Tecnología Aplicada a la Información Contable, Buenos Aires, 2023.

EL CONTADOR Y EL PROCESO DE RESGUARDO DE INFORMACIÓN.

Bornacin, Florencia Victoria.

Cita:

Bornacin, Florencia Victoria (Julio, 2023). *EL CONTADOR Y EL PROCESO DE RESGUARDO DE INFORMACIÓN. Tecnología Aplicada a la Información Contable, Buenos Aires.*

Dirección estable:
https://www.aacademica.org/catedra.de.tecnologia.aplicada.a.la.informacion.contable/2

ARK: https://n2t.net/ark:/13683/p4ts/Noh

Esta obra está bajo una licencia de Creative Commons.
Para ver una copia de esta licencia, visite
https://creativecommons.org/licenses/by-nc-nd/4.0/deed.es.

Acta Académica es un proyecto académico sin fines de lucro enmarcado en la iniciativa de acceso abierto*. Acta Académica fue creado para facilitar a investigadores de todo el mundo el compartir su producción académica. Para crear un perfil gratuitamente o acceder a otros trabajos visite: https://www.aacademica.org*.

.UBAeconómicas | posgrado

ENAP Escuela de Negocios y Administración Pública

UNIVERSIDAD DE BUENOS AIRES

FACULTAD DE CIENCIAS ECONOMICAS

MAESTRIA EN CONTABILIDAD INTERNACIONAL

Materia: Tecnología Aplicada a la Información Contable

Julio de 2023

Título:

EL CONTADOR Y EL PROCESO DE RESGUARDO DE INFORMACIÓN

Bornacin, Florencia Victoria.

florbornacin@gmail.com

PALABRAS CLAVE

Backups – contabilidad – ciberseguridad – datos contables clave – gestión de ERP´s

EL CONTADOR Y EL PROCESO DE RESGUARDO DE INFORMACIÓN

INTRODUCCIÓN

Muchos de nosotros seguramente hemos vivido la pérdida de información debido a una falla del disco duro de nuestra máquina, del robo del equipo o la información en ella contenida, o por haber seleccionado y borrado por error un archivo/carpeta o base de datos. Cualquiera de estas situaciones conlleva pérdidas innecesarias de tiempo, reducen la eficiencia de las tareas y actividades e incluso pueden desencadenar fuertes crisis laborales cuando las fechas límite apremian, así como generar riesgos a la continuidad de las operaciones de la empresa.

Cuando sucede alguna de estas situaciones es cuando realmente lamentamos no contar con un sistema de backups confiable que salvaguarde la información.

Existe la creencia errónea entre contadores de que el realizar backups es una tarea más para los técnicos, para el departamento TI o para otras personas encargadas del mantenimiento de los equipos informáticos, en este artículo se presentan algunas de las razones que justifican el involucramiento de los profesionales en contabilidad en la tarea, así como su entendimiento.

Para acotar el análisis en referencia al tema planteado, en el presente trabajo nos centraremos en mencionar los riesgos referidos a la falta de backup de los sistemas de ERP[1], los cuales son clave en el desarrollo de los procesos organizacionales y considerando que, la información contenida en los mismos, es de gran relevancia en la tarea de los contadores independientemente del área en la que se desempeñen. Por esta razón, hablaremos de la importancia de la participación de dichos profesionales en la definición y planificación de las tareas de los mencionados backup.

[1] ERP son las siglas en inglés de "planificación de recursos empresariales", pero ¿qué significa ERP? La manera más simple de definir el ERP es pensar en todos los procesos de negocio centrales necesarios para operar una empresa: finanzas, RR. HH., fabricación, cadena de suministro, servicios, compras, y otros. En su nivel más básico, el ERP ayuda a gestionar de forma eficiente todos estos procesos en un sistema integrado. A menudo es el sistema de registro de la organización. Obtenido de: https://www.sap.com

DESARROLLO

¿Qué es un backup?

El proceso de backup es aquel en el que se crea una copia de los archivos importantes con el fin de poder recuperarlos en caso de una pérdida de la información. Dicho de otra manera, es el proceso de copiar los datos originales de una organización en una ubicación segura.

Hay que tener en cuenta que, los respaldos corren los mismos peligros que la información de origen. Por este motivo, no es recomendable que las unidades de respaldo no estén conectadas a la misma red de producción todo el tiempo ya que, de esta manera, en caso de una infección de dicha red podrían verse afectados. Por otro lado, es importante que los usuarios no tengan en su poder el disco duro donde guardan el backup de su información junto con el dispositivo respaldado, puesto que de sufrir robos o extravíos también perderían su respaldo.

¿Por qué hacer backups en contabilidad?

1. Riesgos asociados

A la hora de entender la importancia de la generación de backups del sistema administrativo-contable hay que resumir los riesgos asociados a la falta de los mismos, a saber:

1. **Impacto directo en los beneficios y en el futuro del negocio:** Una consecuencia grave es que, si perdemos los datos, vamos a dedicar tiempo y recursos en recuperarlos de una u otra manera, y esto afectará a nuestra producción, beneficios o incluso a la viabilidad futura de la empresa. En algunos casos, la pérdida de datos puede significar que perdamos, literalmente, a todos nuestros clientes. Si perdemos todos los datos personales, de contacto, de historial de compras o contrataciones de nuestros clientes, el caos y las pérdidas económicas serán inevitables. Esto significa que perderemos todo el valor que con tanto esfuerzo hemos ido acumulando y tendremos que empezar de cero. Y eso se traduce en unas pérdidas incalculables que pueden llevar a la organización a la ruina.
2. **Impacto en la reputación de la marca por falta de respaldo de datos:** Si no realizamos copias de seguridad y ocurre algo que implique la pérdida irreversible de los datos, estaremos perdiendo reputación. Es una consecuencia directa y muy fácil de entender, puesto que si solicitamos a un cliente un documento, un dato, un desarrollo —por ejemplo, un contrato, sus datos personales o de su empresa, o cualquier contenido que hayamos hecho—, nuestra credibilidad se verá afectada. Esos clientes que antes confiaban en nuestro buen hacer ahora tendrán sus reservas y empezarán a buscar proveedores alternativos, con mayores garantías de fiabilidad. Todo el trabajo realizado durante años se verá comprometido en poco tiempo.
3. **Costes directos elevados de una falta de respaldo:** En el caso que tengamos suerte y podamos recuperar los datos por completo, o parcialmente, el proceso para ello será costoso. Esto tendrá un impacto directo en el negocio que habrá que sumar a la pérdida de capacidad productiva y a las probables multas y sanciones. Por supuesto, nada nos garantiza que seamos

capaces de volver al punto anterior al desastre. Las consecuencias para el negocio son impredecibles, pero como mínimo habrá una época de transición en la que trabajar mucho para recuperar el control de la situación, y seguir avanzando.

4. **Falta de disponibilidad y accesibilidad a los datos:** Si no se realizan backups periódicos podemos enfrentarnos a situaciones de indisponibilidad o de falta de accesibilidad a nuestros propios datos. Disponer de respaldo en la Nube, por ejemplo, nos permite estar en cualquier lugar y acceder a los datos en cuestión de segundos, siempre que dispongamos de conexión a Internet. Lo contrario significa que estaremos a merced de la disponibilidad de otro colaborador que nos facilite los datos a través de un email, por ejemplo, con la consecuente ineficiencia y perjuicio para todos.

2. Requerimientos legales

Sumado a los riesgos de los que se habló en el apartado anterior, que justifican un adecuado proceso de backups, y sin ánimo de ser exhaustivos en este punto, también hay que tener en cuenta la necesidad de respaldo de información exigida por diferentes requerimientos legales y reglamentarios como ser la conservación de los respaldos de información de las declaraciones juradas impositivas (AFIP, API, AGIP, etc), los papeles de trabajo que respaldan nuestro ejercicio profesional o la auditoría de estados financieros (CCCRA, LSC, CPCE´s, etc), entre otros.

Características de un buen sistema de backups

Existen ciertos requisitos que un buen backup debe cumplir, los cuales aseguran la completa restauración de los sistema y archivos sin mayor problema después de un fallo y que los profesionales contables deberían conocer:

- Seguridad: debe ser seguro, debe estar en un lugar que no sea afectado ante cualquier desastre natural, por ejemplo. Una buena práctica es que el respaldo esté fuera de la oficina, ya que, ante cualquier siniestro, los sistemas de backups no podrían verse afectados junto con los equipos de trabajo.
- Disponibilidad: Esto quiere decir que los respaldos deben ser fácilmente restaurados ante cualquier eventualidad, la información debe estar totalmente funcional en cuestión de minutos o hasta horas después de un fallo grave.
- Periodicidad: Los sistemas de backups deben realizarse a períodos regulares y debe conservarse un historial que permita reconstruir la información a X fecha si así se requiere.

El área de ciberseguridad de la jefatura de gabinete de ministros de la república argentina amplía esta información mencionando:

1. Recomendaciones de carácter general: Se deben considerar como mínimo, la siguiente serie de pautas que orienten las políticas de respaldo y recuperación a desarrollar:
    - de qué debo realizar copias
    - el tipo de copia a realizar
    - el hardware, software y soporte de los mismos, a utilizar para realizar las copias

- la periodicidad y vigencia de las copias
- la ubicación física, y lógica del software asociado a la restauración de las copias
- la prueba de las copias realizadas
- la disponibilidad de los medios, si fuera necesario.

Para cumplir con dichas pautas es necesario realizar una serie de controles que ayuden a dimensionar las infraestructuras críticas de información (ICI) que se verán alcanzadas por las políticas mencionadas, la seguridad en lo relativo al proceso de copia y restauración, el desarrollo de las políticas de resguardo, sus pruebas y mantenimiento. Si bien dichos controles dependerán de cada una de las infraestructuras, mínimamente deben ser contemplados los siguientes aspectos:

a) Identificación de los controles: medible en el esfuerzo necesario, funcionabilidad, aplicación, recursos involucrados, etc.

b) Alcance de los controles: procesos de incidencia, aplicación de recursos técnicos especializados, requerimiento de software específico, ambientes de operación afectados, etc.

c) Revisión de los controles: periodicidad, calidad, actualización y documentación de los mismos.

2. Recomendaciones de carácter administrativo: Es necesario para la creación de una buena política de respaldo de información, tomar a consideración una serie de puntos clave que garanticen su correcta gestión, ayudando además a detectar los focos esenciales para los que, el plan de acción para realizar o restaurar las copias, deberá tener mayor control. Entre los recomendados se encuentran:
    - Inventario de activos de información: la dotación idónea a tal fin debe registrar e identificar toda la información abarcada por las ICI para garantizar las operaciones (incluyendo la detección de los responsables de la información contenida, la ubicación y su transporte), recuperar de forma total o parcial antes eventuales incidentes o pérdida de la misma, y permitir gestionar dichos activos.
    - Clasificación de los activos de información: se debe implementar un sistema de clasificación de los activos de información que permita identificar de forma rápida y sencilla cuestiones como el nivel de protección requerido, el tipo de activo y su criticidad.
    - Conocimiento y control de acceso: las copias de seguridad deben ser almacenadas y resguardadas en sitios correctamente identificados, sean estos lógicos o físicos, donde además se cuente con un control de acceso que lleve el registro de ingresos o egresos de los autorizados y/o de las copias, día y horario de dichos eventos, y cualquier otro dato que ayude a garantizar la seguridad de las mismas, incluyendo su trazabilidad.
    - Roles y procedimientos: es necesario contar con una clara definición de los roles que cumplirán cada uno de los involucrados dentro de los procesos de copia o restauración

de los respaldos de información. Del mismo modo, en los procesos documentados deben estar definidas las tareas y responsabilidades de cada uno, las acciones alternativas en caso de no poder cumplir alguna de ellas, así como registros e información útil para el complimiento del mismo. Los procedimientos deben ser revisados al menos una vez al año, cuando se detecte un cambio significativo de los activos de información, o se decida cambiar las tecnologías asociadas a las ICI afectadas.

- Periodicidad de las copias: se debe estipular y fijar la frecuencia con la cual se realizarán las copias de seguridad, teniendo en cuenta factores tales como:

    a. la cantidad y tiempo de variación estimada de los datos a guardar

    b. el costo del almacenamiento

    c. servicios e infraestructuras afectadas

    d. las obligaciones legales

- Tipo de copias apropiadas: se debe decidir el tipo de copia adecuada para cada una de las ICI afectadas en la política, estimando cuestiones como los recursos y tiempos necesarios para llevarlas a cabo.

  De forma genérica, existen 3 tipos de copias:

    a. Completa: se copian el total de los datos.

    b. Incremental: solo se guardan los datos modificados desde la última copia.

    c. Diferencial: se guardan todos los datos modificados desde la última copia completa.7. Caducidad de las copias: se debe decidir el tiempo adecuado para conservar las copias de seguridad en función a la vigencia de información resguardada, la vida útil del soporte utilizado, la necesidad de conservar copias históricas a la última completa realizada y resultado de pruebas.

- Comprobación de las copias de seguridad: es necesario fijar un período para realizar pruebas de restauración de las copias de seguridad, corroborar la buena salud de los distintos medios utilizados y la efectividad de los procesos destinados a tal fin.
- Destrucción de las copias de seguridad: debe contarse con procesos que garanticen la correcta eliminación de los datos ya sea para la reutilización del medio que los almacena, se haya comprobado la caducidad de los mismos, o incluso cuando su integridad se encuentre afectada. Para tales procesos deberán tomarse en cuenta técnicas como el formateo a bajo nivel, ciclos de sobre-escritura y técnicas de llenado de ceros.
- Control del soporte de copias: los mismos deben estar etiquetados, de forma física y/o lógica, a modo tal de poder ubicar en forma rápida y sencilla la información a guardar

o restaurar. Así mismo, debe llevarse un registro completo y detallado que brinde información útil para identificar los contenidos resguardados.

- Destrucción del soporte de copias: cuando sea necesario la destrucción del soporte que almacenó alguna de las copias de seguridad, esta debe realizarse de forma segura, con un procedimiento que garantice que la información que contuvo no pueda volver a ser accesible.

Importancia de la participación de los profesionales contables en el proceso

La gestión de riesgos es una tarea crucial dentro de la tarea de los profesionales en contabilidad y siendo que, la información en todas sus formas, se ha convertido en unos de los activos intangibles más importantes en las organizaciones impactando transversalmente en ellas, los profesionales en ciencias económicas no pueden permanecer ajenos a la gestión, control y análisis de los soportes y resguardo de la misma.

En este artículo, se buscó entonces comprender la importancia de la gestión de los respaldos de información clave del negocio, poniendo énfasis en el sistema de backup de los procedimientos administrativo-contables del ente, definiendo los elementos necesarios para la correcta planificación del proceso y los puntos que los profesionales contables debieran conocer.

Este sistema adquiere una importancia relevante y se diferencia de los demás al estar presente por obligaciones legales y reglamentarias en todo tipo de entes y, no es posible realizar un correcto análisis de la información a respaldar, si no existe claridad en el impacto que tendría la falta de la misma. Por lo expuesto, no hay nadie más apropiado que el contador para utilizar su amplio conocimiento en negocios y requerimientos legales para lograr un adecuado diseño de las políticas de backup en conjunto con el equipo de TI de la organización. Pudiendo, también, dar lugar al principio de costo-beneficio y logrando identificar los procesos y la información que requiera una mayor salvaguarda.

Dentro del procedimiento de evaluación de riesgos del ente el profesional contable deberá evaluar el sistema de respaldos de información clave con el que cuenta la compañía, definir los puntos prioritarios a atender, colaborar en el diseño del proceso y asesorar acerca de los beneficios y riesgos de no contar con un adecuado manejo de dicho riesgo.

Asimismo, el profesional contable cuenta con suficiente experiencia para colaborar en el diseño del proceso de backup general de la compañía ya que en su tarea identifica procedimientos, sus controles pertinentes, las responsabilidades de los mismos, realiza inventario de los activos clave, entre otras tareas relevantes para lograr un adecuado sistema de backups de acuerdo a lo mencionado en el apartado anterior.

CONCLUSIONES

La información es uno de los activos más importantes para las empresas y las personas, por lo tanto, realizar respaldos periódicos es una tarea que debe considerarse prioritaria y en ningún caso hay que subestimarla. Esto se debe, principalmente, a las múltiples causas por las que podría ocurrir una

situación de pérdida de información y las múltiples consecuencias que podría traer para el negocio. Para garantizar la seguridad de la información es vital realizar el procedimiento de la forma correcta, es decir, considerando la información a resguardar, los tipos de respaldos existentes, los medios de almacenamiento y la frecuencia de los procesos. Para que el procedimiento sea adecuado y lograr reducir el riesgo de negocio al mínimo es necesario que los profesionales contables se involucren en el diseño, planificación y selección de los mecanismos de backup, ya que, si quienes luego serán los mayores afectados por la pérdida de información, no participan en el proceso de su resguardo y no logran interiorizarse en el mismo entonces el proceso estará destinado al fracaso.

Contar con backups es, en resumen, una parte clave de los planes de seguridad de cualquier empresa. Gracias a contar con copias de seguridad se podrá confiar en que la empresa gozará de un plan de actuación ante la adversidad, mejorando su capacidad de respuesta y resguardando su continuidad.

BIBLIOGRAFÍA

Publicaciones:

- Escobar, D. S. (2010). Ley de Protección de Datos Personales. Revista Imagen Profesional, de La Federación Argentina de Consejos Profesionales en Ciencias Económicas.
- Escobar, D. S. (2013). Seguridad informática en los sistemas contables : Un análisis de los aspectos legales, normativos y tecnológicos de la seguridad de la información en el almacenamiento, procesamiento, control y resguardo de los registros contables. (Trabajo Final de Posgrado. Universidad de Buenos Aires.) Recuperado de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0817_EscobarDS.pdf
- Escobar, D. S. (2017). Concientización y capacitación del educando en la criticidad de la información contable en el ámbito de la práctica profesional. XXXIX SIMPOSIO DE PROFESORES DE PRÁCTICA PROFESIONAL. UNIVERSIDAD NACIONAL DE CATAMARCA, San Fernando del Valle de Catamarca.
- Escobar, D. S. (2011). INCLUSIÓN DE CONCEPTOS BÁSICOS DE SEGURIDAD DE LA INFORMACIÓN EN LA FORMACIÓN DEL CONTADOR PÚBLICO. XXXIII Simposio Nacional de Profesores de Práctica Profesional. Universidad de La Plata, La Plata.
- Escobar, D. S. (2023). Características a considerar en la elaboración de planes de concientización en Ciberseguridad para Contadores Públicos. Publicaciones de la Comisión de Estudios sobre Sistemas de Registro, (3-1), 1-7.
- Escobar, D. S. (2017). Formación del contador público en tecnología y seguridad de la información: Propuesta de reforma curricular. (Trabajo Final de Posgrado. Universidad de Buenos Aires.) Recuperado de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1116_EscobarDS.pdf
- Escobar, D. S. (2022). Propuesta de un modelo contable que refleje el carácter de activo que la información corporativa representa para una entidad bancaria. (Tesis de Doctorado. Universidad de Buenos Aires.) Recuperado de http://bibliotecadigital.econ.uba.ar/download/tesis/1501-1323_EscobarDS.pdf
- Escobar, D. S. (2022). El rol del Contador en la era digital. VI Jornadas de Orientación Vocacional. UBA, Buenos Aires.
- Escobar, D. S. (2022). Universo o dominio del discurso contable de los activos de información. ECON 2022. UBA, Buenos Aires.
- Escobar, D. S. (2022). Análisis de los modelos de gestión de Ciberseguridad en la elaboración de planes de concientización y capacitación para Contadores Públicos. Publicaciones de la Comisión de Estudios sobre Sistemas de Registro, (2-5), 1-7.

- Escobar, D. S. (2022). Identificación de los elementos para la descripción de un Modelo contable alternativo para el tratamiento de los activos de información. Sexta Jornada de Investigación Contable, Ética e Innovación: La Obra de Carlos Luis García Casella. Universidad de Buenos Aires - Facultad de Ciencias Económicas, Buenos Aires.
- Escobar, D. S. (2022). Identificación de los riesgos de los registros contables alojados en servicios de computación en la nube. XLIII Simposio Nacional de Profesores de Práctica Profesional. UNCUYO, Mendoza.
- Escobar, D. S. (2019). Repensando la seguridad de los registros contables. I jornada de Ciberseguridad del Consejo Profesional en Ciencias Económicas. Consejo Profesional en Ciencias Económicas, CABA.
- Escobar, D. S. (2017). Ciberseguridad documental de los sistemas contables legales. XI Congreso Internacional de Economía y Gestión. UBA, CABA.
- Escobar, D. S. (Agosto, 2011). La seguridad de la información y su contribución a la contabilidad. Mesa de Ciencias de la Secretaría de Investigación y Doctorado, Rumbo al Centenario 1913-2013. Secretaría de Investigación y Doctorado, FCE, UBA, Ciudad Autónoma de Buenos Aires.
- Escobar, D. S. (2022). Capacitación y concientización en seguridad de la información. Publicaciones de la Comisión de Estudios sobre Sistemas de Registro, (2-2), 1-6.
- Escobar, D. S. (2022). Identificación de los elementos para la descripción de un Modelo contable alternativo para el tratamiento de los activos de información. Sexta Jornada de Investigación Contable, Ética e Innovación: La Obra de Carlos Luis García Casella. Universidad de Buenos Aires - Facultad de Ciencias Económicas, Buenos Aires.
- Escobar, D. S. (2018). Replanteo en el análisis de las contingencias, oportunidades y amenazas de los desvíos en los Estados Financieros Prospectivos. Gestión Joven, (18), 11.
- Escobar, D. S. (2010). Ley de Protección de Datos Personales. Revista Imagen Profesional, de La Federación Argentina de Consejos Profesionales en Ciencias Económicas.
- Montaña Walteros, D.C., Pedraza Montoya, LM., Sandoval Piza, E.L ., Vargas González, S.M., (2016), Parametrización y Fortalecimiento de los Procesos Administrativos, recuperado de: https://repository.uniminuto.edu/handle/10656/4114

Páginas web:

- ARGENTINA.GOV., (21/05/2023), *Recomendaciones mínimas para política de respaldo de información*, recuperado de: https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/cert-ar/publicaciones/respaldo-informacion
- ARSYS (21/05/2023), *Respaldo de información: ¿Qué riesgos corre mi empresa si no tengo backup?,* recuperado de: https://www.arsys.es/blog/riesgos-no-hacer-backup
- CLAVEI (20/05/2023), *¿Qué son las copias de seguridad? Y, ¿qué beneficios tiene realizarlas?*, recuperado de: https://www.clavei.es/blog/backup-que-es/#:~:text=Gracias%20a%20las%20copias%20de,permiten%20operar%2C%20podremos%20recuperarnos%20r%C3%A1pidamente
- Contador22 (21/05/2023), *Porque hacer BackUp en la contabilidad,* recuperado de: https://contador22.com/backup-en-la-contabilidad-consideraciones-legales/
- Contarportable (19/05/2023), *Sistemas de backup en la contabilidad, evitar el desastre,* recuperado de: https://www.contaportable.com/sistemas-de-backup-en-la-contabilidad-evitar-el-desastre/
- DIRyGE (21/05/2023), *Cinco riesgos que pueden evitar las empresas si realizan copias de seguridad*, recuperado de: https://directivosygerentes.es/innovacion/cinco-riesgos-pueden-evitar-empresas-si-realizan-copias-seguridad

- ESET (21/05/2023), *GUÍA DE Backup*, recuperado de: https://www.eset-la.com/pdf/landing/2018/kit-antiransomware/guia-backup-recuperacion.pdf
- SAP (20/05/2023), *¿Qué es ERP?,* recuperado de:https://www.sap.com/latinamerica/products/erp/what-is-erp.html#:~:text=La%20planificaci%C3%B3n%20de%20recursos%20empresariales,%2C%20servicios%2C%20compras%20y%20m%C3%A1s.