economistas
Consejo General

ReDigital economía y transformación digital

REA auditores

FICHA 02 22

grupo de trabajo de auditoría

OCTUBRE 2022

Medidas para la salvaguarda, conservación y custodia de la información

La transformación digital llevada a cabo por las entidades auditadas exige una evolución en el mismo sentido de los auditores de cuentas con objeto de incrementar la calidad de los trabajos, evaluar mejor los riesgos cada vez más amplios de las entidades auditadas, mejorar la eficiencia del trabajo al reducir tareas de poco valor y desplegar acciones que permitan captar y retener el talento.

Respecto al cumplimiento normativo, se han introducido importantes requerimientos en el Reglamento de la Ley de Auditoría que afectan a la forma de trabajar de los auditores a partir del 1 de julio de 2022. Citamos algunos de ellos: la obligación de que todos los papeles de trabajo sean en formato electrónico, con las debidas medidas de seguridad que garanticen su autenticidad; la digitalización de toda la documentación existente en formato papel; procedimientos que aseguren la custodia, integridad y recuperación de la información; garantizar la accesibilidad y autorización restringida para su acceso; y realizar de forma rutinaria copias de seguridad en formato digital en diferentes momentos y, al menos, una vez al año. Todos ellos son retos a los que se enfrenta la actividad profesional.

Se observa, por lo tanto, una exigencia de modernización tecnológica de los despachos de auditoría que es prioritaria y estratégica, teniendo en cuenta la función de interés público de la actividad profesional de la auditoría de cuentas.

Desde el grupo de trabajo de auditoría de ReDigital publicaremos periódicamente estas fichas para ayudar a los auditores de cuentas a cumplir con la normativa y, a su vez, mejorar la eficiencia y eficacia en su trabajo diario.

Continuando con las medidas de protección de los sistemas informáticos de la ficha número 1, las medidas para la salvaguarda, conservación y custodia de la información adquieren la característica de "último bastión" para la continuidad de la organización en caso de producirse un desastre.

El artículo 72.2 del RLAC desarrolla el "Deber de conservación y custodia" para el archivo compilado. No obstante, en esta ficha número 2 hemos querido tratar de forma general dicho deber y hacerlo extensivo a todos los archivos significativos de la firma de auditoría, deban o no compilarse.

Sobre las propias características de la compilación, el Comité de Normas y Procedimientos (CNyP) del REA Auditores- CGE está elaborando un documento sobre *Compilación del Archivo de Auditoría*.

De acuerdo con el artículo 72.2 RLAC sobre el "Deber de conservación y custodia":

> *Durante los plazos de conservación y custodia* ***los auditores de cuentas serán responsables*** *de adoptar las medidas necesarias para la salvaguarda y conservación de la documentación, información, archivos y registros. Para ello, los auditores de cuentas deberán disponer de sistemas informáticos que cuenten con controles, que aseguren la custodia, integridad y recuperación de la información, que permitan emplear la diligencia debida que sea necesaria para reducir el riesgo de deterioro o pérdida, garantizar la accesibilidad y autorización restringida para su acceso, debiendo permitir una identificación única del archivo generado compilado y de la fecha de la compilación. Estos controles serán implementados eficazmente para que no sea posible la modificación de los archivos de cada trabajo de auditoría una vez transcurrido el plazo máximo de compilación, para que quede constancia de las acciones realizadas sobre dichos archivos y se reduzca el riesgo de deterioro o pérdida.*
>
> *A estos efectos, deberán realizarse de forma rutinaria copias de seguridad en formato informático en el momento de su creación, cuando se produzcan modificaciones y, en caso de no haberlas, al menos, una vez al año.*

En este sentido, hay que indicar dos cuestiones clave que debe conocer la firma de auditoría para salvaguardar, conservar y custodiar la información:

1. REALIZACIÓN DE COPIAS DE SEGURIDAD RUTINARIAS, CUANDO SE PRODUZCAN MODIFICACIONES Y, EN CASO DE NO HABERLAS, AL MENOS, UNA VEZ AL AÑO

A. RECOMENDACIÓN

Emplear procesos y herramientas para realizar copias de seguridad de la información con una metodología probada que permita la recuperación de la información en un tiempo oportuno.

Las copias de seguridad deben custodiarse y conservarse en un lugar distinto (servidor *cloud* u otra localización física) a la máquina que contiene la información respaldada.

B. OBJETIVO DEL CONTROL

La firma de auditoría debe implementar controles para garantizar la existencia y validez de las copias de seguridad de los datos, configuraciones de bases de datos, configuraciones de sistemas operativos y aplicaciones.

C. RIESGO ASOCIADO

No disponer de adecuadas copias de seguridad de la información que da soporte a la organización puede conllevar que, en caso de pérdida o deterioro de información, dicha pérdida sea definitiva y la información no pueda ser recuperada.

El impacto de este riesgo puede ser leve (perder información de un fichero concreto que se puede volver a generar) o en su extremo poner en riesgo la continuidad de la organización.

Por lo general un atacante compromete un sistema de información realizando cambios significativos en las configuraciones y los programas. En ocasiones, el atacante también realiza alteraciones sutiles de los datos almacenados en los sistemas de información (en adelante, SI) comprometidos, lo que puede poner en peligro la integridad y confidencialidad de la información de la organización con información contaminada o sustraída. Otras veces simplemente destruye o invalida todo o parte de los datos y programas de la entidad *(ransomware).*

Cuando se descubre el ataque es sumamente difícil para la organización eliminar todos los cambios que ha efectuado el atacante en los SI, no pudiendo garantizarse el restablecimiento a la situación inicial, albergando la sospecha de que el incidente vuelva a reproducirse.

La forma de minimizar los daños que puede causar un ciberataque de *ransomware*[1] es disponer de una copia de seguridad de los datos secuestrados.

Las técnicas de intrusión y acceso a los recursos del sistema empleadas por los ciberdelincuentes han evolucionado con el paso del tiempo sofisticando los métodos empleados de cifrado e intrusión. Todos los indicadores proporcionados por las agencias de ciberseguridad gubernamentales indican que los ciberdelincuentes emplearán cada vez técnicas más sofisticadas y el número de ataques crecerá de forma exponencial, por ello, contar con una copia de seguridad no accesible a nivel de red, es decir, que se encuentre aislada o desconectada, es una buena medida de protección adicional a las de cifrado y seguridad física.

D. DISEÑO DE LA POLÍTICA

La política o procedimientos de respaldo describen los procesos asociados a las copias de seguridad de la organización, considerando:

Las copias poseerán el mismo nivel de seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. Se puede considerar la conveniencia o necesidad, según proceda, de que las copias de seguridad estén cifradas para garantizar la confidencialidad.

Las copias de seguridad deben abarcar:

- Información de la organización a respaldar.
- Aplicaciones en explotación, incluyendo sistemas operativos.
- Datos de la configuración, servicios, aplicaciones, equipos u otros de naturaleza análoga.
- Claves utilizadas para preservar la confidencialidad de la información.

Los procedimientos de copia de seguridad deben establecer:

- Periodicidad de las copias (cada cuántos días, semanas, meses o años).
- Tipo de copias (puede haber copias completas o incrementales. Por ejemplo, cada domingo puede hacerse una copia

1. Ransomware o secuestro de datos. El ransomware es un software malicioso que al penetrar en nuestro equipo le otorga al hacker la capacidad de bloquear un dispositivo desde una ubicación remota. También a encriptar los archivos quitándole al usuario el control de toda la información y datos almacenados.

completa y el resto de los días una copia sólo de lo que ha sido modificado desde el día anterior, es decir, el lunes sólo se copiará lo que se ha modificado el lunes, etc.).

- Almacenamiento de las copias (por ejemplo, en cintas, en discos, unidades de red, nube).
- Retención de las copias (cuánto tiempo se mantienen las copias diarias, semanales, mensuales o anuales).
- Procedimiento de generación de copias de respaldo.
- Procedimiento de recuperación de información en caso necesario.

E. ELEMENTOS DE JUICIO

Disponer de copias de seguridad es un requerimiento legal RLAC 72.2, obligando a que determinada información se conserve como mínimo 5 años. Normativas como la facturación electrónica o la LOPD también ponen de manifiesto la creciente necesidad de conservar la información más tiempo y asegurar que se puede recuperar.

Las copias de seguridad son un buen mecanismo de protección frente a eventos que puedan dañar la información. Un disco duro puede romperse o ser robado, un servidor informático puede sufrir una contingencia y dejar de funcionar, un SI de información puede ser atacado, etc.… Las copias de seguridad garantizan que la información podrá recuperarse de forma satisfactoria.

Cuando se analizan los procedimientos en esta materia, se deben validar los aspectos descritos en el punto anterior. Puede que la firma de auditoría esté realizando copias de seguridad, pero no tenga formalizado el procedimiento. En estos casos lo más importante es que realmente se estén realizando las copias de seguridad de forma razonable.

Por otra parte, **no toda la información es igual de sensible.** La información contable, la confidencial (RRHH) y la directamente relacionada con el negocio (papeles de trabajo, compilaciones, datos de clientes, proveedores, inventarios, etc.), debería disponer de copias de seguridad regulares. Si, por ejemplo, tras un incendio, intentamos recuperar la información pero no conseguimos recuperar la información de clientes, no podremos emitir facturas.

Por este motivo, existen normativas específicas de **"Continuidad de Negocio"**, bajo diversos nombres y modalidades. Este tipo de normativa pone de manifiesto la importancia de salvaguardar la información priorizando los aspectos más críticos para el negocio. A nivel básico únicamente es importante conocer la existencia de estos estándares y validar que la información más "relevante" se encuentra incluida en los procedimientos.

Además, **no únicamente se ha de salvaguardar la información** (papeles de trabajo, compilaciones, datos de clientes, de facturas, de asientos contables…) **sino también la configuración del sistema.** Independientemente de si estamos utilizando un software de auditoría o empleamos hojas de cálculo para nuestros trabajos, estaremos de acuerdo en que no únicamente se deben de guardar los datos, sino también las fórmulas asociadas (configuración).

F. PRUEBA DE EFICACIA OPERATIVA

Solicitar al responsable de los SI de la firma de auditoría la planificación de las copias de respaldo y validar una muestra de estas en función de su periodicidad, es decir, teniendo en cuenta la frecuencia de las mismas.

Para cada una de las copias se debe comprobar que cumple con el procedimiento establecido, que debe incluir los siguientes aspectos:

- Adecuado etiquetado del soporte físico (que impida que se confundan unas copias con otras).
- Evidencia de una adecuada ejecución de la copia. Es decir, debe quedar evidencia de que la copia ha finalizado correctamente (cuando se encuentra automatizada, es un registro electrónico, cuando es manual debe ser un apunte manual, por ejemplo, en una hoja de seguimiento de tareas).
- Adecuado contenido de la copia (validar que realmente se ha copiado la información prevista).
- Adecuado almacenamiento de las copias (en lugar seguro).

2. ELECCIÓN DEL TIPO DE INFRAESTRUCTURA Y ACCESO: EN LOCAL (ON PREMISE) - EN LA NUBE (CLOUD)

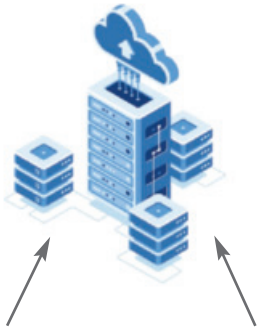
A. RECOMENDACIÓN

La firma de auditoría deberá disponer de una infraestructura cuya utilización y acceso garantice la integridad y seguridad de la información tratada. A veces puede resultar difícil decantarse por un tipo de infraestructura u otra, de los dos grandes grupos que existen: servidor en el despacho y servidor externo.

El acceso por **escritorio remoto** (existen varias formas de acceso, RDS, Citrix, escritorios compartidos), es tan simple como clicar dos veces un icono que tendrá cada usuario en su escri-

torio. El acceso vía **navegador WEB** consta de escribir un enlace (link) en el navegador habitual. Requiere un poco más de configuración en el servidor.

Opción A: On premise – Servidor en el despacho



Opción B: Cloud – Servidor externo

La VPN sólo será necesaria para aquellos lugares no habituales. Para los lugares habituales se necesitará la IP fija que se configurará en la "lista blanca" del servidor para permitir que las conexiones desde esas IP's puedan conectar sin encender la VPN.

Un requisito para evitar intrusiones mediante las conexiones por escritorio remoto o VPN es solicitar un doble factor de autenticación que garantice que únicamente los usuarios autorizados acceden a los archivos de la firma de auditoría.

B. OBJETIVO DEL CONTROL

La firma de auditoría debe implementar controles para garantizar la existencia y validez de copias de seguridad de los datos, configuraciones de bases de datos, configuraciones de sistemas operativos y aplicaciones.

C. RIESGO ASOCIADO

No disponer de adecuadas copias de seguridad de la información que da soporte a la organización puede conllevar que, en caso de pérdida o deterioro de información, dicha pérdida sea definitiva y la información no pueda ser recuperada.

El impacto de este riesgo suele ser extremo, puesto que cualquier ataque o intrusión supone la pérdida de información y la vulneración de los derechos de protección de datos de los terceros implicados.

D. DISEÑO DE LA POLÍTICA

Son varios los **criterios que influyen en la decisión de la implantación de una buena infraestructura,** pero básicamente se podrían resumir en tres: **Técnicos, Económicos y de Seguridad (TES).**

Es importante hacer una buena valoración TES, por lo que conviene realizar una reunión para valorar y evaluar la primera descripción de los criterios de este documento.

- Técnicos: **rendimiento, facilidad de uso, conectividad multidispositivo y multilugar …**

  Por un lado, la implementación de un software local será lenta y costosa, ya que este tipo de instalaciones se hacen a medida de la empresa y este tipo de procesos llevan su tiempo. La implementación de las aplicaciones en la nube, sin embargo, suelen ser mucho más rápidas, pero también es cierto que esta celeridad responde a una menor personalización de partida (que se puede ir mejorando con el tiempo).

Ambos sistemas son altamente personalizables. La diferencia está en que, en el caso de un software en local, la firma de auditoría tendrá que recurrir a profesionales que trabajen directamente el caso concreto de la empresa, mientras que las aplicaciones en la nube suelen contar con servicios técnicos que ayudarán a personalizar el software para adaptarlo a las necesidades particulares.

- Económicos: **coste de implantación, coste de escalabilidad, coste de propiedad …**

  Un software en local implica un menor coste inicial, pero debe tenerse en cuenta que necesita de una infraestructura TI que puede ser necesario ampliar o actualizar y supondrá costes adicionales, y que, además, a la larga implica unos costes de propiedad (consumo eléctrico, contratos de mantenimiento de los equipos, programas y procesos, renovaciones por obsolescencia, ciberseguros), que requieren de un presupuesto anual y una vigilancia de las desviaciones de éste. El caso de la nube permite hacer previsiones a largo plazo (suele implicar un pago por suscripción llaves en mano), sin embargo, debido a su pago continuo puede acabar saliendo más caro que la opción en local.

- Ciberseguridad: **riesgos de pérdida de información, riesgos de indisponibilidad de servicio ("horas muertas") …**

  La seguridad que ofrecen las aplicaciones locales frente a sus versiones instaladas en la nube depende mucho de los profesionales en los que dejemos esa seguridad y de los contratos de servicio firmados. En cualquier caso, la revisión de las propuestas y los contratos para determinar el alcance, el tiempo de respuesta y el nivel de servicio son elementos determinantes que permiten tomar una decisión razonada que va más allá de juicios de valor sobre si los datos estarán más seguros en local o en la nube.