MARCO JURÍDICO DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

Rodolfo Herrera Bravo
Abogado
División Jurídica, Contraloría General de la República
Master en Derecho e Informática, Universidad Complutense de Madrid

PRESENTACIÓN

Agradezco la invitación que se me ha hecho para realizar esta breve charla sobre la auditoría jurídica de sistemas automatizados de información. Atendido que el público asistente está compuesto por una mayoría que no es jurista, trataré de utilizar un lenguaje simple de entender para profesionales de áreas distintas al Derecho. Además, como se trata de una materia que perfectamente daría pie a muchas horas de análisis, centraré esta exposición en algunos puntos, a mi juicio, básicos para comenzar a conocer el marco jurídico de la auditoría informática.

Cabe advertir que, como las áreas técnicas que se analizan en este tipo de auditorías son diversas, por ejemplo, la gestión y administración de los sistemas, el ciclo de desarrollo y mantenimiento de aplicaciones, las áreas de producción y explotación, las técnicas de sistemas, la seguridad lógica y física, las telecomunicaciones, los sistemas de gestión de bases de datos, las redes locales...; en cada punto habrá una normativa específica a la cual someterse, sea legal, reglamentaria, interna o contractual. Esto significa que en cada auditoría de sistemas el marco jurídico puede ser distinto, ya que es un análisis eminentemente casuístico.

Para una mejor comprensión de esta charla, la dividiré en los siguientes puntos:
1.- Una explicación de lo que se entiende por auditoría de sistemas de información y quiénes están llamados a realizarla;
2.- Algunas menciones al marco jurídico aplicable en dos aspectos: los recursos humanos y los contenidos almacenados en bases de datos; y
3.- Una breve mención de otros temas jurídicos que, sin embargo, no abordaré en esta charla.

¿QUÉ ES LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN?

En primer término, un sistema de información es un conjunto de procesos planificados para dar soporte y ejecutar una actividad, y pueden ser manuales, semi-mecanizados y mecanizados.
En el caso que nos ocupa importan dos grandes tipos de recursos dentro de un sistema de información: los humanos y los informáticos.

En segundo lugar, destaca la idea de auditoría, que en su acepción tradicional dirigida a los estados financieros tiene por objeto expresar una opinión sobre si los mismos representan adecuada y razonablemente la situación financiero patrimonial de dicha entidad, el resultado de sus operaciones y los cambios en su situación financiera, de conformidad con los principios y criterios generalmente aceptados y que asimismo no se hayan incumplido requerimientos legales.

Sin embargo, hoy el aumento de la tecnología, la importancia de los sistemas de información y el surgimiento de riesgos específicos a que están expuestos y, por lo tanto, la necesidad de especialización, justifica la existencia de la auditoría informática.

Además, en muchas organizaciones el auditor ha dejado de centrarse en la evaluación y comprobación de resultados de procesos, desplazando su atención a la evaluación de riesgos y la comprobación de controles.

Según don Miguel Ángel Ramos, la auditoría informática es la revisión y evaluación independiente y objetiva, por parte de personas independientes y técnicamente competentes del entorno informático de una entidad, abarcando todas o algunas de sus áreas como equipos, sistemas operativos, paquetes, aplicaciones y el proceso de desarrollo, organización y funciones, las comunicaciones, la propia gestión de todos los recursos informáticos, las políticas, estándares y procedimientos, los objetivos fijados, los contratos y normas legales aplicables, grado de satisfacción de usuarios y directivos, controles existentes, análisis de riesgos, y como consecuencia de la revisión y examen ha de emitirse un informe escrito que resuma la situación desde un punto de vista independiente y objetivo y, en su caso, dicho informe ha de incluir indicación de deficiencias y de aspectos mejorables.

Es decir, se trata de un proceso en el que se recogen, agrupan y evalúan evidencias para determinar si un sistema informático salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo los fines de la organización y utiliza eficientemente los recursos.

¿QUIÉN REALIZA LA AUDITORIA DE SISTEMAS?

Para llevar a cabo este tipo de auditorías no basta un auditor financiero, porque normalmente no contará con conocimientos técnicos y entrenamientos permanentes en tecnologías de información, ni es un experto en materias jurídicas, altamente complejas en estas materias. Tampoco resulta suficiente un profesional informático o un abogado especializado en tecnologías de información, porque suelen carecer de conocimientos sólidos en auditoría.

Por lo tanto, es necesario que cada uno realice coordinadamente su aporte y, en consecuencia, le corresponde llevarla a cabo a un equipo de auditoría multidisciplinario integrado por profesionales especializados en auditoría, en informática y en derecho.

¿QUÉ ABARCA EL MARCO JURÍDICO DE LA AUDITORÍA DE SISTEMAS?

El auditor informático que quiera realizar correctamente su labor está obligado a conocer el marco jurídico que regula el objeto de su trabajo. No puede desconocer las normas sobre la protección de datos personales, la protección de los derechos intelectuales sobre los programas computacionales u otras creaciones digitales, las obligaciones contractuales, los delitos que se cometen en relación con la tecnología, o las responsabilidades civiles, penales y administrativas en que se puede incurrir.

Por lo tanto, en la evaluación que realiza el auditor informático necesitará de un auditor jurídico dentro de su equipo que se ocupe de constatar la existencia de normas específicas (reitero que no sólo legales sino también reglamentarias, internas o contractuales) y su cumplimiento efectivo.

LA AUDITORÍA JURÍDICA DE SISTEMAS DE INFORMACIÓN DESDE EL PUNTO DE VISTA DE LOS RECURSOS HUMANOS

En relación con los recursos humanos directamente vinculados con los sistemas de información podemos advertir que la gestión y administración de los sistemas se expone a riesgos con importantes consecuencias jurídicas, de no contar con una adecuada definición de las responsabilidades y una segregación de funciones en el centro de procesamiento de datos.

La definición de responsabilidades es una medida organizativa básica, imprescindible para la correcta administración de los sistemas. En virtud de ella, se distinguen distintos niveles de responsabilidades, atendiendo a las personas que intervienen.

Por un lado, doña Marina Touriño distingue que la definición, utilización y propiedad de la información o de los datos de la organización es responsabilidad de los usuarios, personalizada en las respectivas jefaturas. Sin embargo, en ocasiones los recursos informáticos están directamente bajo el control del usuario, en cuanto a su gestión y administración, como en el caso de las cuentas personales de correo electrónico, por ejemplo. Así, el personal de informática simplemente es el "custodio" de esa información.

Si la utilización la realiza directamente el usuario desde su computador, sin intervención del personal técnico, será responsable por el contenido y exactitud de la información y el custodio de la misma.

Por otra parte, el administrador de sistemas de información es responsable de identificar riesgos debidos a vulneraciones técnicas que puedan afectar a los sistemas de información bajo su supervisión y responsabilidad, por ejemplo, en caso de accesos no autorizados a los recursos.

Sin embargo, la identificación de los riesgos y soluciones implica su comunicación al nivel directivo de la entidad, quien será responsable de decidir y ordenar la implantación de las soluciones.

Adoptadas dichas decisiones por la Dirección, vuelve la responsabilidad a los administradores de sistemas, encargados de realizar el diseño técnico de las soluciones, de implantarlas y de su mantenimiento, con la salvedad de que en ocasiones, el sistema de protección, de eficiencia, de seguridad y correcta gestión de los sistemas corresponde no sólo a los técnicos, sino a decisiones de las Jefaturas y en cierta medida a los usuarios.

Por lo tanto, existen tres tipos de responsabilidades en la gestión de los sistemas de información: la responsabilidad de la Dirección o Jefatura de la organización, la del administrador de sistemas de información y la de los usuarios.

- La Dirección adopta las decisiones generales y elige las medidas técnicas y, principalmente, organizativas a seguir;

- el administrador de sistemas es responsable de informar a las Jefaturas de los riesgos concretos que existan y de identificar las posibles soluciones para mitigarlos, de evaluar continuamente las medidas adoptadas en informática y supervisar su cumplimiento, y puede responder por los errores o daños que se puedan producir por el incumplimiento, por ejemplo, de los mecanismos de seguridad; y
- los usuarios, que tienen responsabilidad, por ejemplo, en el cumplimiento de las medidas de control y seguridad establecidas, y que deben asumir la propiedad de la información en cuanto a su definición y uso.

El caso de la segregación de funciones es similar, persigue evitar que una misma persona pueda tener bajo su control totalmente la información, sin sujeción a controles sobre la actividad llevada a cabo, para evitar así la comisión de fraudes o errores.

Los riesgos concretos a que se expone la organización en caso de ausencia de estos controles pueden ser la modificación de programas de forma no autorizada, en ocasiones con ánimo de fraude; desorden en el desarrollo de aplicaciones o en el mantenimiento de las existentes; es fácil que se modifiquen los datos sin autorización; que se pierdan los programas fuentes o se cuente con documentación inadecuada; se produzcan alteraciones intencionadas o no del software o parámetros; puede ocurrir un robo de información o activos; se utilizan las instalaciones para fines personales; puede haber pérdida de datos y discontinuidad de las actividades.

Es decir, en este punto las normas jurídicas aplicables son las generales por responsabilidad, tanto las civiles por daños, las administrativas que correspondan, o las penales por delitos cometidos por funcionarios públicos o algunos de los tipificados expresamente en la ley Nº 19.223, como puede ser el caso de la destrucción o inutilización maliciosa de sistemas; la alteración, daño o destrucción maliciosa de los datos contenidos en éstos; la interceptación, interferencia o acceso a un sistema para apoderarse, usar o conocer indebidamente la información contenida en el sistema; o la revelación o difusión maliciosa de los datos. No me extenderé en este punto por ser de conocimiento de los correspondientes asesores jurídicos.

LA AUDITORÍA JURÍDICA DE SISTEMAS DE INFORMACIÓN DESDE EL PUNTO DE VISTA DE LOS CONTENIDOS DE LAS BASES DE DATOS

En el tema que en me quiero detener, porque lo considero más desconocido por la generalidad, es el de la normativa que regula los datos contenidos en las bases de datos de los servicios, en especial, los datos de carácter personal de los ciudadanos y de los funcionarios.

La ley Nº 19.628, sobre Protección de la Vida Privada ha intentado regular esta problemática, y digo “intentado”, porque junto con los principios que declara en su articulado, incurre en contradicciones y carece de mecanismos de aplicación efectiva que la transforman en una norma que no ha resuelto, en absoluto, la materia.

Sin perjuicio, mencionaré algunas disposiciones que directamente atañen al sector público y que deben ser revisadas en una auditoría informática.

Para comenzar el Título IV de la ley se refiere al tratamiento de datos por los organismos públicos, señalando que sólo podrá efectuarse respecto de materias de su competencia y con sujeción a las reglas indicadas en los Títulos anteriores. Eso significa que un órgano público tendrá que respetar el ejercicio gratuito de los derechos que se conceden al titular de los datos, a saber:

- el derecho a exigir información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente.

- el derecho a que, si acredita que los datos personales son erróneos, inexactos, equívocos o incompletos, se modifiquen, o se eliminen cuando el almacenamiento carezca de fundamento legal o estuvieren caducos, salvo excepciones legales.

Además, si los datos personales cancelados o modificados hubieren sido comunicados previamente a otros, el responsable del banco de datos deberá avisarles a la brevedad posible la operación efectuada.

Sin perjuicio de lo anterior, los derechos del titular de los datos ceden en favor de intereses generales al no poder ejercerlos si ello impide o entorpece el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, o afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional.

Por otro lado, el tratamiento de datos personales por parte del sector público goza de una excepción a la regla general en materia de protección de datos: no necesita requerir el consentimiento del titular para utilizar los datos.

Pero no hay que confundir ese privilegio con una carta blanca para “hacer y deshacer”. Los principios que inspiran los sistemas de protección de datos contienen uno que no puede ser desconocido: el tratamiento debe ser legal y leal. En tal sentido, los datos que utilice el servicio se destinarán sólo a las finalidades para las cuales se recolectaron, no obstante haber prescindido del consentimiento del titular. Además, debe contar con información exacta, actualizada y responder con veracidad a la situación real del titular de los datos.

Otra disposición específica para los organismos públicos se refiere a los datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, los cuales no podrán ser comunicados una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena, salvo si esa información les sea solicitada por los tribunales de Justicia u otros organismos públicos dentro del ámbito de su competencia, quienes, a su vez, deberán guardar respecto de ella la debida reserva o secreto.

Esa obligación de guardar secreto sobre los datos no cesa por haber terminado las actividades de una persona en ese campo. Además, el responsable de los registros o bases -normalmente el Jefe del Servicio, ya que es éste quien decide sobre el tratamiento-, deberá cuidar de los datos con la debida diligencia, haciéndose responsable de los daños.

En tal sentido, y como regla general, el responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin

perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal.

Finalmente, la ley exige que el Servicio de Registro Civil e Identificación lleve un registro de los bancos de datos personales a cargo de organismos públicos, regulado reglamentariamente en el decreto 779/2000, del Ministerio de Justicia. Es decir, los organismos públicos tienen que requerir su inscripción en dicho registro dentro de 3 meses para los bancos preexistentes y dentro de 15 días para los nuevos, contados desde la entrada en vigencia del Reglamento, indicando, a lo menos, el nombre del banco de datos personales, el responsable y su RUT, la finalidad del banco, el tipo de datos almacenados, y una descripción del universo de personas que comprende.

ALGUNOS PUNTOS NO ABORDADOS EN ESTA EXPOSICIÓN

En relación con los recursos informáticos cabe señalar la situación relacionada con la adquisición de equipos y programas y su situación contractual y legal específica, que en el caso de la contratación pública impone la obligación adicional a cada servicio de estar consciente de sus facultades legales particulares para actuar dentro sus competencias. Los contratos sobre objeto informático, sean bienes o servicios informáticos, son altamente complejos, normalmente en un mismo contrato van múltiples prestaciones y tanto su redacción como su interpretación deben obedecer a técnicas que no es del caso explicar en esta oportunidad.

Los programas computacionales, por su parte, gozan de una regulación legal y contractual específica. En principio, la ley Nº 17.336 sobre propiedad intelectual dispone dentro de sus obras especialmente protegidas a los programas computacionales y señala algunos preceptos particulares.

Además, la adquisición de programas puede obedecer, por lo general a dos grandes modalidades: la contratación de un desarrollo a medida o la suscripción de licencias de uso; en fin, como se puede observar, existe todo un tema a analizar en materia de contratación y protección jurídica de obras digitales.

El otro tema que simplemente mencionaré y que, sin duda, debe ser objeto de estudio particular y más profundo es el de la transmisión electrónica de documentos digitales y el valor de la firma digital. El sector público ha sido pionero en esta materia a través del decreto Nº 81 de 1999, del Ministerio Secretaría General de la Presidencia, que regula el uso de la firma digital y los documentos electrónicos en la Administración del Estado, como un soporte alternativo a la instrumentalización en papel de las actuaciones de los órganos de la Administración, estableciendo las condiciones para que los datos contenidos en un soporte informático se consideren emanados de una persona determinada.

Hoy se busca ampliar esta regulación a los particulares a través de una ley, ya que el decreto no podía aplicarse a éstos por abordar aspectos cuya competencia es del Poder Legislativo y no del Ejecutivo. En particular, en el proyecto que se encuentra en trámite se regula la situación de las entidades certificadoras que son necesarias crear para imprimir confianza en el sistema.

CONCLUSIÓN

El marco jurídico de la auditoría de sistemas de información es un tema que difícilmente puede abordarse en tan breve tiempo. Hay muchas distinciones que hacer, muchas regulaciones particulares, tanto legales como reglamentarias e incluso, internas de cada servicio y derivadas de sus contratos. Reconozco que han quedado muchos aspectos sin siquiera mencionarse, pero quedaré satisfecho si tras todo este tiempo ustedes sacan en claro las siguientes ideas:

Primero, la auditoría de sistemas debe ser realizada por un equipo multidisciplinario que incluya un experto en técnicas de auditoría, otro en materias informáticas y un asesor jurídico especializado en tecnologías de información.

Segundo, el marco jurídico está determinado en gran medida por el caso concreto a auditar, es decir, por el ente auditado –si es público o privado, si es centralizado o no, si tiene normas especiales o se rige por las generales-, por el área específica de análisis y por múltiples disposiciones aplicables, no sólo legales sino también administrativas y contractuales.

Por ello, esto es sólo la punta del *iceberg*, dentro de un amplio conjunto normativo que conforma el marco jurídico de la auditoría de sistemas de información.

Santiago de Chile, octubre de 2001