LA IMPORTANCIA DE LA AUDITORÍA INFORMÁTICA EN EL MERCADO DE VALORES

Lilia Liu Chung
Directora del Instituto de Gobierno Corporativo de Panamá

Índice

LA IMPORTANCIA DE LA AUDITORÍA INFORMÁTICA EN EL MERCADO DE VALORES

Lilia Liu Chung[1]
Directora del Instituto de Gobierno Corporativo de Panamá

I. Introducción

Hoy en día, la naturaleza del sector financiero y del mercado de valores depende de un 100% de la tecnología, lo que para cualquier negocio representa la innovación en el servicio a sus clientes. Para nosotros, como consumidores finales, nos resulta cómodo sobre todo cuando realizamos cualquier tipo de transacción, como utilizar nuestra tarjeta de crédito para efectuar compras o pagar cuentas vía internet, y realizar movimientos en línea sin tener que hacer filas, o efectuar cualquier transacción sin tener que movernos desde donde nos encontramos. Sin embargo, con las tecnologías emergentes muchos son los negocios que no administran correctamente sus plataformas y no miden el riesgo que pudiera generar hacia terceras personas. Pero ¿qué sucedería si en una subasta está realizándose la compra o la venta de acciones y, repentinamente, en ese momento se paraliza el sistema?

Definamos primero qué es la Auditoría Informática. No es más que el proceso de revisión o verificación de todo el entorno informático con la finalidad de prevenir un riesgo en el negocio. Surgió inicialmente cuando los primeros analistas informáticos desempeñaban el rol de analizar la información que había sido procesada de los sistemas, al transcurrir los años se requerían mayores expertos revisores e identificaron que hacía falta una labor de fiscalización, que no se ejecutara dentro del área de sistemas y que debía ser evaluada por un ente externo o separado del área de tecnología. La auditoría informática surgió casi a la par de la Auditoría financiera ya que a través de los años son dependientes una de la otra.

La persona que realiza la labor de Auditoría informática es el auditor informático, quien debe tener cierta preparación en sistemas. Puede ser un analista de sistemas, un programador, un soporte técnico, un especialista en redes de comunicaciones o cualquiera que haya tenido experiencia o estudios en sistemas. Su carrera se vuelve ascendente una vez salta a la auditoría informática, ya que tiene un panorama completo al ver cualquier tipo de actividad dentro del ámbito de la tecnología, desde analizar procedimientos que se ejecutan, evaluar funciones de personas que interactúan con la información para temas de control interno, realizar análisis de impacto sobre nuevas plataformas o las ya existentes, hasta recomendar ampliamente cambios a procesos del negocio después de un análisis riguroso.

Actualmente la certificación CISA *(Certified Information Systems Auditor)* es una de las más reconocidas.

Las Auditorías Informáticas son utilizadas como:

1. **Apoyo al control interno en la organización,** que permita realizar verificaciones en forma periódica para identificar su exposición al riesgo y de cómo prevenirlos. Algunos ejemplos de fallas de control interno que podemos mencionar:

   a) Fallas de segregación de funciones en el personal del Departamento de Tecnología porque las funciones están concentradas en una sola posición.

1 La autora cuenta con las siguientes certificaciones internacionales: CFE (Certified Fraud Examiner), CRISC (Certified in Risk and Information Systems Control) y COBIT 5.

b) Poca documentación escrita de los procedimientos claves en caso de fallas del sistema y por el cual el personal desconoce cuáles serían los pasos a seguir en caso de un evento.

c) Falta de una planificación estratégica en Tecnología alineado con los objetivos del negocio, de manera que se pueda evaluar a futuro los riesgos, la tecnología a mejorar, los proveedores que brindarán el servicio, los nuevos negocios que requerirán mayor infraestructura o más personal, entre otros.

d) El uso de la tecnología WIFI (o redes inalámbricas gratuitas) creada por la empresa y que no es verificada periódicamente puede generar una exposición al riesgo de que cualquier persona externa penetre a las redes de la corporación.

e) La falta de entrenamiento para el personal que brinda el soporte o administra los sistemas informáticos, que pudieran generar accidentes involuntarios o desconocimiento en el uso de la información que están manejando.

2. **Cumplimiento a regulaciones y normativas.** En varios países de Latinoamérica ya existen regulaciones que contemplan el riesgo tecnológico, tal es el caso para la industria bancaria, pero más que hacer una lista de verificación o checklist de si cumple o no una regulación, es importante que la organización reconozca el impacto que genera al negocio y cómo afrontarlos.

   La utilización de estándares internacionales para el uso y control interno de la tecnología es la mejor opción para poder administrar los recursos tecnológicos de cualquier compañía.

3. **Medida de prevención de riesgo.** Una auditoría informática sirve de apoyo para establecer medidas que permiten prevenir cualquier riesgo con la ayuda de una matriz de riesgos donde se analiza la probabilidad de ocurrencia de un evento y su impacto.

4. **Análisis de desempeño de la función de tecnología.** Con las revisiones es posible medir cómo se ejecutan las funciones, tanto el personal de Tecnología como el grado de aceptación que tienen los usuarios finales, en cuanto al sistema o a la entrega de proyectos que debe realizar el área de tecnología. También se puede medir la eficiencia de las actividades evaluando la posibilidad de que sea requerido un aplicativo o equipo o mayor capacitación. Toda la actividad de tecnología es medible y en muchos casos cuantificable.

5. **Puntos de oportunidad de mejoras.** No todos los casos se consideran riesgosos pero existirán aspectos que podrán ser significativos para mejorar sus procedimientos o para la toma de decisiones y que brinden valor al negocio.

6. **Realizar investigaciones.** La auditoría informática también es un proceso que pudiera convertirse en una investigación para descartar la posibilidad de la existencia de un delito, de fraude o de otro tipo. Habrá situaciones que estarán fuera de nuestras jurisdicciones, sobre todo cuando algunos países no contemplan leyes relacionadas con delitos informáticos, específicamente, en donde se requiere de la cooperación internacional para realizar investigaciones. Sin embargo, el auditor también facilita el proceso de investigación cuando ocurren estas situaciones.

II. Estándares internacionales en Auditoría Informática

- **COBIT 5**

El marco de referencia para la realización de auditorías informáticas a nivel mundial es el COBIT 5 *(Control Objectives for Information Technology)* que va por su versión 5. El COBIT 5 creado por ISACA *(Information Systems Audit and Control Association)* es el estándar internacional por exce-

lencia, utilizado como control interno en Tecnología Informática (TI), para evaluar riesgos, analizar las actividades de control y de supervisión en Tecnología Informática. Es el estándar que se alinea con los objetivos del negocio y se amolda a cualquier tipo de negocio, sea éste pequeño, mediano o grande, y a cualquiera que desee administrar apropiadamente la tecnología en su empresa. El COBIT forma parte del paraguas de Gobierno Corporativo de una organización, ya que también se alinea con las distintas normativas de la industria: normativas ISO, PRINCE 2, PMBOK, ITIL, entre otros tantos.

Está compuesto por 5 dominios y 34 procesos catalizadores.

- **COSO *(Committee of Sponsoring Organizations of the Treadway Commission)***

El marco COSO es otro estándar utilizado internacionalmente para el Control Interno que se define como un proceso diseñado con la finalidad de proporcionar seguridad en cuanto a los objetivos de eficiencia y eficacia en las operaciones, confiabilidad en la información financiera, y cumplimiento de las leyes y normativas.

Está compuesto por 5 componentes: ambiente de control, evaluación de riesgos, actividades de control, información y comunicación, supervisión y monitoreo. Si observamos estos 5 componentes se alinean con el estándar del COBIT 5.

- **SARBANES-OXLEY**

Esta ley nace en Estados Unidos producto de los escándalos financieros de la ENRON, World Comm, y Tyco, con el fin de monitorear a las empresas que cotizan en la Bolsa de Valores, evitando que las acciones de las mismas sean alteradas de manera dudosa, mientras que su valor es menor.

Su finalidad es evitar fraudes y riesgo de bancarrota, protegiendo a los inversionistas. Tiene un segmento que regula todo lo relacionado con Tecnología informática que se llama Sarbanes-Oxley for IT.

III. Tipos de Auditoría informática

Con la evolución de la tecnología, también han evolucionado los tipos de auditorías informáticas. Entre ellos que podemos mencionar los siguientes:

1. **Auditoría de Controles Generales.** Es el diagnóstico general de todo el entorno informático. Se utiliza comúnmente cuando un auditor analiza por primera vez la organización.

2. **Auditoría de Base de datos.** Por ejemplo: Oracle, SAP, SQL, AS400, entre otros. Permite verificar el comportamiento de los archivos de bases de datos.

3. **Auditoría de Sistemas Operativos.** Por ejemplo: Windows, Linux, Unix, OS/400. Permite verificar los sistemas operativos donde descansa una base de datos y ponen a funcionar una aplicación.

4. **Auditoría de Aplicaciones en producción.** Permiten verificar las aplicaciones que se encuentran corriendo en vivo.

5. **Auditoría de Aplicaciones en desarrollo.** Permiten verificar las aplicaciones que son desarrolladas por los programadores, identificando el ambiente en el cual se encuentra antes de ser traspasadas al ambiente de producción.

6. **Migración de aplicaciones.** Valida las aplicaciones que son traspasadas a otro ambiente pudiendo ser otra base de datos u otro sistema operativo.

7. **Migración de base de datos.** Se utiliza cuando se migra los datos, no así la plataforma.

8. **Cambios de infraestructura tecnológica.** Cuando se requiere cambiar las redes o los equipos tecnológicos.

9. **Activos tecnológicos.** Analiza el estado del inventario de hardware y software existente.

10. **Redes y Comunicaciones.** Analiza el estado de las redes alámbricas e inalámbricas, y los métodos de autenticación de los sistemas de información.

11. **Seguridad Informática.** Se analiza el estado de la seguridad de la información, identificando la existencia o no de exposición al riesgo de la información.

12. **Pruebas de vulnerabilidad interna y externa.** Son pruebas que se efectúan para identificar si los sistemas son vulnerables a cualquier ataque, ya sea interno o externo.

13. **Auditoría de Ciberseguridad.** Dirigida a proteger la información existente en las infraestructuras críticas de la empresa y a la vez optimizar procesos empresariales.

Existen también otros tipos de auditorías que generan valor y son tan importantes como las anteriores que ameritan también ser revisados:

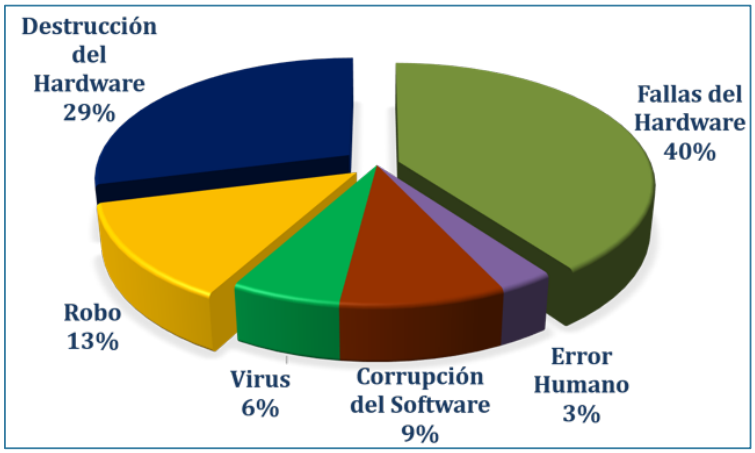
- Administración de proyectos tecnológicos.
- Acuerdos de niveles de servicio (SLA).
- Pruebas de validación.
- Centros de datos.
- Implementación de nuevo sistema.
- Contingencia y Recuperación de Desastres.
- Continuidad de negocios.

Una de las fuentes de información con muchos recursos para aquellos que deseen desarrollar la carrera de auditoría informática es explorando el sitio web de ISACA[2] *(Information Systems Audit and Control Association)*.

La ISACA es una organización líder en seguridad y control de entornos informáticos, con filiales en cerca de 100 países y de interés para profesionales de Ciencias Económicas, Informática e Ingeniería. A través de su Centro de Conocimiento *(Knowledge Center)* posee la guía necesaria para poder realizar auditorías informáticas específicas. Este centro de conocimiento posee una librería completa que ofrece una herramienta para la búsqueda de información que el usuario necesita.

Mucha de esta información ha sido elaborada por expertos de distintas nacionalidades que trabajan en empresas muy reconocidas, incluyendo firmas de auditorías, bancos, o empresas que cotizan en la bolsa de valores, que aportan sus conocimientos en sus áreas de especialidad. Debemos recordar que la auditoría informática es muy amplia si hablamos en general de la Tecnología. A medida que evoluciona la tecnología, aparecerán nuevos riesgos y nuevos métodos que antes no contemplábamos y que hoy en día son cada vez más importantes.

Algo muy importante en los temas de tecnología, es que según los datos reportados en Grupo Albe[3] algunas de las causas de las pérdidas de datos son las que se reflejan en el siguiente gráfico:



Fuente: Beneficios de implementar un DRP (Disaster Recovery Plan) en las Organizaciones Pymes. Grupo Albe

2 https://www.isaca.org

3 http://www.grupoalbe.com/beneficios-de-implementar-un-drp-disaster-recovery-plan-en-las-organizaciones-pymes/

De acuerdo con otra estadística, de Boston Computing Network[4], se menciona lo siguiente:

- 6% los PC's sufren algún evento de pérdida de datos en cualquier año.
- 30% de todas las empresas que tienen un gran incendio se queden fuera del mercado en un año.
- 34% de las empresas no logran probar sus copias de seguridad en cinta, y de las que sí lo hacen, el 77% han encontrado problemas en éstas.
- 60% de las empresas que pierden sus datos cerrarán dentro de los siguientes 6 meses después del desastre.
- Las empresas que no son capaces de reanudar sus operaciones dentro de los diez días siguientes de un desastre, no es probable que sobrevivan.
- Cada semana 140,000 discos duros dejan de funcionar en los Estados Unidos.

IV. La implementación de la Auditoría Informática

La Auditoría Informática se puede implementar mediante un proceso de planificación ordenado y programado. Para ello, se requiere:

1. Definir el alcance y el objetivo de la auditoría para poder limitar las revisiones.
2. Definir los sponsor (promotores) para saber quién o quiénes apoyarán el trabajo a realizar.
3. Definir la metodología de trabajo para conocer los procedimientos que serán utilizados.
4. Definir los recursos requeridos: el personal con el cual vamos a trabajar, con qué capital financiero cuenta en caso de que se requiera movilizar el personal o realizar pruebas que implique costos directos o indirectos, tales como alquiler de equipos o costos por parte de los servicios de los proveedores u horas extras del personal, con qué herramientas se van a contar -hardware, software- entre otros.
5. Definir el tiempo requerido para su realización; estimar el tiempo que será utilizado para efectuar el trabajo.
6. Elaboración de cronograma de auditoría: los pasos de todo el trabajo y llevar una hoja de ruta del trabajo.
7. Elaboración de entrevistas, trabajo de campo, papeles de trabajo.
8. Elaboración de un informe preliminar y discusión con las áreas auditadas.
9. Presentación ejecutiva: comité de auditoría o reunión con directivos.

4 https://www.bostoncomputing.net/consultation/databackup/statistics/

- **Herramientas de apoyo que se utilizan en las Auditorías Informáticas**

Como auditores informáticos existen múltiples herramientas que se pueden utilizar para apoyar el trabajo de revisión, dependiendo del tipo de auditoría que debe realizar. Sin embargo, lo más importante no radica en la herramienta utilizada sino el trabajo que se realice y su informe, porque esto es lo que va a destacar la labor del auditor informático.

Las herramientas más comunes utilizados por los auditores son: ACL, IDEA, TeamMate, IBM Cognos, Excel, Encase y Forensic Toolkit (FTK) para realizar análisis forense de la información, PC Audit o Qlikview.

Existe una multiplicidad de herramientas, sin embargo, lo más importante del trabajo de un auditor es la presentación del informe que debe estar sustentado bajo las evidencias encontradas. El método de observación y de entrevistas que debe realizar el auditor informático es de suma importancia que se realicen para evitar inexactitudes o errores en la auditoría.

- **El Informe: lo más valioso de una Auditoría Informática**

Para cualquier tipo de auditoría que se ejecute es importante la presentación de un informe que comunique de manera formal los objetivos, alcances, herramientas o metodología utilizada, observaciones, recomendaciones y conclusiones del proceso de auditoría.

El Informe de Auditoría debe:

1. Identificar claramente los riesgos potenciales a los cuales la organización se expone.

2. Explicar cómo mejorar el ambiente de control basado en los hallazgos, observaciones y entrevistas efectuadas.

3. Tener recomendaciones y un plan de acción para cada recomendación.

4. Tener un plan de seguimiento y su monitoreo constante.

5. Reflejar el compromiso de la Alta gerencia y de la Junta Directiva.

Sobre este último punto es lo más importante, ya que sin el apoyo de la Alta Gerencia y de la Junta Directiva no es posible lograr los objetivos de la auditoría y no se obtendrían los resultados esperados.