PLAN DE SEGURIDAD PARA PROCESOS ADMINISTRATIVOS INFORMATIZADOS EN ESTUDIOS CONTABLES

Mario Litterio*
Eduardo Luis García**
Ariel Osvaldo Falzoni***
Juan Pablo Guagnini****
Sandra Beryl Otero°
Martín Alberto Domínguez°°
Ignacio Iezzi°°°
Lucas Ariel Ferreira+
Matias Aguiar+
María Reñones Arraras+

Resumen

El presente documento se encuentra realizado en el marco de un Proyecto de Grupo de Investigación que involucró a más de 300 alumnos de las materias "Análisis de Sistemas Administrativos", de la carrera de Contador Público, y "Estudios de Sistemas Administrativos", de la carrera de Licenciatura en Administración, durante los años 2018 y 2019. El mismo tuvo por objetivo contactar a diversos estudios contables y elaborar

* Magíster en Ciencias de la Administración. Docente, Departamento de Ciencias de la Administración. Universidad Nacional del Sur. Correo electrónico: literio@uns.edu.ar
** Contador Público. Docente, Departamento de Ciencias de la Administración. Universidad Nacional del Sur. Correo electrónico: eduardogarcia.uns@gmail.com
*** Contador Público. Docente, Departamento de Ciencias de la Administración. Universidad Nacional del Sur. Correo electrónico: afalzoni@criba.edu.ar
**** Contador Público. Docente, Departamento de Ciencias de la Administración. Universidad Nacional del Sur. Correo electrónico: jpguagnini@yahoo.com.ar
° Contador Público. Docente, Departamento de Ciencias de la Administración. Universidad Nacional del Sur. Correo electrónico: oterosandra_b@hotmail.com
°° Contador Público. Docente, Departamento de Ciencias de la Administración. Universidad Nacional del Sur. Correo electrónico: madomin@criba.edu.ar
°°° Contador Público. Docente, Departamento de Ciencias de la Administración. Universidad Nacional del Sur. Correo electrónico: ignacio.tpd2005@gmail.com
+ Alumnos, Departamento de Ciencias de la Administración. Universidad Nacional del Sur.

un plan de seguridad aplicado a los procesos administrativos-contables que se encontraban informatizados. En esta publicación se exponen los aspectos más relevantes de los planes de seguridad diseñados e implementados.

1. INTRODUCCIÓN - TRABAJO DE CAMPO

1.1. DESCRIPCIÓN DE LA FORMA EN QUE SE REALIZÓ EL TRABAJO DE CAMPO

Al comenzar el dictado de la materia en los años 2018 y 2019, se constituyeron grupos de 2 a 4 alumnos. Cada grupo contactó a un estudio contable y lo presentó al docente responsable de su tarea para su aceptación. El docente realizó una somera evaluación del estudio contable presentado y evaluó si se encontraba dentro de las pautas propuestas. El cronograma del trabajo de campo se encuadró dentro del cronograma general de la materia.

1.2. RESPUESTA A LOS CUESTIONARIOS Y ENTREVISTAS A LOS ESTUDIOS CONTABLES

Una vez aceptado el estudio contable, cada grupo de alumnos invitó al suyo a responder un formulario web. Una segunda instancia fue la realización de una entrevista en la que completaron algunos aspectos planteados en el cuestionario. Luego continuó el proceso programado para que cada grupo resumiera y presentara su caso. Por otro lado, los docentes tabularon y analizaron los resultados obtenidos. Sobre la base de la totalidad de este proceso, que duró aproximadamente dos años, y teniendo en cuenta los cambios vertiginosos propios de la tecnología actual, es que podemos ofrecer a los estudios contables de la ciudad y la zona estas recomendaciones relacionadas con los procesos administrativos informatizados para ellos y para las PyMEs que son sus clientes.

2. 2. RECOMENDACIONES

Cuanto más compleja es la infraestructura informática utilizada, aparecen más vulnerabilidades. A continuación, se enumeran los principales riesgos de seguridad y privacidad y se realizan algunas recomendaciones.

2.1. 1.1. POLÍTICA DE SEGURIDAD – SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

- Por un lado, una correcta política de seguridad limita la libertad de los usuarios para borrar elementos del sistema, protege los equipos ante el ataque de software malintencionado y, además, impide que personas ajenas a la organización accedan o corrompan los datos.
- Por otra parte, una correcta política de copias de seguridad permite recuperar los datos aun cuando todas las medidas de seguridad han fallado o cuando se produce una avería en un componente del hardware. La recuperación frente a un ataque puede ser tan sencilla como la restauración de una copia instantánea, anterior, de otro servidor o de la nube.

2.2. RELACIÓN CON EL PROVEEDOR

Muchos estudios contables han comenzado a realizar su trabajo en la nube, dada las diferentes ventajas de contratar a un tercero para el alojamiento y los procesos.

Como en todo acuerdo empresarial, la relación entre el proveedor de servicios en la nube y el estudio contable debe estar regulada por un contrato. Este contrato debe definir claramente la posición de cada una de las partes, así como sus responsabilidades y obligaciones.

Los términos de uso se encargan de definir las especificaciones técnicas más importantes relacionadas con la entrega y la calidad del servicio. Estas últimas establecen los niveles de rendimiento y disponibilidad garantizados por el proveedor.

2.3. SEGURIDAD POR PARTE DEL PROVEEDOR

Una parte importante de la seguridad del sistema recae sobre la empresa que provee los servicios en la nube

El proveedor de servicios en la nube se encarga de garantizar la seguridad física en sus centros de procesos de datos.

La deslocalización de los datos es una característica que también puede ser explotada como un mecanismo de seguridad en sí misma. La segmentación de datos permite que los datos de un cliente residan en diferentes servidores, incluso en diferentes centros de datos.

2.4. SEGURIDAD POR PARTE DEL ESTUDIO CONTABLE

Todos los sistemas administrativos requieren de medidas preventivas, detectivas y correctivas para proteger la integridad, confidencialidad y disponibilidad de sus recursos o activos informáticos, es decir el hardware, el software, las instalaciones, los datos y las personas.

Uno de los mayores riesgos a los que se enfrenta todo sistema informático es la pérdida de datos, ya sea porque un usuario ha borrado información accidentalmente, porque se produce una falla en algún dispositivo hardware o por culpa de un ataque informático. Perder los datos no solo significa tener que rehacer parte del trabajo realizado, sino que en muchos casos puede significar cuantiosas pérdidas económicas.

Se debe considerar que en los estudios contables encuestados sobre las medidas aplicadas a la seguridad hay una preponderancia (casi 100 %) de la restricciones de acceso a la información y procesos.

2.4.1. DEBE MANTENER POLÍTICAS DE SEGURIDAD TRADICIONALES

- Control de usuarios.
- Revisión y cambio periódico de contraseñas seguras.
- Borrado de cuentas de usuario que ya no se utilizan.
- Revisión del software para comprobar que no tiene vulnerabilidades.

2.4.2. ALGUNAS OTRAS POLÍTICAS DE SEGURIDAD ESPECÍFICAS

- Control Perimetral. Para llevarlo a cabo, es recomendable la instalación y
- configuración de un *firewall* o cortafuegos.
- Criptografía. En el uso de los servicios en la nube proporciona un nivel
- superior de seguridad.
- Control de accesos. Comprobar la actividad informática, detectar incidentes
- y formular un plan de acción.

2.4.3. COPIAS DE SEGURIDAD

- Una correcta política de copias de seguridad permite recuperar los datos aun cuando todas las medidas de seguridad han fallado o cuando se produce una avería en un componente hardware.
- Existen diversas modalidades y mecanismos para hacerlas:
  - Copias en dispositivos físicos o en la nube.
  - Realizadas en forma total, incremental o diferencial.
  - Tomando períodos regulares de tiempo o según las necesidades.
  - Programadas, automatizadas, manuales.
  - Respaldo de información de forma asincrónica o sincrónica.

No puede ignorarse que, cuando todo falle, la copia de seguridad realizada correctamente es la que nos permitirá recuperar la información perdida.

3. CONCLUSIONES

La utilización por parte de los estudios contables de la computación en la nube es una nueva forma de prestación de servicios globales que, apoyándose sobre una infraestructura tecnológica, les permite optimizar costos y recursos en función de sus necesidades de tratamiento de información.

Este paradigma, que se está generalizando rápidamente debido a sus ventajas, supone también un reto importante para la protección y privacidad de datos.

La revolución tecnológica que actualmente estamos viviendo bien podría ser la más profunda de nuestra historia. Los servicios convergen y pasan del mundo físico al mundo digital, siendo accesibles desde cualquier dispositivo. Un hecho relevante es que nuestros datos ya no residen en nuestros ordenadores sino en una Internet Global que adquiere entidad propia y se convierte en mucho más que una simple infraestructura de conexión: es la plataforma que ofrece servicio a millones de dispositivos inteligentes conectados a la red.

Esto permite que los consumidores, empresas o particulares, no se tengan que preocupar por cómo se provee el servicio que necesitan. Los estudios contables deben estar a la vanguardia de este cambio para que ni ellos ni sus clientes pierdan el tren del avance tecnológico.

Algunas decisiones deben tomarse obligatoriamente por el avance en este sentido de los organismos de control. Pasan a tener fundamental relevancia aspectos que hasta no hace mucho no se consideraban, tal es el caso del uso de claves de accesos propias y de los clientes del estudio.

Se comprueba en las encuestas procesadas que los estudios contables van tomando conciencia del valor de la información e intentan resguardarla de diversas formas, sin perder su disponibilidad.

Debemos mencionar que hay que continuar trabajando para crear conciencia respecto de la importancia de contar con un plan de seguridad, dentro de un Sistema de Gestión de la Seguridad de la Información que permita reducir el impacto de una amenaza que se concrete, permitiendo al estudio contable volver a estar en condiciones de continuar trabajando en el menor tiempo posible y con el menor costo para su propia estructura.