Controles aplicables a la administración, a la organización y al procesamiento de los datos.

Por Omar Javier Solano Rodríguez – Profesor Univalle. Apartes del artículo: la auditoría como punto de apoyo al control Interno Informático.

a. **Derechos de Autor.**

El gobierno nacional ha desarrollando un conjunto de normas que regulan, protegen y penalizan a aquellas personas que violen los derechos de autor. La ley 603 del año 2000, obliga a las empresas a reportar en sus informes anuales de gestión, el cumplimiento de las normas de propiedad intelectual y derechos de autor, además faculta a la DIAN y a la Superintendencias para supervisar el cumplimiento de estas leyes. Por ejemplo, la ley 44 de 1993 establece, a quienes cometen delito de piratería de software penas entre dos y cinco años de cárcel, así como el pago de indemnizaciones por daños y perjuicios. Igualmente, la reforma al código de procedimiento penal, que entró en vigencia a partir del mes de julio de 2001, convierte en no excarcelables los delitos en contra de la propiedad intelectual y los derechos de autor. Lo que significa que quien sea encontrado usando, distribuyendo o copiando software sin licencia podría estar en la cárcel hasta por un período de 5 años. En este sentido la Business Software Alliance (BSA), advierte que la gerencia deba contemplar como mínimo los siguientes elementos de control:

a. Compilar e inspeccionar los registros de adquisición de Software.
b. Allegar e investigar los contratos de licencias de programas de software
c. Seleccionar la fecha en que se adelantará el reconocimiento interno y decidir si los empleados serán notificados con anterioridad; siendo así, la gerencia enviará un memorando explicativo, de lo contrario, cuando se realice la inspección, se debe respetar la propiedad de los empleados. Es posible que encuentre programas instalados que son propiedad del empleado que han sido instalados legalmente. Se recomienda no borrar ningún programa sin consultar con el usuario del PC[1].

[1] Sigla en inglés que traduce Computador Personal.

d. Determinar quién adelantará la inspección. Se sugiere que en la revisión se encuentre el jefe o gerente de sistemas, los jefes de cada Departamento, el asesor legal o el contralor de la empresa.

Cuadro No. 2 Evaluación de Controles Sobre Derechos de Autor

CONTROLES SOBRE DERECHOS DE AUTOR	SI	NO	N/A	OBSERVACIONES
1. ¿Los usuarios del sistema de información utiliza únicamente el hardware y el software que el departamento de Sistemas o quien haga sus veces le haya instalado y oficializado mediante el acta de entrega respectiva?				
2. ¿El departamento de Sistemas lleva el control del hardware y el software instalado, basándose en el número de serie y licencia que contiene cada uno?				
3. ¿El área contable posee copia de las licencias que conjuntamente con las facturas se encuentra debidamente en custodia?				
4. ¿El departamento de sistemas instala el software en cada computador y hace entrega al área usuaria los manuales pertinentes los cuales quedaron bajo la responsabilidad del Jefe del departamento respectivo?				
5. ¿Los trámites para la compra de los equipos fueron y son aprobados por el departamento de sistemas, así como la adecuación física de las instalaciones será realizada por la dependencia respectiva?				

Fuente: el autor

De acuerdo con la regulación Colombiana, el uso de programas aplicativos no autorizados o adquiridos ilegalmente, se considera como Software Pirata y es una clara violación a los derechos de autor y la gerencia debe regular el uso del hardware y del software licenciado.

La auditoría debe "validar" el informe de gestión, y es substancial realizar una inspección en forma periódica del software instalado en las empresas; éste procedimiento permitirá evitar problemas posteriores, como: fraudes, pérdida de información, multas, pago de perjuicios a los fabricantes, sentencias de prisión entre otros.

Es importante establecer una metodología de trabajo conjunta entre el auditor de informática y la gerencia, para que no se presenten inconvenientes al verificar el software instalado en los computadores.

b. Seguridad Física

Se considerarán las protecciones físicas de los datos, programas, instalaciones, equipos, redes, dispositivos de networking, etc. (Del Peso y Ramos Miguel: 2002. P.9). En general la seguridad física se refiere a la protección del hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales entre otros.

c. **Seguridad Lógica.**

Se refiere a los controles lógicos dentro del mismo software. Los controles lógicos para los usuarios son contraseñas y códigos de autorización de algún tipo. Kendall & Kendall (1997:p.845). Se considera también a la seguridad de uso de software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información. Es necesario establecer cómo se identifican y sobre todo autentican los usuarios y el modo de autorización en el sistema. Por otro lado, Jorcarno

(2006:pp. 16-18), recomienda para salvaguarda la información, en la empresa es conveniente tener un plan de seguridad que tenga en cuenta la disponibilidad, confidencialidad e integridad de la información. Para ello la seguridad lógica se debe aplicar con una perspectiva global y de gestión permanente, mediante certificaciones digitales y planes de contingencia. La gestión y monitoreo deben considerar dispositivos de seguridad, sistemas de Firewall (cortafuegos), dispositivos de detección de intrusiones (IDS, IPS), redes privadas virtuales (VPN), antivirus y logs de seguridad.

d. **Seguridad de los datos.**

Los datos y la información pueden constituir el activo más crítico de la empresa y en algunas organizaciones la función genérica de administración de seguridad la denominan "Data security". En la protección de los datos se puede considerar dos aspectos: la confidencialidad[2]y la integridad[3] (Del Peso y Ramos Miguel: 2002. P.15). La protección mediante cifrado se refiere a la integridad y sobre todo la confidencialidad.

e. **Segregación de Funciones entre el Servicio de Información y los Usuarios**.

La separación de entornos significa que los distintos usuarios pueden hacer solamente actividades en el sistema de acuerdo con el perfil. En este punto se ha de considerar perfiles definidos por la clasificación de la información, desarrolladores de software, gestión centralizada de la seguridad, integridad de los "log" e imposibilidad de ser desactivados por ningún perfil para poder ser revisados, las contraseñas y los archivos con perfiles y derechos impracticables a todos, incluso a los administradores de seguridad. (Piatinni y Del Peso, 1998:p.75-77)

---

[2] Uno de los pilares de la seguridad en sistemas de información, es la "confidencialidad", que indica que la información de un ambiente de base de datos o un sistema informático únicamente debe ser accedida por personas debidamente autorizadas para ello.

[3] Artículo 9° de la ley 527 de 1999, mediante el cual se establecen las disposiciones legales para el accesos y mensajes de datos a través del comercio electrónico en Colombia; se considera que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. Se puede considerar entonces, la exigencia de integridad de los datos debe garantizar la calidad de los datos de la base de datos.

f. **Controles sobre los equipos**.

Es necesario establecer características para detectar de manera automática errores. Los controles relacionados con los equipos hacen referencia a su utilización mediante el establecimiento de políticas para su uso, dentro de las cuales alberga el mantenimiento de los mismos y los planes de contingencia para circunstancias inevitables.

2.1.2 Controles aplicables al acceso a los sistemas de información y a la información.

a. **Controles de acceso al sistema**, sirven para detectar y/o prevenir errores accidentales o deliberados, causados por el uso o la manipulación inadecuada de los archivos de datos y por el uso incorrecto o no autorizado de los programas. Un método eficaz para proteger sistemas de computación es el software de control de acceso. Es decir los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden del usuario una contraseña antes de permitirle el acceso a información confidencial. Según Patón (2006:p. 70), los procedimientos de identificación se pueden diferenciar de: Verificación: confirma o rechaza que una persona es quien dice ser; Identificación: determina la identificación de una persona desconocida, es un proceso que requiere una base de datos centralizada de datos biométricos.[4]

[4] Los biométricos más utilizados para la identificación son las huellas dactilares y las facciones de la cara. En Emirato Árabes, por ejemplo los pasajeros deben fotografiar su iris para cruzar la frontera. El Enrollment o registro de datos biométricos: es importante el momento de asegurar la seguridad en la toma de datos y en el almacenamiento.