las políticas definidas.
- **Supervisión.** La organización supervisa el sistema y ejecuta las acciones necesarias para mantener la conformidad con las políticas definidas.

Seguidamente, se encuentran los resúmenes de Servicios de seguridad confiables, Disponibilidad, Integridad de procesamiento, Aislamiento, Confidencialidad, y Principios y criterios de la autoridad de certificación. Los Principios y criterios de servicios confiables se pueden utilizar para calificar los contratos de SysTrust y de WebTrust, que son servicios de aseguramiento diseñados para una amplia gama de sistemas basados en TI. Sobre la obtención de un informe de no aptitud sobre aseguramiento, la organización tiene la posibilidad de tener un SysTrust o WebTrust y el correspondiente informe del auditor. Además, este esquema se puede utilizar para proporcionar servicios de consulta. Para obtener un listado detallado de los principios y criterios de servicios confiables, consulte http://www.aicpa.org/los trustservices.

14.8.1 Principios de seguridad. El sistema se debe proteger contra accesos no autorizados (físico y lógico)

En el comercio electrónico y otros sistemas, las partes que intervienen deben asegurarse de que la información intercambiada esté disponible sólo para las personas que necesitan el acceso para ejecutar la transacción o los servicios, o hacer seguimiento de las preguntas o cuestiones que pueden presentarse. La información proporcionada a través de esos sistemas es susceptible de accesos no autorizados durante la transmisión y mientras se almacena en los sistemas de la otra parte. Limitando el acceso a los componentes del sistema, se ayuda a prevenir el potencial abuso de este, el hurto de recursos, el uso erróneo del software y el acceso incorrecto, uso, alteración, destrucción, o acceso a la información. Los elementos claves para la protección de los componentes del sistema incluyen la autorización y permisos de acceso, y la desautorización preventiva de acceso a esos componentes.

14.8.2 Principio de disponibilidad. El sistema está disponible para la operación y el uso según lo convenido

El principio de la disponibilidad se refiere a la accesibilidad al sistema, productos, o servicios según lo acordado por contrato o por el acuerdo de nivel de servicio y otros acuerdos. Este principio no fija, en sí mismo, un nivel de funcionamiento mínimo aceptable para la disponibilidad de sistema. Por lo contrario, el nivel de funcionamiento mínimo se establece por acuerdo mutuo (contrato) entre las partes.

Aunque la disponibilidad del sistema, la funcionalidad y la utilidad estén relacionadas, el principio de disponibilidad no se refiere a la funcionalidad del sistema (las funciones específicas que un sistema realiza) ni al uso del sistema (la capacidad de los usuarios de utilizar las funciones del sistema para atender tareas o problemas específicos), sino al hecho de si se tiene acceso al sistema para las tareas de procesar, supervisar y mantener.

14.8.3 Principio de integridad del proceso. El proceso del sistema es completo, exacto, oportuno y autorizado

La integridad del proceso existe si un sistema realiza su función planificada perfectamente, libre de manipulación desautorizada o inadvertida. Latotalidad generalmente indica que todas las transacciones y servicios son procesados o realizados sin excepción, y que las transacciones y servicios no son procesados más de una vez. La exactitud incluye el aseguramiento de que la información clave asociada a la transacción ejecutada seguirá siendo exacta a través del procesamiento de la transacción y que la transacción o los servicios son procesados o realizados según lo planificado. La oportunidad del abastecimiento de servicios o de la entrega de bienes se trata en el contexto de las obligaciones hechas para tal entrega. La autorización incluye asegurarse de que el proceso es realizado de acuerdo con las aprobaciones y privilegios requeridos definidos por las políticas que gobiernan el proceso del sistema. Los riesgos asociados con la integridad del proceso están relacionados con el individuo que inicia la transacción y que no termina la transacción ni proporciona el servicio correctamente ni de conformidad con la petición deseada o especificada. Sin controles apropiados de la integridad del proceso, el comprador puede no recibir los bienes o servicios solicitados, puede recibir en conjunto más de lo que solicitó, o puede recibir los bienes o servicios incorrectos. Sin embargo, si existen controles de los procesos de integridad apropiados y son operacionales dentro del sistema, entonces el comprador puede razonablemente estar seguro de que recibirá los bienes y servicios correctos según la cantidad y el precio correctos en la fecha prometida. Los procesos de integridad implican todos los componentes del sistema incluyendo los procedimientos para iniciar, registrar, procesar y reportar la información, el producto, o el servicio del tema comprometido. La naturaleza de la entrada de datos en los sistemas de comercio electrónico implican típicamente que el usuario ingrese datos directamente a través de pantallas y formularios en formato Web, mientras que en otros sistemas, la naturaleza de la entrada de datos puede variar significativamente. Debido a esa diferencia en los procesos de ingreso de datos, la naturaleza de los controles sobre la completitud y exactitud de la entrada de datos en sistemas de comercio electrónico pueden ser algo diferente que en otros sistemas.

La integridad del proceso se diferencia de la integridad de los datos porque esta no implica que automáticamente la información almacenada por el sistema sea completa, exacta, actual y autorizada. Si un sistema procesa información de fuentes fuera de los limites del sistema, una organización puede establecer solamente controles limitados de completitud, exactitud, autorización y oportunidad de la información que se procesa. Los errores que se pudieron haber introducido en los procedimientos de control e información en sitios externos están típicamente fuera del control de la organización. Cuando la fuente de información se excluye explícitamente de la descripción del sistema que define el compromiso, es importante detallar esa exclusión en la descripción del sistema. En otras situaciones, la fuente de datos puede ser una parte inherente del sistema que se examina y los controles de completitud, exactitud, autorización y oportunidad de información que se procesen serían incluidos en el alcance del sistema según lo descrito.

[5] El término "políticas" se refiere a pautas escritas que comunican el espíritu de la gestión, los objetivos, requerimientos, responsabilidades y normas para un tema en particular. Algunas políticas pueden ser descritas como explicativas, contenidas en manuales de políticas o documentos de nombres similares. Sin embargo, otras pueden estar documentadas sin esas características explícitas, incluidas por ejemplo, las comunicaciones a empleados o terceros.

14.8.4 Principios y componentes de privacidad. La información personal se recoge, utiliza, conserva y divulga conforme a las obligaciones del aviso de privacidad de la organización y a los criterios de privacidad de los servicios confiables de AICPA/CICA

El principio de privacidad contiene 10 componentes[6] y los criterios relacionados que son esenciales para la protección y la administración apropiada de la información personal. Estos componentes y criterios de privacidad se basan en las prácticas de información razonables incluidas en leyes y regulaciones de privacidad de varias jurisdicciones del mundo y en muchas buenas prácticas reconocidas de privacidad. Los componentes de privacidad son:

- **Administración:** la organización define, documenta, comunica y asigna responsabilidades para sus políticas y procedimientos de privacidad.
- **Aviso:** la organización proporciona el aviso sobre sus políticas y procedimientos de privacidad e identifica los propósitos para los cuales se recoge, utiliza, conserva y divulga la información personal.
- **Opción y consentimiento:** la organización describe las opciones disponibles para el individuo y obtiene consentimiento implícito o explícito respecto a recolección, uso y acceso a la información personal.
- **Recolección:** la organización recoge la información personal solamente para los propósitos identificados en el aviso.
- **Uso y retención:** la organización limita el uso de la información personal a los propósitos identificados en el aviso y para los cuales el individuo ha proporcionado consentimiento implícito o explícito. La organización solamente conserva la información personal el tiempo necesario para satisfacer los propósitos indicados.
- **Acceso**: la organización provee a los individuos el acceso a su información personal para la revisión y actualización.
- **Divulgación y terceros:** la organización divulga información personal a terceros solamente para los propósitos identificados en el aviso y con el consentimiento implícito o explícito del individuo.
- **Seguridad:** la organización protege la información personal contra el acceso no autorizado, físico y lógico.
- **Calidad:** la organización mantiene la información personal exacta, completa y relevante para los propósitos identificados en el aviso.
- **Supervisión e impulso del cumplimiento:** la organización supervisa el cumplimiento con sus políticas y procedimientos de privacidad y tiene procesos para tratar la privacidad relacionada con quejas y conflictos.

14.8.5 Principio de confidencialidad la información señalada como "confidencial" se protege según lo comprometido o acordado

El principio de confidencialidad se centra en la información señalada como "confidencial". No hay definición extensamente reconocida sobre información confidencial, a diferencia de la información personalmente identificable, que muchos países actualmente están definiendo con lasregulaciones. En el curso de la comunicación y las transacciones del negocio, los socios intercambian información que a menudo desean mantener como confidencial. En la mayoría de los casos, las partes desean asegurar que la información que proporcionan esté disponible solamente para los individuos que deben tener acceso para completar la transacción o resolver las cuestiones que que se presenten. Para realzar la confianza de los socios del negocio, es importante informarlos acerca de las prácticas de confidencialidad de la organización, incluidas aquellas que proporcionan el acceso autorizado, el uso y la posibilidad de compartir la información identificada como confidencial.

La información de confidencialidad incluye:

- Detalles de la transacción
- Diseños de ingeniería.
- Planes del negocio.
- Información de las actividades bancarias del negocio.
- Disponibilidad del inventario.
- Ofertas o consultas de precios.
- Listas de precios.
- Documentos legales.
- Listas de clientes normales y preferenciales.
- Rentas para el cliente y la industria.

A diferencia de la información personal, no existen derechos definidos para tener acceso a la información confidencial que aseguren su exactitud y totalidad. Las interpretaciones de qué se considera información confidencial pueden variar significativamente de negocio a negocio y son guiadas por acuerdos contractuales en la mayoría de los casos. Como resultado, las partes implicadas en las relaciones del negocio deben comprender qué información se mantendrá sobre una base confidencial y qué derechos de acceso, u otras condiciones, puede tener una organización para actualizar esa información que asegure su exactitud y totalidad.

La información que se proporciona a la otra parte es susceptible al acceso no autorizado durante su transmisión y mientras se almacena en los sistemas informáticos de la otra parte. Por ejemplo, una parte no autorizada puede interceptar transacciones e información del perfil del socio del negocio y las instrucciones acordadas, mientras estas se están transmitiendo. Los controles tales como encriptación se pueden utilizar para proteger la confidencialidad de la información durante la transmisión, mientras que los filtros de seguridad y los controles de acceso rigurosos pueden ayudar

[6] Aunque cierta regulación sobre privacidad utilice el témino "principio", el término "componente" es el utilizado por el Esquema de criterios de privacidad de servicios confiables de AICPA/CICA para representar este concepto ya que el término "principio" estaba previamente definido en los textos de "Servicios confiables".

a proteger la información mientras esta se almacena en los sistemas informáticos.

14.8.6 Principio de la autoridad de certificación (CA, en inglés)

La autoridad de certificación se encarga de certificar el ciclo de vida de la administración de negocios y divulgar sus respectivas claves y prácticas de privacidad de información y proporciona sus servicios en función de ellas. Esto incluye los conceptos de divulgación de las prácticas de negocios de la CA, la integridad de los servicios y los controles ambientales.

14.9 El gobierno corporativo

14.9.1 Principios de la OCDE del gobierno corporativo

Los principios de la OCDE del gobierno corporativo, modificados en abril de 2004, precisaron una estructura para buenas prácticas acordada por los 30 países miembros de la OCDE y se ha convertido en un principio generalmente aceptado (http://www.oecd.org/corporativo). Publicado originalmente en 1999, los principios se diseñan para asistir a los gobiernos y a los organismos de control en la elaboración y cumplimiento de las reglas, regulaciones y de los códigos del gobierno corporativo de forma efectiva. En paralelo, proporcionan una guía para las bolsas de valores, los inversores, las compañías y otras que tengan algún rol en el proceso de desarrollar un buen gobierno corporativo. Aunque los principios de la OCDE no roporcionan una guía específica para controles de TI, otras unidades de la OCDE proporcionan una guía adicional e investigan en temas de seguridad y privacidad de la información.

14.9.2 Comisión de la EU

El plan de acción de la Comisión Europea sobre la regulación de empresas y gobierno corporativo se lanzó en mayo de 2003 para consolidar mecanismos de gobierno corporativo en entidades de interés público (consulte más detalles en http://europa.eu.int/comm/internal_market/company/index_e n.htm). Las iniciativas de gobierno corporativo de la EU no se refieren específicamente a temas de TI, las actividades de la Sociedad de la información (http://europa.eu.int/information_society/index _en.htm) contienen muchos temas específicos sobre controles de TI.

14.9.3 El código combinado del Reino Unido y la guía de Turnbull

El código combinado y la guía de Turnbull fueron el acercamiento del Reino Unido al gobierno corporativo. Como la Ley Sarbanes-Oxley, no se refieren específicamente al tema de controles de TI, sino que se centran en el marco de control interno de forma global. Se puede encontrar más información del IAI-RU e Irlanda en http://www.iia.org.uk/knowledgecentre/keyissues/corporategovernance.cfm?Actio n=1&ARTICLE_ID = 1185.

14.9.4 Informe King sobre el gobierno corporativo para África del Sur 2002 (Rey II)

Similar al código combinado y a la guía de Turnbull, este código de prácticas está orientado a las organizaciones de África del Sur. Las copias de los informes están disponibles en línea en http://www.ecgi.org/codes/country_pages/codes_south_africa.htm.

14.9.5 Otros requisitos del gobierno corporativo

Muchos otros países tienen requisitos similares de gobierno corporativo. Se puede encontrar una lista extensa y copias de ellos en http:// www.ecgi.org/codes/all_codes.htm.

14.10 Otros temas relacionados

14.10.1 Biblioteca de Infraestructura de TI (ITIL, en inglés)

La ITIL es un acercamiento genérico a la administración del servicio de TI, proporciona un conjunto de las mejores prácticas, enfocados internacionalmente en sectores públicos y privados. Se originó en el Reino Unido, está respaldada por un esquema de calificación, por organizaciones acreditadas de formación y herramientas de implementación y evaluación. Los procesos de las mejores prácticas promovidos en ITIL apoyan y son apoyados por la norma del Instituto Británico de Normas para la gestión de servicio de TI (BS 15000). Mientras que ITIL no exige específicamente tener una estructura para control de TI, se debe reconocer y considerar su uso cuando se determina qué estructura de control se aplicará. Obtenga información adicional en http://www.itil.co.uk/.

14.10.2 ISO 9000:2000

Mientras que la ISO 9000 se relaciona específicamente con los requisitos de calidad de la gestión, no contiene elementos que contribuyen a los controles de TI relacionados con los procesos de control y documentación. A pesar de que no constituye un esquema de control completo de TI, la ISO 9000 puede proporcionar elementos que aporten a la solidez de los controles de TI para implementar procesos sólidos. Para obtener más información, visite http://www.iso.ch/iso/en/iso9000-14000/iso9000/ iso9000index.html.

14.10.3 Marco de calidad del Instituto Nacional de Calidad (NQI) de Canadá para la excelencia del negocio

El marco de calidad canadiense para la excelencia del negocio, desarrollado por el Instituto Nacional de Calidad (NQI), es una estructura para mejorar la calidad. Se basa en los principios de calidad y en los criterios originales del sector privado que se han adaptado también al sector público. Además, forman la base de la evaluación para las concesiones de calidad de

Manitoba y de Canadá para los programas de excelencia, son utilizados por las organizaciones canadienses de todo tamaño y en todos los sectores. Obtenga más información en http://www.qnet. mb.ca/quality_cdncriteria.htm.

14.10.4 Instituto OCTAVE (CMU/SEI) de Ingeniería de Software de la Universidad de Mellon Carnegie

La amenaza crítica operacional, el activo y la evaluación de la vulnerabilidad (OCTAVE) es una técnica autodirigida, basada en riesgos y con un planeamiento y evaluación estratégica para las organizaciones que desean entender sus necesidades de seguridad de información. Un equipo pequeño de personas que corresponden a las operaciones, negocio, unidades y al departamento de TI de la organización trabajan en conjunto con el objetivo de dirigir las necesidades de seguridad de la empresa. Este equipo utiliza los recursos del conocimiento de muchos empleados para definir el estado actual de la seguridad, identificar los riesgos de los activos críticos y fijar una estrategia de seguridad. OCTAVE se centra en la estrategia, el riesgo organizativo, los temas relacionados con la práctica, balance del riesgo operativo, prácticas de seguridad y tecnología. Los métodos separados están disponibles para las organizaciones grandes y pequeñas. Para más información, consulte http://www.cert.org/octave/.

El enfoque integrado de control interno de COSO es reconocido como modelo formal para la certificación de Sarbanes-Oxley por el SEC y proporciona una categorización jerárquica de controles. Además, la norma de auditoría del PCAOB establece:

> "Debido a la frecuencia con la cual se espera que la dirección de las empresas que cotizan en bolsa utilice COSO como enfoque de referencia para la evaluación, las instrucciones de la norma están basadas en el enfoque COSO. Otos esquemas de control se han publicado en diversos países y probablemente otros nuevos salgan a la luz en el futuro. Aunque los diversos enfoques probablemente no contengan exactamente los mismos elementos que COSO, deben tener elementos que abarquen todos los temas generales de COSO".

El modelo de COSO fue mejorado durante el año 2004 con el desarrollo del Enfoque Integrado de Gestión de Riesgo Empresarial, enfoque integrado COSO, (http://www.coso.org). Este apéndice describe el enfoque anterior, que es la versión referenciada para el cumplimiento legal. No obstante, el director ejecutivo de auditoría interna debe investigar el enfoque mencionado.

15.1 Definición de control interno en COSO

COSO define el control interno (http://www.coso.org/) como "el proceso, efectuado por el consejo de administración, la dirección y demás empleados de una entidad, diseñado para proporcionar un grado de seguridad razonable en la consecución de los objetivos en las siguientes categorías:

- Eficacia y eficiencia de las operaciones.
- Fiabilidad de la información financiera.
- Cumplimiento con las leyes y regulaciones aplicables.

Estas distintas categorías, aunque superpuestas, se remiten a diversas necesidades de tal forma que cada una requiere un enfoque específico. La primera categoría se centra en los objetivos básicos de negocio de una entidad, incluyendo metas de rendimiento, beneficios y salvaguarda de recursos, afectados en gran medida por el uso de TI.

La segunda categoría se relaciona con la preparación y publicación de estados contables fiables, incluidos los estados contables provisionales y abreviados, así como la publicación de ganancias y otros datos financieros emitidos públicamente que derivan de esos estados. Los sistemas de TI suelen producir tales informes y los controles sobre estos sistemas juegan un papel importante a nivel del control interno.

La tercera categoría se ocupa del cumplimiento de aquellas leyes y regulaciones a las cuales la entidad está sujeta. Los sistemas de control interno funcionan según diversos niveles de eficacia. El control interno se puede considerar eficaz en cada una de las tres categorías si el consejo de administración y la dirección tienen razonable confianza de que:

- Entienden la medida en que se logran los objetivos operativos de la entidad.
- Los estados contables publicados se están elaborando de forma fiable.
- Se cumple con leyes y regulaciones aplicables.

Aunque el control interno es un proceso, su eficacia es un estado o una condición del proceso en unos o más puntos en un momento.

15.2 Control interno de COSO. Estructura integral de control interno

El control interno consiste en cinco componentes correlacionados que se derivan de la manera en que la dirección ejecuta el negocio y se integran con el proceso de gestión. Aunque los componentes se aplican a todas las entidades, las organizaciones pequeñas y de tamaño mediano pueden ponerlos en ejecución de manera diferente a las grandes empresas. Los controles de una organización pequeña pueden ser menos formales y estructurados, pero aún así pueden tener un control interno eficaz. Los componentes son:

15.2.1 Entorno de control

El entorno de control fija el nivel dentro de una organización, influenciando la conciencia de control de su personal, estableciendo la base para el resto de los componentes de control interno y proporcionando disciplina y estructura. Los factores estructurales de control incluyen la integridad, los valores éticos y la competencia del personal de la entidad; la filosofía de la dirección y el estilo de operación, la manera en que la dirección asigna autoridad y responsabilidad, y organiza y desarrolla a su gente; la atención y dirección proporcionadas por el consejo de administración.

15.2.2 Evaluación de riesgos

Cada entidad hace frente a numerosos riesgos de origen externo e interno, que deben ser evaluados. Una condición previa a la evaluación de riesgos es establecer los objetivos que están conectados a diferentes niveles y que son consistentes internamente. La evaluación de riesgos identifica y analiza los riesgos relevantes para alcanzar esos objetivos, y forma una base para determinar cómo se deben gestionar los riesgos. Debido a que las condiciones económicas, industriales, legales y operativas continuarán cambiando, las organizaciones necesitan mecanismos para identificar y ocuparse de los riesgos específicos asociados al cambio.

15.2.3 Actividades de control

Las actividades de control son las políticas y los procedimientos que ayudan a asegurar que las directivas de la dirección se lleven a cabo y que las acciones necesarias se implementen para identificar los riesgos y alcanzar los objetivos. Las actividades de control existen en la organización, en todos los niveles y en todas las funciones. Incluyen una gama de actividades tan diversas como aprobaciones, autorizaciones, verificaciones, reconciliaciones, revisiones de rendimiento operativo, seguridad de activos y separación de funciones.

15.2.4 Información y Comunicación

La información relevante se debe identificar, capturar y comunicar en un marco de tiempo y forma tal que permita al personal de la organización cumplir con sus responsabilidades. Los sistemas de información producen la información operativa, financiera y de cumplimiento que posibilita el funcionamiento y control del negocio. Se ocupan no solamente de datos generados internamente, sino así también sobre cómo las actividades individuales duales se relacionan con el trabajo de otros. Deben existir medios de comunicación de información significativa en sentido ascendente. También necesita ser eficaz la comunicación con las partes externas, tales como clientes, proveedores, entes reguladores y accionistas.

15.2.5 Vigilancia/supervisión

Los sistemas de control interno deben ser supervisados para evaluar la calidad de su funcionamiento en un cierto plazo. Esto se logra mediante actividades de supervisión, evaluaciones específicas, o una combinación de ambas. La supervisión tiene lugar durante la ejecución de las operaciones e incluye la gestión y supervisión regular de las actividades y de las otras acciones que realiza el personal en la ejecución de sus deberes. El alcance y la frecuencia de las diversas evaluaciones dependerán sobre todo de la evaluación de riesgos y de la eficacia de los procedimientos de supervisión en curso. Las deficiencias de control interno se deben comunicar de manera ascendente en la organización y las cuestiones de importancia se deben informar a la alta dirección y al consejo de administración.

Existe sinergia y acoplamiento entre los componentes, formando un sistema integrado que reacciona dinámicamente a las condiciones cambiantes. El sistema de control interno está interrelacionado con las actividades operativas de la entidad y existe por razones fundamentales de negocio. El control interno es más eficaz cuando los controles se construyen en la infraestructura de la entidad y son una parte de la esencia de la empresa. Los controles incorporados a los procesos apoyan iniciativas de calidad, potenciación y desarrollo, evitan costes innecesarios y permiten dar rápida respuesta a condiciones cambiantes.

Hay una relación directa entre las tres categorías de objetivos de COSO (eficacia, fiabilidad, cumplimiento), que son los que la entidad se esfuerza por alcanzar, y los componentes necesarios para alcanzar los objetivos. Todos los componentes son relevantes para cada categoría de objetivos. Al mirar una categoría cualquiera, por ejempo, la eficacia y eficiencia de las operaciones, los cinco componentes deben estar presentes ejecutándose con eficacia para concluir que el control interno sobre las operaciones es eficaz.

La definición de control interno, con su identificación de conceptos fundamentales de un proceso, afectados por la gente, proveyendo una garantía razonable, junto con la clasificación de objetivos, con sus componentes y criterios para la eficacia y los debates asociados, constituyen esta estructura de control interno.

GTAG – Apéndice F — Objetivos de control de información y tecnologías relacionadas (CobiT) de ITGI — 16

Las organizaciones deben satisfacer los requisitos de calidad, fiduciarios y de seguridad para su información, como también para todos los activos. La dirección debe también optimizar el uso de los recursos disponibles, incluidos datos, sistemas de aplicación, tecnología, instalaciones y el personal. Para cumplir con esas responsabilidades, así como para alcanzar sus objetivos, la dirección debe establecer un adecuado sistema de control interno. Por consiguiente, debe existir un marco o sistema de control interno para dar soporte a los procesos del negocio y debe estar claro cómo cada actividad de control individual satisface los requerimientos de información e impacta sobre los recursos. El impacto sobre los recursos de TI se destaca en el esquema de CobiT junto con los requerimientos del negocio que se deben satisfacer para la efectividad, eficacia, confidencialidad, integridad, disponibilidad, cumplimiento, y fiabilidad de la información. El control, que incluye políticas, estructuras organizativas, prácticas y procedimientos, es responsabilidad de la dirección. La dirección, a través de su gobierno corporativo y de TI, debe asegurar que la diligencia debida sea ejercida por todos los individuos implicados en la gestión, así como el uso, diseño, desarrollo, mantenimiento, o la explotación de los sistemas de información.

La orientación del negocio es el tema principal de CobiT. Está diseñada no sólo para ser empleada por los usuarios y los auditores, sino que también y mucho más importante, como una lista de comprobación exhaustiva para los propietarios de los procesos de negocio. Cada vez más, la práctica de negocio implica la autorización total de los propietarios de los procesos de negocio así ellos tienen la responsabilidad total de todos los aspectos de los procesos de negocio. En particular, esto incluye proporcionar controles adecuados. El marco de CobiT proporciona una herramienta para el propietario de los procesos de negocio que facilita el cumplimiento de esta responsabilidad. El marco empieza con una premisa simple y pragmática: para proporcionar la información que la organización necesita para alcanzar sus objetivos, es necesario que los recursos de TI sean gestionados por un conjunto de procesos agrupados de forma natural.

CobiT continúa con un conjunto de 34 objetivos de control de alto nivel, uno para cada uno de los procesos de TI, agrupados en cuatro dominios:

Planificación y Organización – Este dominio cubre estrategias y tácticas, y se refiere a la identificación de la forma en que TI puede contribuir de la mejor manera posible al logro de los objetivos del negocio.

1. Definir un plan estratégico de TI.
2. Definir la arquitectura de información.
3. Determinar la dirección tecnológica.
4. Definir la organización y las relaciones de TI.
5. Gestionar las inversiones de TI.
6. Comunicar los objetivos y las directrices de la gerencia.
7. Gestionar los recursos humanos.
8. Asegurar el cumplimiento con requerimientos externos.
9. Evaluar los riesgos.
10. Gestionar los proyectos.
11. Gestionar la calidad.

Adquisición e Implementación – Para realizar la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas, o adquiridas, así como ser implementadas e integradas dentro del proceso de negocio. Además, los cambios internos y el mantenimiento de los sistemas existentes son cubiertos por este dominio para asegurar que el ciclo de vida es continuo para estos sistemas.

12. Identificar las soluciones automatizadas.
13. Adquirir y mantener el software de aplicaciones.
14. Adquirir y mantener la arquitectura de tecnología.
15. Desarrollar y mantener los procedimientos de TI.
16. Instalar y acreditar los sistemas.
17. Gestionar los cambios.

Entrega y Soporte– Este dominio se refiere a la entrega real de los servicios requeridos, que se extienden desde operaciones tradicionales sobre seguridad y continúan con aspectos de formación. Este dominio incluye el proceso real de los datos por los sistemas de aplicación.

18. Definir y gestionar los niveles de servicio.
19. Gestionar los servicios de terceros.
20. Gestionar el rendimiento y la capacidad.
21. Asegurar la continuidad del servicio.
22. Asegurar la seguridad de los sistemas.
23. Identificar y asignar los costes.
24. Educar y entrenar a los usuarios.
25. Asistir y aconsejar a los clientes de TI.
26. Gestionar la configuración.
27. Gestionar los problemas y los incidentes.
28. Gestionar los datos.
29. Gestionar las instalaciones.
30. Gestionar las operaciones.

Supervisión y evaluación – Todos los procesos de TI necesitan ser evaluados regularmente en un cierto plazo respecto a su calidad y cumplimiento con los requerimientos de control. Este dominio trata así, que la dirección supervise el proceso de control de la organización y el aseguramiento independiente proporcionado por la auditoría interna y externa u obtenidos desde fuentes alternativas.

31. Supervisar los procesos.
32. Evaluar la adecuación del control interno.
33. Obtener el aseguramiento independiente.
34. Proporcionar la auditoría independiente.

Esta estructura cubre todos los aspectos de la información y de la tecnología que la soporta. Por medio del enfoque en esos 34 objetivos de control de alto nivel, el propietario de los procesos de negocio puede asegurar que se proporciona un sistema de control adecuado para el entorno de TI.

CobiT consta de:

- Un resumen ejecutivo, que proporciona una visión general de los temas y premisas fundamentales de CobiT*.
- El marco de CobiT, que describe detalladamente los objetivos de control de TI de alto nivel e identifica los requerimientos del negocio para la información y los recursos de TI afectados primariamente por cada objetivo del control.
- Los objetivos de control, las declaraciones de los resultados deseados o propósitos a ser alcanzados para la implementación de los objetivos de control específicos detallados*.

- Las pautas de auditoría, pasos sugeridos para la auditoría que se corresponden con cada uno de los objetivos de control de TI.
- Un conjunto de herramientas de implementación, que proporciona las lecciones aprendidas desde las organizaciones que aplicaron exitosamente CobiT en sus entornos de trabajo y diversas herramientas para ayudar a la dirección a evaluar su entorno de control relacionado con la información y sus recursos de TI.
- Las pautas de la gestión, que están compuestas por modelos de madurez para ayudar a determinar las etapas y expectativas de los niveles de control; factores críticos de éxito para identificar las acciones más importantes para alcanzar el control sobre los procesos de TI; indicadores claves de las metas para definir niveles objetivos del rendimiento e indicadores clave de rendimiento para medir si el control del proceso de TI logra su objetivo*.

* Diseñado por ITGI e ISACA como norma abierta, esta parte de COBITse puede descargar de http://www.itgi.org y de http://www.isaca.org.

CobiT, está ahora en su tercera edición y está disponible en copia impresa o en formato interactivo (CobiT en línea), se acepta cada vez más internacionalmente como buena páctica para control de la información, TI y riesgos relacionados. Esta guía permite a la empresa implementar un efectivo gobierno sobre TI que sea dominante e intrínseco a través de la empresa.

Copyright © 2000 del ITGI y reproducido con el permiso del ITGI. No se concede ningún otro derecho o permiso con respecto a este trabajo.

Las siguientes descripciones de métricas se toman del informe borrador de los Equipos de mejores prácticas y métricas, 17 de noviembre de 2004, del Grupo de Trabajo de Seguridad de la Información Corporativa (CISWG, en inglés). Durante la Fase I del CISWG, convocado en noviembre de 2003 por el Representante Adam Putnam (Florida), el Equipo de mejores prácticas examinó la información disponible de seguridad de la información. Concluyó el informe[7] de marzo del 2004 que gran parte de esta guía está expresada en un nivel relativamente alto de abstracción y por lo tanto no es inmediatamente útil como guía para ser procesada sin una elaboración significativa y a menudo costosa. Se creó un listado de una página de los Elementos del programa de seguridad de la información, considerado un contenido esencial para la dirección de una entidad en su conjunto en los temas de seguridad de la información de la empresa, y en el futuro se espera que se desarrollen guías manejables para su uso en una amplia variedad de organizaciones.

Los Equipos de métricas y mejores prácticas de la Fase II del CISWG, convocados en junio de 2004, fueron designados para ampliar el trabajo de la Fase I, refinaron los Elementos del programa de seguridad de la información y desarrollaron métricas para respaldar cada uno de los elementos. La meta fue desarrollar un recurso que ayudara a los miembros del consejo, a los gerentes y al personal técnico a establecer una estructura global de principios, políticas, procesos, controles y métricas de rendimiento para apoyar a la gente, los procesos y los aspectos de la tecnología de seguridad de la información.

Estas métricas genéricas se pueden utilizar como base para determinar informes regulares de los requerimientos para el comité de auditoría, aunque no es una solución del tipo "una sola talla para todos".

Los Elementos del programa de seguridad de la información y las Métricas de respaldo tienen la Intención de hacer posible que los consejos de administración, la dirección y el personal técnico puedan supervisar el estado y el progreso, en un cierto plazo, del programa de seguridad de la información de su organización. Cada organización debe considerar cuidadosamente qué elementos y métricas del programa pueden ser útiles en sus propias circunstancias. Deben entonces, fijar sus propias prioridades de implementación y establecer una política, un proceso, y una estructura apropiada de control. Las organizaciones más grandes y complejas crearán políticas, procesos y controles en cadaelemento del programa, estos inevitablemente serán más extensos que los que una organización más pequeña puede elegir para implementar.

17.1 Métricas para la junta directiva o el consejo de administración

Establecer un programa competente de seguridad de la información requiere que los miembros del consejo presten atención a ciertos elementos de programa. Los miembros del consejo pueden utilizar las siguientes métricas como parte de sus responsabilidades en cuanto a seguridad de la información.

Los miembros del consejo generalmente deben encontrar el mejor objetivo para cada métrica, más alto o más bajo, para que sean evidentes en sí mismos.

- Supervisar los programas de gestión de riesgos y cumplimiento relacionados con la seguridad de la información.
  - Porcentaje de los activos clave de información para los que se ha implementado una estrategia global para mitigar los riesgos de la seguridad de la información, según sea necesario, y mantener esos riesgos dentro de limites aceptables.
  - Porcentaje de las funciones claves organizativas para las que se ha implementado una estrategia global para mitigar los riesgos de la seguridad de la información, según sea necesario, y mantener esos riesgos dentro de limites aceptables.
  - Porcentaje de los requerimientos claves externos por los cuales la organización ha sido calificada como satisfactoria por una auditoría objetiva u otros medios.
- Aprobar y adoptar principios amplios del programa de seguridad de la información y aprobar la asignación de los gerentes clave responsables de la seguridad de la información.
  - Porcentaje de los principios del programa de seguridad de la información para los cuales las políticas y controles aprobados han sido implementados por la dirección.
  - Porcentaje de las funciones gerenciales clave de la seguridad de la información para las cuales se determinan las responsabilidades, las asignaciones y la autoridad, y se identifican las habilidades requeridas.
- Esforzarse en proteger los intereses de todos los accionistas, esto depende de la seguridad de la información.
  - Porcentaje de las reuniones del consejo y/o de las reuniones del comité designado para quienes la seguridad de la información es parte de la agenda.
  - Porcentaje de los incidentes de seguridad que causaron daño, riesgos, o pérdidas más allá de los límites establecidos para los activos, funciones o accionistas de la organización.
  - Daños o pérdidas estimadas en valor económico como resultado de todos los incidentes de seguridad en cada uno de los informes de los últimos cuatro períodos.
- Revisar las políticas de seguridad de la información considerando los socios estratégicos y a otros terceros.
  - Porcentaje de las relaciones de socios estratégicos y otros terceros, para quienes se han implementado mediante acuerdos los requisitos de seguridad de la información.
- Esforzarse en asegurar la continuidad del negocio.
  - Porcentaje de unidades organizativas con un plan establecido para la continuidad del negocio.
- Revisar las provisiones para las auditorías internas y externas del programa de seguridad de la información.
  - Porcentaje de auditorías internas y externas requeridas que hayan sido terminadas y revisadas por el comité.
  - Porcentaje de los hallazgos de auditoría que no se

7 http://reform.house.gov/TIPRC/

han resuelto.
- Colaborar con la dirección para especificar las métricas de seguridad de la información que se informarán al consejo.

17.2 Métricas para la dirección

Las siguientes métricas y elementos del programa han sido pensados para ayudar a la dirección a implementar las metas y políticas de seguridad de la información establecidas por el consejo como parte de un programa efectivo para dicha seguridad:

- Establecer las políticas y controles de gestión de seguridad de la información y de supervisión del cumplimiento.
  - Porcentaje de los elementos del programa de seguridad de la información para los cuales las políticas y controles aprobados son operativos.
  - Porcentaje de responsabilidades asignadas al personal para los controles y políticas de seguridad de la información, quienes han reconocido las responsabilidades asignadas en relación con esas políticas y controles.
  - Porcentaje de las revisiones de cumplimiento de las políticas de seguridad de la información que observaron infracciones.
  - Porcentaje de los responsables de unidades de negocio y gerentes de rango superior, quienes han implementado los procedimientos operativos para asegurar el cumplimiento con los controles y las políticas de seguridad de la información aprobados.
- Asignar las funciones, responsabilidades y habilidades requeridas para la seguridad de la información y asegurar su cumplimiento basándose en las funciones y los privilegios de acceso a la información.
  - Porcentaje de los nuevos empleados contratados en el período informado que realizaron con éxito su capacitación de concienciación en seguridad antes de otorgarles acceso a la red.
  - Porcentaje de los empleados que han completado su capacitación de actualización periódica en concienciación en seguridad, tal como lo requieren las políticas.
  - Porcentaje de las descripciones de los puestos de trabajo que definen, en relación con la seguridad de la información, las funciones, responsabilidades, habili dades, y las certificaciones para:
    + Gerentes y administradores de seguridad.
    + Personal de TI.
    + Personal en general usuario de los sistemas.
  - Porcentaje de las revisiones de desempeño de los puestos de trabajo que evalúan las responsabilidades de seguridad de la información y de cumplimiento de las políticas.
  - Porcentaje de las funciones de usuario, sistemas y aplicaciones que cumplen con el principio de separación de funciones.
- Número de individuos con acceso al software de seguridad que no han sido capacitados ni autorizados como administradores de seguridad.
- Número de individuos que pueden asignar los privilegios de seguridad a los sistemas y a las aplicaciones, que no están formados ni autorizados como administradores de seguridad.
  - Porcentaje de usuarios cuyos privilegios de acceso han sido revisados en el período informado, se incluyen:
    + Empleados con privilegios de alto nivel a los sistemas y a las aplicaciones.
    + Todos los demás empleados.
    + Contratistas.
    + Vendedores.
    + Empleados y contratistas que han causado bajas
  - Porcentaje de usuarios a quienes se les han verificado las referencias.
- Evaluar los riesgos de la información, establecer los limites del riesgo y gestionar activamente su mitigación.
  - Porcentaje de los activos críticos de información y las funciones dependientes de la información para los cuales se ha realizado y documentado alguna evaluación de riesgos según lo requieren las políticas.
  - Porcentaje de las funciones y los activos críticos para los cuales se ha cuantificado el coste del riesgo (pérdidas, daños, divulgación, o problemas de acceso).
  - Porcentaje de los riesgos identificados que tienen un plan definido de mitigación, contra el cual se informa la situación, de acuerdo con la política.
- Asegurar la implementación de los requerimientos de seguridad de la información para los socios estratégicos y otros terceros.
  - Porcentaje de los riesgos conocidos para la seguridad de la información, vinculados a las relaciones con terceros.
  - Porcentaje de las funciones o activos críticos de información, a los cuales el personal de terceros tiene acceso.
  - Porcentaje del personal de terceros con privilegios actualmente de acceso a la información que una autoridad determinada ha considerado como necesidad de acceso continuo de acuerdo con las políticas.
  - Porcentaje de sistemas con funciones y activos críticos de información que están conectados electrónicamente con sistemas de terceros.
  - Porcentaje de los incidentes de seguridad que implican a personal de terceros.
  - Porcentaje de los acuerdos con terceros que incluyen o demuestran verificación externa de políticas y de procedimientos.
  - Porcentaje de las relaciones con terceros que se han revisado en cuanto al cumplimiento con requerimientos de seguridad de la información.
  - Porcentaje de los hallazgos de no cumplimientos, que se han corregido desde la ultima revisión.
- Identificar y clasificar los activos de información.
  - Porcentaje de los activos de información que han sido revisados y clasificados por el propietario designado de acuerdo con el esquema de clasificación establecido por la política.
  - Porcentaje de los activos de información con privilegios

de acceso definidos que han sido asignados en base a las funciones y de acuerdo con la política.
  - Fecha de última actualización del inventario de activos.
- Implementar y probar los planes de continuidad del negocio
  - Porcentaje de unidades organizativas con un plan de continuidad del negocio documentado para los cuales se han asignado responsabilidades especificas.
  - Porcentaje de los planes de continuidad del negocio que se han revisado, ejercitado y probado y actualizado de acuerdo con la política.
- Aprobar la arquitectura de los sistemas de información durante la adquisición, el desarrollo, las operaciones y el mantenimiento
  - Porcentaje de los riesgos de seguridad de la información relacionados con la arquitectura de sistemas, que han sido identificados en la evaluación de riesgos más reciente y que se han mitigados adecuadamente.
  - Porcentaje de los cambios en la arquitectura de sistemas (adiciones, modificaciones, o eliminaciones) que fueron revisados en relación con los impactos de seguridad, luego, fueron aprobados por la autoridad apropiada y documenta dos vía formularios de peticiones de cambios.
  - Porcentaje de las funciones y activos críticos de información que residen en los sistemas que no cumplen con la arquitectura de sistemas aprobada.
- Proteger el entorno físico.
  - Porcentaje de las funciones y activos organizativos y críticos de información que han sido revisados desde la perspectiva de riesgos físicos, como controlar el acceso físico y la protección física de medios de respaldo.
  - Porcentaje de las funciones y activos organizativos y críticos de información expuestos a riesgos físicos, para los que se han implementado acciones de mitigación de riesgos.
  - Porcentaje de activos críticos que se han revisado desde la perspectiva de riesgos ambientales, como temperatura, fuego, e inundaciones.
  - Porcentaje de servidores en lugares con acceso físico controlado.
  - Porcentaje de los requerimientos de ley y regulaciones aplicables a la seguridad de la información, que se incluyen en los programas y calendarios de auditoría interna y externa.
  - Porcentaje de las auditorías de seguridad de la información realizadas en cumplimiento de los programas y calendarios aprobados de auditoría interna y externa.
  - Porcentaje de las acciones gerenciales en respuesta a los resultados de los hallazgos y recomendaciones de auditoría, que fueron implementadas según lo acordado en relación con la oportunidad y al grado de completado.
- Colaborar con el personal de seguridad para especificar las métricas de seguridad de la información que serán informadas a la dirección.

GTAG — Apéndice H — Cuestionario del DEA — 18

Los directores de auditoría interna pueden utilizar este cuestionario para examinar su estructura de control de TI a fin de asegurar que la organización ha considerado todos los elementos de control. El cuestionario puede ayudar al director ejecutivo de auditoría interna a entender los elementos y el plan para una cobertura total de auditoría interna de las áreas de control.

Acciones	Preguntas
1. Identificar el entorno de control de TI de la organización, se incluyen: a. Valores. b. Filosofía. c. Estilo de gestión. d. Conocimiento de TI. e. Organización. f. Políticas. g. Normas.	1. ¿Existen políticas y normas corporativas que describan la necesidad de controles de TI?
2. Identificar la legislación relevante y la regulación que afectan al control de TI, como a. Gobierno. b. Información a emitir. c. Protección de datos. d. Cumplimiento legal	2. ¿Qué legislación existe que impacte sobre la necesidad de controles de TI? 3. ¿La dirección ha tomado medidas para asegurar el cumplimiento de esta legislación?
3. Identificar las funciones y responsabilidades sobre los controles de TI en relación a lo siguiente: a. Consejo de administración i. Comité de Auditoría ii. Comité de Riesgos iii. Comité de Gobierno iv. Comité de Finanzas b. Dirección i. Presidente ii. Director Financiero y Contralor iii. Director de TI iv. Director de Seguridad v. Director de Seguridad de la Información vi. Asesoría Jurídica vii. Director de Riesgos c. Auditoría. i. Interna ii. Externa	4. ¿Se han asignado todas las responsabilidades relevantes de controles de TI a funciones individuales? 5. ¿Es compatible la asignación de responsabilidades con la aplicación de la separación de funciones? 6. ¿Están documentadas las responsabilidades deTI? 7. ¿Se han comunicado las responsabilidades de control de TI a toda la organización? 8. Los responsables individuales de cada función, ¿entienden claramente sus responsabilidades en cuanto a controles de TI? 9. ¿Qué evidencia hay de que los titulares de las funciones han ejercido sus responsabilidades? 10. ¿La auditoría interna emplea los suficientes especialistas de auditoría de TI para centrarse en aspectos del control de TI?

Acciones	Preguntas
4. Identificar el proceso de evaluación de riesgos. ¿Este cubre los siguientes aspectos?: a. Aceptación del riesgo. b. Tolerancia al riesgo. c. Análisis de riesgos. d. Comparación de riesgos con los controles de TI.	11. ¿Cómo se determina la aceptación de riesgo y la tolerancia al riesgo de la organización? 12. ¿La aceptación y tolerancia al riesgo de la organización han sido autorizadas en el nivel del consejo? 13. ¿La aceptación y tolerancia al riesgo son conceptos claramente comprendidos por todos aquellos que tienen responsabilidad en el control de TI? 14. ¿Existe un proceso formal de análisis de riesgos dentro de la organización? 15. ¿Todos aquellos con responsabilidades en el control de TI comprenden el proceso? 16. ¿Se utiliza el proceso de manera consistente en toda la organización?
5. Identifique todos los procesos de supervisión, incluidos los siguientes: a. Regulatorios. b. Internos a la empresa. c. Otros, excepto los de auditoría interna.	17. ¿Qué procesos existen para supervisar el cumplimiento de la legislación relevante, además de las políticas y las normas internas? 18. ¿Hay procesos de supervisión realizados por la dirección por fuera de las revisiones de auditoría interna?
6. Identifique los mecanismos de información y de comunicación: a. Información de control. b. Fallos de control.	19. ¿Qué métricas se proporcionan al consejo de administración, sus comités y a la dirección en lo referente a seguridad de TI? 20. ¿Qué informes adicionales se proporcionan al consejo de administración y a la dirección de regularmente? 21. ¿Está la dirección siempre informada cuando hay fallos de los controles de TI? 22. ¿El consejo de dirección y sus comités reciben informes similares de los fallos de TI?

La siguiente lista de material de referencia sobre la seguridad de la información, ha sido tomada de una lista compilada por el CISWG del Subcomité de Política de Tecnología de la Información, Relaciones Intergubernamentales y Censo; Comité de Reforma de Gobierno, de la Cámara de Representantes de Estados Unidos.

Los documentos se clasifican en tres secciones referentes a gobierno, dirección y aspectos técnicos.

19.1 Gobierno

Board Briefing on IT Governance, ITGI http://www.itgi.org/Template_ITGI.cfm?Section=ITGI&CONTENTID=6658&TEMPLATE=/ContentManagement/ContentDisplay.cfm.

Information Security Governance: Guidance for Boards of Directors and Executive Management, ITGI, http://www.itgi.org.

Information Security Management and Assurance, Three report series from The IIA National Association of Corporate Directors (NACD), U.S. Critical Infrastructure Assurance Office, et al., http://www.theiia.org/esac/index.cfm?fuseaction=or&page=rciap.

Information Security Oversight: Essential Board Practices, NACD, http://www.nacdonline.org/publications/pubDetails.asp?pubID=138&user=6158BBEB9D7C4EE0B9E4B98B601E3716.

IT Governance Implementation Guide, ISACA, http://www.isaca.org/Template.cfm?Section=Browse_By_Topic&Template=/Ecommerce/ProductDisplay.cfm&ProductID=503.

Turnbull Report - Internal Control - Guidance for Directors on the Combined Code, Institute of Chartered Accountants in England & Wales, http://www.icaew.co.uk/index.cfm?AUB=TB2I_6242,MNXI_47896.

19.2 Dirección

BS 7799 – Parts 1 & 2, Code of Practice for Information Security Management, British Standards Institution, http://www.bsi.org.uk.

Common Sense Guide for Senior Managers, Internet Security Alliance, www.isalliance.org.

Corporate Information Security Evaluation for CEOs, TechNet, http://www.technet.org/cybersecurity.

Generally Accepted Information Security Principles (GAISP), Information Systems Security Association. Currently available: ***Generally Accepted Systems Security Principles (GASSP)*** consisting of Pervasive Principles and Broad Functional Principles. Detailed Principles are under development. http://www.issa.org/gaisp/gaisp.html.

Generally Accepted Principles and Practices (GAPP), NIST SP 800-18. "Guide for Developing Security Plans for Information Technology Systems," December 1998 (Marianne Swanson & Barbara Guttman), eight generally accepted principles (see OECD) and "Common IT Security Practices." http://csrc.nist.gov/publications/nistpubs/index.html.

ICC Handbook on Information Security Policy for Small to Medium Enterprises, International Chamber of Commerce (ICC), http://www.iccwbo.org/home/e_business/word_documents/SECURITY-final.pdf.

IFAC International Guidelines on Information Technology Management – Managing Information Technology Planning for Business Impact, International Federation of Accountants, http://www.ifac.org.

Information Security for Executives, Business and Industry Advisory Committee to the OECD and ICC, http://www.iccwbo.org/home/e_business/word_documents/SECURITY-final.pdf.

ISO 17799 – Information Technology – Code of Practice for Information Security Management, International Organization for Standardization (ISO), http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441&ICS1=35&ICS2=40&ICS3.

OECD Guidelines for the Security of Information Systems and Networks, nine pervasive principles for information security upon which several other guides are based, OECD, http://www.oecd.org/document/42/0,2340,en_2649_33703_15582250_1_1_1_1,00.html.

Standard of Good Practice for Information Security, Information Security Forum, http://www.isfsecuritystandard.com/index_ie.htm.

Trust Services Criteria (including SysTrust and WebTrust), American Institute of Certified Public Accountants, http://www.aicpa.org/trustservices.

19.3 Aspectos Técnicos

Consensus Benchmarks, Center for Internet Security, http://www.cisecurity.org.

DISA Security Technical Implementation Guides, http://www.csrc.nist.gov/pcig/cig.html.

ISO 15408 Common Criteria, http://www.csrc.nist.gov/cc/ccv20/ccv2list.htm.

ISO TR 13335 – Guidelines for the Management of Information Security, Parts 1-5, http://www.iso.org/iso/en/StandardsQueryFormHandler.StandardsQueryFormHandler.

IT Baseline Protection Manual (P BSI 7152 E 1), Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.bund.de/gshb/english/menue.htm.

ITCG: Information Technology: Control Guidelines, Canadian Institute of Chartered Accountants (CICA), http://www.cica.ca.

NIST Configuration Guides, National Institute of Standards and Technology (NIST), http://www.csrc.nist.gov/pcig/cig.html.

NIST 800-12 The Computer Security Handbook, NIST, http://www.csrc.nist.gov/publications/nistpubs/index.html.

NIST 800-30 Risk Management Guide for Information Technology Systems, NIST, http://www.csrc.nist.gov/publications/nistpubs/index.html.

NSA Configuration Guides, http://www.nsa.gov/snac.

SANS Step-by Step Guides, SANS Institute, http://www.store.sans.org.

19.4 Auditoría de TI

Control Objectives for Information and Related Technologies (CobiT), ISACA, http://www.isaca.org.

Federal Information Systems Controls Audit Manual (FISCAM), U.S. Government Accountability Office, http://www.gao.gov.

Information Technology: Control Guidelines (ITCG), CICA, http://www.cica.ca.

Se adjunta un listado de los términos técnicos usados en la guía con una definición simple y sencilla.

Activos de información– Los activos de información están basados en el valor de la información para la importancia y la existencia continua de la organización. Se hace una distinción entre activos de información y recursos de información, porque se considera que estos últimos generalmente incluyen los relacionados con recursos humanos y los recursos humanos no son considerados como propiedad de la organización.

Aseguramiento – Se refiere al acto de asegurar; una declaración que tiende a inspirar plena confianza; algo que se diseña para dar confianza.

Ataque cibernético – Un acto criminal perpetrado mediante el uso de computadoras y capacidades de telecomunicaciones que da como resultado violencia, destrucción y/o problemas en los servicios para crear temor al causar confusión e incertidumbre dentro de una población dada, con el objetivo de influir en un gobierno o una población para que cumplan con una agenda especial: política, social, o ideológica.

CAE – Chief audit executive, se traduce como Director Ejecutivo de Auditoría (DEA).

CEO – Chief executive officer, se traduce como Presidente.

CFO – Chief financial officer (Controller), se traduce como Director Financiero (Contralor)

CIO – Chief information officer, se traduce como Director de TI.

CISO – Chief information security officer, se traduce como Director de Seguridad de la Información.

CLC – Chief legal council, se traduce como Asesoría Jurídica.

Control general – Un control que se aplica generalmente al entorno de TI o al conjunto mixto de sistemas, redes, datos, personas, o procesos (también conocido como infraestructura de TI).

Controles de aplicación– Un control relacionado con el funcionamiento específico de un sistema de aplicación que da soporte a un proceso de negocio específico. Las aplicaciones habituales incluyen cuentas a pagar, gestión de inventarios y libro mayor. Las aplicaciones integradas combinan las funciones de muchos procesos de negocio en sistemas integrados que comparten bases de datos comunes.

Controles de TI – Aquellos controles que proporcionan garantía razonable de desempeño seguro, fiable y "resilient" del hardware, software, procesos y el personal, así como de la fiabilidad en la información de la organización.

COSO – Son las siglas del Comité de Organizaciones Patrocinadoras de la Comisión de Treadway. Consulte http:// www. coso.org/key.htm.

CRM – Customer resource management, se traduce como Gestión de recursos de clientes.

CSO – Director de Seguridad.

Efectividad / Eficacia – Realizar un trabajo con o sin condición de eficiencia. Si la legislación requiere que se realice algo, es probable que no requiera que se realice de manera eficiente, tal como se evidencia con el cumplimiento de la Ley Sarbanes-Oxley y las quejas frecuentes sobre este cumplimiento que hace que las empresas gasten grandes sumas sin valor agregado aparente para la organización o para los accionistas.

Eficiencia – Para ser eficiente, un proceso o una actividad debe ser también eficaz. Los estudios del instituto Information Technology Process Institute muestran cómo las organizaciones mejor consideradas disfrutan de la eficiencia al mantener un conjunto de controles eficaces que supervisan y resuelven el origen del problema, antes que responder solamente a los síntomas.

Gestión de riesgos – La permanente identificación, medición y mitigación del riesgo a través de una implantación de medidas demostrables, eficientes en relación al coste, y la administración del control sobre los riesgos y amenazas conocidos o conocibles que pueden afectar negativamente la confidencialidad, integridad o disponibilidad de la información de una organización.

GLBA – U.S. Gramm-Leach-Bliley-Act, Ley Gramm-Leach-Bliley de EE. UU.

Gobierno – La combinación de procesos y estructuras implantadas por el Consejo para informar, dirigir, gestionar y supervisar las actividades de la organización para el cumplimiento de sus objetivos.

Grado de aceptación de riesgo – Definido por COSO como "el grado de riesgo, en términos generales, que una compañía u otra organización, está dispuesta a aceptar en la consecución de sus objetivos. La dirección considera el "grado de aceptación del riesgo" de la organización, primero, al evaluar alternativas estratégicas, luego, al

establecer los objetivos en línea con la estrategia seleccionada y por último, al desarrollar mecanismos para gestionar los riesgos relacionados.

GTAG – Global Technology Audit Guide – Guía de Auditoría de Tecnología Global.

HIPAA – U.S. Health Information Portability and Accountability Act, se ha traducido como Ley de Responsabilidad y Portabilidad del Seguro Médico de EE. UU.

Infraestructura de TI – El entorno global de TI, incluyendo sistemas, redes, datos, personas y procesos. Las infraestructuras pueden también incluir la interacción de negocios e industrias a través de un soporte mutuo por medio de compartir recursos y servicios, como Internet, energía, servicios financieros, empresas de servicios, gobierno y transportes. En la medida en que estas infraestructuras soportan economías nacionales o regionales, defensas y continuidad de negocio, se conocen como infraestructuras crítica.

ISO 17799 – Código de buenas prácticas para la gestión de seguridad de la información. Consulte http://http://www.iso27000.es

ITPI – IT Process Institute. Consulte http://www.itpi.org.

Marco – Un marco para organizar algo (por ejemplo aspectos de gobierno, controles) con el fin de identificar necesidades en diferentes niveles de la organización, así como actividades y procesos. Un marco de control es una definición que identifica las necesidades de control pero que no describe cómo deben ser aplicados. Cada organización y sus unidades operativas proporcionan el nivel de detalle en relación con sus propios objetivos y prácticas de control.

Public Company Accounting Oversight Board (PCAOB) – PCAOB, Consejo Supervisor Contable de Empresas Públicas, un consejo de la Comisión del Mercado de Valores de EE. UU., establecido por la Ley Sarbanes-Oxley del año 2002, como órgano supervisor de los informes financieros y de auditoría.

Recursos de información – Incluye todos lo elementos de la organización que incumben a los procesos de información (por ejemplo, adquisiciones, procesamiento, comunicaciones y almacenamiento) incluyendo el hardware, software, procesos y personal relacionados.

Seguridad de la información – Los conceptos, técnicas y mediciones (técnicas y administrativas) utilizados para proteger los activos de información de la obtención no autorizada, daños, divulgación, manipulación, modificación, pérdida, uso, tanto intencional como accidental.

Tecnología de la información (TI) – Todos los componentes de hardware y software utilizados para procesar información y proporcionar comunicaciones, los procesos de administración y mantenimiento de tecnología y los recursos humanos asociados con el uso de la tecnología.

Tolerancia al riesgo – Definida por COSO como "el nivel aceptable de variación relativa al logro de objetivos. Al determinar las tolerancias específicas al riesgo, la dirección considera la importancia relativa de los objetivos relacionados y alinea la tolerancia al riesgo con su grado de aceptación de riesgo (o con el riesgo que está dispuesta a asumir).

Esta guía de controles de TI es la primera de una serie de GTAG que dará a los directores de auditoría interna y a los auditores internos, como a otros integrantes de la organización que tengan responsabilidades relacionadas con los controles de TI, una fuente de información para formarse en este tema.

Las guías GTAG proporcionarán orientación en una variedad de aspectos de TI. Cada guía describirá suficientemente los hechos subyacentes de la tecnología y los aspectos relacionados para explicar las oportunidades de negocio, los riesgos y los controles relacionados; y sus impactos en el sistema general de controles internos. Los temas que se tratarán en la serie de GTAG serán determinados por los que sean de actualidad en el marco de la TI y los que resulten de las áreas de tecnologías emergentes y sus implicaciones potenciales sobre los controles internos y el aseguramiento. Los temas previstos para las guías incluyen la protección contra intrusiones, la gestión de seguridad, la gestión de cambios, la seguridad de comunicaciones inalámbricas, la gestión de la identificación y la autentificación.

21.1 Partes del programa GTAG

Cada guía GTAG se desarrolla con la participación de expertos técnicos de auditoría y de seguridad, ejecutivos de auditoría, proveedores de tecnología y las asociaciones e individuos que representan a los miembros del consejo, la alta dirección, los ejecutivos de finanzas, los profesionales de tecnología de la información y los ejecutivos de seguridad. La participación de los institutos internacionales del IIA y los socios respaldan la filosofía global de las guías. Otros profesionales que presentan sus visiones especializadas en cuanto a temas legales, de seguros, regulatorios y normas, serán incluidos, según sea aplicable, dentro de los proyectos individuales de GTAG.

En este proyecto de GTAG, se han unido al IIA, un equipo especialmente seleccionado de asociaciones profesionales, instituciones académicas y profesionales de auditoría y de tecnología. El IIA está agradecido por el respaldo proporcionado por este equipo ya que la guía no hubiera sido posible sin ellos. Para que el IIA pueda proporcionar orientaciones a los auditores sobre cómo relacionarse con los clientes de auditoría, ha sido esencial obtener el consenso de los representantes clave de estos clientes. Para dirigirse a una audiencia global, la guía debe tener el consenso de un amplio grupo representante de los diversos países donde los auditores realizan su trabajo. Por lo tanto, agradecemos a las personas y a las organizaciones que han contribuido tanto a esta guía.

22.1 Consejo de Asesoramiento sobre los controles de TI

El Consejo de Asesoramiento está compuesto por personas que han contribuido al desarrollo de esta guía desde el comienzo de la planificación del proyecto del GTAG, pasando por el diseño y desarrollo inicial y diversos borradores de la Guía de Controles de TI, hasta completar el producto final. Estas personas han ido más allá de su función de un equipo de soporte voluntario actuando realmente con una función de liderazgo.

Julia H Allen, CMU/SEI Carnegie-Mellon University/Software Engineering Institute

Michael R. Dickson, Business Technology Group, LLC

Clint Kreitner, President/CEO, CIS, The Center for Internet Security

Alex Lajoux, NACD, National Association of Corporate Directors

Will Ozier, Vice Chair, the ISSA GAIS Committee CEO & President OPA Inc., The Integrated Risk Management Group, USA

Mark Salamasick, CIA, University of Texas at Dallas

Karyn Waller, AICPA, American Institute of Certified Public Accountants

22.2 Organizaciones asociadas

AICPA – Michael R. Dickson, Karyn Waller, American Institute of Certified Public Accountants

CIS – Clint Kreitner, Center for Internet Security

CMU/SEI – Julia Allen, Bob Rosenstein, Carnegie-Mellon University/Software Engineering Institute

ISSA – Dave Cullinane, President; Bob Daniels, Exec Vice President, Information Systems Security Association

NACD – Peter Gleason, Alex Lajoux, National Association of Corporate Directors

SANS Institute – Alan Paller, Director of Research, Stephen Northcutt, COO

22.3 Equipo de Revisión del Proyecto

Peter Allor, ISS, Internet Security Systems

Jack Antonelli, ADP

Ken D. Askelson, CIA, JC Penney Co. Inc.

Becky Bace, Infidel Inc.

Kevin Behr, IPSI, Institute for Integrated Publication and Information Systems

Jeff Benson, BearingPoint

Robert S. Block, Chairman, 3D Business Tools, USA

Sylvia Boyd, The IIA

Alexandra Branisteanu, Information Security Officer, Scripps Health, San Diego, USA

Larry Brown, Options Clearing Corp.

Stephanie Bryant, University of South Florida

Phil Campbell, Specialized IT, LLC, USA

John Carlson, BITS, Banking Industry Technology Secretariat

Chris Compton, Intrusion Labs

Guy Copeland, CSC, Computer Sciences Corp.

Rich Crawford, Vice President/Senior Security Advisor, Janus Risk Management, USA

Bob Daniels, EDS

Bob Dix, U.S. House of Representatives

GTAG — Apéndice L — Socios y Equipo Global del Proyecto GTAG — 22

Jerry E. Durant, CIA, President, Certifiable Technologies Ltd., Orlando, Fla., USA

Emily Frye, Critical Infrastructure Protections Program, George Mason University, School of Law, USA Protections Program

Greg Garcia, ITAA, Information Technology Association of America

Russ Gates, Dupage Consulting LLC

Lou Giles, Chevron Phillips Chemical Co.

Doug Guerrero, EDS

Kai Tamara Hare, Nuserve

Michael S. Hines, CIA, Purdue University

Bob Hirth, Protiviti

Don Holden, CISSP, Concordant Inc., USA

Dave Kern, Ethentica

Gene Kim, CTO, Tripwire Inc., USA

Jim Kolouch, BearingPoint

David Kowal, VP, JP Morgan Chase

Paul Kurtz, CSIA, Cyber Security Industry Alliance

Cindy LeRouge, Ph.D., Decision Sciences/MIS Department

John Cook School of Business, St. Louis University, USA

Andrée Lavigne, CICA, Canadian Institute of Chartered Accountants

Debbie Lew, Guidance Software

Brenda Lovell, CIA, CCSA, CGAP, The IIA

Warren Malmquist, Adolph Coors Co.

Stacy Mantzaris, CIA, IIA

Dennis Miller, Heritage Bank

Patrick Morrissey, Auditwire

Bruce Moulton, Symantec

Paul Moxey, ACCA, Association of Chartered Certified Accountants

Roseane Paligo, CIA, Chief Financial Officer, 1st Choice Community Federal Credit Union, USA

Fred Palmer, Palmer Associates

Xenia Parker, CIA, CFSA, VP, Enterprise Technology Group, Marsh Inc.,

Bernie Plagman, TechPar Group

Heriot Prentice, MIIA, FIIA, QiCA, The IIA

Dick Price, Beacon IT Ltd., BS 7799 Consultancy, USA

Michael Quint, Corporate Compliance Officer, EDS Corporate Audit, USA

Sridhar Ramamoorti, CIA, CFSA, Ernst & Young LLP, Chicago, IL, USA

Amy Ray, Bentley College

Martin Ross, GSC, Global Security Consortium

Chip Schilb, EDS, USA

Howard Schmidt, eBay

Mark Silver, Symantec

George Spafford, President, Spafford Global Consulting, Saint Joseph, IL, USA

Adam Stone, Assurant

Jay H. Stott, CIA, Fidelity Investments

Dan Swanson, CIA, IIA

Jay R. Taylor, CIA, CISA, CFE, General Motors Corporation

Bill Tener, University & Community College System of Nevada

Archie Thomas

Fred Tompkins, BearingPoint

Don Warren, Rutgers University

Dominique Vincenti, CIA, The IIA

Mark Winn, Intrusec

Amit Yoran

22.4 Institutos internacionales del IIA

Frank Alvern, CIA CCSA, Nordea Bank, Noruega

Alexandre Alves Apparecido, Brasil

Dror Aviv, Israel

David F. Bentley, England, RU e Irlanda.

Gerardo Carstens, CIA, IIA Argentina

Richard Cascarino, Sudáfrica.

Iftikhar Chaudry, Pakistan

Hisham T. El Gindy, Manager, KPMG Hazem Hassan,Egipto

Dr. Ulrich Hahn, CIA, Suiza

Rossana S. Javier, Makati City, Filipinas

Andras Kovacks, Hungría

Christopher McRostie, Australia

Furqan Ahmad Saleem, Partner, Avais Hyder Nauman Rizwani RSM, Pakistan

Kyoko Shimizu, CIA, Japón.

John Silltow, Security Control and Audit Ltd., Reino Unido

Ken Siong, Federación Internacional de Contadores

Anton van Wyk, PwC, Sudáfrica

Nick Wolanin, Conferencista Senior Adjunto, graduado universitario de Australia.

Julie Young, Australia

22.5 Otros profesionales internacionales

Carolee Birchall, Vice President and Senior Risk Officer, Bank of Montreal, Canada

P. J. Corum, Quality Assurance Institute, Middle East and Africa, United Arab Emirates

Ariel Peled, President, ISSA Israeli Chapter
P. Shreekanth, India

Karen Woo, Selangor, Malaysia

22.6 Comité Internacional de Tecnología Avanzada del IIA

Anton van Wyk, (Chairman), CIA, PricewaterhouseCoopers, South Africa

Alexandre Alves Apparecido, Brasil Telecom, Brazil

Ken D. Askelson, CIA, JC Penney Co. Inc., USA

Dror Aviv, CFSA, IIA Israel

Donald L. Bailey, Grant Thornton, LLP, USA

E.W. Sean Ballington, PricewaterhouseCoopers, LLP, USA (originally South Africa)

Norman F. Barber, Microsoft Corp., USA

David F. Bentley, QiCA, Consultant, England

Claude Cargou, GIE AXA, France

Michael P. Fabrizius, CIA, Bon Secours Health System Inc., USA

Ramiz Tofigi Ganizade, Azerbaijan Republic Chamber of Auditors, Azerbaijan

Douglas Guerrero, EDS Corp., USA

Dr. Ulrich Hahn, CIA, Syngenta International, Switzerland

David J Hill, IBM Corp., USA

Michael S. Hines, CIA, Purdue University, USA

Mark J. Hornung, Ernst & Young LLP, USA

Gene Kim, CTO, Tripwire Inc., USA

David S. Lione, KPMG LLP Southeast Region, USA

Peter B. Millar, ACL Services Ltd., Canada

Allan M. Newstadt, CIA, World Bank/International Finance Corp., USA

Brenda J. S. Putman, CIA, City Utilities of Springfield, USA

Kyoko Shimizu, CIA, Shin Nihon & Co., Japan

Brian M. Spindel, CIA., SecurePipe Inc., USA

Rajendra P. Srivastava, University of Kansas, USA

Jay Stott, CIA, Fidelity Investments, USA

Jay R. Taylor, CIA, CISA, CFE, General Motors Corp., USA

Thomas Jason Wood, CIA, Ernst & Young LLP, USA

Akitomo Yamamoto, IIA, Japan

22.7 Equipo de redacción

David A. Richards, CIA, President, The IIA

Alan S. Oliphant, MIIA, QiCA, MAIR International

Charles H. Le Grand, CIA, CHL Global

22.8 Equipo de producción y personal de la oficina central del IIA

Michael Feland

Trish Harris

Tim McCollum

GTAG

Controles de tecnología de la información

Esta guía describe cómo se distribuyen los roles de TI y las responsabilidades en la organización, cómo se logra una evaluación precisa de los controles de TI y cómo la organización puede fomentar la confiabilidad y eficiencia de TI.

¿Qué es GTAG?

La Guía de Auditoría de Tecnología Global (GTAG) ha sido preparada por el Instituto de Auditores Internos y está escrita en un lenguaje de negocios claro y directo para abordar temas de actualidad relacionados con la gestión, el control o la seguridad de la tecnología de la información. GTAG es una colección de recursos lista para ser utilizada por los directores ejecutivos de auditoría en la educación de los miembros del Consejo de Administración y del Comité de Auditoría, Dirección, propietarios de los procesos y otros en lo que respecta a riesgos asociados a la tecnología y prácticas recomendadas.

The Institute of Internal Auditors

www.theiia.org