III FORO DE PROFESIONALES DE LA CONTABILIDAD

JUNTA ÉCNICA DE CONTABILIDAD

MINISTERIO DE COMERCIO E INDUSTRIAS

TECNOLOGÍA: SISTEMAS DE SEGURIDAD EN LOS PROCESOS DE CONTABILIDAD

POR:

DR. CARLOS A. CHANGMARÍN R., PhD, CPA

Panamá, 19 de noviembre de 2015

CONTENIDO

1. INTRODUCCIÓN

La Junta Técnica de Contabilidad, del Ministerio de Comercio e Industrias, ha solicitado la preparación de un trabajo para ser expuesto en el III Foro de profesionales de la contabilidad, con el tema: Sistemas de seguridad de los sistemas contables.

Debido a los avances tecnológicos de nuestros días, se hace necesario que todos contemos con los conocimientos necesarios sobre lo que está ocurriendo, en relación con el robo, uso no autorizado y destrucción de los datos almacenados en las bases de datos de las instituciones y cómo podemos evitarlo.

1.1 Antecedentes

Sin ánimo de presentar toda la historia de los antecedentes de los computadores, se puede decir, que uno de los primeros dispositivos mecánicos para contar fue el ábaco, cuya historia se remonta a las antiguas civilizaciones griega y romana. Este dispositivo es muy sencillo, consta de cuentas ensartadas en varillas que a su vez están montadas en un marco rectangular. Al desplazar las cuentas sobre las varillas, sus posiciones representan valores almacenados, y es mediante dichas posiciones que éste representa y almacena datos. A este dispositivo no se le puede llamar computadora por carecer del elemento fundamental llamado programa.

Otro de los inventos mecánicos fue la Pascalina inventada por Blaise Pascal (1623-1662). Con esta máquina, los datos se representaban mediante las posiciones de los engranajes, y los datos se introducían manualmente estableciendo dichas posiciones finales de las ruedas, de manera similar a como se leen los números en el cuentakilómetros de un automóvil.

En las dos primeras generaciones, las unidades de entrada utilizaban tarjetas perforadas, retomadas por Herman Hollerith (1860 - 1929), quien además fundó una compañía que con el paso del tiempo se conocería como IBM (International Bussines Machines).

Mientras tanto Charles Jacquard (francés), fabricante de tejidos, había creado, en el año 1801, un telar que podía reproducir automáticamente patrones de tejidos leyendo la información codificada en patrones de agujeros perforados en tarjetas de papel rígido.

En la cuarta generación aparecen los *microprocesadores* que es un gran adelanto de la microelectrónica, son circuitos integrados de alta densidad y con una velocidad impresionante. Las microcomputadoras con base en estos circuitos son extremadamente pequeñas y baratas, por lo que su

uso se ha extendido al mercado industrial. Aquí nacen las computadoras personales que han adquirido proporciones enormes y que han influido en la sociedad en general sobre la llamada *"revolución informática"*.

Los sistemas manuales y los sistemas informáticos de registros de contabilidad producen información idéntica; éstos de forma más veloz. Se considera que los registros de contabilidad por medios informáticos son más vulnerables a alteraciones maliciosas.

El grado de exposición potencial al riesgo de accesos indebidos a los sistemas se incrementa junto con la mayor complejidad y autonomía de los componentes de los sistemas. Es necesario formular políticas que definan cómo y cuándo deben entrar y salir mensajes y datos a través de la red, lo que usualmente requerirá la utilización de software de seguridad (firewalls, routers). *El contador puede identificar la vulnerabilidad y a minimizar los accesos no autorizados a su sistema* (Von Bischhoffhausen 2005).

1.2 Medidas de seguridad

Es importante que en la empresa se realice un análisis de riesgos de la información procesada, a efectos de identificarlos y establecer su importancia.

A partir de este análisis se podrán desarrollar los mecanismos básicos de seguridad, que dependerán de la tecnología utilizada. Estos mecanismos deben formar parte de una Política de Seguridad, la cual debe estar formalmente documentada y adecuadamente divulgada entre los funcionarios para lograr la concientización, entendimiento y compromiso de todos los involucrados.

Según la IFAC (1998): "El concepto de seguridad aplica a todo tipo de información y hace referencia a la protección de valiosos activos y su resguardo contra pérdidas y daños".

Agregan Espiñeira, Sheldon & Asociados (2008), manifiestan: “La incertidumbre presenta riesgos y oportunidades y es un gran potencial para erosionar o aumentar valor para los grupos de interés”. (p.2)

Asimismo, deben llevarse a cabo tareas de mantenimiento de dichos sistemas, que podrán consistir en revisar y actualizar las bases de datos generales, de modo de lograr una mayor eficiencia o seguridad (Anónimo, 2004).

Según Castellanos (2013), existen factores que han permitido el incremento de delitos por computador:

- Aumento de personas estudiando computación

- Aumento en número de empleados con acceso a los equipos
- Facilidad en el uso de los equipos
- Incremento en la concentración del número de aplicaciones y de la información en las empresas y organizaciones

Agrega Ayala (2014), en su estudio sobre Seguridad de información y privacidad de datos, en Panamá, en sus preguntas: ¿Cómo el riesgo tecnológico relacionado a la operación de la organización, ha cambiado en los últimos 12 meses? El 61% de los encuestados contestó que ha aumentado debido al incremento de amanazas externas, el 36% que ha aumentado debido al increment de vulnerabilidades internas, mientras que el 27% que ha disminuido debido a la reducción de vulnerabilidades internas y el 15% que ha disminuido debido a la recución de amenazas externas.

En otra de sus preguntas ¿Considera que su organización puede ser susceptible al espionaje digital corporativo a fin de que personas no autorizadas roben secretos, planes o documentos confidenciales alojados en los computadores, servidores o medios digitales de su organización? El 85% contestó que Sí, el 8% que No, mientras que el 7% no estaban seguros.

En la siguiente pregunta En caso de llegar a ser una víctima de espionaje digital corporativo, ¿Considera que su organización tiene los controles necesarios (herramientas de software, políticas y procedimientos) para identificar quiénes fueron los perpetradores? El 24% contestó que Sí, el 46% contestó que No, mientras que el 30% No están seguros.

Su conclusión fue, que la privacidad y protección de datos no puede ser un proyecto para "después".

Según la Universidad de Pamplona (2008): "Hablamos de seguridad en términos de usuarios, de integridad de los datos y de acceso a la base de datos. Debe permitir definir claramente a qué módulos, a qué opciones del sistema y a realizar qué operaciones, tiene derecho cada usuario. Además debe contener internamente los controles necesarios sobre los datos y brindar las pistas de auditoría suficientes para monitorear el sistema. La base de datos deberá brindar herramientas de recuperación de los datos en casos de contingencia, además de la seguridad propia de la misma".(p.101)

Advierte el autor Delgado (2015): "Para que el FRAUDE se cometa deben conjugarse los 3 elementos siguientes: a) incentivo o presión del personal, b) oportunidades originadas por debilidades en el control interno y c) escasos o nulos valores morales del personal".(p.6)

Añaden los autores Montes & Porras (2015): "El sistema de administración de riesgos también puede definirse como un sistema de alertas tempranas, donde el Auditor Interno en el proceso de evaluación del sistema de control interno puede plantear la creación y aplicación de controles

preventivos que contribuyan al cumplimiento de los objetivos trazados por la organización en su plan estratégico" (p.31).

De acuerdo con los conceptos vertidos por los autores de párrafos anteriores, se hace necesaria la implantación de un sistema de seguridad eficiente para la protección de archivos de datos del sistema informático de contabilidad de la entidad, que va de acuerdo con una normativa establecida y que el contador juega un papel muy importante para lograrlo.

2. NORMAS Y PROCEDIMIENTOS DE SEGURIDAD

Para dar solución a la pregunta: *¿Contamos con algún sistema para lograr una seguridad eficiente en los registros de contabilidad por medios informáticos?,* tomaremos el modelo del sistema de Aytos.

Aytos es la compañía de referencia en el desarrollo e implantación de soluciones de gestión y administración electrónica para las entidades públicas.

Aytos es reconocido por su amplia gama de productos, los cuales gestionan en su totalidad todas las áreas internas de una entidad local, cubriendo ámbitos como el económico financiero (SicalWin), gestión de nóminas y recursos humanos, recaudación y gestión tributaria, padrón municipal de habitantes, gestión de procesos y expedientes electrónicos, portal del ciudadano, del proveedor y del empleado, gestión patrimonial, entre otros.

Además de estas soluciones, Aytos sigue mejorando para ofrecer lo mejor a sus clientes y sus nuevas necesidades, como puede ser la administración electrónica que se encuentra recogida en el conjunto de una Smart City. Veremos cuáles son sus normas y procedimientos de seguridad.

2.1 Centros de tratamiento y locales

Los locales donde se ubiquen los computadores que contienen el ARCHIVO, deben ser objeto de especial protección que garantice la disponibilidad y confidencialidad de los datos protegidos, especialmente en el caso de que el ARCHIVO esté ubicado en un servidor accedido a través de una red.

1. Los locales deben contar con los medios mínimos de seguridad que eviten los riesgos de indisponibilidad del ARCHIVO que pudieran producirse como consecuencia de incidencias fortuitas o intencionadas.
2. El acceso a los locales donde se encuentre el ARCHIVO deben estar

restringido exclusivamente a los administradores del sistema que deban realizar labores de mantenimiento para las que sean imprescindibles el acceso físico.

2.2 Puestos de trabajo

Son todos aquellos dispositivos desde los cuales se puede acceder a los datos del ARCHIVO, como, por ejemplo, terminales o computadores personales.

Se consideran también puestos de trabajo aquellas terminales de administración del sistema, como, por ejemplo, las consolas de operación, donde en algunos casos también pueden aparecer los datos protegidos del ARCHIVO.

2.2.1 Cada puesto de trabajo debe estar bajo la responsabilidad de una persona autorizada por la administración, que garantizará que la información que muestra no pueda ser vista por personas no autorizadas.

2.2.2 Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deben estar físicamente ubicadas en lugares que garanticen esa confidencialidad.

2.2.3 Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, debe dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.

2.2.4 En el caso de las impresoras, debe asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos del ARCHIVO, los responsables de cada puesto deben retirar los documentos conforme vayan siendo impresos.

2.2.5 Debe ser expresamente prohibida la conexión a redes o sistemas exteriores de los puestos de trabajo desde los que se realiza el acceso al ARCHIVO. La revocación de esta prohibición debe ser autorizada por el responsable del ARCHIVO, quedando constancia de esta modificación en el Libro de Incidencias.

2.2.6 Los puestos de trabajo desde los que se tiene acceso al ARCHIVO,

deben contar con una configuración fija en sus aplicaciones, sistemas operativos que sólo podrá ser cambiada bajo la autorización del responsable de seguridad o por administradores autorizados por la administración.

2.3 Entorno de Sistema Operativo y de Comunicaciones

Aunque el método establecido para acceder a los datos protegidos del ARCHIVO es el sistema informático autorizado, debe estar el ARCHIVO ubicado en un computador con un sistema operativo determinado y poder contar con unas conexiones que le comunican con otros computadores, es posible, para las personas que conozcan estos entornos, acceder a los datos protegidos sin pasar por los procedimientos de control de acceso con los que pueda contar la aplicación.

Esta normativa debe, por tanto, regular el uso y acceso de las partes del sistema operativo, herramientas o programas de utilidad, o del entorno de comunicaciones, de forma que se impida el acceso no autorizado a los datos de ARCHIVO.

2.3.1 El sistema operativo y de comunicaciones del ARCHIVO debe tener al menos un responsable, que, como administrador debe estar autorizado por la administración.

2.3.2 En el caso más simple, como es que el ARCHIVO se encuentre ubicado en un computador personal y accedido mediante una aplicación local monousuario, el administrador del sistema operativo debe ser el mismo usuario que accede usualmente al ARCHIVO.

2.3.3 Ninguna herramienta o programa de utilidad que permita el acceso al ARCHIVO debe ser accesible a ningún usuario o administrador no autorizado.

2.3.4 En la norma anterior se incluye cualquier medio de acceso en bruto, es decir no elaborado o editado, a los datos del ARCHIVO, como los llamados "queries", editores universales, analizadores de archivos, entre otros, que debe estar bajo el control de los administradores autorizados.

2.3.5 El administrador debe responsabilizarse de guardar en lugar protegido las copias de seguridad y respaldo del ARCHIVO, de forma que ninguna persona no autorizada tenga acceso a las mismas.

2.3.6 Si la aplicación o sistema de acceso al ARCHIVO utilizase usualmente archivos temporales, archivos de "logging", o cualquier otro medio en

el que pudiesen ser grabados copias de los datos protegidos, el administrador debe asegurarse de que esos datos no son accesibles posteriormente por personal no autorizado.

2.3.7 Si el ordenador en el que está ubicado el ARCHIVO está integrado en una red de comunicaciones de forma que desde otros computadores conectados a la misma sea posible el acceso al ARCHIVO, el administrador responsable del sistema debe asegurarse de que este acceso no se permita a personas no autorizadas.

2.4 Sistema Informático o aplicaciones de acceso al ARCHIVO

Son todos aquellos sistemas informáticos, programas o aplicaciones con los que se puede acceder a los datos del ARCHIVO y que son usualmente utilizados por los usuarios para acceder a ellos.

Estos sistemas pueden ser aplicaciones informáticas expresamente diseñadas para acceder al ARCHIVO o sistemas preprogramados de uso general como aplicaciones o paquetes disponibles en el mercado informático.

2.4.1 Los sistemas informáticos de acceso al ARCHIVO debe tener acceso restringido mediante un código de usuario y una contraseña.

2.4.2 Todos los usuarios autorizados para acceder al ARCHIVO, deben tener un código de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocido por el propio usuario.

2.4.3 Si la aplicación informática que permite el acceso al ARCHIVO no cuenta con un control de acceso, debe ser el sistema operativo, donde se ejecuta esa aplicación, el que impida el acceso no autorizado, mediante el control de los citados códigos de usuario y contraseñas.

2.4.4 En cualquier caso se deben controlar los intentos de acceso fraudulento al ARCHIVO, limitando el número máximo de intentos fallidos, y cuando sea técnicamente posible, guardando en un ARCHIVO auxiliar la fecha, hora, código y clave erróneas que se han introducido, así como otros datos relevantes que ayuden a descubrir la autoría de esos intentos de accesos fraudulentos.

2.4.5 Si durante las pruebas anteriores a la implantación o modificación de la aplicación de acceso al ARCHIVO se utilizasen datos reales, se debe aplicar a esos archivos de prueba el mismo tratamiento de seguridad que se aplica al mismo ARCHIVO.

2.5 Salvaguarda y protección de las contraseñas personales

Las contraseñas personales constituyen uno de los componentes básicos de la seguridad de los datos, y deben por tanto estar especialmente protegidas. Como llaves de acceso al sistema, las contraseñas debe ser estrictamente confidenciales y personales, y cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al administrador y subsanada en el menor plazo de tiempo posible.

2.5.1 Sólo las personas autorizadas por la administración deben tener acceso a los datos del ARCHIVO.

2.5.2 Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, debe registrarlo como incidencia y proceder inmediatamente a su cambio.

2.5.3 Las contraseñas se deben asignarn y se cambian mediante el mecanismo y periodicidad que sea determinada de acuerdo con procedimientos nomales de seguridad de datos.

2.5.4 El ARCHIVO donde se almacenen las contraseñas debe estar protegido y bajo la responsabilidad del administrador del sistema.

3. ¿CÓMO DISEÑAR UN PROGRAMA DE CONTROL DE AUDITORÍA?

Para preparar el programa de auditoria, es necesario tomar en cuenta el Método de los Debes; el auditor debe verificar las políticas de la empresa sobre el tema y donde aparecen lass palabras [debe] [deben] [deberá], para realizar la pregunta correspondiente.

Tomando en cuenta las políticas establecidas sobre el Centro de Tratamientos y Locales, queue indican:

1. Los locales [deben] contar con los medios mínimos de seguridad que eviten los

riesgos de indisponibilidad del ARCHIVO que pudieran producirse como consecuencia de incidencias fortuitas o intencionadas.

2. El acceso a los locales donde se encuentre el ARCHIVO [debe] estar restringido exclusivamente a los administradores del sistema que deban realizar labores de mantenimiento para las que sean imprescindibles el acceso físico. Véase cómo se convierte la política de la empresa en dos preguntas del cuentionario que sigue:

CUESTIONARIO DE CONTROL INTERNO
CENTRO DE TRATAMIENTOS Y LOCALES
PRUEBAS DE CUMPLIMIENTO

Empresa: …….. Entrevistado: …… Cargo: …… Sector: ……	Preparado por: …… Fecha: …… Revisado por: …… Fecha: ……			
PREGUNTAS	RESPUESTAS			
	SI	**NO**	**N/A**	**Observaciones**
1. ¿Los locales cuentan con los medios mínimos de seguridad que eviten los riesgos de indisponibilidad del ARCHIVO que pudieran producirse como consecuencia de incidencias fortuitas o intencionadas?				
2. ¿ El acceso a los locales donde se encuentre el ARCHIVO están restringido exclusivamente a los administradores del sistema que deban realizar labores de mantenimiento para las que sean imprescindibles el acceso físico.?				

Fuente: del autor

CONCLUSIONES

Luego de terminar este trabajo, se puede concluir en los siguinetes puntos:

1. El programa de control y la seguridad de los procesos de contabilidad es algo que no se puede dejar para mañana.
2. El personal responsable de los sistemas de contabilidad de la entidad, debe contar con una preparación tecnológica de primera.
3. Los contadores financieros son responsables de que los sistemas sean desarrollados de acuerdo con las normas de auditoría.

4. Las auditorías financieras deben ser muy exigentes al momento de auditar el software de contabilidad.
5. Los encargados de los sistemas de contabilidad y los contadores deben estar preparados, tecnológicamente, para elegir o verificar los diseños del sistema que va a utilizar la entidad.

BIBLIOGRAFÍA

Anónimo (2004) Seguridad de los sistemas contables informatizados en las PyMEs. Facultad de Ciencias Económicas y de Administración, de la República del Uruguay *www.ccee.edu.uy/ensenian/catcomp/material/Inform.../**Seguridad**.pdf*

Ayala I. Antonio (2014) Cómo el contador puede ser más eficiente utilizando tecnología. Conferencia dictada en el XII Seminario Regional de Contabilidad, Panamá, 22 de agosto de 2014.

Aytos (2006) Documento de seguridad. España: Barcelona Plaza de Europa 17-19, planta 4, 08907 L'Hospitalet de Llobregat (Barcelona), Teléfono: 937 379 947, desarrolladores del SilcaWin, ver. 1.

Castellanos Hurtado, Luis (2013) Proyecto de sistemas de información. Venezuela: 79 diapositivas http://desarrollodesistemas.wordpress.com

Delgado Loor, Fabián (2015) Programa antifraude: Guía para prevenir y detectar el fraude. Ecuador: *Revista de Auditores y Asesores Gerenciales Cía. Ltda*. 10 pp.

Espiñeira, Sheldon & Asociados (2008) Gestión integral de riesgos (GIR): Alternativas de organización. Venezuela: Boletín Asesoría Gerencial No. 5, 9 pp.

IFAC (1998) International Information Guidelines: Managing Security of Information. Ney York: Information Technology Committee.

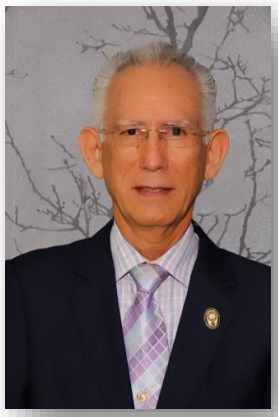
Montes S., Carlos A. & Porras C., Cornelio (2015) Los mapas de riesgos en la auditoria interna. Trabajo Interamericano presentado en la XXXI Conferencia Interamericana de Contabilidad, en el área de Auditoría, Punta Cana, Santo Domingo

Universidad de Pamplona (2008) Análisis y diseño de sistemas de información. Colombia: Facultad de studios a distancia, Programas de studio a distancia, 143 pp.

Von Bischhoffhausen, Werner (2005) La tecnología de la información en la formación del contador. Chile: *Revista Contabilidad y Sistemas*, Vol.1 / Nº 1 Departamento de Sistemas de Información y Auditoría Facultad de Ciencias Económicas y Administrativas Universidad de Chile.

HOJA DE VIDA RESUMIDA

Dr. CARLOS A. CHANGMARÍN R., PhD
6672-3816 capsa@cableonda.net



Por la Universidad de Panamá:

1. Doctor PhD en Ciencias Empresariales, con Especialización en Contabilidad.
2. Magíster en Admón. de Empresas, con Especialización en Mercadeo Internacional.
3. Especialista en Comercio Internacional.
4. Licenciado en Administración de Empresas.
5. Profesor de Segunda Enseñanza con Especialización en Contabilidad.
6. Licenciado en Contabilidad.
7. Diploma de Contador.

Por la Universidad Tecnológica de Panamá:

1. Técnico en Análisis y Programación de Sistemas.

Avance académico:

1. Profesor Titular de la Universidad de Panamá.
2. Ex Director de la Escuela de Contabilidad.
3. Ex Director del Departamento de Sistemas de la Computación.
4. Ex Director de los Laboratorios de Informática.
5. Evaluador de la Revista científica SOCIETAS de la Universidad de Panamá.
6. Evaluador de ejecutorias para Concursos de Cátedras y Banco de Datos, para profesores, de la Universidad de Panamá.
7. Evaluador de Trabajos Nacionales de la AIC.
8. Evaluador de la Asociación Latinoamericana de Facultades Empresas y Contabilidad (ALAFEC).

Avance profesional local e internacional:

1. Socio Director de la firma de contadores Changmarín & Asociados, firma miembro del Foro de Firmas Interamericanas de la AIC.
2. Contador Público Autorizado # 1429.
3. Analista por la Junta Técnica de Ingeniería y Arquitectura.
4. Auditor Interno Certificado de ISO 9000 por SGS.
5. Socio Vitalicio del Colegio de Contadores Públicos Autorizados de Panamá (CCPAP).
6. Socio Global de The Institute of Internal Auditors (IIA).
7. Socio Adherente Individual de la Asociación Interamericana de Contabilidad (AIC).
8. AIC: Diploma de honor al mérito profesional.
9. Ex Vicepresidente de la Comisión de Ética y Ejercicio Profesional de la AIC.
10. Ex Director Nacional, representando en Panamá a la AIC, para los años 2014 – 2015.
11. Autor del Trabajo Nacional: *El ejercicio profesional de lass firmas panameñas de contadores públicos pymes en un mundo lobalizado*, en la XXIX Conferencia Interamericana de Contabilidad, Puerto Rico.
12. Autor del Trabajo Interamericano: *La ética y el jercicio profesional en la docencia y los pensum de contaduría*, en la XXX Conferencia Interamericana de Contabilidad, Punta del Este, Uruguay.
13. Autor del Trabajo Interamericano: *La ética y el ejercicio profesional del contador*, en la XXXI Conferencia Interamericana de Contabilidad 2015, Punta Cana, Santo Domingo.
14. Autor de artículos en las Revistas: Contadores Públicos Autorizados de Panamá; III Conauditec, Panamá; Universidad de Panamá; Universidad de Puerto Rico.