Gestión TI

Controles internos en una organización TI

Índice

Esquema 3

Ideas clave 4

2.1. Introducción y objetivos 4

2.2. Control interno informático 5

2.3. Clasificación de los controles internos 9

2.4. Controles generales de una organización TI 11

2.5. Controles de aplicación 15

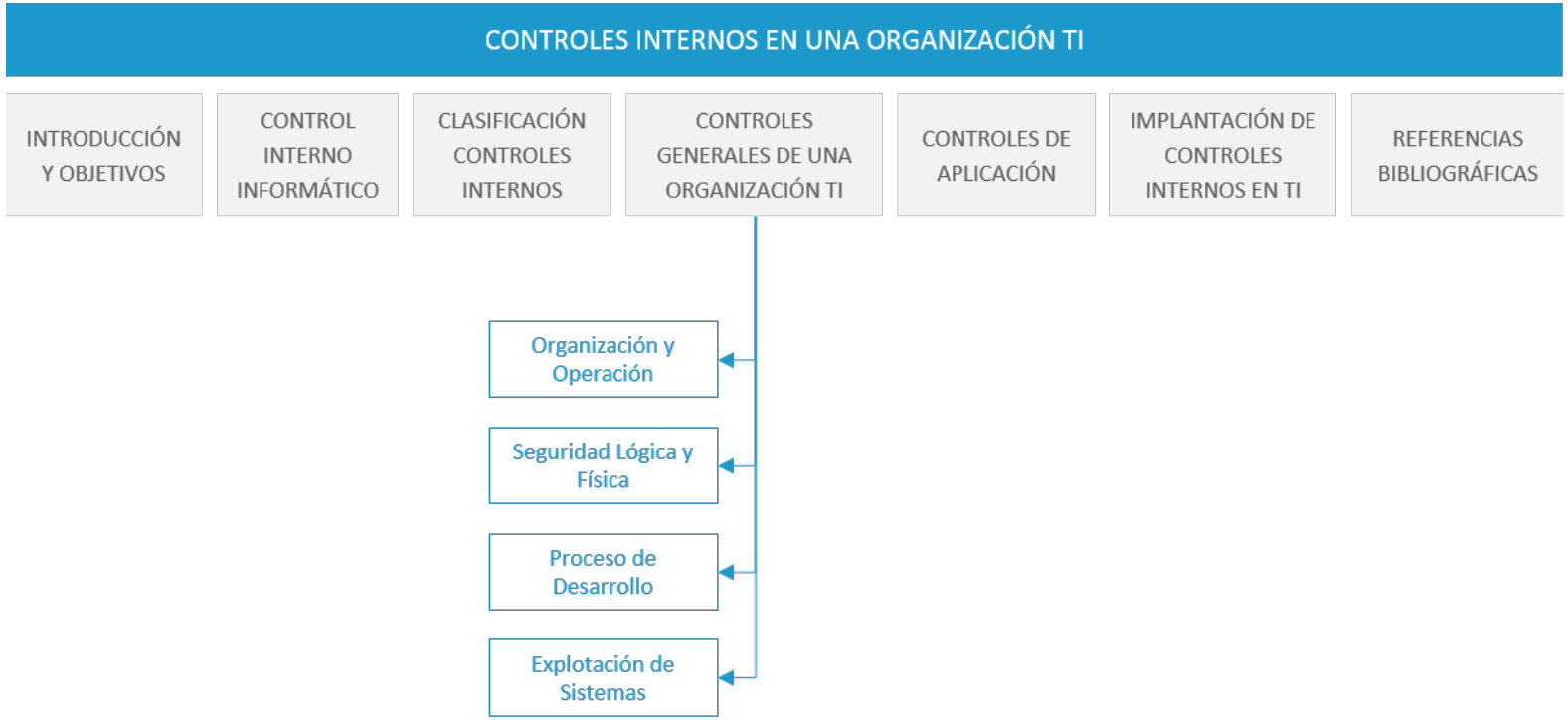
2.6. Implantación de controles internos en una organización TI 17

2.7. Referencias bibliográficas 20

A fondo 21

Test 25

Esquema



Ideas clave

2.1. Introducción y objetivos

Los controles internos presentes en una organización TI son los encargados de detectar las posibles amenazas que pueda sufrir la información, y de su buen funcionamiento dependerá la precoz activación de las medidas oportunas para mitigar las amenazas detectadas y las posibles pérdidas económicas de la organización.

Este tema está estructurado en 5 apartados que abordarán los principales aspectos a considerar en la dirección de una organización tecnológica con respecto a los controles internos. Quién se responsabiliza de los controles internos, cómo proceder a su implantación, o un análisis más profundo de los controles generales y los controles de aplicación como principales controles internos a considerar, son los capítulos que conforman el temario.

Los objetivos que se pretenden conseguir son:

- Conocer el control interno informático de una organización TI.
- Describir los principales controles internos a considerar en una organización tecnológica.
- Exponer la clasificación de los controles internos.
- Comprender la implementación de controles internos en una organización

2.2. Control interno informático

La Real Academia Española define el término control como: «comprobación, inspección, fiscalización o intervención». En términos de gestión tecnológica podemos definir control como el conjunto de acciones y mecanismos que establece una organización para prevenir o reducir el impacto que los posibles riesgos, o eventos no deseados, puedan causar a los activos de una organización.

ISACA (2016) define los controles internos como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para proporcionar, con una garantía razonable, el logro de los objetivos empresariales y la prevención, detección y corrección de eventos no deseados.

Hasta hace poco tiempo, un control se solía abordar solo desde un punto de vista de la gestión de riesgo, lo cual limita el potencial de las organizaciones TI a la hora de emplear el concepto. Si los controles se pueden utilizar para mitigar las posibles consecuencias negativas, por ejemplo, los riesgos, también pueden ser utilizados para asegurar resultados positivos deseables que proporcionen valor adicional a las empresas, por lo que se podría definir a los controles internos como:

Aquellas estructuras específicas, herramientas, procesos u otros mecanismos que se utilizan para garantizar un resultado.

El framework 2013 del *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) (COSO, 2013) establece cinco componentes integrados de control interno:

- **Ambiente de control:** El ambiente de control describe un conjunto de normas, procesos y estructuras que proporcionan la base para llevar a cabo el control interno en la organización.

- **Evaluación de riesgos:** La evaluación de riesgos es la base para determinar la forma de administrar los riesgos. El riesgo se define como la posibilidad de que un evento suceda y afecte negativamente al cumplimiento de los objetivos de la organización. La evaluación del riesgo exige que se considere el impacto de posibles cambios en el entorno y se tomen medidas para gestionar el impacto.
- **Actividades de control:** Las actividades de control son acciones que ayudan a mitigar los riesgos, a fin de asegurar el logro de los objetivos. Las actividades de control puede ser preventivas o detectivas y pueden realizarse en todos los niveles de la organización.
- **Información y comunicación:** La información se obtiene de fuentes internas y externas a fin de prestar apoyo a los órganos de control interno. La comunicación se utiliza para difundir información importante dentro y fuera de la organización, así como para apoyar los requisitos de toda reunión.
- **Actividades de monitoreo:** Las actividades de monitoreo son las evaluaciones periódicas o permanentes para verificar que cada uno de los cinco componentes del control interno, incluyendo los controles que afectan los principios de cada componente, están presentes y en funcionamiento.

El cumplimiento de las actividades integradas en estos componentes, especialmente la monitorización, permitirá establecer un proceso de mejora de los controles internos que asegure su alineamiento con la estrategia empresarial.

Definición de control interno informático

El control interno informático controla diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijadas por la Dirección de la organización y/o la Dirección de informática, así como los requerimientos legales. (Piattini y del Peso, 2008)

Para realizar llevarlo a cabo, la organización implementa un conjunto de controles, que, de forma eficiente y con eficacia, aseguren diariamente que las TIC de la organización están alineadas con sus objetivos estratégicos.

Aunque son varios los objetivos que Piattini y del Peso (2008) establecen para el control interno informático a alcanzar, se quiere resaltar los siguientes:

- **Definir e implantar controles y mecanismos** para comprobar el correcto funcionamiento del entorno TI, estableciendo responsabilidades en todos los niveles de la organización.
- Realizar en los diferentes entornos de trabajo tecnológico **el control de las diferentes actividades operativas** para cumplir con los procedimientos, normas y controles establecidos. Especial atención merecen el control de cambios y de versiones del software.
- **Controlar la producción diaria**, la calidad y eficiencia del desarrollo y el mantenimiento de los sistemas de información.
- **Asesorar** y transmitir **cultura** sobre el **riesgo** informático.

Diferencias entre control interno y auditoría informática

Considerando las definiciones y conceptos vistos hasta el momento en los temas 1 y 2, resulta interesante destacar las diferencias que hay entre el control interno y la auditoría informática con el fin de esclarecer los límites de cada una de las actividades.

Así, el control interno informático vendría definido por las siguientes características:

- Efectúa un análisis diario de los controles de la organización.
- Reporta el informe diario a la Dirección del Departamento de Informática.
- Es efectuado por personal propio o interno de la organización.
- El límite de sus funciones es únicamente sobre el Departamento de Informática.

Frente a estas características del control interno informático, las características que presenta la auditoría informática serían las siguientes:

- El análisis de los controles de la organización se efectúa en un momento determinado de tiempo.
- Reporta un informe final de la auditoría informática a la Dirección General de la Organización.
- Suele efectuarse con personal externo a la organización, pero también puede incluir personal propio o interno a la organización.
- Carece de límites en sus funciones al cubrir cualquier componente de un sistema de información que esté presente en la organización.

Una comparativa de estas diferencias queda resumida en la tabla 1:

DIFERENCIAS			
CONTROL INTERNO INFORMÁTICO		AUDITORÍA INFORMÁTICA	
1	Análisis diario de los controles	1	Análisis de controles en un momento determinado de tiempo
2	Reporta a la Dirección del Departamento de Informática	2	Reporta a la Dirección General de la organización
3	Efectuado solo por personal interno	3	Efectuado tanto por personal externo cómo externo
4	Funciones limitadas al Departamento de Informática	4	Funciones afectan a todos los componentes de los sistemas de información en la organización

Tabla 1. Diferencias entre control interno y auditoria informática.

A la vista de estas características cabe destacar como **la principal diferencia** entre ambos conceptos el momento temporal en que se efectúa cada uno:

El control interno informático realiza un proceso de verificación diario para mantener la eficiencia y eficacia de los controles internos, mientras que la

auditoría informática analiza los controles con una base temporal puntual establecida por la dirección de la organización. A modo de metáfora sería un «retrato de los sistemas de información» en un instante concreto.

Es igualmente interesante resaltar que ambas actividades no solo presentan diferencias, sino que también presentan algunas semejanzas:

- El personal interno que participa en las actividades debe poseer sólidos conocimientos de Tecnologías de la Información.
- En ambos casos, el objetivo es verificar tanto el cumplimiento de las normativas o procedimientos que ha redactado para los sistemas de información, bien la dirección informática, bien la dirección general, como la eficiencia y eficacia de los controles internos implantados.

2.3. Clasificación de los controles internos

A la hora de establecer una clasificación de los controles internos existen múltiples posibilidades en función de las características que se emplean en la clasificación.

Una primera **clasificación general** de los controles internos permite establecer dicotomías excluyentes entre ellos:

- **Voluntarios**: cuando son diseñados por la organización con el fin de alcanzar una mejora de sus procesos.
- **Obligatorios**: cuando son las autoridades externas o reguladoras quienes imponen la implementación de esos controles.

- **Manuales**: las personas se encargan de ejecutar estos controles.
- **Automáticos**: son los sistemas de información automatizados quienes activan de forma automática estos controles ante la llegada de un evento.

- **Generales**: están orientados a establecer un entorno de desarrollo donde van a establecerse otros controles.
- **De aplicación**: son controles internos plenamente orientados hacia una aplicación o software concreto.

Si se profundiza un poco más en la clasificación y se procede a atender a su **naturaleza**, podríamos clasificar los controles internos en tres tipos de controles:

- **Preventivos**: buscan eliminar la vulnerabilidad de un activo o mitigar el impacto que podría tener un riesgo sobre dicho activo. Por ejemplo, impedir los accesos no autorizados al sistema.
- **Detectivos**: los controles detectivos se activan cuando fallan los preventivos y su función es notificar cuanto antes el evento ocurrido para evitar que la vulnerabilidad vaya a mayores. Las alarmas o el simple de registro de accesos no autorizados son alguna muestra de este tipo de controles.
- **Correctivos**: son controles internos cuya funcionalidad es restablecer la actividad del sistema una vez que se ha producido la incidencia. Buscan localizar y eliminar la causa de la incidencia para minimizar nuevas incidencias. Un ejemplo sería el empleo de copias de seguridad para restaurar un fichero dañado.

Figura 1. Clasificación controles internos por naturaleza.

Además, coexisten otros controles internos que deben ser igualmente considerados para garantizar la seguridad de la información:

- **Controles por área**: Son controles internos que analizan alguna de las áreas funcionales en que está dividido un Centro de Proceso de Datos. Este tipo de controles son particulares de cada organización, ya que en función de su distribución funcional, así será el área a controlar.
- **Controles de productos informáticos**: Están asociados a un software comercial para que la organización TI pueda observar que el producto informático ofrece todas las especificaciones dadas por la empresa desarrolladora y cumple correctamente con las funcionalidades deseadas.
- **Controles por motivos legales**: La legislación vigente en cada territorio aporta otro tipo de controles internos de cara a garantizar su cumplimiento. Puede ser una legislación nacional, internacional o propia de un territorio (UE) y con frecuencia las organizaciones recurren al asesoramiento de un auditor legal. (*Ley de protección de datos (LOPD), Reglamento Europeo de protección de datos (RGPD)).*

2.4. Controles generales de una organización TI

Para garantizar que los sistemas de información funcionan correctamente surgen los controles generales de una organización TI que se encargan de crear un entorno de desarrollo adecuado donde puedan aplicarse los controles de aplicación.

Existe una máxima en la relación entre los controles generales y los controles de aplicación:

Si bien la eficacia de los controles generales no garantiza por sí sola de la eficacia de los controles de aplicación, su ineficacia implicará con altas dosis de probabilidad la ineficacia de los controles de aplicación.

De entre los controles generales existentes, en este apartado vamos a referenciar cuatro de ellos:

- Controles de organización y operación.
- Controles de seguridad lógica y física.
- Controles del proceso de desarrollo.
- Controles de explotación de sistemas.

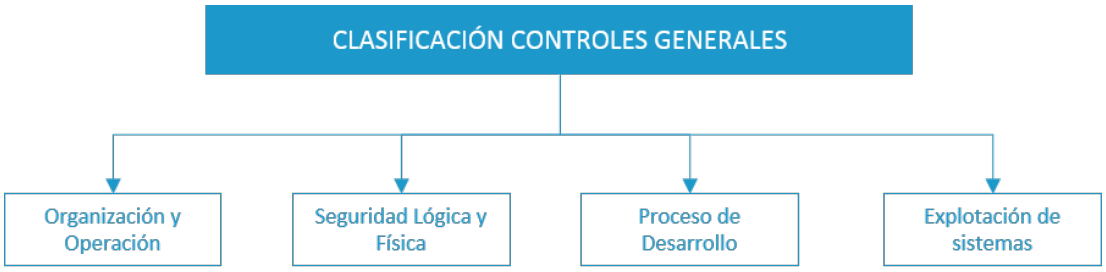


Figura 2. Clasificación controles generales.

Controles de organización y operación

Los controles de organización y operación se encargan de garantizar que la organización TI tiene definida una estructura y unas normas operativas para toda su empresa. Sin estos controles la efectividad del resto de los controles se verá claramente mermada, sino inutilizada. Algunos de los controles que deberán existir son:

- **Políticas y planes estratégicos de TI:** Debe existir un alineamiento entre el plan estratégico de la empresa y su plan estratégico de tecnologías de la información.
- **Gestión del presupuesto:** Debe existir un presupuesto de TI y efectuar un control sobre su cumplimiento.
- **Definición de las estructuras organizativas:** Las estructuras operacionales en la organización deben estar claramente definidas.

- **Marco procedimental de operación:** Toda organización TI deben crear normas y procedimientos de funcionamiento que permitan integrar los estándares del mercado.

Controles de seguridad lógica y física

La seguridad lógica se encarga de comprobar que el sistema está bien configurado evitando el acceso a las personas no autorizadas, mientras que la física se encarga de la seguridad que ofrece el entorno de trabajo donde se encuentra el equipo. Alguno de los controles a implementar son:

- Comprobar que exista una **política de seguridad** conocida por todo el personal.
- Pruebas **de identificación de usuarios**.
- Política de **contraseñas**.
- **Gestión de usuarios**.
- **Seguridad Física** de servidores y equipos críticos.
- Programas de protección frente a malware (**antivirus**).

Controles del proceso de desarrollo

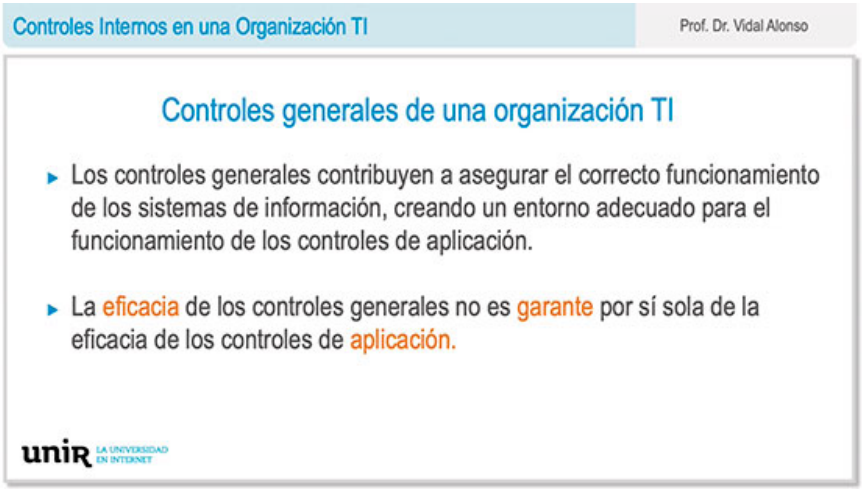
Los controles del proceso de desarrollo buscar dotar a los sistemas de información de la eficacia y eficiencia que exige la organización. Para ello dispondrá de una serie de normas, procedimientos o estándares de desarrollo que todo empleado debe conocer y utilizare en el desarrollo de su labor. Entre estos controles cabe destacar:

- Control para **gestionar** que los **cambios** a efectuar han sido aprobados.
- Comprobar que los **cambios** los realiza **personal autorizado**.
- Existencia de un control para **garantizar** el proceso de implementación de **cambios de emergencia**.
- Existencia de un **entorno de pruebas** completo que cumpla la segregación de funciones.

Controles de explotación de sistemas

Los controles de explotación de sistemas están orientados a que exista una correcta gestión en el departamento de explotación. Son controles generales orientados más a la relación con el exterior de la organización TI. Así, deberían implantarse los siguientes controles:

- Adquisición de aplicaciones y servidores.
- Integración de nuevas aplicaciones en la explotación de sistemas.
- Selección de proveedores bajo condiciones de servicio certificadas.
- Gestión de incidencias.
- Supervisión del proceso productivo.
- Control de la ejecución de procesos automáticos.



Vídeo. Controles generales de una organización TI.

Accede al vídeo a través del aula virtual

2.5. Controles de aplicación

Hoy en día las organizaciones tecnológicas son altamente dependientes de los sistemas de información o de las aplicaciones para cumplir con sus objetivos estratégicos. Por tal motivo, la auditoría informática debe abordar el funcionamiento de estas aplicaciones y conocer los riesgos que éstas pueden acarrear a la organización y establecer medidas de monitorización para mitigar esos posibles riesgos.

COBIT establece que los controles de aplicación consisten en actividades manuales y/o automáticas que aseguran que la información y los sistemas de información que procesan esa información cumplen con ciertos criterios. Estos controles de aplicación garantizan una seguridad razonable del alcance de los objetivos que la gerencia establece sobre las aplicaciones.

Los criterios establecidos son 7, de los cuales dos afectan a los sistemas de información y cinco a la información:

- **Efectividad** (requerimiento para los sistemas de información).
- **Eficiencia** (requerimiento para los sistemas de información).

- **Confidencialidad** (requerimiento para la información).
- **Integridad** (requerimiento para la información).
- **Disponibilidad** (requerimiento para la información).
- **Cumplimiento** (requerimiento para la información).
- **Confiabilidad** (requerimiento para la información).

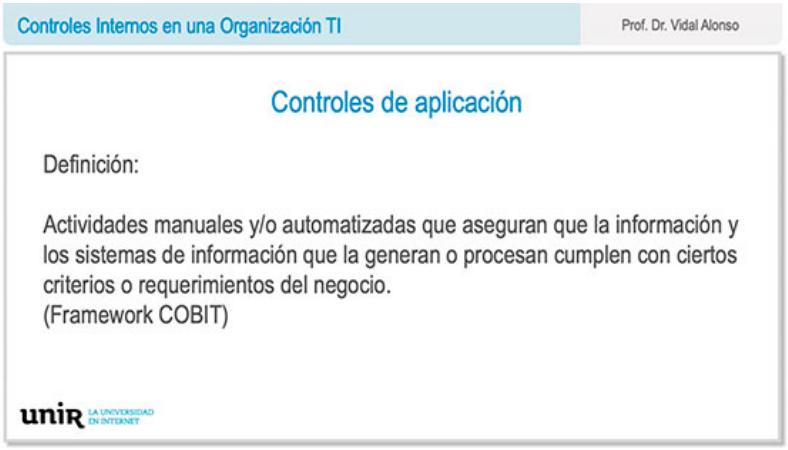
Adicionalmente a esta definición proporcionada por COBIT, también es posible definir un control de aplicación como aquellos controles que son aplicables para un determinado proceso de negocio o aplicación, como puedan ser la edición de registros, los logs de transacciones o los informes de errores de la aplicación.

Estos controles de aplicación se emplean para garantizar alguno de los siguientes objetivos:

- Que la inserción de datos a la aplicación sea exacta, completa, autorizada y correcta.
- Que el procesamiento de éstos datos se efectúe en el tiempo previsto.
- Que los datos se almacenen de forma completa y adecuada.
- Que las salidas del sistema sean salidas correctas y completas.
- Que exista un mantenimiento de registros que permita monitorizar las entradas y salidas del sistema.

Bajo estas consideraciones es posible establecer algunos ejemplos de controles de aplicación:

- **Controles de entrada de datos:** Se utilizan para garantizar la integridad de los datos que entran al sistema. Procedimientos de conversión, de validación o corrección de datos.
- **Controles de tratamiento de datos:** Sirven para garantizar un procesamiento de transacciones completo, adecuado y autorizado, evitando que procesos no autorizados actualicen datos.
- **Controles de salida de datos:** permiten conocer las operaciones realizadas con los datos para obtener las salidas. Además genera los informes de errores de la aplicación.
- **Logs:** Se utilizan a modo de pistas de auditoría (*Audit trails*), que permiten analizar hechos anormales en el funcionamiento de la aplicación.



Vídeo. Controles de aplicación.

Accede al vídeo a través del aula virtual

2.6. Implantación de controles internos en una organización TI

La implementación de controles internos en una organización TI toma como punto de referencia los cinco componentes integrados de control interno definidos por el framework 2013 del *Committee of Sponsoring Organizations of the Treadway Commission* (COSO). De esta forma, esta implantación va a constar de cinco pasos:

Paso 1: Establecer un ambiente de control

El ambiente de control es la cultura, los valores y las expectativas que las organizaciones inculquen en sus trabajadores. Algunas formas de establecer este ambiente de control son:

- Aplique y promocione las normas éticas y la integridad.
- Comunique la planificación estratégica para que la organización conozca qué es lo que va a hacer.

- Establezca una estructura organizativa y asigne responsabilidades.
- Contrate personal competente y fiable y proporciónele la formación necesaria.
- Destaque que el cumplimiento de leyes y reglamentos es un objetivo imprescindible de la organización.

Paso 2: Realizar evaluaciones de riesgo

En el pasado, la gestión de riesgos se centraba exclusivamente en los peligros financieros. Ahora hay que evaluar estos riesgos en la totalidad de la organización, con especial hincapié en los sistemas de información y todo lo que pudiera afectar a la misma. Algunas actividades para realizar esta evaluación de riesgos son:

- Cada función debe tener identificados los riesgos para las operaciones y el rendimiento.
- Reúnete con el personal para determinar posibles riesgos externos
- Prioriza y clasifica los riesgos, y discute con los responsables los controles necesarios para eliminar o reducir el riesgo.
- Obtenga información acerca de riesgos emergentes a través de encuestas de empleados o informes sectoriales.

Paso 3: Implementar actividades de control

Las actividades de control son políticas y procedimientos para ejecutar las operaciones, lograr los objetivos y evitar el fraude. Los métodos básicos de control interno son:

- Establecer responsabilidades:
  - Asignar cada tarea a una sola persona.
  - Establecer la estructura organizacional.
- Aplicar la segregación de funciones:
  - No hagas a un empleado responsable de todas las partes de un proceso.

- Restringir el acceso:
  - Deniegue el acceso a los sistemas, a la información o a los activos, salvo que sea necesario.
- Crear políticas y procedimientos:
  - Redacte instrucciones con las directivas a seguir.
  - Garantice que los controles cubren todas las áreas a auditar.

Paso 4: Implementar sistemas de información y comunicación

La comunicación es esencial para una organización. A través de ella es posible difundir de forma eficaz la calidad de las informaciones de una organización. Utilice alguna de las siguientes sugerencias para crear sus protocolos de comunicación e información:

- Establezca sistemas de información confiables para efectuar el seguimiento de las operaciones y el progreso y cumplimiento de los objetivos.
- Distribuya la información en su organización con la garantía de que la información crítica se entrega al personal adecuado en forma y tiempo correcto. Pregunte al personal qué información necesitan pero no están recibiendo.
- Cree líneas de comunicación independientes para la información confidencial, informando a los empleados los protocolos de estas líneas de comunicación.
- Establezca líneas de comunicación para informar a entidades externas.

Paso 5: Monitorizar los controles internos

El establecimiento de controles no es suficiente. Una vez que están implantados, es necesario comprobar su la eficacia por lo que precisan una monitorización. Algunas formas de monitorizarlos son:

- Establezca un sistema de control de calidad en todos los procesos.
- Realice revisiones independientes de una función para determinar si está funcionando como se pretendía, o los controles deben ser rediseñados.
- Organice auditorías externas y sea responsable con los resultados.

- Utilice la monitorización para buscar señales de la presencia de algún problema en los controles.

Para una mayor especificidad en la implantación de controles internos en sistemas de información debemos abordar la incorporación de los controles internos en un sistema de gestión de seguridad de la información (SGSI) que se verá más adelante.

Señalar que esta incorporación de controles internos en el SGSI sigue la norma ISO 27001 la cual se apoya en una Guía de controles, ISO27002, donde se especifican 115 posibles controles a implantar.

2.7. Referencias bibliográficas

COSO. (2013). *Internal control – integrated framework: Executive summary*. COSO. https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf

ISACA (2016). *Internal control using COBIT5*. ISACA. https://community.mis.temple.edu/mis5202online2016/files/2016/03/Internal-Control-Using-COBIT-5_whp_eng_0316.pdf

Piattini, M. y del Peso, E. (2008). *Auditoría de tecnología y sistemas de información*. Madrid: RA-MA.

Suffield, M. (2020). Auditors of the future-what are the skills needed in a digital age? *Journal Big Data and Digital Audit*, *1*, 23-26.

A fondo

COSO internal control-integrated framework: An implementation guide for the healthcare provider industry

Schandl, A., y Foster,P. (2019). *COSO internal control – integrated framework: an implementation guide for the healthcare provider industry*. Recuperado de: https://www.coso.org/Shared%20Documents/CROWE-COSO-Internal-Control-Integrated-Framework.pdf

The *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) ha publicado en el año 2019 esta guía para ayudar a implementar COSO en cualquier organización y establecer los necesarios controles internos. La guía focaliza su actuación, a modo de ejemplo, en organizaciones sanitarias.

Evaluating Internal Control Systems

Dittmeier, C. y Casati, P. (2014). *Evaluating Internal Control Systems. A comprehensive assessment model for enterprise risk management*. Recuperado de: https://www.interniaudit.cz/download/IIA/Evaluating-Internal-Control-Systems.pdf

Documento del *Institute of Internal Auditors Research Foundation (IIARF)* donde recomienda una serie de conceptos y actividades a modo de ayuda para profundizar en la evaluación de los sistemas de control interno de una organización empresarial.

General IT Controls. Risk and impact

Deloitte (2018). *General IT Controls (GITC). Risk and impact*. Recuperado de: https://pdf4pro.com/amp/view/general-it-controls-gitc-deloitte-us-audit-797f5b.html

Deloitte, una de las principales empresas consultoras, ante la importancia que los controles de las tecnologías de la información han adquirido para las empresas, facilita este documento para abordar la utilización de productos y servicios tecnológicos para controlar de forma general los sistemas de información.

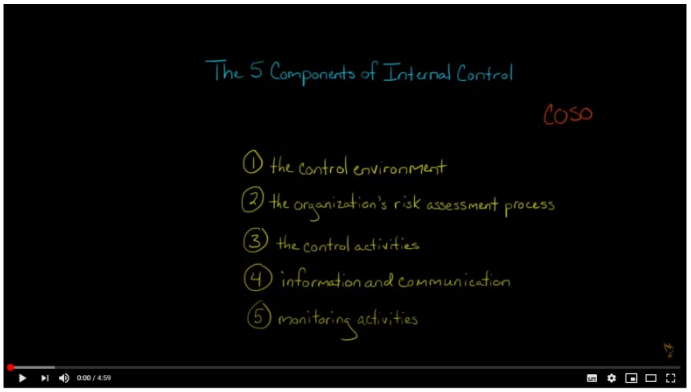
The KPMG Review. Internal Control: A practical guide

KPMG (1999). *The KPMG Review. Internal Control: a practical guide*. Recuperado de: https://ecgi.global/sites/default/files/codes/documents/kpmg_internal_control_practical_guide.pdf

La empresa consultora KPMG proporciona en este enlace una guía con los principales fundamentos de los controles internos y su importancia para lograr unos sistemas de información eficientes. Igualmente facilita unas bases para la auditoría interna.

The 5 Components of Internal Control

Edspira. (5 de marzo de 2019). *The 5 Components of Internal Control* [Vídeo]. Youtube. Recuperado de https://www.youtube.com/watch?v=l5_n4yi9dMU



Archivo de vídeo donde Edspira, the Free Business School, nos muestra de forma resumida cuales son los cinco componentes principales de un control interno en una organización tecnológica.

Test

1. Dentro de los controles de aplicación, los procedimientos de conversión de datos están considerados cómo:

   A. Controles de entrada de datos.

   B. Controles de tratamiento de datos.

   C. Controles de salida de datos.

   D. Controles tipo audit trails.

2. La segregación de funciones, ¿en qué paso se aplica de la implantación de controles internos en una organización TI?

   A. Establecer un ambiente de control.

   B. Realizar evaluaciones de riesgo.

   C. Implementar actividades de control.

   D. Monitorizar los controles internos.

3. ¿Cuál de los siguientes controles se puede considerar detectivo?

   A. Activación de una alarma.

   B. Impedir acceso no autorizados.

   C. Empleo de backups.

   D. Registro de accesos autorizados.

4. ¿Qué criterio de los que deben cumplir los controles de aplicación no afecta a la información?

   A. Efectividad.

   B. Confidencialidad.

   C. Integridad.

   D. Disponibilidad.

5. Indique la sentencia correcta:

A. El control interno informático es efectuado por personal interno o externo de la organización.

B. La auditoría informática reporta el informe final a la Dirección General de la Organización.

C. El control interno informático carece de limitaciones en la realización de sus funciones.

D. La auditoría informática efectúa el análisis de los controles de la organización diariamente.

6. ¿Cuál es el componente integrado de control interno que describe un conjunto de normas, procesos y estructuras que proporcionan la base para llevar a cabo el control interno en la organización?

A. Evaluación de riesgos.

B. Información y comunicación.

C. Ambiente de control.

D. Actividades de control.

7. En una clasificación general, ¿cómo se consideran los controles legislativos?

A. Voluntarios.

B. Obligatorios.

C. Opcionales.

D. Por área.

8. Indique la sentencia incorrecta:

A. El control interno informático efectúa un análisis diario de los controles de la organización.

B. La auditoría informática cubre cualquier componente de un sistema de información que esté presente en la organización.

C. El control interno informático reporta el informe diario a la Dirección del Departamento de Informática.

D. La auditoría informática se efectúa solo con personal externo a la organización.

9. ¿Qué control no se enmarca entre los controles de seguridad física y lógica?

A. Pruebas de identificación de usuarios.

B. Política de contraseñas.

C. Gestión de cambios.

D. Antivirus.

10. ¿Cuál de los siguientes controles generales se encarga de controlar el cumplimiento del presupuesto TI?

A. Control del desarrollo

B. Control de organización y operación.

C. Control de explotación de sistemas.

D. Controles de seguridad.