AUDITORÍA INTERNA

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Auditoría Interna del proceso de inversión en tecnologías emergentes

The Institute of Internal Auditors

Instituto de Auditores Internos de España

El INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA es una asociación profesional fundada en 1983, cuya misión es contribuir al éxito de las organizaciones impulsando la Auditoría Interna como función clave del buen gobierno. En España cuenta con cerca de 3.500 socios, auditores internos en las principales empresas e instituciones de todos los sectores económicos del país.

LA FÁBRICA DE PENSAMIENTO es el laboratorio de ideas del Instituto de Auditores Internos de España sobre gobierno corporativo, gestión de riesgos y Auditoría Interna, donde participan más de 150 socios y profesionales técnicos expertos.

AUDITORÍA INTERNA
BUENAS PRÁCTICAS EN GESTIÓN DE RIESGOS
OBSERVATORIO SECTORIAL
PRÁCTICAS DE BUEN GOBIERNO

El laboratorio trabaja con un enfoque práctico en la producción de documentos de buenas prácticas que contribuyan a la mejora del buen gobierno y de los sistemas de gestión de riesgos en organizaciones de habla hispana. Además de desarrollar contenido, fomenta el intercambio de conocimientos entre los socios.

ENCUENTRA TODOS LOS DOCUMENTOS DE LA FÁBRICA EN www.auditoresinternos.es

AUDITORÍA INTERNA

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Auditoría Interna del proceso de inversión en tecnologías emergentes

Noviembre 2020

MIEMBROS DE LA COMISIÓN TÉCNICA

COORDINACIÓN:
Eva López de Sebastián Miró. VIESGO.

Juan Armendáriz Vergarajaúregui, CIA, CRMA. ALLFUNDS BANK.
Santiago Cardona Torres. EY.
Cristina Fabre Chicano, ROAC, COSO-CI. CEPSA.
Pablo Gallego Tortuero, FRM. WIZINK.
Juan Palomo Cisneros. DELOITTE.
Rubén de Miguel Esteban, CISA, PMI-PMP. MAPFRE.
Carlos Morales Luchena, CIA, CISA. GRUPO BBVA.
Yolanda Pérez Pérez, CIA, CRMA, COSO-ERM. KPMG.
Julio Somoza Sáez. GRUPO SANTANDER.
Marina Touriño Troitiño, CIA, CISA, CRMA, CPA, CISM, TEAI.

The Institute of Internal Auditors

Instituto de Auditores Internos de España

El mundo, en todas sus vertientes, está inmerso en una profunda trasformación digital de sus usos y costumbres. La nueva revolución ha venido de la mano de las tecnologías de la información y la comunicación, y la utilización masiva de la información es el centro sobre el que pivotan muchas de estas nuevas tecnologías.

Estas nuevas tecnologías provocan necesariamente la readaptación al medio y, dado el alto grado de automatización y de engranaje de procesos, las líneas de control se pueden diluir. Por tanto, es esencial redefinir el hábitat de Auditoría Interna.

Auditoría Interna está obligada a transformarse para dar respuesta a las nuevas necesidades en este contexto de evolución de los modelos de negocio hacia entornos cada vez más tecnológicos, con gran volumen de transacciones y datos generados por las organizaciones.

Este documento incluye información para comprender mejor qué son y cómo evolucionan las tecnologías emergentes, el posicionamiento de Auditoría Interna frente a estas nuevas tecnologías, y un análisis de riesgos en una auditoría interna de inversiones en tecnologías emergentes.

Desde el Instituto agradecemos a la comisión su esfuerzo compartiendo su conocimiento, que ha resultado en un documento que será de gran utilidad para los auditores internos.

Instituto de Auditores Internos de España

Índice

Resumen ejecutivo

Auditoría Interna debe proporcionar a los órganos de gobierno información relevante durante el ciclo de vida de las tecnologías emergentes.

La transformación digital está en la agenda de la mayor parte de las organizaciones. Las tecnologías emergentes que, en su mayoría, tienen en común el tratamiento y gestión de la información, han permitido mejorar la eficiencia de los procesos, desarrollar nuevos productos, acceder a nuevos mercados y, lo que es más relevante, seguir provocando cambios a un ritmo vertiginoso, al encontrarse en constante evolución.

Adoptar nuevas tecnologías, reduciendo en muchos casos la intervención humana *(blockchain,* computación en la nube, inteligencia artificial, automatización de procesos mediante robots –RPA–, gestión masiva de datos, etc.), supone un alto grado de automatización, o tratamiento diferente de los procesos, que afecta a las líneas de control, pudiendo éstas modificarse e incluso diluirse tras la implantación.

Auditoría Interna debe estar alerta para adaptarse a los nuevos entornos organizativos más tecnológicos, comprender los riesgos asociados y proporcionar el aseguramiento necesario como Tercera Línea*.

Una Auditoría Interna alineada con la estrategia de su organización debe proporcionar a la Comisión de Auditoría y a la Alta Dirección información relevante para la toma de decisiones clave durante el ciclo de vida de las tecnologías emergentes (embrionario, prueba, adopción, madurez y obsolescencia). De hecho, se recomienda que las Comisiones de Auditoría cuenten con conocimientos y experiencia en tecnologías de la información para evaluar sistemas internos de control y gestión de riesgos, especialmente cuando se utilizan entornos computacionales o sistemas digitales complejos.

Las inversiones en tecnologías emergentes tienen varias características, a observar desde distintos enfoques:

- **Consideraciones previas a la inversión:** contexto y alcance de la inversión, impacto económico, consideraciones técnicas y de acceso a comunicaciones y expectativas de mantenimiento y crecimiento.
- **Modelo de gobierno de la inversión/transformación:** órganos de decisión y seguimiento y órganos operativos y de control.
- **Impacto en los procesos:** dependiendo de si se trata de una transformación de procesos internos o lanzamiento de un producto para cliente final.
- **Perspectivas de la organización:** tipo de desarrollo, equipos, producto e iteraciones, etc.

* THE INSTITUTE OF INTERNAL AUDITORS. *The IIA Three Lines Model 2020. An update of the Three Lines of Defense.* Julio 2020

El posicionamiento de Auditoría Interna frente a la inversión en tecnología debería tener en cuenta los siguientes aspectos:

- **Soporte a la Comisión de Auditoría y a la Dirección:** en el aseguramiento de los procesos asociados con la estrategia de inversión, la identificación y evaluación de riesgos, actividades de control, información y reporte, así como el seguimiento de las inversiones (por ejemplo, en lo referente al cumplimiento de objetivos, monitorización de riesgos, etc.).
- **Adecuación del Plan de Auditoría:** tratar de que responda a cuestiones fundamentales sobre el impacto de las inversiones en tecnologías emergentes en función de su riesgo (por ejemplo, proyectos estratégicos o con grandes partidas presupuestarias), considerando, además, las propias habilidades dentro del equipo de Auditoría Interna.
- **Rol de Auditoría Interna:** aportar valor como asesor de confianza o consultor –dentro del alcance establecido en las *Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna*– en todos los componentes del sistema de control interno, siempre y cuando no comprometa su independencia.

Además, Auditoría Interna debe comprender y evaluar los riesgos asociados a las inversiones en tecnologías emergentes:

- **Riesgos vinculados a la propia tecnología:** madurez, obsolescencia, posibles dilemas éticos, calidad y cantidad de los datos que se emplean en la solución o costes imprevistos derivados de la implantación.
- **Riesgos vinculados al proveedor:** situación económica y financiera, negociación y contratos, falta de alineación con el proveedor en lo referente al apetito de riesgo, excesiva dependencia del proveedor o decisiones inadecuadas sobre desarrollo interno/externo.
- **Riesgos vinculados a la inversión:** valoración incorrecta en el análisis de la inversión, rentabilidad no adecuada, problemas de liquidez o posibles errores en la contabilidad y reporte.
- **Riesgos regulatorios y de cumplimiento:** normativas de protección y privacidad de los datos; contra el abuso de mercado o sobre el uso de información privada; sobre infraestructuras críticas; o normativa interna.
- **Riesgos de seguridad (ciberseguridad):** derivados del incremento del perímetro de ataque, ciberseguridad en la nube, en el *Internet of Things* (Internet de las Cosas) o la creciente sofisticación de los ciberataques. También incluye el riesgo de que los empleados de la organización no estén suficiente concienciados o no dispongan del conocimiento necesario sobre la seguridad de información.
- **Riesgos derivados de la posible carencia de competencias tecnológicas** en la organización, incluyendo las funciones de control y aseguramiento: falta de capacidades técnicas o retraso en el uso de nuevas herramientas.

En definitiva, para auditar las inversiones en tecnologías emergentes, Auditoría Interna debe entender el razonamiento estratégico que subyace tras la inversión e identificar los riesgos asociados a las mismas. Solo así podrá identificar las debilidades de control que puedan existir en este proceso para aportar valor a la organización y cumplir con su misión de proporcionar aseguramiento a la Comisión de Auditoría y a la Alta Dirección.

Para auditar inversiones en tecnologías emergentes, Auditoría Interna debe entender el razonamiento estratégico de la inversión e identificar los riesgos asociados a las mismas.

Introducción

Definir *tecnología emergente* es arriesgado porque la tecnología emerge y se hace obsoleta con cierta rapidez, debido al potencial que nos ofrecen las nuevas capacidades computacionales.

En este documento se considera que tecnología emergente es la ciencia que se aplica a la resolución de problemas concretos que –de forma disruptiva– modifica, transforma, innova y genera nuevas oportunidades en el uso de sistemas, entendidos en el sentido más amplio, para cubrir las necesidades de la sociedad, sus empresas y sus personas.

Muchas tecnologías emergentes son tubos de ensayo y es posible que algunas nunca alcancen casos reales de uso, si bien el reto actual es ese probar y probar para asegurar que son sostenibles en su aplicación. Esta evolución continua es otro elemento clave de los procesos (nuevos, cambiantes) que se impone en la transformación de los mundos empresariales donde Auditoría Interna desarrolla su actividad de Tercera Línea.

La transformación a la que está obligada Auditoría Interna –para alinearse con los objetivos de negocio y cumplir con el *Marco Internacional para la Práctica Profesional de la Auditoría Interna*– se basa en el uso de nuevas herramientas (por ejemplo, para tratamiento, análisis y visualización de datos); en la evolución del enfoque de los trabajos hacia un modelo de seguimiento continuo integral (auditoría continua); en nuevas metodologías de trabajo que ayuden a mejorar la eficiencia y distribuyan resultados más rápido proporcionando información relevante y oportuna para la toma de decisiones; y en un cambio de perfiles en los auditores internos.

Tecnologías emergentes

TECNOLOGÍAS COMO SOPORTE Y NUEVAS SOLUCIONES

La tecnología sirve para mejorar la eficiencia en los entornos empresariales, permitiendo el tratamiento y acceso a la información de una forma más rápida, sencilla y ordenada. La transformación tecnológica actual ha aumentado esas capacidades, que podrían denominarse «tradicionales», hacia soluciones mucho más completas, replicando procesos ente-

ros y ofreciendo soluciones integrales donde, en muchos casos, el factor humano ha dejado de ser una dependencia natural del proceso.

Algunos ejemplos donde la tecnología está cambiando procesos en los que la intervención humana era esencial serían las cadenas de montaje de vehículos, la gestión logística de almacenes, las transacciones bancarias básicas, los vehículos autónomos, los sistemas predictivos de enfermedades, etc.

Las soluciones tecnológicas conllevan, por tanto, nuevas facetas en la gestión de los riesgos empresariales y, a medida que maduran, implican nuevos mecanismos de monitorización y control de esos riesgos.

Auditoría Interna, en su papel independiente, debe ser capaz de entender los riesgos en la definición de esas nuevas tecnologías, los asociados a su implantación, los inherentes de los nuevos procesos y sus controles mitigadores, y los riesgos derivados de la propia utilización de la tecnología.

Identificar adecuadamente los riesgos (evaluación de riesgos) en los procesos de inversión en estas tecnologías es fundamental para evitar que la mera reducción del coste que, en general, suponen las nuevas tecnologías enmascare otros riesgos a considerar para una adecuada toma de decisiones.

Las soluciones tecnológicas implican nuevos mecanismos de monitorización y control de los riesgos empresariales.

PRINCIPALES TECNOLOGÍAS EMERGENTES

Las tecnologías más relevantes (descritas en el Anexo I) son las siguientes:

- *Blockchain.*
- Computación en la nube *(Cloud Computing).*
- Inteligencia Artificial (AI, *Artificial Intelligence).*
- Robótica (en particular, RPA, *Robot Process Automation).*
- Internet de las Cosas *(Internet of Things, IoT).*
- Utilización masiva de datos *(Big Data/Data Analytics/Advanced Analytics).*
- Otras tecnologías, como asistentes de voz *(chatbot),* drones, impresión en 3D, realidad virtual, etc.
- Entorno 5G.

Estas tecnologías, que tratan y sistematizan información, introducen nuevos riesgos y formas de trabajar, y son un reto tanto para aquellos que las utilizan y consumen, como para asegurar que su uso no induce a riesgos no controlados o desconocidos, labor de Auditoría Interna.

CICLO DE VIDA DE LAS TECNOLOGÍAS EMERGENTES

El ciclo de vida actual de la tecnología es, en general, relativamente corto dado el constante y rápido avance con el que se producen componentes más baratos, accesibles y donde los desarrollos son más dinámicos (nuevas metodologías ágiles) con software de código

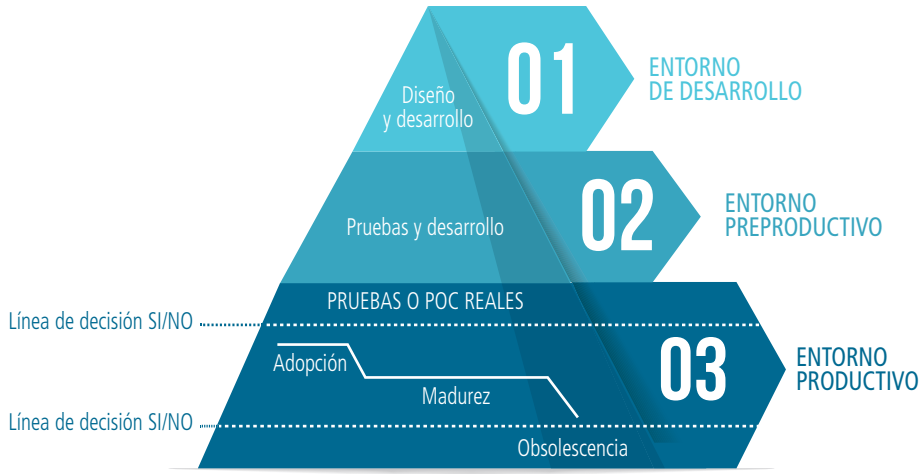
El ciclo de vida de las tecnologías emergentes pasa por un estado embrionario; de prueba; adopción; madurez; y obsolescencia.

abierto *(open source).* En los últimos años ha habido una importante aceleración de ese ciclo de vida, que ha propiciado el éxito o la desaparición de algunas tecnologías con una rapidez nunca vista antes.

El ejemplo más palpable son las criptomonedas, en especial *Bitcoin*. Una atracción por la tecnología propició su crecimiento (burbuja, en términos financieros) en un corto plazo de tiempo que se ha revertido considerablemente. Su atractivo actual como moneda se ha diluido por el momento, pero la tecnología subyacente, *blockchain*, es en la actualidad un reto de uso y de aplicación en el mundo empresarial.

De manera general podemos indicar que estas tecnologías pasan por los siguientes estados:

- **Embrionario** (entornos de desarrollo): priman desarrollos y pruebas para validar la tecnología desde un punto de vista técnico.
- **Prueba** (entornos de desarrollo o pre-productivos): la tecnología validada se prueba para ciertos casos de uso (pilotos, pruebas de concepto) y así conocer el grado de aceptación y adaptación a la necesidad de los usuarios.
- **Adopción** (entorno productivo): la tecnología se implanta en entornos productivos, alcanza volumetría y precisa mantenimiento y actualización.
- **Madurez** (entorno productivo): consolidación de la tecnología, con estabilidad en su funcionamiento, pero ya nacen otras que podrían sustituirla.
- **Obsolescencia** (entorno productivo): pese a su funcionamiento, la tecnología muestra debilidades relevantes (seguridad, soporte, estabilidad, disponibilidad, continuidad), es superada por otras tecnologías y los propios desarrolladores ya no tienen interés en su mantenimiento. La decisión es desmantelarla y sustituirla por otra tecnología más moderna con, al menos, las mismas prestaciones.



Fuente: Elaboración propia

En la vida tecnológica de un activo la **línea de decisión** tiene dos momentos clave: el primero, decidir si conforme a las pruebas realizadas y el caso de uso *(business case),* es el momento de pasar al estado de Adopción; y el segundo, decidir si el activo –que tiene un nivel de obsolescencia notable– debe desmantelarse y sustituirse por tecnologías más avanzadas o debe continuar, asumiéndose los riesgos existentes y que podrían impactar en la producción.

Este ciclo de vida es variable en función de varios aspectos, pero fundamentalmente depende del contexto de innovación, del nivel de inversión, la adopción y resistencia al cambio de sus consumidores y del coste de reposición.

Para Auditoría Interna es muy relevante determinar el estado del ciclo de vida donde se encuentre la tecnología objeto del trabajo porque, dependiendo del mismo, los objetivos, alcances o técnicas de trabajo serán diferentes, al igual que los riesgos por revisar. Dado que la intensidad y visibilidad de los riesgos es distinta, será necesario acentuar la existencia de buenos procesos de evaluación de riesgos que complementen la visión coste/beneficio.

En general el ciclo de vida depende del nivel de inversión, de la adopción y resistencia al cambio de sus consumidores y del coste de reposición.

Inversiones en tecnologías emergentes y posicionamiento de Auditoría Interna

Muchas organizaciones están inmersas en una transformación digital que se materializa a través de inversiones en tecnologías emergentes. Para que sea exitosa, esta transformación debe apoyarse sobre palancas fundamentales que Auditoría Interna debe reconocer para maximizar su contribución de valor:

- Definición de la estrategia con una agenda clara.
- Modelo de gobierno con asignación unívoca de roles y responsabilidades.
- Gestión del cambio y su impacto en procesos y la organización.
- Gestión tecnológica. Al abordar las inversiones en tecnologías emergentes se deberán tener en cuenta los riesgos asociados (qué hacer con las antiguas, qué infraestructuras y tecnologías son adecuadas, etc).

CONSIDERACIONES PREVIAS A LA INVERSIÓN EN TECNOLOGÍAS EMERGENTES

La concepción de la estrategia digital y su encaje puede ser significativamente muy diferente, en función de cada tipo de servicio a ofrecer por una empresa (empresas financieras o aseguradoras, servicios de distribución, inspecciones, venta en línea, empresa industrial, como metalúrgicas o de energía, entre otras, sin olvidar sistemas de control remoto como los SCADA[1]). A modo de ejemplo, las tecnologías emergentes basadas, fundamentalmente, en telecomunicaciones y en el uso de dispositivos móviles apropiados no son aplicables en la misma medida a todos los procesos de negocio.

La irrupción de las tecnologías emergentes implica, necesariamente, que una empresa reflexione sobre el impacto que sobre un proceso de negocio tienen la vertiginosa diversidad y cambios tanto del software y hardware como de la tipología de proveedores y la competitividad en el mercado por el uso de las mismas.

Consecuentemente, en la definición y encaje de la estrategia digital en los procesos de negocio, es necesario que Auditoría Interna evalúe si en los análisis preliminares del proyecto, se han considerado, como mínimo, los siguientes fundamentos:

	ELEMENTOS CLAVE A EVALUAR
ALCANCE Y CONTEXTO	· **Identificación del ámbito/alcance** (público/clientes/áreas) al que irán dirigidos estos servicios que incorporan nuevas tecnologías. · **Nivel de inmersión (conocimiento) de los usuarios** que son objetivo de estas tecnologías emergentes digitales (aplicaciones para móviles, etc.). · **Capacidad de absorción** de las nuevas tecnologías por los actuales usuarios/clientes *versus* los potenciales. · **Ámbito geográfico de implantación** de estas tecnologías (nacional y/o internacional). · **Integración con la tecnología actual** utilizada teniendo en consideración las adaptaciones necesarias para la comunicación con los sistemas existentes y el modelo de arquitectura a implementar.
IMPACTO DE LA ESTRATEGIA DE INVERSIÓN	· **Coste de inversión** para la puesta en ejecución. · **Coste de mantenimiento** de las soluciones. · **Beneficios cualitativos generados** (ampliación de negocio, beneficios operativos, etc.). · **Estimación de ingresos** generados en el medio y largo plazo.
COBERTURA/ DISPONIBILIDAD DE SERVICIOS DE COMUNICACIONES Y OTRAS CONSIDERACIONES TÉCNICAS	· **Acceso a servicios de comunicaciones:** líneas ADSL, fibra óptica o teléfonos (condicionantes geográficos según el objetivo del servicio a prestar), wifi, comunicaciones móviles, 4G, 5G... · **Tipología de dispositivos** móviles y tradicionales y amplitud de expansión. · **Sinergias e incompatibilidades con los sistemas tecnológicos actuales:** ecosistema de la infraestructura tecnología actualmente en producción y el encaje de la nueva tecnología en la misma, como un factor de la estrategia.
EXPECTATIVAS DE MANTENIMIENTO Y CRECIMIENTO DEL CONJUNTO DE ESTAS TECNOLOGÍAS	· **Validez en el tiempo** del modelo a desarrollar. · **Perspectivas de innovación** del software y el hardware y potencial compatibilidad con tendencias futuras de la tecnología para mantener el modelo tecnológico definido. · **Cambios en la legislación** nacional e internacional. · **Progresión/aumento de vulnerabilidades** de seguridad y protección de la información y los clientes. · **Nivel de dependencia de la tecnología** en cuestión.

1. Supervisory Control and Data Acquisition.

Fuente: Elaboración propia

CARACTERÍSTICAS DE LAS INVERSIONES

Modelo de gobierno de las inversiones

Las nuevas tecnologías permiten pensar en multitud de acciones que contribuyen a mejorar los procesos de una empresa (de cualquier sector) u ofrecer nuevos productos y servicios.

Esta variedad en las posibles soluciones exige la existencia de un marco de gobierno que controle todas las inversiones realizadas, analizando su coste frente al beneficio que se puede obtener, ya sea económico, de posicionamiento, de aumento de clientes, etc., así como los riesgos de seguir realizando las operaciones de la forma habitual frente a los riesgos originados por el cambio.

Los puntos más relevantes relacionados con este marco de gobierno y sobre los que Auditoría Interna debería prestar especial atención son:

Estructura del modelo de gobierno de inversiones

ELEMENTOS CLAVE A EVALUAR	
· **Existencia de órganos que analicen las distintas posibilidades de inversión** en distintas perspectivas (tecnológicas, de seguridad, de imagen, económicas). · **Cumplimentación de actas** formalmente documentadas de las decisiones tomadas. · **Existencia de procedimientos** sobre cómo tomar las decisiones sobre conceptos en los que invertir y que contengan: a. Alineación con la estrategia definida a nivel global por la empresa. b. Estimación de los posibles impactos de esa inversión, indicadores de desempeño, tanto en rentabilidad económica, posicionamiento de marca, captación de clientes, apertura de nuevas líneas de negocio, etc. · **Existencia de esquemas de seguimiento** que verifiquen, de manera temprana, si se cumplen o no las hipótesis de negocio. · **Existencia de esquemas de financiación** incrementales para desarrollar definitivamente los procesos.	ÓRGANOS DE DECISIÓN Y SEGUIMIENTO
· **Análisis de riesgos** para las nuevas inversiones y establecimiento de recomendaciones o limitaciones en cómo implantar estas soluciones. · **Establecimiento de responsabilidade**s sobre los riesgos detectados y planes de actuación que los mitiguen.	ÓRGANOS OPERATIVOS Y DE CONTROL

Fuente: Elaboración propia

Impacto en los procesos y aspectos organizativos

La inclusión de tecnologías emergentes tiene como principal fin el de poder ofrecer nuevos productos o mejorar los procesos o productos para hacerlos más eficientes, adecuando la oferta de valor a la realidad de lo que los clientes están demandando o agregando eficiencia a los procesos internos (dependiendo del sector en que cada empresa desarrolle su actividad). Es decir, en la mayoría de los casos, no es posible disociar la tecnología que se quiere implantar del proceso de negocio o proceso operativo que se quiere desarrollar o mejorar.

Dependiendo de qué tipo de uso tienen las nuevas tecnologías se pueden clasificar en:

- **Productos o procesos para clientes:** Estas nuevas tecnologías pretenden mitigar el riesgo del modelo de negocio, como el derivado de la entrada de nuevos competidores basados 100% en tecnología, que ofrecen productos y servicios que pueden competir con las empresas tradicionales gracias a procesos eficientes y automatizados.

  Adicionalmente, las nuevas tecnologías incorporan nuevos focos de atención en el desarrollo de los procesos, como la experiencia de cliente (es decir, cómo están diseñados los procesos desde el punto de vista del usuario, ya que será él quien de forma autónoma y desatendida accederá a estos procesos).

- **Transformación de procesos internos:** Las nuevas tecnologías permiten desarrollar nuevos procesos o reconfigurarlos de manera más eficiente.

Con independencia de la finalidad de la tecnología emergente, los aspectos organizativos son clave para asegurar que los procesos incorporan de manera adecuada las nuevas tecnologías. Auditoría Interna debería tener en cuenta:

Perspectivas de las inversiones en tecnologías emergentes respecto a la organización

	ELEMENTOS CLAVE A EVALUAR
TIPO DE DESARROLLO	· Valorar si se han tenido en cuenta, para la decisión de la inversión, **el coste de realizar un desarrollo interno, o la adquisición de la tecnología** y los procesos de un tercero. · **Metodología** de trabajo a seleccionar *(Agile vs. Waterfall).* · Valoración de la **gestión del cambio** que implica la transformación.
FORMACIÓN DE LOS EQUIPOS	· Determinar si los equipos están compuestos por **personal multidisciplinar** que permita tomar las decisiones, fundamentalmente en materia de tecnología, negocio y, en su caso, experiencia de cliente. · Evaluar si el equipo dispone del **conocimiento suficiente en la nueva tecnología** para poder implantarla de manera adecuada.
PRODUCTO E ITERACIONES	· Valorar los esquemas de **entrega de valor de los productos o procesos** relacionados con las nuevas tecnologías. En los casos en los que exista un producto mínimamente viable (o MVP, *Minimum Viable Product),* valorar si: - Se ha identificado el colectivo de clientes sobre los que se aplicará el MVP. - En los casos en los que se hayan tenido que firmar Condiciones de Uso, se indica al usuario que el producto está en fase de prueba (fase beta) y, por tanto, puede contener errores. - Existen mecanismos para medir el impacto que ha tenido en los procesos modificados o creados y se establecen mecanismos de decisión para decidir seguir invirtiendo o no en el desarrollo de un proceso o producto basado en los resultados medidos. - Definición de controles para detección de los riesgos asociados al MVP. - Se recogen los comentarios de clientes para mejorar los procesos e iterar en nuevas soluciones.

Fuente: Elaboración propia

POSICIONAMIENTO Y ROL DE AUDITORÍA INTERNA

Plan de Auditoría Interna

La evolución tecnológica y, en particular, las inversiones en las tecnologías emergentes, están ganando protagonismo en la agenda de la Comisión de Auditoría, cuyos principales retos fundamentales son velar por que los conocimientos tecnológicos de sus miembros sean apropiados según lo establecido en algunas regulaciones (por ejemplo, la Ley de Auditoría de Cuentas) e incrementar la supervisión de estas nuevas tecnologías en el ámbito de sus funciones.

La Guía Técnica de la CNMV 3/2017, sobre *Comisiones de Auditoría de Empresas de Interés Público,* recomienda que al menos uno de los miembros de la Comisión tenga experiencia en tecnologías de la información, para propiciar una supervisión eficiente de los sistemas internos de control y gestión de los riesgos –que generalmente utilizan aplicaciones informáticas complejas– así como poder evaluar adecuadamente riesgos emergentes, como el de ciberseguridad. Por eso el papel de Auditoría Interna cobra una mayor relevancia en su apoyo en estas crecientes responsabilidades de supervisión.

Responsabilidades de la Comisión de Auditoría frente a las inversiones en tecnologías emergentes

ASPECTOS CRÍTICOS SOBRE INVERSIONES EN TECNOLOGÍAS EMERGENTES	
· **Prioridades en las inversiones** en tecnologías emergentes (órgano decisor, criterios, plan de despliegue, prototipos o pilotos de prueba, etc.). · **Riesgos y oportunidades** comparados con el sector, mercado, etc. · Alineamiento de los objetivos de la inversión con los objetivos estratégicos de la empresa. · **Integración en otros proyectos estratégicos** (plan de transformación digital, innovación, etc.). · **Impacto** de esa inversión en el modelo de negocio y en el reporte financiero. · **Uso de recursos** internos y externos con conocimiento y experiencia adecuados.	ESTRATEGIA DE INVERSIÓN
· **Evaluación de los nuevos riesgos** (legales, regulatorios, cumplimiento, Shadow IT, sesgo en los algoritmos y segregación de funciones, riesgos de terceros, propiedad del dato, calidad del dato, retorno de la inversión, seguridad, ciberseguridad digital etc.).	PROCESO DE IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS
· **Evaluación del nivel de efectividad de nuevos controles** (segregación de funciones, accesos restringidos, salvaguarda de datos de clientes y propiedad intelectual, certificaciones de terceros, planes de contingencia, etc.).	EVALUACIÓN DE ACTIVIDADES DE CONTROL
· **Protocolos de comunicación, coordinación y reporte** entre las Tres Líneas.	INFORMACIÓN Y REPORTE
· **Adecuación de los mecanismos actuales de seguimiento** de las inversiones a las tecnologías emergentes y análisis de las deficiencias identificadas.	SEGUIMIENTO DE LAS INVERSIONES

Fuente: Elaboración propia basada en el documento *Center for Audit Quality. Emerging technologies: an oversight tool for Audit committees,* 2018

En este contexto, es fundamental que Auditoría Interna elabore un Plan de Auditoría que cubra estos aspectos críticos y que evolucione a la misma velocidad con la que su organiza-

ción adopta nuevas tecnologías, integrando en él los aspectos relevantes asociados a las tecnologías emergentes y dando respuesta a preguntas relevantes que podrían cuestionar los miembros de la Comisión de Auditoría:

Preguntas desde la Comisión de Auditoría sobre la auditoría de las inversiones en tecnologías emergentes

	ASPECTOS CLAVE A CONSIDERAR
¿Cómo se ha considerado el impacto de las tecnologías emergentes en el proceso de evaluación de riesgos de Auditoría Interna?	· **Alineamiento del Plan de Auditoría Interna** con el plan estratégico y, en particular, con el plan de transformación digital, innovación, etc. · **Coordinación con la función de Gestión de Riesgos** para asegurar la integridad y adecuada mitigación de estos riesgos.
¿Tienen las tecnologías emergentes un impacto significativo en el alcance de la planificación de Auditoría Interna?	· **Enfoque para la planificación:** aseguramiento para auditorías puntuales y/o a lo largo del proyecto y consultoría. · Incorporación de la auditoría de procesos asociados a las inversiones en nuevas tecnologías emergentes en el Plan de Auditoría Interna, en función de su ciclo de vida. · **Definición de programas de trabajo *ad hoc*** para cada inversión específica.
¿El equipo de Auditoría Interna tiene conocimiento y experiencia adecuados para afrontar estos nuevos retos?	· **Análisis de competencias del equipo** de Auditoría Interna. · **Estrategia de personal** para cubrir un posible déficit y definición de programas de formación en aspectos técnicos para cubrir las posibles carencias en las competencias del equipo de Auditoría Interna.

Fuente: Elaboración propia

Propuestas para la generación de valor

Auditoría Interna, como asesor de confianza, debe prestar servicios que aporten valor añadido a la organización a través de un asesoramiento proactivo y estratégico que va mucho más allá de la mera ejecución eficiente y eficaz del Plan de Auditoría que, en el caso de las inversiones en tecnologías emergentes, suele ser a través de auditorías *a posteriori (post mortem)* o de aseguramiento durante la realización del proyecto (por fases).

La orientación proactiva hacia los nuevos riesgos y tecnologías emergentes permitirá a Auditoría Interna identificar los problemas con mayor antelación a través de un aseguramiento preventivo (detectar los riesgos digitales antes de que se materialicen, detección de fallos en procesos *ex ante,* etc.). Todo ello aportando valor en una fase más temprana y manteniendo, a su vez, su aportación de valor durante todo el ciclo de auditoría, contribuyendo al fortalecimiento de los sistemas de control y a la generación de una mayor confianza de la Dirección y de la Comisión de Auditoría (acercamiento al negocio, mayor visibilidad para la función, participar de las iniciativas que se emprenden, etc.).

Algunos ejemplos de servicios de consultoría podrían ser los reflejados en la tabla siguiente.

Posibles servicios de consultoría prestados desde Auditoría Interna relativos a las inversiones en tecnologías emergentes

POSIBLES SERVICIOS DE CONSULTORÍA	
· Evaluación de marcos de control y gobierno adecuados sobre los procesos digitales y sistemas. · Análisis de las implicaciones de cambios en los procesos de negocio como resultado de la nueva inversión en el entorno de control existente. · Soporte a la función de gestión de riesgos en la identificación de nuevos riesgos. · Supervisión de la gestión del cambio (formación, reorganización de personal, valoración de talento, procedimientos, etc.).	ENTORNO DE CONTROL
· Análisis de los riesgos y los controles previos a la implementación de las inversiones en nuevas tecnologías emergentes. · Comparativa *(gap analysis)* del mapa de riesgos asociados a los procesos de inversiones en las nuevas tecnologías de la información de la organización (por ejemplo, ciberseguridad) con respecto a buenas prácticas de estándares de la industria y recomendaciones de mejora.	EVALUACIÓN DE RIESGOS
· Evaluación *ex ante* de procesos y controles afectados por las nuevas tecnologías emergentes. · Revisión de la selección de terceros y el proceso de diligencia debida (solicitud de certificaciones SSAE16, ISAE 3402 o ISO 27001), así como los requerimientos que permitan su supervisión efectiva posterior. · Asesoramiento en la revisión de nuevas políticas y procedimientos relacionados con las nuevas tecnologías emergentes, tales como redes sociales, seguridad de los datos, etc.	ACTIVIDADES DE CONTROL
· Asesoramiento en la creación de procesos de extracción, transformación y carga automática (ETL). · Apoyo en el desarrollo de herramientas de analítica de datos y cuadros de mandos para monitorizar el desempeño de la inversión en términos operativos y financieros.	INFORMACIÓN Y COMUNICACIÓN
· Revisión de las estructuras de gobierno corporativo, incluyendo la monitorización periódica y los informes dentro de la organización para evaluar si existe una supervisión corporativa adecuada.	SUPERVISIÓN

Fuente: Elaboración propia basada en el documento de KPMG *20 key risks to consider by internal audit before 2020,* 2018

En el rol de asesor de confianza, Auditoría Interna debe velar por su independencia, cumpliendo con el *Marco Internacional para la Práctica Profesional de Auditoría Interna.* Para ello, debería considerar los servicios «incompatibles» como la definición, decisión, diseño, implantación, control y aprobación de los proyectos asociados a las inversiones en tecnologías emergentes y establecer determinadas salvaguardas que garanticen la independencia en todo el proceso de asesoramiento en las inversiones en tecnologías emergentes.

Posibles salvaguardas para preservar la independencia de Auditoría Interna

· Definición clara de roles y responsabilidades previas al comienzo del trabajo. Auditoría Interna no podrá liderar el proyecto de inversión, tomar decisiones para la ejecución y seguimiento del proyecto, validar los resultados y tomar las decisiones en relación con las posibles alternativas asociadas a cada fase del proyecto de inversión en cada tecnología emergente.

· Participación con voz, pero sin voto, en Comités como los de Inversiones, Innovación, Transformación Digital, etc.

· Establecer un procedimiento de conflictos de interés y asegurar su cumplimiento.

Cómo auditar los riesgos del proceso de inversión en tecnologías emergentes

Una buena práctica es realizar un análsis de riesgos y oportunidades junto con el planteamiento de la idea/proyecto.

Las tecnologías emergentes pueden proporcionar grandes beneficios a las empresas. Sin embargo, es necesario tener en consideración también los riesgos asociados, parte de los cuales no difieren mucho de los riesgos tecnológicos tradicionales. Una vez identificados los riesgos, se podrán definir los controles necesarios que permitan maximizar el beneficio y mitigar los riesgos.

Una buena práctica es realizar un análisis de riesgos y oportunidades junto con el planteamiento de la idea/proyecto. Para realizar este análisis de riesgos y oportunidades es necesario entender en profundidad el contexto externo e interno de cada empresa, los objetivos del negocio y cómo la tecnología emergente ayuda a la consecución de los mismos. En este sentido cabría diferenciar:

- **Contexto interno:** hace referencia al modelo de gobierno de la empresa, sus objetivos, las políticas y procedimientos internos, los flujos de información y los procesos de toma de decisiones. Para realizar un adecuado análisis de riesgos y oportunidades de estas inversiones, es fundamental conocer el tamaño y madurez de la empresa y del sector en el que opera, su nivel de internacionalización y, para cada inversión concreta, conocer el proceso de adopción de tecnología que se está llevando a cabo, junto con los intereses origen de ese proceso y objetivos de la misma.
- **Contexto externo:** hace referencia, entre otros aspectos, al entorno cultural, social, político, legal, reglamentario, tecnológico, económico, natural y competitivo, a nivel internacional, nacional, regional y local.

La identificación de riesgos es clave en un proceso de inversión. Consideramos que los riesgos más relevantes en los proyectos de inversión en tecnologías emergentes son los siguientes:

- Riesgos vinculados a la propia tecnología emergente.
- Riesgos vinculados al proveedor de la tecnología emergente.
- Riesgos económico-financieros vinculados a la inversión en una tecnología emergente.
- Riesgos de regulación y cumplimiento.
- Riesgos de seguridad (ciberseguridad).
- Riesgos de competencias tecnológicas en la organización, incluyendo las funciones de control y aseguramiento.
- Riesgos vinculados a la gestión del cambio, incluyendo el impacto en la infraestructura tecnológica actual y los procesos de negocio.

RIESGOS MÁS RELEVANTES EN LOS PROYECTOS DE INVERSIÓN EN TECNOLOGÍAS EMERGENTES

Estos riesgos, que se desarrollan a continuación, han de ponerse en el contexto externo e interno de cada empresa mencionado antes, incluyendo el marco sectorial y la tipología de la inversión.

Los auditores internos pueden, además, utilizar para su trabajo los estándares y guías de referencia específicos que sean aplicables a la inversión, como los publicados por el Instituto de Auditores Internos, el National Institute of Standards and Technology (NIST); la Cloud Security Alliance (CSA); la International Standards Organization (ISO); la IoT Security Foundation; etc., y que recogemos en el capítulo de bibliografía.

RIESGOS VINCULADOS A LA PROPIA TECNOLOGÍA EMERGENTE

Apostar por una corriente tecnológica emergente en fase temprana puede aportar una ventaja competitiva frente a competidores, pero también puede encaminar al fracaso.

En este sentido, por lo general, sería recomendable evitar fases tempranas de desarrollo y comenzar mediante un enfoque de pruebas de concepto *(POC: Proof of Concept),* o pilotos, planteando casos de estudio pequeños y fácilmente aplicables, con el objeto de ir haciéndolo extensible, de manera progresiva, a escenarios más complejos a medida que se adquiere la experiencia necesaria.

RIESGO: INMADUREZ DE LA TECNOLOGÍA

Descripción: No adopción de la tecnología por parte del mercado o los consumidores, que podría incluso llegar a descontinuar su desarrollo.

Objetivos de control	Cómo auditarlo
Existencia de un análisis sobre la tecnología por parte del personal experto en la empresa.	Verificar que existe un análisis sobre la tecnología y que, con base en el nivel de adopción que se pretende dar en la empresa, el nivel de madurez de esta tecnología no implica riesgos inasumibles.

Ejemplo de riesgo: HD DVD frente a Blu-ray en la competición por suceder al DVD.

Descripción: Incertidumbre sobre su aplicación real y sobre la posibilidad de diseñar modelos de negocio rentables.

Objetivos de control	Cómo auditarlo
Definición del caso de negocio o de los objetivos de los proyectos basados en tecnologías emergentes.	Comprobar que los proyectos disponen de un objetivo claro, bien ligado a un caso de negocio o a la experimentación para evaluar posibles líneas de negocio futuras.

Ejemplo de riesgo: En la actualidad aún son pocas las empresas que disponen de soluciones con gran número de transacciones sobre *blockchain.*

Descripción: Inversión elevada con un retorno a largo plazo (no obstante, adquirir el *know-how* puede suponer una ventaja competitiva).

Objetivos de control	Cómo auditarlo
Valoración de la inversión y su alineación con los objetivos de la empresa.	Si la inversión es elevada, comprobar que el proyecto está alineado con los objetivos estratégicos de la empresa y que existe un análisis del retorno sobre la inversión *(ROI)*.

RIESGO: DILEMAS ÉTICOS

Descripción: Algunas tecnologías emergentes pueden plantear dilemas éticos y morales que pueden tener consecuencias legales o dañar la reputación de la empresa.

Objetivos de control	Cómo auditarlo
Análisis de las consecuencias generadas por los dilemas éticos que puedan plantearse, así como de la legislación que sería de aplicación.	Comprobar que en el caso de uso se respetan los principios éticos y de cumplimiento de la organización y evaluar el grado de incertidumbre existente en la legislación aplicable.

Ejemplos de riesgo: a. Responsabilidad en un accidente provocado por un coche autónomo. b. Impacto sobre el empleo debido a la transición hacia sistemas automatizados.

RIESGO: CALIDAD Y CANTIDAD DE LOS DATOS

Descripción: Una calidad de datos pobre puede derivar en la toma de decisiones incorrectas a través de soluciones tecnológicas basadas en la recogida y análisis de grandes cantidades de datos.

Objetivos de control	Cómo auditarlo
Existencia de controles y pruebas de validación que aseguren la calidad de los datos utilizados.	Comprobar que existen controles que aseguren la calidad de los datos.

Ejemplo de riesgo: Soluciones de inteligencia artificial y análisis de datos que arrojan resultados ambiguos o imprecisos.

Descripción: Si no se dispone de conjuntos de datos de entrenamiento y prueba con el tamaño necesario, podrían incrementarse los errores en los algoritmos de procesamiento y afectar negativamente a los resultados.

Objetivos de control	Cómo auditarlo
Disposición de datos suficientes para abordar el desarrollo de soluciones basadas en inteligencia artificial.	Comprobar que se dispone de un conjunto de datos de entrenamiento y prueba suficiente antes de plantear soluciones relacionadas con inteligencia artificial.

Ejemplo de riesgo: Sesgo en los resultados debido a una muestra de datos no suficientemente representativa.

RIESGO: COSTES DERIVADOS NO CONTEMPLADOS INICIALMENTE

Descripción: Apostar por una corriente tecnológica emergente en ocasiones podría implicar costes adicionales, más allá de la adquisición de licencias o proyectos, para el desarrollo de soluciones que las implementen.

Objetivos de control	Cómo auditarlo
Consideración de costes derivados en el análisis de las soluciones.	Verificar que el análisis del caso de negocio contempla cuestiones como las necesidades de infraestructura, comunicaciones, modelo de autenticación, privacidad de los datos y mantenimiento de las soluciones.

Ejemplo de riesgo: El ancho de banda de internet requerido para una empresa podría requerir una ampliación al adoptar soluciones en la nube.

RIESGO: USO DE TECNOLOGÍAS NO GESTIONADAS POR LAS ÁREAS DE TECNOLOGÍA Y SEGURIDAD (SHADOW IT)

Descripción: La fácil adquisición, implantación y uso de soluciones tecnológicas (sobre todo las basadas en la nube) hace que, en ocasiones, sean obtenidas directamente por las áreas de negocio sin tener en consideración mecanismos de control y gestión bajo la supervisión de las áreas de Tecnología y Seguridad. Esta situación incrementa la exposición a riesgos operativos, legales y de seguridad.

Objetivos de control	Cómo auditarlo
Existencia de mecanismos de control que garantizan que todas las soluciones tecnológicas son evaluadas por las áreas expertas de tecnología y seguridad.	Verificar los procedimientos de contratación y compras definidos y comprobar que el flujo definido asegura la valoración de las soluciones tecnológicas por parte de las áreas expertas (TI y Seguridad).

Ejemplo de riesgo: Utilización de aplicaciones que no cumplen con los requisitos de seguridad definidos por la empresa ni con los requisitos de protección de datos y legales aplicables.

Ej. El departamento de Clientes adquiere una solución CRM como servicio cloud que le ofrece un tercero. TI y seguridad lo desconocen por lo que la configuración de contraseñas no cumple la normativa establecida permitiendo contraseñas sencillas y tampoco se monitorizan intentos de acceso fallidos. Un atacante realiza un ataque de fuerza bruta y obtiene acceso a los datos de nuestros clientes con el consiguiente daño comercial, reputacional y económico por las sanciones recibidas.

RIESGOS VINCULADOS AL PROVEEDOR

Las organizaciones son proclives a realizar su inversión en tecnologías emergentes a través de proveedores especializados. Esto tiene beneficios evidentes como el ahorro en costes y el uso de capacidades técnicas no disponibles en la empresa, aunque también comporta riesgos que se deben gestionar desde el momento de la decisión de externalización y durante el ciclo de vida completo de la externalización. En la práctica, no se trata de crear un proceso específico para invertir en tecnologías emergentes a través de la utilización de terceros, sino de adaptar los procesos existentes de externalización a la realidad y el perfil de riesgo específico de estas tecnologías.

Utilizar proveedores para invertir en tecnologías emergentes implica entender qué procesos concretos está externalizando la organización y sus riesgos propios, analizando su impacto operacional y tecnológico en aspectos como ciberseguridad, protección de datos, continuidad del negocio, gobierno de los datos y, en general, cumplimiento normativo.

Los reguladores son cada vez más conscientes de estos retos. Específicamente, para el sector financiero, existen directrices publicadas por la Autoridad Bancaria Europea. En este ámbito es preciso construir un marco de control robusto que permita gestionar los requerimientos normativos para el uso de proveedores, así como los requerimientos que dichos proveedores deben cumplir; situación que puede afectar al desarrollo de los proyectos incrementando costes o tiempos de ejecución.

La empresa usuaria de proveedores sigue manteniendo su responsabilidad en materias sensibles como la protección de datos personales y no puede trasladarla al proveedor. También los proveedores tienen un interés comercial obvio en aplicar medidas mitigadoras de los riesgos. Aquellas empresas que cuenten con una función específica de Cumplimiento Normativo, que sea capaz de influir en las decisiones y la estrategia de la empresa respecto a la inversión en tecnologías emer-

gentes, estarán mejor preparadas para afrontar este riesgo.

En el momento de la decisión de inversión en tecnologías emergentes utilizando terceros es preciso reflexionar, de modo estratégico, sobre el modelo de control operativo y de seguridad, y sobre cómo verificarlo y proporcionar aseguramiento al respecto, por lo que una manera eficaz de centrar la conversación es involucrar a áreas como Tecnología, Seguridad, Control Interno, Servicios Jurídicos, Cumplimiento Normativo y Auditoría Interna. Al realizar este análisis, las empresas pueden encontrar que el modelo adecuado es más costoso que el previsto intuitivamente, lo que constituye un elemento indispensable en la toma de decisiones de la inversión. El negocio y las áreas de control han de trabajar de forma coordinada y entendiendo sus necesidades mutuas, para valorar los riesgos e implantar controles conmensurados al apetito asumible, tanto en el momento de la contratación como en el de la gestión del servicio externalizado durante todo su ciclo de vida. Un modo eficaz de que esto ocurra es imponer este modo de operar a través de políticas y procedimientos internos que se difundan eficazmente por la organización.

RIESGO: SITUACIÓN ECONÓMICA Y FINANCIERA ADVERSA DEL PROVEEDOR

Descripción: Incapacidad de proporcionar soporte a medio-largo plazo por caer en una situación financiera adversa.

Objetivos de control	Cómo auditarlo
Comprobación de la situación económica y financiera del proveedor durante la vida del contrato.	Revisar el análisis económico-financiero al inicio de la contratación y durante la vida del contrato, y las medidas a tomar en caso de deterioro.

Ejemplo de riesgo: Contar como proveedores clave con empresas altamente especializadas en tecnologías emergentes, pero poco sólidas en términos financieros.

RIESGO: NEGOCIACIÓN Y FIRMA DEL CONTRATO CON EL PROVEEDOR

Descripción: Los grandes proveedores no son flexibles para incluir, retirar o modificar las cláusulas de sus contratos de adhesión en consonancia con las necesidades/condiciones de la empresa usuaria de estos servicios.

Objetivos de control	Cómo auditarlo
Existencia de medidas alternativas para hacer frente a cláusulas inflexibles y consideración de la flexibilidad como criterio a la hora de seleccionar el proveedor.	Revisar cómo el proceso de selección considera la capacidad de negociación y si se imponen herramientas de mitigación, tales como controles internos compensatorios, o si admite la subcontratación, a su vez, en otros proveedores.

Ejemplo de riesgo: Proveedores de servicios en la nube (Google, Amazon, Apple, Microsoft, IBM), que imponen sus condiciones.

Descripción: Entornos multicliente, dispersión geográfica del proveedor, barreras físicas a las instalaciones y visibilidad limitada sobre los recursos del proveedor y su disponibilidad.

Objetivos de control	Cómo auditarlo
El contrato regula específicamente responsabilidades de una y otra parte, y considera los niveles de interlocución, cómo se accede a las evidencias, los tiempos de respuesta a solicitudes y la extensión del derecho de auditoría más allá del tiempo de prestación de los servicios. El proveedor tiene certificados, tales como la implantación de normas ISO[2] o CSA STAR[3], o informes ISAE[4], SOC[5], que no cubren todas las necesidades de control.	Verificar que existen cláusulas que permiten ejercer los derechos de auditoría en la práctica o una monitorización adecuada del proveedor. Valorar, en los certificados: - La cobertura de las necesidades de la organización que externaliza. - El alcance de los certificados. Por ejemplo, si evalúan solamente diseño o también efectividad operativa de los controles. - La posibilidad de acceso al informe de certificación completo frente a únicamente saber que el proveedor ha obtenido una certificación. - La necesidad de recibir evidencias adicionales con su consecuente coste.

Ejemplo de riesgo: Limitaciones a los derechos de auditoría al proveedor, que hacen que su desarrollo sea más difícil o menos eficaz.

RIESGO: FALTA DE ALINEACIÓN ENTRE EL APETITO DE RIESGO DEL PROVEEDOR Y EL DE LA ORGANIZACIÓN

Descripción: Las políticas y procedimientos del proveedor en la prestación del servicio no son equivalentes a las del cliente.

Objetivos de control	Cómo auditarlo
Homologación del proveedor a través de criterios concretos y alineados con el conocimiento, compatibilidad entre sistemas de ambas empresas para facilitar el intercambio de datos, planes de marcha atrás (en la implantación) y salida (tras la implantación). Análisis en el proceso de selección y los pliegos de condiciones asociados, así como en la revisión periódica de estos servicios externalizados.	Revisar que existen procesos consistentes de homologación. Revisar que tanto al inicio de la relación como durante la vida del contrato se cumplen los criterios de riesgo.

Ejemplo de riesgo: Diferente apetito de riesgo del proveedor, en cuanto a costes, dependencias, medidas de seguridad, respuesta a la necesidad del negocio, etc.

Objetivos de control	Cómo auditarlo
Valoración sobre cómo complementar el uso de certificados con revisiones directas a través de auditorías específicas y controles por parte de la organización que externaliza. En caso necesario, opción de paralizar funcionalidades y acometer mejoras, estableciendo controles compensatorios.	Verificar y valorar: - Que existen certificados complementados con controles compensatorios en el lado de la empresa que externaliza. - La inclusión del proveedor y su servicio en las herramientas de seguimiento empresariales. - La implantación de canales de comunicación y mantenimiento correctivo, exigibles contractualmente, sujetos a monitoreo y acciones correctivas para volver a ajustarlos al apetito de riesgo.

Ejemplo de riesgo: El nivel de control es inferior al que sería posible de no haber externalizado el servicio.

2. ISO: Siglas de la International Organization for Standarization (organización internacional para la estandarización), sistema de normalización internacional para productos y procesos de áreas diversas.
3. El registro de evaluación, confianza y seguridad CSA STAR (Security, Trust & Assurance Registry) de la organización CSA es un mecanismo de evaluación de la seguridad de los proveedores de servicios en la nube.
4. ISAE: International Standard on Assurance Engagement, in accounting (estándares internacionales de los Servicios de aseguramiento).
5. SOC: Service Organization Control, control sobre organización de servicio, proporciona informes de control interno de proveedores de servicio.

RIESGO: DEPENDENCIA DEL PROVEEDOR

Descripción: El servicio contratado al proveedor que desarrolla la tecnología emergente puede ser crítico para la empresa contratante, pero no necesariamente crítico para el proveedor.

Objetivos de control	Cómo auditarlo
Especificación en los contratos de los niveles de servicio y control y monitorización de su cumplimiento.	Verificar que: - El contrato regula niveles de servicio relativos a la integridad, la disponibilidad y la seguridad de la información. - Existen planes de salida que pueden requerir acciones por parte del proveedor. - Funciones como Control Interno y Seguridad están involucradas en la externalización. - La organización mide regularmente el cumplimiento de los niveles de servicio acordados y acuerda con el proveedor acciones en caso de incumplimiento, a las que a su vez da seguimiento.

Ejemplo de riesgo: El proveedor deja de prestar el servicio y la organización no tiene capacidad de reacción.

RIESGO: DECISIONES ESTRATÉGICAS INADECUADAS SOBRE DESARROLLO INTERNO/EXTERNO

Descripción: Decisiones sobre externalización sin tener en cuenta todos los elementos relevantes.

Objetivos de control	Cómo auditarlo
Análisis del nivel de esfuerzo (recursos, inversiones económicas, etc.) de las opciones para el desarrollo con recursos internos o externos.	Evaluar, ya sea como un trabajo de aseguramiento a lo largo del desarrollo del proyecto, o como asesoría/consultoría (a petición de la Dirección), si en la gestión del proyecto se han tenido en cuenta o considerado las perspectivas/disyuntivas adecuadas.
Elaboración de un mapeo de fases y proveedores del proyecto.	Comprobar si: - Los servicios a contratar o desarrollar están determinados por fases desde el inicio a la implantación, para alcanzar los objetivos del proyecto. - Los costes de la tecnología a adquirir o seleccionar están identificados. - Se ha analizado la complejidad de la compatibilidad entre las soluciones ofrecidas por distintos proveedores que deben interactuar o confluir para la ejecución del proyecto (encadenamiento de proveedores subyacentes).
Conocimiento de los costes reales de los recursos necesarios.	Valorar: - La definición de los componentes de los recursos (recursos humanos y técnicos, control del proyecto, instalaciones, costes de software y similares). - La extensión y particularidad de la contratación de cada uno de los proveedores externos (recursos humanos) frente a los recursos internos presentes y futuros. - Los requerimientos de conocimientos y su adquisición (contratación) para el desarrollo interno. - Las licencias de uso por el software y similares, presentes y futuras. - La consideración de la gratuidad de determinado software para los usuarios (clientes). - La previsión de costes adicionales por mal funcionamiento. - La potencial conflictividad por una contratación en cadena de proveedores: cláusulas contractuales de protección para la empresa (responsabilidades y funciones de cada parte). - La dependencia en proveedores y recursos internos para el mantenimiento futuro de la infraestructura creada.

Objetivos de control	Cómo auditarlo
Efectividad del control del proyecto.	Valorar si: - Se ha determinado la centralización del control del proyecto. - Se ha analizado la pérdida potencial de control sobre los sistemas y configuraciones del software, por la intervención de diversos proveedores externos de tecnologías heterogéneas, complementarias y/o híbridas. - Se ha evaluado la trazabilidad futura de los servicios tanto en su comportamiento presente como en cambios (mejora continua) que se vayan sucediendo.
Requerimientos específicos a proveedores.	Verificar las certificaciones de proveedores (alcance y objetivo de la certificación, como empresa o del software o hardware adquirido), y seguimiento de su renovación mientras se mantenga el servicio acordado.
Otros aspectos.	Evaluar los acuerdos sobre: - Continuidad de negocio. - La salida ordenada, en caso necesario, hacia otras soluciones. - Las cadenas de proveedores.

Ejemplo de riesgo: Impacto negativo en la inversión por no tener en cuenta los aspectos mencionados.

RIESGOS ECONÓMICO-FINANCIEROS VINCULADOS A LA INVERSIÓN

Como en cualquier inversión, los riesgos económico-financieros son un factor fundamental en el análisis que se realiza. En la siguiente tabla solo se desarrollan aquellos riesgos económico-financieros que se consideran especialmente impactados por ser la inversión en una tecnología emergente.

RIESGO: VALORACIÓN INCORRECTA EN EL ANÁLISIS DE LA INVERSIÓN

Descripción: Dado que son tecnologías emergentes, suele haber pocas experiencias históricas y pocos estudios de mercado que permitan hacer una aproximación técnica a los ingresos a tener en cuenta para el cálculo del flujo de caja libre de la inversión, por lo que se ha de valorar si los ingresos considerados en los flujos de caja siguen los criterios usuales o se han incluido ingresos atípicos y, por tanto, pueden poner en duda la razonabilidad de su inclusión y su cálculo.

Objetivos de control	Cómo auditarlo
Razonabilidad del cálculo.	Considerar en el análisis de la inversión si los objetivos de negocio y los objetivos de las áreas que lideran los procesos de transformación digital, o las áreas técnicas, están influyendo en la valoración económica de la inversión porque haya introducido ciertos sesgos o parámetros no usuales a considerar en los flujos de caja.

Ejemplo de riesgo: Errores o falta de rigor en la valoración de eficiencias en los procesos: ahorros de costes directos e indirectos (horas hombre), etc.

RIESGO: RENTABILIDAD NO ADECUADA

Descripción: Es posible que estas inversiones no sean aprobadas siguiendo los requerimientos de las inversiones más tradicionales.

Objetivos de control	Cómo auditarlo
Asignación y priorización de inversión adicional para este tipo de tecnologías emergentes o *startups.*	Evaluar cómo se está asignando/priorizando la inversión en estos proyectos, tal y como una bolsa presupuestaria específica.
Definición y uso de criterios específicos de rentabilidad en inversiones en tecnologías emergentes.	Revisar si la rentabilidad está calculada de acuerdo con los criterios de la empresa. Debido a que estas inversiones tienen unos riesgos diferentes no incluidos generalmente en la tasa de descuento habría que revisar si la rentabilidad exigida se está ajustando a esos niveles de riesgo.

Ejemplo de riesgo: En el proceso de aprobación de la inversión en una tecnología emergente no se pide una rentabilidad superior (para compensar el riesgo) ni un plazo de recuperación de la inversión *(payback)* más corto (para asegurar que los ingresos son suficientes para compensar la inversión en un breve plazo de tiempo).

Descripción: Escenario para la valoración de la inversión y estimación de evolución flujos de caja que no tiene en cuenta la madurez y continuidad de la tecnología.

Objetivos de control	Cómo auditarlo
Cálculo de *payback* ajustado a escenarios específicos de la inversión.	Analizar si el *payback* requerido es el ajustado para poder recuperar la inversión.

Ejemplo de riesgo: Contratación de un servicio a un proveedor o implantación de una nueva tecnología en los procesos existentes, que una vez puesta en marcha no encaje adecuadamente, no tenga lo controles necesarios, o sea incompatible con el resto de los sistemas.

RIESGO: LIQUIDEZ

Descripción: No contar con un presupuesto firme y realista de CAPEX/OPEX que, en el caso de tecnologías emergentes en fase de desarrollo, resulta complicado realizar una adecuada estimación de la inversión.

Objetivos de control	Cómo auditarlo
Gestionar la ejecución del proyecto en términos de gastos operativos y de capital	En la fase de aprobación del proyecto, revisar que existía ese presupuesto para ejecutar la inversión En la fase de ejecución, valorar si existen o no desviaciones respecto a las partidas indicadas en el caso base y, por tanto, para las que inicialmente existe presupuesto. Si existen desviaciones, averiguar por qué se están produciendo. Comprobar si los trámites de aprobación de las partidas extrapresupuestarias están pasando por los comités correspondientes y no se están produciendo desviaciones de fondos.

Ejemplo de riesgo: Los retrasos en la entrega del producto por parte del proveedor pueden conllevar retrasos en la ejecución del proyecto que, a su vez, puede conllevar retrasos en la propia entrega y, en su caso, incluso exponerse a penalizaciones.

Descripción: Gestión inadecuada de compromisos de pago diferentes en función del escenario.

Objetivos de control	Cómo auditarlo
Incorporar los compromisos en la planificación del proyecto.	Chequear que las previsiones de flujo de efectivo del área incluyen el escenario vinculado al acuerdo y por los importes necesarios y suficientes.

Ejemplo de riesgo: No tener claro, en función del contrato con el proveedor, si se está comprando la tecnología o pagando por el uso de esta (licencias) y, por tanto, hacer una incorrecta previsión y gestión de pagos.

RIESGO: CONTABILIDAD Y REPORTE	
Descripción: En función del contrato con el proveedor, existen diferentes estándares contables aplicados para la contabilización del activo o del uso del mismo.	
Objetivos de control	**Cómo auditarlo**
Clarificar los estándares contables utilizados en el proyecto	En el caso de que la inversión en la tecnología emergente haya sido contabilizada como un activo de la empresa habría que verificar que los criterios seguidos para su amortización son acordes al caso de negocio presentado y aprobado, en cuanto a la vida útil del mismo.

RIESGO REGULATORIO Y DE CUMPLIMIENTO

Las tecnologías emergentes, como computación en la nube, implican que la empresa puede estar operando en un país y, sin embargo, sus datos (su información) pueden encontrarse en otra jurisdicción. Esta globalización implica que los riesgos regulatorios, de cumplimiento y geopolíticos deben estar bien presentes en el análisis de riesgos que se realiza cuando se abordan estas inversiones, conociendo la regulación concreta aplicable en cada caso.

La utilización de datos para el desarrollo de una nueva tecnología conlleva la responsabilidad y la obligación de custodiar los datos que sean personales, de forma responsable y de acuerdo con la normativa aplicable.

Tras la entrada en vigor en la Unión Europea del Reglamento General de Protección de Datos (en adelante, RGPD), en mayo de 2018, en los estados miembros es necesario considerar la privacidad por defecto y desde el diseño. Esto supone que la protección de datos debe ser un aspecto clave más a tener en cuenta durante el proceso de inversión de cualquier tecnología emergente.

En este contexto, se incluyen a continuación algunos aspectos o cuestiones que deberían considerarse con el objeto de cumplir con el principio de la privacidad por defecto y desde el diseño, tanto desde un punto de vista general como para algunas tecnologías emergentes.

DISEÑO DE PROYECTOS	ELEMENTOS CLAVE PARA EL PRINCIPIO DE PRIVACIDAD POR DEFECTO
ASPECTOS GENERALES	• ¿Se ha involucrado al Delegado de Protección de Datos de la empresa para evaluar el impacto en el tratamiento de datos personales? • ¿Se ha tenido en cuenta la necesidad de cumplir con los principios normativos de la protección de datos desde el diseño y por defecto? • ¿Se han identificado los datos personales que pueden verse afectados por la nueva tecnología? • ¿Se ha confirmado si se va a realizar una transferencia internacional de datos personales? • ¿Se ha realizado una evaluación del impacto en las medidas de seguridad necesarias para garantizar que la implantación de una nueva tecnología no va a afectar a la seguridad de los datos personales que se vayan a utilizar? • ¿Se han tenido en cuenta las guías emitidas por la Agencia Española de Protección de Datos[6], relacionadas con la aplicación de los principios de protección de datos de carácter personal desde la perspectiva de los desarrollos innovadores y de su aplicación técnica?

6. https://www.aepd.es/guias/index.html

DISEÑO DE PROYECTOS	ELEMENTOS CLAVE PARA EL PRINCIPIO DE PRIVACIDAD POR DEFECTO
COMPUTACIÓN EN LA NUBE	• ¿Se han analizado los datos que se van a migrar a la nube para comprobar si son personales o no? • ¿Se va a encriptar la transmisión de datos entre la empresa y el proveedor de servicios en la nube? • ¿Se ha previsto un plan de recuperación de la información en la nube?
ROBOTIZACIÓN DE PROCESOS *(ROBOTIC PROCESS AUTOMATION* O RPA)	• ¿Se ha definido la información que se va a tratar y si la misma es personal o sensible? • ¿Se ha acordado qué personas podrán acceder a la información que procese el RPA? • ¿Se conoce dónde se va a transmitir la información procesada por el RPA?
GESTIÓN MASIVA DE DATOS *(BIG DATA)*	• ¿Existe una política de gestión de los datos que permita conocer la trazabilidad de los datos y las personas que la van a utilizar? • ¿Se ha definido la finalidad del tratamiento de la información que se va a analizar y quién la va a utilizar? • ¿Existe interés por comercializar esta información y, en su caso, se ha previsto obtener el consentimiento de las personas afectadas?

En base a los elementos descritos previamente, se indican a continuación los principales riesgos que habrá que afrontar:

RIESGO: PROTECCIÓN Y PRIVACIDAD DE DATOS

Descripción: No cumplir con regulaciones de protección y privacidad de datos.

Objetivos de control	Cómo auditarlo
Las plataformas colaborativas, las bases de datos de almacenamiento y los reportes navegables y visualizables desde aplicaciones están adecuadamente securizados.	Verificar si: - Se conoce no solo dónde se encuentra la infraestructura y cómo está protegida, sino dónde está la plataforma de almacenamiento de datos. - La plataforma de almacenamiento de datos puede moverse sin consentimiento por parte del propietario.

Ejemplo de riesgo: Las herramientas actuales permiten tener la infraestructura en países europeos con normativa desarrollada, pero los datos personales están almacenados en países sin regulación alguna.

RIESGO: NORMATIVA CONTRA EL ABUSO DE MERCADO O SOBRE EL USO DE INFORMACIÓN PRIVILEGIADA

Descripción: No cumplir con la normativa que pretende evitar prácticas abusivas en el mercado y delitos vinculados al uso de información privilegiada, de especial importancia en empresas cotizadas.

Objetivos de control	Cómo auditarlo
La información está adecuadamente catalogada (sensible, confidencial, privada, pública…) y se establecen las medidas de seguridad necesarias y suficientes.	Comprobar que la nube donde las empresas tienen almacenados los datos tiene garantías de seguridad necesarias y suficientes, acordes con la sensibilidad de la protección que se está almacenando.

Ejemplo de riesgo: Los datos de las empresas y, en muchos casos, los *data lakes* están siendo almacenados en la nube, dado que esto otorga flexibilidad para manejarlos, pero podría perderse control sobre ellos.

RIESGO: NORMATIVA SOBRE INFRAESTRUCTURAS CRÍTICAS

Descripción: Cuando la inversión en tecnologías emergentes impacta sobre activos catalogados como infraestructuras críticas en el plan nacional de protección de infraestructuras críticas, no cumplir con la normativa correspondiente, al ser estructuras que están sobreprotegidas en las que no debe producirse un incidente grave.

Objetivos de control	Cómo auditarlo
Existencia de un análisis de riesgos detallado y profundo con el posible impacto que podría tener en los procesos productivos y operativos.	Revisar que existe un análisis de los riesgos mucho más detallado y profundo y del posible impacto que podría tener en los procesos productivos y operativos (por ejemplo, la gestión de accesos, monitorización de alteraciones o la revisión periódica de las configuraciones de seguridad).
Existencia de controles más allá de que estén establecidas contraseñas seguras, hacer copias de seguridad y que todo el entorno de la empresa funciona correctamente, para garantizar la continuidad operativa de estas infraestructuras.	Revisar el proceso de gestión de contraseñas, copias de seguridad, etc. que garantizan una continuidad en la operativa.

Ejemplo de riesgo: En ocasiones, se instalan dispositivos para operar los activos críticos cuya seguridad depende del proveedor contratado.

RIESGO: NORMATIVA INTERNA

Descripción: Las políticas y procedimientos internos de la empresa no están adaptados a las inversiones en tecnologías emergentes.

Objetivos de control	Cómo auditarlo
Desarrollo de procedimientos específicos para cubrir la especificidad.	Comprobar la adaptación de la normativa interna de la empresa al nuevo contexto de inversión.
Modelo de gobierno para la generación/inversión en esas tecnologías emergentes.	Verificar que existen unas adecuadas políticas y procedimientos, roles y responsabilidades y formación y concienciación sobre la materia.
Aplicación de las políticas y procedimientos internos definidos por la empresa.	Una vez definido el marco de gobierno, verificar no solo que esté adecuadamente diseñado, sino también que esté siendo efectivo.

Ejemplo de riesgo: Posibles incumplimientos de la normativa interna de segregación de funciones por la implantación de robots.

RIESGOS DE SEGURIDAD (CIBERSEGURIDAD)

En el contexto actual de transformación digital, el volumen de datos que manejan las empresas, su relevancia y el valor de los mismos se incrementan. Por ello, los datos y la información que con ellos se obtiene forman uno de los activos estratégicos de cualquier empresa y, por ende, son cada vez más uno de los objetivos principales de los ciberdelincuentes.

Al mismo tiempo que las tecnologías emergentes pueden permitirnos desarrollar soluciones que nos ayuden a detectar y evitar incidentes de ciberseguridad, también pueden

ser aprovechadas para desarrollar nuevos tipos de ataques.

Por lo tanto, en el desarrollo de cualquier tecnología emergente la ciberseguridad es un aspecto que debe tenerse en cuenta desde el principio.

El Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, es de aplicación a un amplio número de sectores y subraya la importancia de la fiabilidad y seguridad de las redes y los sistemas de información para el correcto desarrollo de las actividades económicas y sociales. Asimismo, contempla la necesidad de contar con medidas para gestionar los riesgos en las redes y sistemas de información que utilizan.

En definitiva, el uso de tecnologías emergentes puede aportar enormes ventajas, pero, a la vez, expone la información que trata a amenazas externas que deben identificarse para poder implantar los controles necesarios. Por lo tanto, Auditoría Interna debería evaluar los siguientes aspectos:

- ¿Se ha involucrado al área de Seguridad, en particular al Director de Seguridad de la Información *(Chief Information Security Officer* - CISO)?
- ¿Se ha realizado una evaluación de los riesgos de ciberseguridad derivados de la nueva tecnología que se está abordando?
- ¿Los desarrollos que han dado lugar a la nueva tecnología se han realizado bajo la metodología de desarrollo seguro de modo que el software (o incluso el hardware) no aflore "sorpresas no deseadas"?

RIESGO: INCREMENTO DEL PERÍMETRO EXPUESTO

Descripción: Incremento de la superficie de ataque al exponer un mayor número de sistemas y servicios a Internet, lo que aumenta las posibilidades de las que dispone un atacante para encontrar y explotar vulnerabilidades y entrar a los sistemas.

Objetivos de control	Cómo auditarlo
Sistemas y servicios correctamente configurados, parcheados y actualizados y que las medidas de control de acceso son adecuadas.	Comprobar que la empresa (normalmente el área de Seguridad) realiza análisis periódicos sobre el control de acceso, bastionado y parcheado de los elementos de infraestructura.
Creación de registros *(logs)* de los distintos eventos que ocurren en los servicios y sistemas, que permitirán investigar cualquier incidente y atribuir responsabilidades.	Comprobar que los procedimientos operativos incluyen la necesidad de generar *logs* de los sistemas y que se han establecido mecanismos para evitar que los usuarios puedan alterarlos.
Monitorización activa de los *logs*, para detectar posibles incidentes de seguridad y poder evitarlos o actuar lo antes posible.	Comprobar si la empresa monitoriza los logs generados. Por ejemplo, a través de un sistema de gestión y correlación de eventos (SIEM).

Ejemplo de riesgo: Las empresas cada vez están más conectadas y tratan de ofrecer un mayor número de servicios digitales tanto a empleados como a clientes y proveedores, de manera que estos servicios son accesibles desde cualquier parte del mundo con cualquier tipo de dispositivo, incrementando la posibilidad de ataque y sus orígenes o destinos.

RIESGO: CIBERSEGURIDAD EN LA NUBE

Descripción: Las empresas que ofrecen servicios en la nube no son inmunes a sufrir un incidente.

Objetivos de control	Cómo auditarlo
Indicación en el contrato de las medidas de seguridad establecidas y las responsabilidades en caso de sufrir un incidente.	Evaluar si las medidas de seguridad establecidas en los contratos con proveedores *cloud* son suficientes. Comprobar que la responsabilidad en caso de sufrir un incidente está definida y es acorde a los intereses de la empresa.

Ejemplo de riesgo: Las empresas en la nube suponen un objetivo muy suculento para los cibercriminales, ya que una brecha en estas empresas puede dar acceso a información de numerosos clientes.

RIESGO: CIBERSEGURIDAD EN INTERNET DE LAS COSAS (IoT, *INTERNET OF THINGS)*

Descripción: Las medidas de seguridad con las que cuentan los dispositivos *IoT* no son lo suficientemente fuertes y, a menudo, estos dispositivos son vulnerables.

Esta situación es aprovechada por los ciberdelincuentes, bien para obtener acceso a la red, bien para utilizar el dispositivo en la realización de otros ataques *(botnets).*

Objetivos de control	Cómo auditarlo
Seguridad de que el firmware de estos dispositivos se encuentra actualizado.	Comprobar que los dispositivos *IoT* también se incluyen dentro del proceso de parcheado.
Establecimiento de controles que mitiguen los riesgos asociados a la conexión (crear una red específica para dispositivos *IoT* separada de la red interna, establecer reglas restrictivas en los *firewalls* para este tipo de conexiones…).	Comprobar que los dispositivos *IoT* se encuentran en una red controlada y protegida, separada de la red interna.

RIESGO: SOFISTICACIÓN DE CIBERATAQUES

Descripción: Sofisticación de las herramientas y técnicas utilizadas por los ciberatacantes.

Objetivos de control	Cómo auditarlo
Uso de herramientas avanzadas de detección y prevención de intrusiones (IDS o IPS), así como de software heurístico de detección de *malware*.	Valorar si las herramientas y mecanismos de detección y prevención de intrusiones de la empresa son suficientes y acordes a la relevancia de los activos a proteger.

Ejemplo de riesgo: *Malware* inteligente que se adapta y muta en función del entorno las necesidades.

Concienciación y formación en materia de ciberseguridad para los empleados, ya que comúnmente es uno de los puntos débiles aprovechados por los ciberdelincuentes.	Comprobar si la empresa realiza periódicamente campañas de concienciación.

Ejemplo de riesgo: La identificación de anomalías en el comportamiento de los usuarios podría ser un indicio de un incidente de fuga de información, o anomalías en el tráfico de red/servidor web podrían ser un indicio de estar sufriendo un ataque.

RIESGOS DE COMPETENCIAS TECNOLÓGICAS EN LA ORGANIZACIÓN, INCLUYENDO LAS FUNCIONES DE CONTROL Y ASEGURAMIENTO

Con la irrupción de nuevas tecnologías, las organizaciones de hoy realizan cada vez un número mayor de transacciones y producen más datos asociados a sus operaciones de negocio. Por tanto, los equipos involucrados en tecnologías emergentes deben contar con conocimientos y herramientas para el análisis masivo de datos, robótica y aprendizaje automático e incluso conocimientos matemáticos y estadísticos. La organización debería utilizar la cantidad incremental de datos de forma que permita a la Dirección tomar decisiones de una manera más efectiva.

Además, a medida que aumenta el volumen de las transacciones, surge la necesidad de que las empresas respondan más rápidamente a los fallos de control. En particular, las funciones de control y aseguramiento, incluyendo Auditoría Interna, han de tener conocimientos y habilidades para responder a los avances tecnológicos que afectan a la industria donde opera la empresa, y capacidad de respuesta ágil para complementar sus conclusiones mediante el análisis masivo de datos.

RIESGO: LA ORGANIZACIÓN NO CUENTA CON LAS CAPACIDADES TÉCNICAS NECESARIAS

Descripción: A medida que aumenta el volumen de las transacciones, la empresa no responde rápidamente a los fallos de control.

Objetivos de control

Los equipos involucrados en tecnologías emergentes, incluyendo las funciones de control y aseguramiento, cuentan con los conocimientos y capacidades técnicas necesarias para desempeñar de forma competente sus tareas.

Cómo auditarlo

Cuestionar si los profesionales cuentan con las habilidades necesarias para responder a los avances tecnológicos que afectan a la industria donde opera la organización.

RIESGO: RETRASO EN EL USO DE NUEVAS HERRAMIENTAS PARA EL TRATAMIENTO MASIVO DE DATOS

Descripción: La organización no llega a utilizar la cantidad incremental de datos de forma que permita a la Dirección tomar decisiones de una manera más efectiva y a las funciones de control y aseguramiento complementar sus conclusiones.

Objetivos de control

Los equipos involucrados en tecnologías emergentes cuentan con conocimientos y herramientas para el análisis masivo de datos (extracción, tratamiento y visualización), robótica y aprendizaje automático *(machine learning)* e, incluso, conocimientos matemáticos y estadísticos.

Cómo auditarlo

Cuestionarse la necesidad y viabilidad de la implantación de nuevas herramientas que permitan a la organización, incluyendo las funciones con control y aseguramiento, cumplir sus funciones de forma competente y eficiente.

RIESGOS DE GESTIÓN DEL CAMBIO, INCLUYENDO EL IMPACTO EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA ORGANIZACIÓN

Los procesos de inversión deben observar con atención, y con cierto grado de anticipación, los riesgos derivados de los cambios por la introducción de nuevas tecnologías en la organización. Estos cambios pueden adoptar múltiples formas con diferentes efectos, que pueden suponer efectos en la organización (por ejemplo, creación de nuevos entes jurídicos, nuevos departamentos y gerencias); en los procesos (nuevos "caminos" de hacer otras cosas, reingeniería de los mismos); en los empleados (creando nuevas posiciones, simplificando plantilla, nuevas formas de trabajar); en la arquitectura tecnológica (dando de baja aplicativos sustituidos, generando nuevos conectores y controles); en costes y en otros aspectos que se ven impactados de forma directa o indirecta por ese proyecto y su implantación. Por tanto, es de importancia en la gestión y en el entendimiento de la inversión en estas tecnológicas –como lo es, en realidad, con cualquier proyecto que suponga un cambio– medir de forma proactiva los posibles impactos y consecuencias que el proyecto pueda tener para los diferentes *stakeholders*, desde los empleados hasta clientes. Sin duda, en la fase de implantación, la gestión del cambio es un factor a considerar para el éxito del proyecto.

Este ejercicio de anticipación y en cierto modo, de visión estratégica, de los impactos que puede tener una tecnología en los aspectos mencionados anteriormente, hace necesario que se valore de forma estricta y con visión de riesgos en la planificación y estimación de la inversión. Para Auditoría Interna debe ser un indicio de buena cultura de riesgos que estos aspectos sean contemplados junto con los económicos-negocios y los técnicos puros. La expectativa debería ser que los *Business cases* y/o los *Risk Assessments* incluyan este tipo de aspectos e impactos, de modo que las decisiones de negocio se nutran de suficiente información para afrontar de forma adecuada los riesgos tanto de la inversión como de sus consecuencias de implantación.

RIESGO: LA ORGANIZACIÓN NO HA IDENTIFICADO LOS IMPACTOS DE LA INVERSIÓN EN SU "ECOSISTEMA" TECNOLÓGICO

Descripción: Cambios en la arquitectura tecnológica sin adecuado análisis en sus riesgos e impactos en el modelo de servicio, gestión de riesgos o negocio.

Objetivos de control	Cómo auditarlo
Visibilidad objetiva y documentada de las implicaciones de una nueva arquitectura en la organización, con adecuados análisis de riesgos e impactos.	Revisión de los análisis realizados sobre la nueva arquitectura técnica y *challenge* sobre las decisiones adoptadas.

Descripción: El uso de nuevas tecnologías puede generar problemas de compatibilidad con la infraestructura tecnológica instalada.

Objetivos de control	Cómo auditarlo
Los equipos involucrados en tecnologías emergentes, junto con los equipos del CIO responsables de la producción y del CTO en su labor de estrategia tecnológica deben valorar los impactos y adecuación de la tecnología sobre los elementos instalados, en especial con los que va a interactuar.	Revisión de los análisis realizados sobre la arquitectura técnica existente y aquellos sistemas que se encuentren afectados por la futura instalación de nuevas tecnologías, poniendo atención a los efectos identificados y las potenciales soluciones o planes de acción planteados.

Descripción: Inadecuada gestión de aplicativos o sistemas que deben ser decomisionados o son redundantes.

Objetivos de control	Cómo auditarlo
Asegurar una gestión ordenada y adecuada de activos tecnológicos.	Revisión del plan de baja de activos (decomisionado) y de los efectos en el inventario.

Descripción: Falta de conocimiento del funcionamiento operativo de la nueva tecnología, originándose una serie de riesgos no controlados o que descansan en los proveedores sin una adecuada supervisión.

Objetivos de control	Cómo auditarlo
Identificación de los roles y responsabilidades de los diferentes *stakeholders* en la gestión de la nueva tecnología, y por tanto sus implicaciones en la organización de áreas de tecnología, seguridad y gestión de terceros (si procede).	Identificación de los aspectos que afectan a la organización (incluido el entendimiento de roles y responsabilidades) por la implementación futura de la nueva tecnología.

Conclusiones

La irrupción de nuevas tecnologías es una realidad y es imparable, y Auditoría Interna debe adaptarse para responder a este desafío con las máximas garantías. El objetivo es seguir proporcionando aseguramiento a la Comisión de Auditoría y a la Alta Dirección sobre los principales riesgos que afectan a la organización. De esta manera, Auditoría Interna podrá seguir actuando como asesor de confianza.

Para alcanzar estos objetivos y poder auditar las inversiones en tecnologías emergentes, Auditoría Interna precisa una comprensión profunda del razonamiento estratégico que subyace tras la inversión, un análisis minucioso de las características de dicha inversión y un conocimiento de los riesgos que pueden venir asociados a la misma, con el fin de ser capaz de identificarlos y valorarlos correctamente.

Por este motivo, aunque, a nivel metodológico, Auditoría Interna puede emplear un enfoque tradicional para auditar las inversiones en tecnologías emergentes, necesita nuevas capacidades y conocimientos para poder evaluar los riesgos tecnológicos. En este sentido, la evolución de Auditoría Interna debería ser paralela a la de la organización, a ser posible enriquecida por un equipo multidisciplinar.

Esto significa que hay que trasladar el entorno auditor (preocupaciones, metodologías, etc.) a un entorno de tecnologías diferentes afrontando un tipo distinto de auditoría, pero, en esencia, se trata del mismo proceder auditor de siempre.

En lo referente a auditoría de inversiones como tal, el hecho de invertir en tecnologías emergentes eleva la relevancia de aspectos cualitativos (por ejemplo, el modo en que se toman las decisiones o el nivel de conocimiento en aquello en lo que se va a invertir). No obstante, considerando aspectos cuantitativos, los controles sobre la inversión deberían ser equivalentes a los aplicados sobre otras inversiones menos disruptivas.

Una vez acometida la inversión e implantada la tecnología, para poder revisar el impacto de esta, es muy posible que Auditoría Interna precise modernizar su enfoque, apoyándose en capacidades tecnológicas adicionales y herramientas actuales de análisis basadas, a su vez, en nuevas tecnologías.

En definitiva, para auditar las inversiones en tecnologías emergentes, Auditoría Interna no debe modificar, *a priori,* su metodología de análisis y acercamiento a la materia, pudiendo efectuar la extracción de conclusiones y la definición de planes de mejora mediante un enfoque tradicional.

Sin embargo, sí resulta imprescindible, para extraer las conclusiones adecuadas, hacer las recomendaciones pertinentes y aportar valor y aseguramiento a la organización.

Auditoría Interna necesita nuevas capacidades y conocimientos para evaluar los riesgos tecnológicos, evolucionando a la par que la organización.

Bibliografía

- BACHMAIER, CARLOS; BLANCO, PABLO; FERNÁNDEZ, DIEGO; LOZANO, GUSTAVO; PONZ, DANIEL; RUBIO, JAVIER; SAGRADO, JAVIER; CIRIACO, ALFREDO; MATEOS, ASCENSIÓN; y MENDIOLA, MANUEL. *Retos en seguridad, control y auditoría de los servicios en la nube* [en línea]. [Consulta: 1 de julio de 2019]. Disponible en https://www.pkf-attest.es/wp-content/uploads/2019/06/Gu%C3%ADa_de_buenas_practicas_auditoria_riesgos_tecnologicos.pdf.
- COPNELL, T. *Tendencias disruptivas en la tecnología.* Noticias ACI 18. Enero, 2019.
- CENTRE FOR AUDIT QUALITY. *Emerging technologies: an oversight tool for Audit committees,* 2018.
- GARTNER. *Robotic Process Automatization (RPA) and Internal Audit.* 4 de marzo de 2019.
- GILES, MARTIN. Five emerging cyber-threats to worry about in 2019. *Mit Tecnnology Review.* Enero 2019.
- CNMV. *Guía Técnica 3/2017 sobre comisiones de auditoría en entidades de interés público.* Junio 2017.
- HEINEMEYER, MAX. *The Next Paradigm Shift: AI-Driven Cyber-Attacks, Dark Trace.* 14 May 2019.
- INTERNAL AUDIT FOUNDATION. *Aligning Internal Audit Activities and Scope to Organizational Strategy. How the Business Environment and Organizational Strategy Impact Internal Audit.* 2018.
- INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA. LA FÁBRICA DEL PENSAMIENTO. *Más allá del aseguramiento. El auditor como asesor de confianza.* 2017.
- KPMG. *Board´s-eye view of data and analytics.* 2018.
- KPMG. *Top 10 Considerations for impactful internal Audit departments in 2019.* 2018.
- KPMG. *20 key risks to consider by internal audit before 2020.* 2018.
- KPMG. *Impact of New Technologies on Audit and Assurance.* 2018.
- KPMG. *Are you ready for the next big wave? Make the right decisions about emerging technologies.* 2017.
- THE INSTITUTE OF INTERNAL AUDITORS. *Marco Internacional para la Práctica Profesional de la Auditoría Interna.* Enero 2017.
- PWC. *Internal Audit takes on emerging technologies.* 2012.
- PWC. *How can boards tackle the Essential eight and other Emerging technologies?* 2017.
- REAL DECRETO-LEY 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

PARA AMPLIAR INFORMACIÓN:

- https://www.nist.gov/
  - https://www.nist.gov/tpo/return-investment-roi-initiative - Return on Investment Initiative
  - https://www.nist.gov/cyberframework
  - https://www.nist.gov/topics/artificial-intelligence
  - https://csrc.nist.gov/publications/detail/sp/1800-21/draft - Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)
  - https://csrc.nist.gov/publications/sp - Computer Security Resource Center
  - https://www.nccoe.nist.gov/sites/default/files/library/sp1800/tc-hybrid-nist-sp1800-19b-preliminary-draft.pdf - Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments
  - https://csrc.nist.gov/publications/detail/sp/1800-16/draft - Securing Web Transactions: TLS Server Certificate Management –
  - https://www.nist.gov/news-events/news/2019/02/nist-blockchain-provides-security-traceability-smart-manufacturing
  - https://www.nist.gov/publications/nist-big-data-interoperability-framework-volume-4-big-data-security-and-privacy-version
  - https://www.nist.gov/publications/blockchain-technology-overview
  - https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program
  - https://www.nist.gov/publications/evaluation-cloud-computing-services-based-nist-sp-800-145
  - https://www.nist.gov/publications/cryptographic-key-management-issues-challenges-cloud-services

- Institute of Internal Auditors
  - Global Technology Audit Guide (GTAG): Understanding and Auditing Big Data - 2017
  - RISK IN FOCUS 2020 - Hot topics for internal auditors.

Anexo: Tecnologías y glosario de términos

Principales tecnologías emergentes

- ***Blockchain:*** es una estructura de datos en la que la información contenida se agrupa en conjuntos (bloques) a los que se les añaden metainformaciones relativas a otro bloque de la cadena anterior en una línea temporal, de manera que, gracias a técnicas criptográficas, la información contenida en un bloque solo puede ser repudiada o editada modificando todos los bloques posteriores. Esta propiedad permite su aplicación en entorno distribuido, de manera que la estructura de datos *blockchain* puede ejercer de base de datos pública no relacional que contenga un histórico irrefutable de información.

  Esta tecnología ha sido implantada, principalmente, en el mundo de las criptomonedas *(Bitcoin,* con origen en 2009) y se ha extendido a sistemas de pagos y para operativas de *trade finance*[7] (fundamentalmente para intercambio de información). Sus casos de uso todavía son limitados y continúan buscándose aplicaciones en diferentes industrias (principalmente la financiera).

- ***Cloud Computing*** o computación en la nube: es una tecnología que permite acceso remoto a software, almacenamiento de archivos y procesamiento de datos por medio de Internet, siendo así una alternativa a la ejecución en una computadora personal, servidor local o un centro de proceso de datos *(on premises).* En el modelo de *cloud*, no hay necesidad de instalar aplicaciones residentes en computadoras.

  La computación en la nube ofrece a los individuos y a las empresas la capacidad de un fondo *(pool)* de recursos de computación con buen mantenimiento, seguro, de fácil acceso y bajo demanda. Como consecuencia de su flexibilidad, escalabilidad y modelo de coste/precio se ha convertido en una solución estratégica para la mayor parte de los sectores industriales, al tiempo que ha favorecido que las grandes empresas tecnológicas (Amazon, Microsoft, Google) se hayan convertido en relevantes proveedores de servicios *cloud,* pivotando sobre ellos soluciones de diferente índole (IaaS - *Infraestructure as a Service;* PaaS - *Platform as a Service;* SaaS - *Software as a Service).*

- **Inteligencia artificial:** Andreas Kaplan y Michael Haenlein definen[8] la inteligencia artificial como "la capacidad de un sistema

7. *Trade Finance* se refiere a financiación de comercio exterior.
8. Artículo: *A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence* (Julio 2019)

para interpretar correctamente datos externos, para aprender de dichos datos y emplear esos conocimientos para lograr tareas y metas concretas a través de la adaptación flexible".

La inteligencia artificial ha estado muy presente desde hace años en la industria del videojuego si bien su expansión a otros sectores y usos está hoy en día muy extendida, con múltiples aplicaciones en procesos, controles y servicios. El uso de la inteligencia artificial está muy ligado a modelos (escenarios) de predicción y de los posibles resultados a futuro. Su atractivo es indudable, pero el debate sobre su regulación (que alcanza la ética) hace que la rodee un cierto nivel de incertidumbre.

- **Robótica:** ciencia o rama de la tecnología que estudia el diseño y construcción de máquinas capaces de desempeñar tareas realizadas por el ser humano o que requieren del uso de inteligencia. Las ciencias y tecnologías de las que deriva podrían ser: el álgebra, los autómatas programables, las máquinas de estados, la mecánica o la informática. Podríamos considerar que, en algunos casos de uso concretos, la robótica es un subconjunto de la inteligencia artificial.

  Como parte de esta tecnología citamos de forma especial los RPA *(Robotics Process Automatization)* que ha dado lugar a la automatización mediante robots (software) de tareas recurrentes y que permiten una optimización de tiempo y de recursos con poca o ninguna interacción humana

- **Internet de las cosas** (IoT en sus siglas en inglés, por *Internet of Things*): un concepto que nació en el Instituto de Tecnología de Massachusetts (Kevin Ashton a finales del siglo pasado, directivo de Procter & Gamble, concretamente en el Auto-ID Center del MIT celebrado en 1999). Se trata de una revolución en las relaciones entre los objetos y las personas, incluso entre los objetos directamente, que se conectan entre ellos y con internet y ofrecen datos en tiempo real. O, dicho de otro modo, la digitalización del mundo físico.

- ***Big Data:*** se refiere a conjuntos de datos o combinaciones de conjuntos de datos, estructurados o no estructurados, cuyo tamaño o volumen, complejidad o variabilidad y velocidad de crecimiento dificultan su captura, gestión, procesamiento o análisis mediante tecnologías y herramientas convencionales, tales como bases de datos relacionales y estadísticas convencionales o paquetes de visualización, dentro del tiempo necesario para que sean útiles.

- **Entorno 5G:** nueva generación de tecnologías y estándares de comunicación que incrementa ampliamente la velocidad de red, reduce la latencia e incrementa el número de dispositivos posibles conectados. Estas características ayudarán a impulsar la implantación y uso de elementos IoT y el desarrollo de nuevos modelos de negocio.

- **Otras tecnologías,** tales como asistentes de voz, *chatbots,* drones, impresión tridimensional (3D), o realidad virtual, entre otras, constituyen usos extendidos y emergentes que combinan parte de las tecnologías comentadas anteriormente con otros desarrollos emergentes y, todas ellas, aunque con finalidades diferentes, tienen objetivos comunes de eficacia, eficiencia y mejora de la productividad.

Otros términos

- Metodología *agile:* método para el desarrollo de software que permite incorporar cambios con rapidez y en cualquier fase del proyecto. Se trata de un desarrollo iterativo e incremental, donde los requerimientos y soluciones evolucionan a medida que lo hace el proyecto.

- Metodología *waterfall:* es utilizada en el desarrollo de proyectos, fácilmente trasladable a proyectos de tecnologías de información. La metodología *waterfall* también es conocida como modelo de desarrollo en cascada. Consiste en el desarrollo de un proyecto de manera secuencial: los requerimientos preceden al diseño y posteriormente se realiza la implementación.

- *Open source:* también llamado código abierto, se utiliza para denominar a cierto tipo de software que se distribuye mediante una licencia que le permite al usuario final, si tiene los conocimientos necesarios, utilizar el código fuente del programa para estudiarlo, modificarlo y realizar mejoras.

- Criptomoneda: un tipo de moneda virtual que se sirve del encriptado para garantizar seguridad a las transacciones bancarias hechas por Internet. Existen diversos tipos de monedas digitales: *Bitcoin* es la más conocida de ellas.

- SCADA: acrónimo de *Supervisory Control And Data Acquisition* (Supervisión, Control y Adquisición de Datos), es un concepto que se emplea para realizar un software para ordenadores que permite controlar y supervisar procesos industriales a distancia. Facilita retroalimentación en tiempo real con los dispositivos de campo (sensores y actuadores) y controla el proceso automáticamente. Provee de toda la información que se genera en el proceso productivo (supervisión, control calidad, control de producción, almacenamiento de datos, etc.) y permite su gestión e intervención.

- *Data lake:* es un repositorio de almacenamiento que contienen una gran cantidad de datos en bruto y que se mantienen allí hasta que sea necesario. A diferencia de un *data warehouse* jerárquico, que almacena datos en ficheros o carpetas, un *data lak*e utiliza una arquitectura plana para almacenar los datos.

- MVP *(Minimum Viable Product):* un producto mínimo viable es una versión de un producto que permite a un equipo recabar la mayor cantidad de aprendizaje validado sobre los clientes con el menor esfuerzo posible. Es una estrategia y un proceso enfocados en crear y vender un producto a un grupo de clientes.

- Fase beta: es una fase previa a la puesta en servicio, en el desarrollo de una aplicación informática o servicio de internet, durante la cual se prueban, en un entorno controlado, todas las funcionalidades del mismo, eliminando errores activamente.

- *Shadow IT:* se refiere a la tecnología de la información, las aplicaciones y la infraestructura que son gestionadas y utilizadas sin el conocimiento o control del área de Tecnología de Información de la organización.

- *Startup:* empresa que se encuentra en una etapa temprana o de nueva creación, con posibilidades de crecimiento.

- POC - *Proof of Concept:* Realización piloto de un cierto método o idea para demostrar su viabilidad.
- *Botnet:* Hace referencia a un conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática. El artífice de la *botnet* puede controlar todos los ordenadores/servidores infectados de forma remota.
- CAPEX y OPEX: CAPEX, acrónimo de *Capital Expenses* (gastos de capital), engloba aquellas partidas de compras o inversiones en bienes físicos que aumenten la capacidad productiva y que, son propiedad de la entidad. OPEX, acrónimo de *Operational Expenses* (gastos operativos), abarca la mayoría de movimientos de efectivo, costes de explotación, costes recurrentes de un producto, sistema o empresa, costes de empleados y alquileres de instalaciones.
- SIEM: *Security Information and Event Management,* gestión de eventos e información de seguridad.
- *Firmware:* Soporte lógico inalterable.
- *Malware:* Software maligno que trata de afectar a un dispositivo.
- IDS *(Intrusion Detection System):* Programa para detectar accesos no autorizados.
- IPS *(Intrusion Prevention System):* Programa para prevenir accesos no autorizados.

Glosarios adicionales

- National Institute of Standards and Technology (NIST). *Glossary of Computer Security Terminology.* https://www.nist.gov/publications/glossary-computer-security-terminology
- Information Systems and Control Association (ISACA). https://www.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf

Instituto de Auditores Internos de España

Santa Cruz de Marcenado, 33 · 28015 Madrid · Tel.: 91 593 23 45 · Fax: 91 593 29 32 · www.auditoresinternos.es

Depósito Legal: M-23825-2020
ISBN: 978-84-120500-8-0

Diseño y maquetación: desdecero, estudio gráfico

OTRAS PRODUCCIONES DE LA FÁBRICA DE PENSAMIENTO

AUDITORÍA INTERNA DE LA GESTIÓN DE PROYECTOS

Gestionar un proyecto implica planificar, organizar y dirigir el conjunto de procesos y operaciones diseñados para manejar el proyecto de inicio a fin. Este documento, basado en la metodología PMBOK del Project Management Institute (PMI), ayudará al auditor interno a afrontar la auditoría de un proyecto en sus diferentes fases, áreas de conocimiento y procesos.

MÁS ALLÁ DEL ASEGURAMIENTO. EL AUDITOR INTERNO COMO ASESOR DE CONFIANZA

La labor de Auditoría Interna abarca mucho más que el aseguramiento clásico: examina hechos, identifica mejoras, emite recomendaciones… Este documento define los roles de asesoramiento, identifica áreas y cualidades para llevarlos a cabo, y marca los límites y riesgos cuando Auditoría Interna realiza estas tareas.

AUDITORÍA INTERNA DE LA INFORMACIÓN EXTERNALIZADA

Las empresas deben garantizar la adecuada gestión de los riesgos derivados del acceso a la información externalizada por parte de terceros. Este documento recoge los principales aspectos normativos a considerar, y recomendaciones relativas al rol que Auditoría Interna debe desempeñar en el proceso de externalización, desde la fase de precontratación hasta la finalización de la prestación del servicio.

AUDITORÍA INTERNA DEL GOBIERNO DEL DATO

Aborda los problemas existentes y las mejores prácticas para resolverlos en lo referente a la definición de un buen gobierno del dato. Se analizan a fondo varios aspectos, desde el ciclo de vida del dato –incluyendo su trazabilidad y calidad– hasta metodologías y normativas aplicables en el proceso de gobierno del dato. Todo desde la perspectiva de Auditoría Interna.

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Las nuevas tecnologías provocan necesariamente la readaptación al medio y, dado el alto grado de automatización y de engranaje de procesos, las líneas de control se pueden diluir, siendo esencial redefinir el hábitat de Auditoría Interna.

Este documento incluye información para comprender mejor qué son y cómo evolucionan las tecnologías emergentes, el posicionamiento de Auditoría Interna frente a esas nuevas tecnologías, y un análisis de riesgos en una auditoría interna de inversiones en tecnologías emergentes.

Instituto de Auditores Internos de España
The Institute of Internal Auditors