¿CÓMO SE DEBEN CONTROLAR LOS SISTEMAS DE INFORMACIÓN?

ALONSO TAMAYO ALZATE*, NÉSTOR DARÍO DUQUE MÉNDEZ*

Una de las razones fundamentales que justifican la aplicación del control en el área de informática se debe a la creciente dependencia de las industrias y empresas de producción, de servicios y de educación, en los equipos de computación, en el software, en el procesamiento de la información, en la vulnerabilidad creciente de los sistemas, en el costo de las actuales y futuras inversiones en recursos informáticos, en los dramáticos cambios organizacionales que puedan acarrear las nuevas tecnologías, todo ello debido a que el uso de las computadoras conlleva riesgos de errores, omisiones, fraudes y otros sucesos adversos, que ameritan su permanente control y supervisión en mayor grado a los procesos que se llevan manualmente, para garantizar la confiabilidad, confidencialidad y seguridad de los sistemas de información; es por ello, que para lograr el éxito y supervivencia de las organizaciones, es necesario contar con una efectiva administración de la tecnología informática, que pueda responder adecuadamente a los problemas anteriormente señalados.

¿Qué concepto tenemos de Control? Por control podemos entender el conjunto de normas, técnicas, acciones y procedimientos que interrelacionados e interactuando entre sí con los sistemas y subsistemas organizacionales y administrativos, permite evaluar, comparar y corregir aquellas actividades que se desarrollan en las organizaciones, garantizando la ejecución de los objetivos y el logro de las metas institucionales. El control actúa sobre las personas, cosas, situaciones específicas, fuentes de información y organizaciones, las cuales requieren con urgencia el diseño de estrategias que le permitan controlar y corregir los resultados de sus actividades.

Los Controles se pueden clasificar en Controles Internos y Controles Externos.

---

* Profesores Universidad Nacional de Colombia. Sede Manizales. Departamento de Administración y Sistemas

- **Control Interno.** Es aquel proceso que se ejerce internamente en las organizaciones y es impulsado por las directivas, administradores y demás personal que está vinculado a ella, el cual posee la suficiente ética y moral, así como formación académica, que le amerite credibilidad a sus hallazgos y conclusiones y tiene como propósito lograr el cumplimiento de los objetivos institucionales.

- **Control Externo.** Es aquel ejercido por personal ajeno a la organización y su propósito es establecer en que medida, los resultados alcanzados por las entidades o personas sujetas al control, satisfacen las metas y objetivos trazados en las políticas, planes, programas y propósitos fijados por la administración.

Resumiendo, se puede decir que el Sistema de Control Interno comprende un conjunto integrado por todos los planes, métodos, normas y procedimientos que adopta la administración para coadyuvar al logro de los objetivos institucionales, asegurar la conducción ordenada y eficiente de la entidad, prevenir fraudes y errores, salvaguardar los activos y bienes, garantizar la correcta aplicación de los registros financieros, administrativos y técnicos y preparar oportunamente los informes necesarios para asegurar la marcha normal de la organización.

El incremento masivo en el uso de las computadoras y el desarrollo de aplicaciones cada vez más sofisticadas han creado la necesidad de adaptar técnicas de auditoría a través de la aplicación de controles para poder hacer frente a esos cambios y priorizando un enfoque preventivo e intentando actuar antes o durante el hecho, asegurando que los activos de la compañía permanezcan protegidos y que se han establecido los controles internos adecuados para salvaguardar los recursos informáticos.

Qué papel juega el control en los Sistemas de Información.? El Control en los sistemas computarizados propende porque los datos sean un fiel reflejo de la realidad, que sean exactos, oportunos, suficientes; que durante su procesamiento no se vean afectados por pérdida, omisión o redundancia, que proporcione la información necesaria y que sea de utilidad para futuros procesos y consultas. Los Controles en los Sistemas de Información se pueden clasificar en Controles Generales, Controles Operativos y Controles Técnicos.

- **Controles Generales.** Son aquellos controles ejercidos sobre las actividades y recursos comprendidos en el desarrollo de los Sistemas de Información e implica procesos de planeación, definición clara y precisa de metas y objetivos institucionales, definición de valores de la organización, políticas, procedimientos, estándares, gerencia participativa, apertura a la comunicación, desarrollo de equipos de mejoramiento continuo, programas de capacitación y entrenamiento, etc.

A continuación se presentan algunos ejemplos de controles generales que deben ser considerados en los Sistemas de Información:

• Se debe supervisar el cumplimiento de políticas con respecto a la aplicación y dar aviso a las instancias pertinentes, tanto sobre su cumplimiento como sobre sus desviaciones, para que se tome el curso de acción a seguir. Debe existir una estrecha relación entre las políticas particulares de la aplicación en estudio con las políticas generales de la organización y su supervisión es indispensable.

• Las políticas de orden fiscal deben estar claramente consignadas por escrito y ampliamente difundidas entre el personal que tiene la aplicación a cargo. Toda aplicación está sujeta a ciertas normas o regulaciones, las cuales deben estar plenamente identificadas en forma escrita.

• Constatar que el manual de procedimientos se encuentre en forma escrita, que describa claramente todas aquellas actividades relacionadas con la aplicación y velar por su permanente actualización, así como por su amplia difusión; igualmente se debe revisar que exista el manual de funciones por escrito y propender por su constante actualización y difusión, puesto que se pueden presentar novedades como la incorporación de nuevas funciones, fusión de cargos, promociones, exigencias del entorno, etc., que obligan a su constante revisión.

• La administración de la aplicación en lo atinente a entrada y salida de datos, distribución de reportes, etc., debe corresponder a la unidad usuaria de la aplicación y lo relacionado con el análisis, programación, pruebas a programas, mantenimiento y documentación técnica, debe ser responsabilidad del centro de informática.

• Se debe establecer un procedimiento que señale los mecanismos necesarios a seguir para que garanticen la integridad de aquella información considerada confidencial y evitar su indebida utilización.

• Deben existir políticas plenamente establecidas sobre planeación del talento humano, que determine el número y tipo de personal requerido y deben estar enmarcadas dentro de la Planeación Estratégica de la empresa u organización, así mismo se debe ejercer la función de auditoría al talento humano, puesto que es la responsable de controlar y evaluar los procesos de selección, vinculación, promoción, entrenamiento, capacitación y desarrollo, evaluación del desempeño, ambiente laboral, etc.

• Se debe establecer como política de la empresa, la obligatoriedad de tomar las vacaciones en el período y tiempo correspondiente, esto permite que durante la ausencia del titular del cargo se detecten posibles fallas procedimentales.

• Toda empresa debe planear las actividades relacionadas con el entrenamiento y capacitación que permitan desarrollar en sus trabajadores habilidades, conocimientos y actitudes, proporcionando un desempeño más eficiente en el cargo; éstos programas deben ser evaluados para determinar si cumplió con los objetivos y metas fijadas, igual procedimiento se debe efectuar a los participantes a los cursos de entrenamiento y capacitación, con el propósito de determinar si como consecuencia de éstos, se redujo la rotación de personal, disminuyó el ausentismo, aumentó la eficiencia y habilidad de la persona para desempeñar el cargo, aumentó la calidad de los productos y servicios y se incrementó la productividad.

• Se deben atender los reclamos y quejas, limitando así los conflictos laborales que causan desmotivación y apatía; del oportuno y buen tratamiento que se le den a las quejas y reclamos efectuados por los trabajadores, manteniendo los conflictos dentro de un margen funcional aceptable, depende en gran parte el clima laboral de la empresa.

▪ **Controles Operativos.** Son controles diseñados, desarrollados e implementados para sistemas específicos, buscando garantizar con ellos que todas las operaciones sean autorizadas, registradas y procesadas de una manera completa, exacta y oportuna y tiene que ver con control y organización de proyectos, control de flujos de información, revisiones del diseño del sistema, administración de bases de datos, controles de cambios a programas, bitácoras de cambios, mantenimiento y documentación, control de programas, reportes varios, diseño y control de formatos, comunicaciones, etc.

Ejemplos de algunos controles operativos a ser tenidos en cuenta en los sistemas de Información son presentados a continuación:

• Deben existir procedimientos escritos relacionados con la entrada de datos, con el fin de proporcionar al usuario instrucciones comprensivas que le señalen los pasos a seguir de una manera directa y concisa.

• Se debe realizar un análisis general de los reportes generados, con el objeto de determinar si existen algunos de ellos que puedan ser eliminados, reemplazados, reagrupados o simplificados, o si hay que diseñar reportes adicionales debido a la

dinámica permanente de los sistemas de información; así mismo, se debe controlar la distribución de los reportes para que se envíen únicamente al personal indicado y se debe realizar mediante oficio remisorio.

• Se deben comparar los resultados esperados contra los resultados producidos por el sistema, para verificar que todo ha sido procesado correctamente o en su defecto para establecer oportunamente los correctivos que sean necesarios procurando la integridad de la información; aquellos reportes o transacciones que presenten discrepancias, se deben relacionar y dirigirlos al centro de informática señalando la ocurrencia del error. Los reportes y en general toda aquella información dispuesta en documentos, incluyendo el papel carbón, que ya cumplieron con su propósito, debe ser destruida bajo la supervisión de una persona responsable, previa elaboración del acta respectiva.

• Se debe controlar que las personas encargadas de efectuar el mantenimiento al software sean totalmente confiables; no obstante, se debe ejercer control sobre el acceso de ellos al sistema.

• Se debe registrar en una bitácora todas aquellas anomalías que presenta el sistema de información, señalando el día y hora de la ocurrencia y sus posibles causas.

• Como política general de la empresa, todo software adquirido debe tener contrato de mantenimiento que incluya actualización de versiones.

• Se debe llevar un registro formal relacionado con los cambios hechos a los programas que incluya información como: fecha de solicitud, persona solicitante, justificación, viabilidad técnica, tiempo estimado para la puesta en marcha, recursos demandados, costos, fecha de inicio, autorizaciones, persona responsable, etc. Se deben implementar controles especiales cada que se realice un ajuste o cambio al sistema, evitando caídas del mismo o posibles intentos de fraude o fuga de información.

▪ **Controles Técnicos.** Tiene que ver con la tecnología de la información como son los controles de operación del hardware, seguridad sobre los Sistemas de Información, integración de los Sistemas de Información, reporte de fallas, control de usuarios, restricción de accesos a datos, archivos y programas; utilización de hardware, controles lógicos del sistema, sistemas operativos, sistemas de seguridad, respaldo y confidencialidad, control de acceso al sistema, sistema de mantenimiento, planes de contingencia, etc.

Los siguientes son algunos ejemplos de controles técnicos que deben estar presentes durante el análisis, diseño, desarrollo y puesta en marcha de los Sistemas de Información:

• Los datos de entrada se deben validar, probar y verificar, para prevenir errores o fraudes, evitando inconsistencias en el flujo de información y buscando siempre mantener la integridad de los datos. Se deben producir mensajes de error y reportes de excepción que listen aquellos registros o transacciones que presentaron alguna inconsistencia durante el proceso de entrada o captura de datos.

• Durante la preparación de los datos se debe incluir la fecha de elaboración y firma de la persona responsable, así mismo, se debe llevar un registro de autorizaciones de acceso a los documentos fuente. En lo posible se debe procurar que la entrada al sistema se lleve a cabo a través de menús obligatorios y adicionalmente solicitar contraclaves en aquellos programas interactivos de grabación que sean críticos.

• Se debe exigir la identificación del usuario y clave de entrada para permitir el acceso personal al sistema, así como la debida autorización para utilizar recursos específicos tales como archivos, programas, librerías, lenguajes, etc.

• Los discos y cintas deben estar etiquetadas tanto interna como externamente para evitar confusiones y facilitar su localización.

• Se debe inhabilitar la clave de acceso de aquellos usuarios que entran a disfrutar de vacaciones o son retirados de la empresa.

• Se debe diseñar un procedimiento que consigne todo lo relativo a las copias de seguridad, como son los instructivos para llevarlas a cabo, periodicidad, persona responsable de su ejecución, número de copias a realizar, lugar de almacenamiento de las copias, etc.

• Se debe tener especial cuidado para que el software empleado en la empresa, posea las debidas autorizaciones o patentes, evitando así posibles demandas.

• Se deben establecer procedimientos que garanticen que los programas se encuentran funcionando correctamente, y cuando se le han hecho adecuaciones o ajustes, éstos deben corresponder a lo programado y autorizado; igualmente se deben diseñar las salvaguardas necesarias para que los programas no sean modificados, sustituidos o ejecutados por personas no autorizadas.

• Se debe establecer como política de la empresa, la aplicación de software genérico de auditoría a los sistemas que se encuentren en funcionamiento.

• Deben existir procedimientos debidamente establecidos en donde se señale la forma como se deben realizar las pruebas a los programas, las condiciones para llevarlas a cabo, el tiempo estimado para realizar las pruebas y registro de los resultados producidos, entre otros. Se debe solicitar al centro de informática la asignación de librerías especiales para realizar las pruebas a los programas, de tal manera que no se vayan a causar trastornos en el desenvolvimiento normal de los sistemas de información.

• Se debe establecer un procedimiento que indique que pasos se deben seguir para reportar aquellas inconsistencias o dificultades que se puedan presentar durante la corrida de un programa y proporcionar algunas alternativas de solución.

• Con el propósito de brindar mayor seguridad a la aplicación y cuando se presenten aquellas situaciones que así lo ameriten, previo estudio de las mismas, se debe limitar la ejecución de la aplicación a ciertas terminales o estaciones de trabajo durante determinados días y horas, evitando así las corridas no autorizadas de programas.

• Se deben definir controles suficientes, confiables, económicos y fáciles de implementar, que permitan prevenir y detectar aquellas inconsistencias presentadas durante el procesamiento de datos, haciéndoles un seguimiento hasta encontrar el origen de su causa y tomar los correctivos necesario, igualmente se deben diseñar mecanismos que permitan restaurar cualquier proceso a partir del punto donde se encuentre la falla, mediante la aplicación de los debidos controles, no permitiendo su vulnerabilidad.

• Se debe diseñar un plan de contingencias y ponerlo en marcha lo mas pronto posible, de tal manera que incluya convenios con otras entidades o instituciones que posean equipos con características similares, para que sirvan de respaldo en caso de presentarse una eventualidad.

BIBLIOGRAFÍA

Instituto Canadiense de Contadores Públicos. Procedimientos de auditoría en computación. Editado por el Instituto Mexicano de Contadores Públicos. 1982.

GAVIRIA CORREA, Gonzalo. El Control Interno. Biblioteca Jurídica Dike. Primera edición.

THOMAS A. J., I. J. Douglas. Auditoría Informática. Editorial Paraninfo. S.A. 1987.

ECHENIQUE, José Antonio. Auditoría en Informática. Editorial Mc. Graw Hill. 1990.

I Simposio Internacional y VI Colombiano de controles, seguridad y auditoría de sistemas. ACDAS. 1991.

PINILLA. F, José Dagoberto. Auditoría Informática. Un enfoque operacional. Editorial Ecoe. 1992.