IX Jornada Nacional de Derecho Contable. Consejo Profesional de Córdoba, Córdoba, 2016.

Hacia un protocolo de pericia e incautación en sistema de registro informático.

Silvia Iglesias y Diego Sebastian Escobar.

IX Jornada Nacional de Derecho Contable

11 y 12 de Agosto de 2016

Ciudad de Córdoba

Presentación de Ponencias

Tema de referencia:

IV Registros Pericias

Título:

Hacia un protocolo de pericia e incautación en sistema de registro informático.

Autores:

Silvia Iglesias
Contadora Pública
siglesias@itsb.com.ar

Diego Escobar
Contador Público, Maestrando en Seguridad Informática
escobards@gmail.com

Resumen de la ponencia:

“Hacia un protocolo de pericia e incautación en sistema de registro informático”

La tarea pericial contable habitual consta de dos partes en general: una relacionada con las formas y otra con el fondo de lo que se compulsara en un sistema registral. En este contexto, el perito se encuentra limitado a la exhibición del sistema que realizan las partes. Su tarea como se encuentran redactadas las normativas vigentes, no incluye verificar el nivel de seguridad de lo que se registra en forma informatizada. Por tal razón, el Contador siempre debe emitir su opinión en la pericia con esta limitación en el alcance.

Aunque existan entes de control como la Comisión Nacional de Valores y la Dirección Nacional de Protección de Datos Personales, ninguno de estos controla o exige la auditoría de cumplimiento de la seguridad, sino que se limitan a pedir que se documenten los procesos. Por lo tanto, en las organizaciones hay documentos y muy pocos o nulos controles de cumplimiento de los procedimientos de seguridad en los sistemas de registros contables.

Del mismo modo que en las organizaciones existen diferentes procesos, las pericias no son todas iguales. Existen fueros en donde no se discuten delitos y aquellos donde no se analiza un concurso o quiebra, existen funciones diferentes para los peritos, ya que en estos casos se pudiera sumar la necesidad de incautar el sistema de registro.

Por tal razón un protocolo de pericia de sistemas informatizados se daría en tres protocolos diferenciados:

1. El que pruebe además el nivel de seguridad del mismo y evite la limitación al alcance con el que emitimos opinión.

2. El que permita incautar en forma ordenada y pautada.

3. El que permite incautar en forma compulsiva.

El objetivo principal del presente trabajo, radica en analizar un protocolo para el punto N° 1, en el caso de necesitar probar el nivel de seguridad del mismo y evitar una limitación en el alcance con el que se emite una opinión en la pericia.

Hacia un protocolo de pericia e incautación en sistema de registro informático

1. Diferencia de tareas en un posible protocolo

La tarea pericial contable habitual consta de dos partes en general: una relacionada con las formas y otra con el fondo de lo que se compulsara en un sistema registral.
El perito se encuentra limitado a la exhibición del sistema (Art. N° 331 del CCyCN)[1] que realizan las partes. Su tarea como se encuentra redactado el CCyCN y las normativas asociadas, nunca incluyen verificar el nivel de seguridad de lo que se registra en forma informatizada, ya que si esta se copia a un soporte de papel encuadernado tiene sus condiciones formales y si es posterior de su encuadernación o su grabado en un soporte digital (CD, lo que hasta ahora se permite) solamente con las formas que el Registro Público exige. Por tal razón, el Perito Contador siempre debe emitir su opinión en la pericia con esta limitación al alcance.

De más está decir que si la verificación de la seguridad es algo que debe necesitarse probar, obliga al Perito a especializarse en una nueva disciplina a la hora de realizar esta tarea.
Aunque existan entes de control como la Comisión Nacional de Valores y la Dirección Nacional de Protección de Datos Personales, ninguno de estos controla o exige la auditoría de cumplimiento de la seguridad, sino que se limitan a pedir que se documenten los procesos. Por lo tanto, en las organizaciones hay documentos y muy pocos o nulos controles de cumplimiento de los procedimientos de seguridad.

Para que el Perito realice esta tarea, se precisarían asignar más horas y el costo de los mismos es alto. Si hoy una pericia simple no está en menos de $ 30.000 al valor de los honorarios mínimos sugeridos por el CPCECABA y las regulaciones muchas veces no son ni de un 10% de ese monto. Y si se debiera probar también el nivel de seguridad, el valor de esta nueva tarea no podría ser menor a $ 50.000.

Pero las pericias no son todas iguales, los fueros en donde no se discuten delitos y aquellos donde no se analiza la situación de un concurso o quiebra tienen funciones diferentes para los peritos, porque en estos casos se puede sumar la necesidad de incautar el sistema de registro.

---

[1] ARTÍCULO 331.- Investigaciones. Excepto los supuestos previstos en leyes especiales, ninguna autoridad, bajo pretexto alguno, puede hacer pesquisas de oficio para inquirir si las personas llevan o no registros arreglados a derecho.
La prueba sobre la contabilidad debe realizarse en el lugar previsto en el artículo 325, aun cuando esté fuera de la competencia territorial del juez que la ordena.
La exhibición general de registros o libros contables sólo puede decretarse a instancia de parte en los juicios de sucesión, todo tipo de comunión, contrato asociativo o sociedad, administración por cuenta ajena y en caso de liquidación, concurso o quiebra. Fuera de estos casos únicamente puede requerirse la exhibición de registros o libros en cuanto tenga relación con la cuestión controvertida de que se trata, así como para establecer si el sistema contable del obligado cumple con las formas y condiciones establecidas en los artículos 323, 324 y 325

Por tal razón un protocolo de pericia de sistemas informatizados se daría en tres protocolos diferenciados:

4. El que pruebe además el nivel de seguridad del mismo y evite la limitación al alcance con el que emitimos opinión.

5. El que permita incautar en forma ordenada y pautada.

6. El que permite incautar en forma compulsiva.

En el presente trabajo, vamos a tratar el punto N° 1, en el caso de necesitar probar el nivel de seguridad del mismo y evitar la limitación en el alcance con el que emitimos opinión en la pericia.

Para los casos N° 2 y 3, recomendamos la lectura de la Resolución N° 234/2016 "Protocolo General de la Actuación para las fuerzas policiales y de Seguridad de la Investigación y Procesos de recolección de pruebas en ciberdelitos" del Ministerio de Seguridad; y el trabajo titulado "Proceso de cadena de custodia en la intervención e incautación judicial de los sistemas de registros contables informatizados para preservación de la prueba" publicado por Silvia Gladys Iglesias y Jorge Luis López Aranguren.

2. Desarrollo del protocolo para nivel de seguridad del sistema de registro

Se deberá comprobar el cumplimiento legal del sistema registral tomando los puntos básicos de control especificados en algún marco de buenas prácticas de seguridad[2] y verificar si se cumplen los controles documentados o implantados sin documentar.

Los principales riesgos que puede contener un sistema registros se basa en la afectación de la Integridad, Disponibilidad y Confidencialidad de la información de los mismos.

Riesgos inherentes a la Integridad de la información:

Se pierde integridad si se realizan cambios no autorizados en los sistemas o se pierde parte de los datos almacenados sea por un evento accidental o intencional. Si uno de estos hechos ocurriera, deberían existir pistas de auditoría en donde se puedan identificar quienes y cómo se realizaron los cambios. También deben existir controles en donde se documenten todas las consultas y modificaciones que se realicen en el sistema de registros.

[2] *La incorporación de buenas prácticas internacionales en la normativa legal que regulan el sistema de registros contables* Libro de Ponencias VI Jornada de Derecho Contable Ed. Universidad Nacional de Santiago del Estero 2013 ISBN 978-987-1986-09-15, en Cdad. de Santiago del Estero Santiago del Estero, Argentina. Comisión I Aspectos generales, tributación y normas Pág. 7

Riesgos inherentes a la disponibilidad de la información:

El hecho de que la información o un sistema no esté disponible para los usuarios, ya sea por la pérdida de datos o la destrucción de elementos necesarios, puede afectar a la efectividad la labor de un perito. Las organizaciones deberían contar con planes de contingencia en caso de desastres y backups periódicos, para tener un resguardo de los datos contenidos en un sistema de registros para poder garantizar el acceso a ellos.

Riesgos inherentes a la Confidencialidad de la información:

La confidencialidad hace referencia a la protección de la información contra el acceso o a la divulgación no autorizada. El impacto producido por un evento de estas características, sea en forma no autorizada, intencional o inadvertida, puede variar entre la pérdida de confianza en la institución hasta la posibilidad de acciones legales contra la misma.
Las organizaciones deberían administrar todos los accesos de usuarios para disminuir los riesgos de los datos que se encuentran productivos en el sistema.

Probar el nivel de seguridad del sistema de registro y la documentación

Para el caso particular del presente trabajo y con el objetivo de orientar los pasos para verificar la seguridad de los registros contables, y basándonos en buenas prácticas de Seguridad de la Información disponibles gratuitamente y publicadas por organismos públicos nacionales, tomamos la Política de Seguridad de la Información Modelo emitida por la Oficina Nacional de Tecnologías de Información a través de la Disposición N° 03/2013 para la Administración Pública Nacional[3].

En el citado Marco se transcriben los principales controles que deberían tenerse en cuenta en una pericia para verificar cada uno de los siguientes puntos en forma muestral como en cualquier procedimiento de Auditoría.

Previa revisión de la evaluación y tratamiento de riesgos verificando que los mismos no vulneren en su aceptación o evaluación las normas vigentes para el Sistema de Registro, se debería realizar el control sobre los siguientes tópicos:

Cláusula: Política de Seguridad de la Información

1. Categoría: Política de Seguridad de la información
1.1. Control: Documento de la política de seguridad de la información
1.2. Control: Revisión de la política de seguridad de la información

[3] Verificado en Infoleg el 26 de julio de 2016 http://servicios.infoleg.gob.ar/infolegInternet/anexos/215000-219999/219163/norma.htm

Cláusula: Organización

1 Categoría: Organización interna
1.1 Control: Compromiso de la dirección con la seguridad de la información
1.2 Control: Coordinación de la seguridad de la información
1.3 Control: Asignación de responsabilidades de la seguridad de la información
1.4 Control: Autorización para Instalaciones de Procesamiento de Información
1.5 Control: Acuerdos de confidencialidad
1.6 Control: Contacto con otros organismos
1.7 Control: Contacto con grupos de interés especial
1.8 Control: Revisión independiente de la seguridad de la información
2 Categoría: Grupos o personas externas
2.1 Control: Identificación de los riesgos relacionados con grupos externos
2.2 Control: Puntos de seguridad de la información a considerar en Contratos o Acuerdos con terceros
2.3 Control: Puntos de Seguridad de la Información a ser considerados en acuerdos con terceros

Cláusula: Gestión de Activos

1 Categoría: Responsabilidad sobre los activos
1.1 Control: Inventario de activos
1.2 Control: Propiedad de los activos
1.3 Control: Uso aceptable de los activos
2 Categoría: Clasificación de la información
2.1 Control: Directrices de clasificación
2.2 Control: Etiquetado y manipulado de la información

Cláusula: Recursos Humanos

1 Categoría: Antes del empleo
1.1 Control: Funciones y responsabilidades
1.2 Control: Investigación de antecedentes
1.3 Control: Términos y condiciones de contratación
2 Categoría: Durante el empleo
2.1 Control: Responsabilidad de la dirección
2.2 Control: Concientización, formación y capacitación en seguridad de la información
2.3 Control: Proceso disciplinario
3 Categoría: Cese del empleo o cambio de puesto de trabajo
3.1 Control: Responsabilidad del cese o cambio
3.2 Control: Devolución de activos
3.3 Control: Retiro de los derechos de acceso

Cláusula: Física y Ambiental

1 Categoría: Áreas Seguras
1.1 Control: Perímetro de seguridad física

1.2 Control: Controles físicos de entrada
1.3 Control: Seguridad de oficinas, despachos, instalaciones
1.4 Control: Protección contra amenazas externas y de origen ambiental
1.5 Control: Trabajo en áreas seguras
1.6 Control: Áreas de acceso público, de carga y descarga
2 Categoría: Seguridad de los equipos
2.1 Control: emplazamiento y protección de equipos
2.2 Control: Instalaciones de suministro
2.3 Control: Seguridad del cableado
2.4 Control: Mantenimiento de los equipos
2.5 Control: Seguridad de los equipos fuera de las instalaciones
2.6 Control: Reutilización o retiro seguro de equipos
2.7 Control: Retirada de materiales propiedad de la empresa
2.8 Políticas de Escritorios y Pantallas Limpias

Cláusula: Gestión de Comunicaciones y Operaciones

1 Categoría: Procedimientos y Responsabilidades Operativas
1.1 Control: Documentación de los Procedimientos Operativos
1.2 Control: Cambios en las Operaciones
1.3 Control: Separación de Funciones
1.4 Control: Separación entre Instalaciones de Desarrollo e Instalaciones Operativas
2 Categoría: Gestión de Provisión de Servicios
2.1 Control: Provisión de servicio
2.2 Control: Seguimiento y revisión de los servicios de las terceras partes
2.3 Control: Gestión del cambio de los servicios de terceras partes
3 Categoría: Planificación y Aprobación de Sistemas
3.1 Control: Planificación de la Capacidad
3.2 Control: Aprobación del Sistema
4 Categoría: Protección Contra Código Malicioso
4.1 Control: Código Malicioso
4.2 Control: Código Móvil
5 Categoría: Respaldo o Back-up
5.1 Control: Resguardo de la Información
5.2 Control: Registro de Actividades del Personal Operativo
5.3 Control: Registro de Fallas
6 Categoría: Gestión de la Red
1 Control: Redes
7 Categoría: Administración y Seguridad de los medios de almacenamiento
7.1 Control: Administración de Medios Informáticos Removibles
7.2 Control: Eliminación de Medios de Información
7.3 Control: Procedimientos de Manejo de la Información
7.4 Control: Seguridad de la Documentación del Sistema
8 Categoría: Intercambios de Información y Software
8.1 Control: Procedimientos y controles de intercambio de la información
8.2 Control: Acuerdos de Intercambio de Información y Software
8.3 Control: Seguridad de los Medios en Tránsito

8.4 Control: Seguridad de los la Mensajería
8.5 Control: Seguridad del Gobierno Electrónico
9 Categoría: Seguridad del Correo Electrónico
9.1 Control: Riesgos de Seguridad
9.2 Control: Política de Correo Electrónico
9.3 Control: Seguridad de los Sistemas Electrónicos de Oficina
9.4 Control: Sistemas de Acceso Público
9.5 Control: Otras Formas de Intercambio de Información
10 Categoría: Seguimiento y control
10.1 Control: Registro de auditoría
10.2 Control: Protección de los registros
10.3 Control: Registro de actividad de administrador y operador
10.4 Control: Sincronización de Relojes

Cláusula: Gestión de Accesos

1 Categoría: Requerimientos para el Control de Acceso
1.1 Control: Política de Control de Accesos
1.2 Control: Reglas de Control de Acceso
2 Categoría: Administración de Accesos de Usuarios
2.1 Control: Registración de Usuarios
2.2 Control: Gestión de Privilegios
2.3 Control: Gestión de Contraseñas de Usuario
2.4 Control: Administración de Contraseñas Críticas
2.5 Revisión de Derechos de Acceso de Usuarios
3 Categoría: Responsabilidades del Usuario
3.1 Control: Uso de Contraseñas
3.2 Control: Equipos Desatendidos en Áreas de Usuarios
4 Categoría: Control de Acceso a la Red
4.1 Control: Política de Utilización de los Servicios de Red
4.2 Control: Camino Forzado
4.3 Control: Autenticación de Usuarios para Conexiones Externas
4.4 Control: Autenticación de Nodos
4.5 Control: Protección de los Puertos (Ports) de Diagnóstico Remoto
4.6 Control: Subdivisión de Redes
4.7 Control: Acceso a Internet
4.8 Control: Conexión a la Red
4.9 Control: Ruteo de Red
4.10 Control: Seguridad de los Servicios de Red
5 Categoría: Control de Acceso al Sistema Operativo
5.1 Control: Identificación Automática de Terminales
5.2 Control: Procedimientos de Conexión de Terminales
5.3 Control: Identificación y Autenticación de los Usuarios
5.4 Control: Sistema de Administración de Contraseñas
5.5 Control: Uso de Utilitarios de Sistema
5.6 Control: Alarmas Silenciosas para la Protección de los Usuarios
5.7 Control: Desconexión de Terminales por Tiempo Muerto

5.8 Control: Limitación del Horario de Conexión
6 Categoría: Control de Acceso a las Aplicaciones
1 Control: Restricción del Acceso a la Información
2 Control: Aislamiento de los Sistemas Sensibles
7 Categoría: Monitoreo del Acceso y Uso de los Sistemas
7.1 Control: Registro de Eventos
7.2 Control: Procedimientos y Áreas de Riesgo
8 Categoría: Dispositivos Móviles y Trabajo Remoto
8.1 Control: Computación Móvil
8.2 Control: Trabajo Remoto

Cláusula: Adquisición, desarrollo y mantenimiento de sistemas

1 Categoría: Requerimientos de Seguridad de los Sistemas
1.1 Control: Análisis y Especificaciones de los Requerimientos de seguridad
2 Categoría: Seguridad en los Sistemas de Aplicación
2.1 Validación de Datos de Entrada
2.2 Control: Controles de Procesamiento Interno
2.3 Control: Autenticación de Mensajes
2.4 Control: Validación de Datos de Salidas
3 Categoría: Controles Criptográficos
3.1 Control: Política de Utilización de Controles Criptográficos
3.2 Control: Cifrado
3.4 Control: Firma Digital
3.5 Control: Servicios de No Repudio
3.6 Control: Protección de claves criptográficas
3.7 Control: Protección de Claves criptográficas: Normas y procedimientos
4 Categoría: Seguridad de los Archivos del Sistema
4.1 Control: Software Operativo
4.2 Control: Protección de los Datos de Prueba del Sistema
4.3 Control: Cambios a Datos Operativos
4.4 Control: Acceso a las Bibliotecas de Programas fuentes
5 Categoría: Seguridad de los Procesos de Desarrollo y Soporte
5.1 Control Procedimiento de Control de Cambios
5.2 Control: Revisión Técnica de los Cambios en el sistema Operativo
5.3 control: Restricción del Cambio de Paquetes de Software
5.4 Control: Canales Ocultos y Código Malicioso
5.6 Control: Desarrollo Externo de Software
6 Categoría: Gestión de vulnerabilidades técnicas
1 Control: Vulnerabilidades técnicas

Cláusula: Gestión de Incidentes de Seguridad

1 Categoría: Informe de los eventos y debilidades de la seguridad
1.1 Reporte de los eventos de la seguridad de información
1.2 Reporte de las debilidades de la seguridad
1.3 Comunicación de Anomalías del Software

2 Categoría: Gestión de los Incidentes y mejoras de la seguridad
2.1 Control: Responsabilidades y procedimientos
2.2 Aprendiendo a partir de los incidentes de la seguridad de la información
2.3 Procesos Disciplinarios

Cláusula: Gestión de la Continuidad

1 Categoría: Gestión de continuidad del Organismo
1.1 Control: Proceso de Administración de la continuidad del Organismo
1.2 Control: Continuidad de las Actividades y Análisis de los impactos
1.3 Control: Elaboración e implementación de os planes de continuidad de las Actividades del Organismo
1.4 Control: Marco para la Planificación de la continuidad de las Actividades del Organismo
1.5 Control: Ensayo, Mantenimiento y Reevaluación de los Planes de continuidad del Organismo

Cláusula: Cumplimiento

1 Categoría: Cumplimiento de Requisitos Legales
1.1 Control: Identificación de la Legislación Aplicable
1.2 Control: Derechos de Propiedad Intelectual
1.3 Control: Protección de los Registros del Organismo
1.3 Control: Protección de Datos y Privacidad de la Información Personal
1.4 Control: Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información
1.6 Regulación de Controles para el Uso de Criptografía
1.7 Recolección de Evidencia
1.8 Delitos Informáticos
2 Categoría: Revisiones de la Política de Seguridad y la Compatibilidad
2.1 Control: Cumplimiento de la Política de Seguridad
2.2 Verificación de la Compatibilidad Técnica
3 Consideraciones de Auditorías de Sistemas
3.1 Controles de Auditoría de Sistemas
3.2 Protección de los Elementos Utilizados por la Auditoría de Sistemas
3.3 Sanciones Previstas por Incumplimiento

3. Reflexiones a modo de conclusión

En base a todo lo expuesto, en el caso de que se necesitara probar el nivel de seguridad de un sistema de registros y evitar una limitación en el alcance con el que se emite una opinión en la pericia, se debería comprobar el cumplimiento legal del mismo tomando los puntos básicos de control especificados en algún marco de buenas prácticas de seguridad y verificar si se cumplen los controles documentados o implantados sin documentar.

Con el objetivo de orientar los pasos para verificar la seguridad de los registros contables en base a los riesgos de la afectación de la Integridad, Disponibilidad y Confidencialidad de la información contenida en los mismos; se debería tomar la Política de Seguridad de la Información Modelo emitida por la Oficina Nacional de Tecnologías de Información a través de la Disposición N° 03/2013 para la Administración Pública Nacional.

Previa revisión de la evaluación y tratamiento de riesgos, y verificando que los mismos no vulneren en su aceptación o evaluación las normas vigentes para el Sistema de Registro, se realiza el control sobre los siguientes tópicos en forma muestral como en cualquier procedimiento de Auditoría:

- Política de Seguridad de la Información
- Organización
- Gestión de Activos
- Recursos Humanos
- Física y Ambiental
- Gestión de Comunicaciones y Operaciones
- Gestión de Accesos
- Adquisición, desarrollo y mantenimiento de sistemas
- Gestión de Incidentes de Seguridad
- Gestión de la Continuidad
- Cumplimiento

Los autores consideran que la implantación de protocolos para analizar el nivel de seguridad de un sistema de registros que evite una limitación al alcance en la opinión, o que permita incautar en forma ordenada y pautada, o en forma compulsiva, es una necesidad imperiosa para que se perfeccione el avance en las causas judiciales y se permita que se provea acorde al plexo normativo vigente.