Resumenes sesiones

Sesión 1: Los retos de los modelos de *compliance* y la seguridad

La sesión se estructuró en dos intervenciones claramente definidas, con dos visiones del *compliance*: una más técnico-jurídica y otra más tecnológica

Juan Luque comenzó presentando las vinculaciones entre las NIA-ES y el *compliance*, por la introducción de conceptos como la identificación de riesgos y el control de los mismos. Hizo especial hincapié en las NIA-ES 240 y 250 sobre el incumplimiento normativo, que constituye la puerta de entrada hacia el *compliance*, en un sentido amplio.

También vinculó el *compliance* con COSO, como el marco de referencia para la implementación, gestión y control del sistema de control interno y hizó un resumen de la evolución de COSO desde 1992 hasta la actualidad, momento en el que se pone el foco en la gestión estratégica de la compañía, indicando que el cumplimiento normativo está implícito en la propia gestión estratégica de la compañía.

A continuación presentó la evolución del *compliance* desde sus orígenes en 1977 hasta la actualidad y resaltó el carácter transversal del *compliance*, no sólo penal, sino también laboral, fiscal, medioambiental etc. A continuación presentó varios de los modelos o referencias para la implementación del *compliance* y sus características.

La última parte de su intervención la dedicó a las posibles actuaciones del auditor en esta materia: señalando que para ello contamos con estándares tales como la ISAE 3000, la ISAE 3402 y la ISRS 4400. Y por último explicó cuáles son los 8 retos del *compliance*, entre otros, la autorregulación de las entidades frente a la hiperregulación, la cultura del control en la organización y la ventaja competitiva del *compliance*, la tecnología y la seguridad en las organizaciones y que el *compliance officer* no se vea como una figura aislada sino integrada en todas las áreas del negocio.

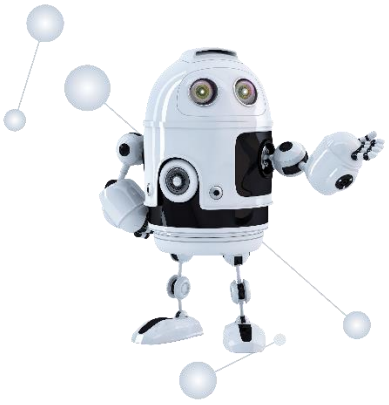
Óscar López explicó qué está pasando en las empresas, cómo han evolucionado hacia un entorno tecnológico y cómo afrontar el *compliance* bajo estas premisas. Los principales retos del *compliance* en materia de tecnología son: la protección de los datos, la seguridad de la información, la protección del consumidor y el comercio electrónico, entre otros.
A continuación abordó el *compliance* y el gobierno IT, cómo los departamentos IT han de gestionar los riesgos y también hizo mención a cómo la regulación financiera cada vez está más enfocada al *compliance*.

Sesión 2: Nuevas herramientas para los auditores en la era digital

A lo largo de la sesión se hizo un análisis de las herramientas de las que disponemos para realizar una auditoría. Comienzó Manuel Cortes indicando que en el año 2000 tan solo teníamos Lotus 123 y hoy en día tenemos *cloud, big data, data analytics*, robots… Si o si vamos a tener que utilizar la tecnología y esto nos va a ayudar a ganar eficiencia, adaptarnos, hacer la auditoría con más calidad, también nos ayuda a corregir errores manuales y disminuir los riesgos a los que nos enfrentamos.

A continuación, pasó a describir cada una de estas herramientas:

- *Cloud*: Trabajar en *cloud* nos permite tener una única versión de un documento.
- *Big data*: Nos permite coger información de los clientes, tratarla y obtener conclusiones para focalizar el trabajo en los riesgos, así como realizar una auditoría continua para ir sacando conclusiones parciales, lo que nos permite desestacionalizar la auditoría.
- Con ACL y macros predefinidas podemos hacer más de 100 pruebas similares y más homogeneas.
- Robots: Son pequeños procesos que automatizan tareas.
- Herramientas para documentación: Se puede llegar a no utilizar papeles. Las bases de datos con gestión documental de plantillas tienen un esqueleto de *Excel* y *Word* dónde hay pruebas predefinidas para homogeneizarla, con lo que se estructuran las tareas y aumenta la eficiencia. También ayuda a ordenar la información, alertando cuando alguien no realice una tarea o lo haga fuera de tiempo. Un ejemplo de esto es *Project planning* de Microsoft, para planificación de tareas, que da información de quien lo hace, cuando lo hace y porque no lo hace.



A continuación, nos indica cosas que están viniendo, como es el *blockchain* y la ciberseguridad para poder afrontar los cambios. Concluye que a la tecnología no hay que tenerle miedo porque nos ayuda y existen soluciones sencillas que nos solucionan el día a día.

A continuación, Sergio González-Isla relacionó las herramientas que ya se pueden utilizar, explicando las ventajas e inconvenientes de cada una de ellas.

1. Herramientas de documentación**,** las cuales nos facilitan la gestión de proyectos y garantizan la consistencia de los procedimientos:

Tipo	Nombre	Ventaja	Inconveniente
Flujogramas	Microsoft Visio, Word, Power Point, excel	- Funcionalidades - Coste	- Coste por licencia - No tiene funcionalidades añadidas
Colaboración	*Skype y Teams Sharepoint* de colaboración	- Eliminan muchos correos electrónicos - Permiten teletrabajo - Presentaciones a distancia	
Envío de datos	USB	Encriptado	Requiere transportarlo, se puede perder
	SFTD	Envío instantáneo por internet	Requerimientos legales a tener en cuenta

Herramientas de extracción de datos, que requieren tener un script que instalo en el sistema del cliente para obtener lo que necesito; aunque la barrera es que al fichero a veces le faltan datos que necesito y hay que trabajarlos, si consigo los datos permiten estandarizar el análisis y automatizar el proceso.

Tipo	Nombre	Ventaja	Inconveniente
Procesamiento de datos	IDEA y ACL	Enfocado a auditoría	Capacidad e procesamiento
		Interface amigable	Formación muy limitativa
		Funcionalidades específicas de auditoría - muestreo monetario …	
	SQL de Microsoft	Formación específica - enriquece CV	Es nueva y no específica para auditoría
	Alteryx		No pensada para auditoría
Visualización	Powe B.I. de Microsoft Tableau Qlikview Excel	Conexión directa con SQL	
Otras	Monitorización de redes sociales	Puede identificar riesgos reputacionales Sirve para análisis de hechos posteriores	No reconocen la ironía

Hay otras herramientas que en combinación con robots ayudan a automatizar un procedimiento manual, como OCR (reconocimiento óptico de caracteres), que ayuda a obtener información de cartas y contratos, aunque el inconveniente es que la información tiene que estar en el mismo sitio.

Para terminar, indica que también hay otras herramientas de “minería de procesos” como “Cetonis”, cuyo inconveniente es el coste por licencia, que en auditoría ayuda a confirmar que las transacciones han pasado por los controles que se han testeado.

Sesión 3. Daño causado por el administrador social: enfoque pericial

En la primera parte de la sesión Alicia Herrador dio respuesta los interrogantes que se plantean en una demanda contra los administradores societarios: ¿cuándo puede reclamarse el resarcimiento del daño?, ¿cómo se prepara la demanda? y ¿con qué argumentos puede rechazarse? Así, en primer lugar destacó los diferentes ámbitos de responsabilidad de los administradores sociales:

- responsabilidad mercantil/civil (cuatro tipos: responsabilidad contractual por daños causados a la sociedad o acción social de responsabilidad; responsabilidad extracontractual por daños causados a socios y a terceros o acción individual de responsabilidad; responsabilidad por no disolución o no solicitud de concurso de acreedores, que no tiene carácter indemnizatorio sino que se trata de una responsabilidad por deudas; y responsabilidad concursal),
- responsabilidad administrativa y, incardinada con ella en muchos casos, responsabilidad tributaria, pudiendo ser chocante que dichas responsabilidades del administrador sean cubiertas con pólizas pagadas por la sociedad, y
- responsabilidad penal.

Incidiendo más en la acción social y acción individual de responsabilidad (la responsabilidad civil clásica por daños), destacó los elementos necesarios para que prospere la demanda, cuya ausencia también será el argumento que esgrima la parte demanda para rechazarla. Así, respecto al ámbito objetivo de la responsabilidad, será necesario que haya un acto u omisión antijurídico (por ejemplo, irregularidades contables, despatrimonialización, paralización de la actividad, percepción de retribuciones no autorizadas por la junta, etc.), que se haya producido un daño (sin daño patrimonial no puede exigirse responsabilidad) y que exista una relación de causalidad entre ambos elementos. Respecto al ámbito subjetivo, la responsabilidad solo puede exigirse a los administradores, de hecho y de derecho, que lo eran en el momento en el que tuvo lugar el acto u omisión dañosos.

Concluyó su exposición destacando algunos aspectos de la responsabilidad por no disolución o no solicitud de concurso de acreedores y de la responsabilidad concursal.

Por su parte Victor Benedito incidió en los elementos a considerar en la preparación de un informe pericial por un experto en materias contable, económica y financiera, que pretenda acreditar la concurrencia del daño patrimonial y su cuantificación. En ese sentido, destacó que en la gran mayoría de casos la metodología de análisis a seguir por el perito tiene similitudes con el análisis de irregularidades económicas en contextos de fraude, por lo que deberán tenerse en cuenta tres elementos básicos: la conducta irregular, el *modus operandi* y las consecuencias; elementos de los que expuso ejemplos para cada uno de los tres tipos de conductas fraudulentas (excluyendo el soborno que tiene su tratamiento específico) en las que puede concretarse el concepto económico, que no jurídico, más amplio, de fraude: información financiera fraudulenta, apropiación indebida de activos y conflicto de intereses.

Finalizó la sesión recordando que la adecuada coordinación entre el perito y el abogado es imprescindible para que el informe pericial sirva a los efectos de fundamentar la demanda interpuesta o, si fuera el caso, la contestación a la misma.

Sesión 4: ¿Qué retos normativos tendrá que afrontar el auditor en el futuro?

Gemma Soligó inicia la sesión repasando los requerimientos que establece el artículo 28 de la vigente Ley de Auditoría de Cuentas (en adelante, Ley de Auditoría o Ley) sobre organización interna, requerimientos generales para los que habrá que ver si el Reglamento, cuando se publique, los concreta más. Recordó que la Ley establece que el responsable último del sistema de control de calidad debe ser un ROAC ejerciente y que es imprescindible una adecuada segregación de funciones. Recordó también que la Ley establece como obligatorios una serie de registros que deben estar actualizados y coincidir con la información que se remita al ICAC, entre los que se incluye el de infracciones graves y muy graves, para el que no se específica sí son las que haya podido identificar el propio auditor o las que haya impuesto el ICAC al auditor.

Repasó seguidamente los requerimientos establecidos en el artículo 29 de la Ley sobre organización del trabajo, remarcando que es necesario tener un archivo de auditoría para cada informe y que el auditor designado para realizar el trabajo debe cumplir con los requerimientos establecidos en la Ley incluyendo el hecho de que debe acreditar una participación activa en el trabajo. Repasó la consulta número 1 de auditoría del BOICAC 108 en la que se específica que la entrada en vigor de los diferentes apartados de la Ley. En concreto en relación a estos dos artículos de la Ley aclara que las cuestiones reguladas *ex novo* son exigibles para los trabajos de auditoría correspondientes a los ejercicios que se inicien con posterioridad al 17 de junio de 2016 y el resto, como mínimo a partir de dicha fecha. Finalizó su exposición resumiendo los aspectos de mejora aflorados por el ICAC en sus revisiones en relación a la organización interna y de los trabajos.

A continuación Silvia López destacó los siguientes aspectos sobre la organización interna:

- Que la asignación de responsabilidades debe estar formalmente aprobada.
- Que todos los aspectos regulados sobre el sistema de control de calidad interno tienen como base la norma de control de calidad y que cabe esperar que el Reglamento, cuando se publique, incluya requerimientos adicionales para garantizar una aplicación homogénea.
- Que cuando la Ley de Auditoría trata de procesos de administración fiable el fin es que los diferentes registros sean trazables.
- Que es necesaria una adecuada segregación de funciones entre los diferentes elementos del sistema de control de calidad, en especial en el de seguimiento, y que en caso de externalización de funciones, se incorpora ya el concepto de servicios compartidos.
- Obligación de un código ética y de cumplir determinados requisitos de comunicación.

En relación a la organización del trabajo indicó que el objetivo final es que todos los archivos sean electrónicos (independientemente del formato original) y que deberá definirse que se entiende por archivo. Recordó que la Ley de Auditoría, igual que la norma de control de calidad establece el plazo de 60 días para el cierre administrativo de los archivos y que posiblemente el Reglamento, cuando se publique, establezca la obligación de dejar evidencia del cumplimiento de dicho plazo con requerimientos adicionales de información al ICAC.

En relación al registro de infracciones al que se había referido Gemma Soligó, entiende que al menos deben constar las infracciones graves o muy graves declaradas mediante Resolución firme en vía administrativa por el ICAC.

A continuación explicó que a nivel internacional, la IAASB está revisando la norma de control de calidad —ISQC1— y trabajando en el desarrollo de una norma de revisión de control de calidad del encargo —ISQC2—.

La revisión de la ISQC1 tiene por objetivo modernizar la actual norma con un enfoque de gestión de calidad permanente, que sea preventivo de los riesgos y que sea una norma escalable para que cada auditor pueda adaptarla en función de sus características y circunstancias. La norma está planteada por objetivos de calidad en los que el auditor identifica y evalúa cuales son los riesgos para conseguirlos y así poder diseñar e implementar una respuesta adecuada, estando prevista su publicación para finales del 2018.

La ISQC2, norma de revisión de control de calidad de los encargos, establece los criterios a seguir por las firmas en la determinación de los encargos sujetos a revisión, los objetivos de la revisión, naturaleza, momento y extensión.

En la última parte de la sesión Josep-Domènec Salas trató sobre la auditoría de los grupos consolidados regulada actualmente por la Ley de Auditoría y la NIA-ES 600, norma que actualmente está siendo revisada por la IAASB. Centra su exposición en evaluar cuál debe ser la implicación del auditor del grupo en las auditorias de los componentes y hasta qué punto éste debe revisar la documentación de los diferentes componentes. Recuerda, en este sentido, que tanto la Ley como la norma establecen la plena responsabilidad del auditor del grupo, repasando las obligaciones que establece el artículo 7 de la Ley y la NIA-ES 600, incluyendo las obligaciones de documentación. También explicó las actuaciones a llevar a cabo por el auditor del grupo cuando no puede revisar el trabajo realizado por otros auditores y resumió los aspectos destacados en el plan de revisiones del ICAC en relación a las auditorías del grupo.

En este apartado interviene Silvia López indicando que al determinar la involucración del auditor del grupo, deben tratarse los estados financieros consolidados como si fueran una sola entidad y que el nivel de implicación se basa en la importancia relativa de los componentes pero que la interactuación debe ser permanente, debiendo quedar perfectamente documentada (cuestionarios detallados y firmados, revisión *in situ* o remota, etc.), lo que no implica necesariamente que deba tenerse copia completa de todos los papeles de trabajo.

Cerró la sesión presentación Josep-Domènec Salas explicando brevemente los aspectos que tienen una regulación específica para los auditores y trabajos de auditoría de las entidades de interés público, indicando Silvia López que está pendiente de incorporar la normativa española un registro con acreditación específica para los auditores de estas entidades.

Sesión 5: Ciberseguridad y protección de datos

En la actualidad, la ciberseguridad es un problema importante en el mundo de las empresas, dado que todos estamos sujetos a ataques cibernéticos.

En primer lugar, Andreu Bravo analizó la visión de la transformación digital, desde el punto de vista de la ciberseguridad y comienza aclarando un concepto: la transformación digital no es lo mismo que la digitalización, sino que es mucho más. La transformación digital supone aprovechar las nuevas tecnologías para hacer cosas que antes no se hacían lo que implica un cambio de modelo de negocio.

Lo que distingue la 4ª revolución industrial es la velocidad con la que se intercambia la información. El nuevo modelo supone un intercambio continuo de información que implica un cambio de paradigma y la aparición de nuevos retos y dificultades, pero también una serie de beneficios (p.e. el incremento de la seguridad física que supone la realización por máquinas de actividades antes realizadas por humanos).

La aparición de nuevas tecnologías, como la IoT (Internet de las cosas) o IIoT (Internet Industrial de las cosas) supone la aparición de nuevos riesgos y de amenazas hibridas, donde convergen tanto amenazas físicas como lógicas.

Además de los riesgos que arrastramos de las tecnologías industriales, hay 6 nuevos riesgos derivados de la ciberseguridad:

- tecnología poco testada,
- falta de perímetro,
- nuevos actores que quieren utilizar la tecnología con otros fines,
- amenazas hibridas,
- regulación tardía: para cuando se elabora ya forma parte del pasado, y
- falta de profesionales: son necesarios cientos de miles.

Desde el punto de vista de la privacidad también aparecen nuevos retos, como la información en la nube o la certificación de la información.

Otro tema relevante que cada vez preocupa más son las infraestructuras críticas. Se están identificando y regulando, pero la regulación siempre va bastante por detrás de la realidad. Quien pone las medidas de seguridad es la empresa., pero debería contar con el apoyo del Gobierno, no con la amenaza de un régimen sancionador.

A continuación, Albert Lladó analizó el nuevo Reglamento de la Ley Orgánica de Protección de Datos (en adelante, el Reglamento), que establece dos objetivos:

- Regular la evolución tecnológica y la globalización.
- Intentar armonizar la normativa sobre los diferentes niveles de protección de datos.

Entre los principios en que se basa el Reglamento, se incluyen dos grandes cambios:

- Hay que identificar el plazo de conservación de los datos.
- Responsabilidad proactiva: el responsable del tratamiento de los datos debe ser capaz de demostrar el cumplimiento de lo establecido en el Reglamento.

Otras novedades del Reglamento son:

- Algunos de los conceptos que se consideran datos de carácter personal (como datos de localización, identificador en línea o genética), así como algunas categorías especiales de datos personales (orientación sexual, datos genéticos o datos biométricos).
- Obligación de información al interesado sobre determinada información (delegado de protección de datos, plazo de conservación, derechos,etc.).
- Necesidad del consentimiento expreso de los interesados.
- Código de conducta y mecanismos de certificación, sellos y marcas.

Asimismo, surgen nuevas obligaciones:

- Protección desde el diseño y por defecto
- Registro de las actividades del tratamiento: no es necesaria la notificación de ficheros a la AEPD, pero hay que saber lo que se está haciendo.
- Evaluación de impacto: conocer el impacto, a través del análisis de riesgos de privacidad, para saber qué medidas de seguridad hay que aplicar.

- Medidas de seguridad: no se regula específicamente las medidas de seguridad que se tendrán que aplicar, sino que se limita a indicar que habrá que aplicar las medidas técnicas y organizativas adecuadas al riesgo que comporte el tratamiento.
- Encargos de tratamiento: el gran cambio es la obligación de diligencia debida en la selección de encargados.
- Notificación de las violaciones de seguridad.
- Delegado de Protección de Dtos (DTD): con diferentes niveles de acceso en función de sus características.

En cuanto a las infracciones y sanciones, la persona que denuncie tendrá derecho a una indemnización. El nivel de las sanciones hace que sea más práctico disponer de las medidas requeridas.

Sesión 6: Informes de auditoría: experiencias después de un año de aplicación

A lo largo de la sesión se visualizan tres videos que nos cuentan las experiencias que han tenido diferentes auditores en este primer año de aplicación de las NIA-ES revisadas sobre informes. Entre las apreciaciones realizadas durante los vídeos y el debate entre los ponentes destacamos:

1º vídeo: EIP vs no EIP

- Se audita y se planifica de forma diferente en una entidad de interés público (EIP) que en una no EIP.
- Respecto a la comunicación con los responsables de gobierno de las entidades (RGE) auditadas, se documenta e informa más en las EIP. En las EIP se requiere la comunicación por escrito de los aspectos relacionados con la independencia del auditor.
- Hay requerimientos para EIP que han caído en el ámbito de las no EIP: aspectos más relevantes de la auditoria (AMRA).
- Los requerimientos para las EIP son diferentes, es normal que los informes de auditoría sean diferentes.
- Es más complicado auditar una EIP.

Manuel V. Martínez presentó el estudio realizado por KPMG sobre las "Cuestiones clave en los nuevos informes de auditoría. Lecciones de la experiencia en 2017-2018". Comenta que en su firma emiten muchos más informes no EIP que EIP. La media de cuestiones clave por informe es de 3 para cotizadas y de 3,7 para las que componen el IBEX. Al no ser todavía públicos los informes no EIP, no se dispone todavía de un análisis similar para los AMRA.

2º vídeo: Modelos de informe

Emili Coll indica que, en firmas pequeñas, al no haber departamento técnico, los cambios y novedades como estos se afrontan por parte de los socios directamente. El socio de la firma que más cualidades tiene es el que asume el impulso y la expansión del conocimiento de las novedades dentro de la firma (formación interna/externa).

Manuel Martínez comenta que ya en el 2016 empezaron a hablar con los clientes no EIP sobre los nuevos informes. En un principio les extrañó mucho y no lo entendían, aunque ha ido evolucionando, sobre todo cuando ya han visto la redacción de los AMRA. Ha habido de todo, a quien ha gustado y a quien no. En EIP ha sido más fácil, en general la respuesta ha sido positiva.

Emili Coll comenta que su experiencia personal es que al final no era para tanto.

3º vídeo: ¿Cómo comunicar los AMRA?

La NIA-ES 260 está en vigor desde hace 3 años. No obstante, la NIA-ES 260 Revisada incorpora elementos nuevos que se derivan de la NIA-ES 701, por ejemplo la comunicación de los riesgos significativos.

En EIP está todo más reglado: comunicación a la Comisión de Auditoría de la EIP. En no EIP está menos estructurado.

El ICJCE ha sacado dos documentos sobre la comunicación con los RGE. Cuanto más comuniquemos los auditores mejor.

Para Emili Coll los pros y contras de los nuevos informes de auditoría se pueden resumir en:

PROS	**CONTRAS**
La opinión se sitúa en primer lugar	Informe muy largo
Más transparencia	Informe confuso: salvedades/ AMRA/ énfasis
Se comunica más y mejor	Redacción compleja
Se entiende mejor el rol del auditor	Mayor dedicación
Reflexión sobre los riesgos	Nuevo frente de discusión
	No homogéneo con UE (allí solo requerido para EIP)

El estudio de KPMG pone el foco en las empresas cotizadas. Su experiencia les lleva a concluir que los 3 o 4 cuestiones clave que más se reflejan en los informes de auditoría de las cotizadas, excluyendo la recuperabilidad del fondo de comercio, son también AMRA en los informes de auditoría de no EIP. Entre ellos están: reconocimiento de ingresos, provisiones, contingencias y litigios, recuperabilidad de activos por impuestos diferidos y recuperabilidad de activos no corrientes. Se espera también que se vaya reduciendo el número de cuestiones clave y su extensión.

Sesión 7: *Assurance*. Verificación de ámbitos no financieros

A lo largo de esta sesión, Patricia Reverter abordó cuales son las principales novedades en *reporting* de información no financiera así como el rol del auditor.

Respecto al *reporting* de información no financiera, destacó la publicación de Real Decreto-ley 18/2017, de 24 de noviembre, en materia de sobre información no financiera y diversidad (en adelante el RD-ley), aplicable a EIP con un determinado tamaño (>500 empleados), consecuencia de la trasposición a nuestro ordenamiento jurídico de la Directiva 2014/95/UE.

Si bien los requerimientos de información que establece este RD-ley no son nuevos (en España el 87% de las 100 mayores compañías ya los cumple), lo que se produce es una ampliación de los mismos, planteándose ciertos desafíos, entre otros, en cuanto a la determinación de los ámbitos a reportar, calidad de la información reportada, la participación de Consejo de Administración o el papel del auditor.

En este sentido, el contenido de la información, que según sus palabras ha de elaborarse bajo el principio de *cumple o explica*, debe ser el siguiente:

- Descripción del Modelo de negocio.
- Identificación, gestión y mitigación de riesgos.
- Políticas y debida diligencia para prevenir y mitigar riesgos adversos.
- Indicadores clave para lograr una información más comprensible y comparativa.
- Resultados: información equilibrada y concisa.

Destacó que si bien el RD-ley 18/2017 exige informar sobre determinados aspectos, no indica, por ejemplo, qué ratios o indicadores han de emplearse para ello, de manera que los responsables de su elaboración habrán de seleccionar el modelo a emplear, entre otros:

- *GRI*: Es el más común. Se basan en estándares universales que facilitan la información.
- *Informe integrado*: Se basan en la capacidad de crear valor de la compañía. Exigen referirse más al futuro y menos al pasado.

¿Y cuál es el papel del auditor? Actualmente, la norma solo exige que realice un chequeo, esto es, verificar que la información se ha suministrado. No obstante, existe cierta tendencia en el ámbito de la UE para que se incremente el nivel de revisión, de modo que se proporcione cierto nivel de *assurance*. En su opinión, en el plazo de 5 años se prevé un alcance en la revisión de la información no financiera asimilable a la auditoría.

Marga de Roselló centrósu exposición en dar una visión práctica y explicar en qué consiste un encargo de aseguramiento (NAAE, por sus siglas en inglés).
Un encargo de aseguramiento es aquel en el que un profesional independiente intenta obtener evidencia apropiada y suficiente para expresar en su informe escrito una conclusión sobre una información relativa a un tema o sobre una materia subyacente preparada por un tercero o parte responsable con el objetivo de incrementar el grado de confianza de los usuarios de esta información.

Todo encargo de aseguramiento debe incluir necesariamente todos y cada uno de los siguientes elementos:

- Relación de tres partes (profesional independiente, parte responsable y usuario)
- Materia/ objeto de revisión apropiado.
- Criterio de evaluación adecuado.
- Evidencia apropiada y suficiente.
- Conclusión (informe escrito).

La norma aplicable a un encargo de aseguramiento es la ISAE 3000R (revisada en 2015); no obstante, los encargos sobre emisiones de gases efecto invernadero se rigen por una norma específica (ISAE 3410). La estructura de la ISAE 3000R es la siguiente:

- *Alcance y objetivos*: Obtener cierto nivel de aseguramiento (razonable/limitado) y proporcionar una conclusión por escrito.
- *Aceptación del encargo*: se tienen que cumplir determinados requisitos para que el profesional independiente pueda aceptar el encargo (por ejemplo, existe un acuerdo sobre el encargo y una carta de contratación, el profesional espera obtener la evidencia que necesita, la materia objeto del NAAE es apropiada y consistente, sus criterios de preparación con adecuados y están disponibles para los usuarios, etc.)
- *Control de calidad y responsabilidades*: entre otros, cumplir con el Código de ética de IESBA, contar con conocimiento y competencia profesional, actuar con escepticismo y aplicar el juicio profesional.

- *Planificación, obtención de evidencia, procedimientos*: Son similares a una auditoría financiera aunque señala la importancia de contar con equipos multidisciplinares. Destaca la complejidad que tiene en este tipo de encargos determinar la materialidad, puesto que ha considerar qué es importante para los usuarios de la información. Así, debe considerar aspectos cualitativos y cuantitativos y requiere de mucho juicio profesional.
- *Informe*: La propia ISAE 3000R proporciona un modelo de informe. Su conclusión puede ser de dos tipos: 1) seguridad razonable, en el que se emite una conclusión positiva y 2) seguridad limitada, en el que se emite una conclusión en negativo.

Una vez dicho esto, ¿cuáles son los retos a los que se enfrentan los encargos de aseguramiento?. En su opinión son múltiples y contemplan aspectos tales como mejorar el entendimiento del informe, la madurez en los procesos de reporte, fomentar la claridad de las definiciones o incluso incrementar las directrices de IFAC.

Sesión 8: Relación entre el auditor interno y el auditor externo

La sesión se estructuró en dos intervenciones, la primera a cargo de Javier Faleato se centró en el trabajo realizado por el auditor interno y la segunda, de Daniel Artigas, en cómo emplear el trabajo del auditor interno siendo el auditor externo.

Javier Faleato comenzó explicando el modelo de control interno y gestión de riesgo basado en las 3 líneas de defensa:

- controles de negocio;
- el cumplimiento, control de riesgos y control interno; y por último
- la auditoría interna, cuyos principales retos son la independencia y la objetividad.

Las dos primeras líneas de defensa reportan a la alta dirección y la tercera a la alta dirección y al órgano de administración.

A continuación explicó que los auditores internos trabajan bajo las pautas definidas por las entidades auditadas y que es una profesión autorregulada, a diferencia de la auditoría externa. En cuanto al perfil del auditor interno, se busca un perfil multidisciplinar porque auditan todo tipo de procesos de negocio y la auditoría interna no ha de ser un área al margen de la organización sino que ha de estar alineado con la estrategia de ésta.
Desde la institución que Javier Faleato representa han preguntado a los directores de auditoría interna cuáles son a su juicio los principales riesgos a los que se enfrentan, y han señalado 9, entre los cuales, y sin que esto represente un orden de prioridades, destacan: ciberseguridad, complejidad regulatoria, innovación, incertidumbre política, gestión del riesgo en la cadena de suministro y la cultura de las organizaciones.

Daniel Artigas explicó que la relación entre el auditor interno y el externo la determinan los órganos de gobierno de la entidad.

El auditor externo si decide utilizar el trabajo del auditor verificará que el auditor interno cumpla con los requisitos de objetividad, competencia, diligencia y comunicación eficaz.
Asimismo, revisará la naturaleza y el alcance de las pruebas realizadas por el auditor interno y si los riesgos detectados por éste son los mismos que él ha identificado.

A continuación presenta la NIA-ES 610. El enfoque que el auditor externo da al trabajo realizado por el auditor interno es: o bien testeo independiente de las pruebas realizado por el auditor interno o bien retesteo de las pruebas que consiste en documentar el trabajo del auditor interno y valorar si el auditor externo está confortable con el trabajo realizado por el auditor interno.

A juicio de Daniel Artigas, es adecuado utilizar el trabajo del auditor interno, para los fines o el trabajo del auditor externo, para entender mejor los negocios, identificar adecuadamente los riesgos de fraude, identificar transacciones significativas, evaluar los procesos IT y verificar la idoneidad de la información producida por la entidad.

Sesión 10: La fiscalidad de las criptomonedas y de la nueva economía digital

Albert Sagués inició su exposición explicando brevemente el origen del *bitcoin*, basado en una cadena alfanumérica que permite la fragmentación de la titularidad, cuya seguridad se basa en el control que realizan los denominados *mineros* certificando la titularidad del código mediante los libros mayores (*ledgers*). La base de todas las criptomonedas es el *blockchain*, "tecnología que ha venido para quedarse" y lo que falta por ver es si los diferentes Estados serán capaces de regularlo.

Explicóque actualmente la mayor parte de las criptomonedas que circulan tienen un carácter meramente especulativo, para seguidamente debatir sobre qué calificación deberían tener. Explica que para calificarse como moneda debería ser un medio de cambio, depósito de valor y unidad de cambio y que, actualmente, las criptomonedas no cumplen la parte de depósito de valor debido a su alta volatilidad y, por tanto, no son propiamente una moneda pero que es necesario clasificarlas o etiquetarlas para poder, entre otros, centrar cuál es su fiscalidad, tanto a nivel de imposición directa como indirecta, que es el tema de esta sesión.

En la actualidad hay dos consultas de la Dirección General de Tributos, la CV1029-15 que las califica como otros efectos comerciales y por tanto establece que es una cesión a terceros de capitales propios y su renta tributa como rendimientos del capital inmobiliario y otra consulta la CV0999-18 (hay alguna consulta más en el mismo sentido) que indican que deben tributar como ganancias patrimoniales. También señala que en una consulta privada el ICAC las califica como intangibles, o existencias si se trata de una actividad habitual de la empresa, y por último señala que hay una propuesta de directiva en la que se califican como monedas virtuales.

Realiza un resumen de cuáles serían los diferentes impuestos directos a los que deberían estar sujetos:

- Patrimonio: Indica la dificultad de acreditar el valor a la fecha de cierre al no ser un mercado organizado, si bien actualmente existen *traders* reconocidos.
- Sucesiones: Señala la dificultad para acreditar la propiedad.
- IRPF: para este impuesto será el hecho económico el que marcará la tributación. Por ejemplo los *mineros* o los intermediarios tributaran como actividad económica y aquellas personas que lo posean como medio de ahorro o de pago por la alteración patrimonial que tenga la criptomoneda.
- En relación a la declaración del Modelo 720 se pregunta si es necesaria al no estar claro si entra o no dentro de la clasificación de bien en el extranjero.

- Impuesto sobre sociedades: indica que al determinarse la base imponible partiendo del resultado contable +/- los ajustes, como en el caso de las criptomonedas no hay ajustes, es necesario considerar la normativa contable (artículo 10.3 de la LIS) y plantea la problemática en función de la clasificación contable (intangible, cuenta a cobrar o inversión financiera) en aspectos como el deterioro y su deducibilidad, registro contable del resultado, etc., así como el posible enfoque como permuta.

En relación a la fiscalidad indirecta indica que la actividad de los *mineros* es una actividad económica sujeta a IVA, para la que es necesario establecer reglas de localización, ubicación de servidores, etc. y en relación al ITP es necesario ver si es un valor y, por tanto, una operación financiera.

Concluye señalando que es necesario regularlo. No se trata tanto de poner las criptomonedas en el sistema si no de reconocer que existen y que, aunque no se puedan controlar, debe indicarse que son y cómo deben tratarse. Recomienda que en caso de auditar clientes que tengan criptomonedas les exijamos la máxima información posible en las cuentas anuales del tratamiento contable que han realizado —apunta que hay un problema de trazabilidad de la propiedad de estos instrumentos— y que por supuesto los clientes deben tributar por la posesión de estas. Cierra la sesión con una noticia de abril del 2018 en el que la Agencia Tributaria anuncia que ha programado formación en inspección sobre comercio electrónico y criptromonedas así como un plan para estudiar la incidencia fiscal de éstas.

Sesión 11: Neurociencia aplicada a los negocios

Con el objetivo de enfocar la sesión, Silvia Cubo comenzó aclarando a algunos interrogantes:

- ¿Cuál es el objetivo de la neurociencia? No es otro que tratar de explicar por qué sentimos como sentimos y como es el proceso por el que los humanos pensamos y tomamos decisiones.
- Y, ¿en qué consiste la neurociencia aplicada a la empresa? De manera sencilla, podemos decir que es explicar y conocer como la gente (empleados, directivos, …) piensa y actúa con el objetivo de aplicar este conocimiento al logro de los objetivos personales y empresariales. La idea subyacente es que en el trabajo hay que disfrutar.

Señaló que el proceso de toma de decisiones se asienta sobre tres bases: consciente, inconsciente y observable. Sólo procesamos de manera consciente una pequeña parte de la información que llega a nuestro cerebro; el resto, la almacenamos de manera inconsciente aunque también la utilizamos para tomar decisiones. De hecho, las personas no somos tan racionales como creemos, sino que tenemos nuestros sesgos.

Este proceso de toma de decisiones se desarrolla en las siguientes etapas:

1º. Procesamos la información.
2º. Determinamos su valor.
3º. Deliberamos y analizamos.
4º. Actuamos.

Explica que el cerebro tiene dos formas de procesar, una rápida y otra lenta. Esta última implica un mayor esfuerzo y consumo de energía, de modo que el cerebro siempre intenta de manera instintiva aplicar la forma rápida.

La neurociencia aplicada a la empresa se relaciona con múltiples elementos que forman parte de su organización, por ejemplo:

- Neuromanagement,
- Neuroliderazgo,
- Neurobranding (mi marca y como conseguir que mi cliente tenga un anclaje positivo con la misma siendo fundamental para ello no solo el logo, sino la personas y la imagen que proyecto)
- Neuroaprendizaje (explica cómo es el proceso de aprendizaje, con el objetivo de lograr que las personas aprendan; para ello es esencial que la información conecte, sino no hay aprendizaje).
- Neuronegociación.
- Gestión emocional.
- Comunicación (con mis compañeros, con mis clientes). Hemos de ser conscientes de que con nuestra forma de comunicar (verbal, no verbal, entonación, etc.) afectamos a los demás.

Xavier Sardá inició su exposición con esta última cuestión: la comunicación. ¿Por qué el interés en la comunicación? Porque es imprescindible para una adecuada gestión de proyectos y de personas.

A continuación, abordó determinados aspectos relacionados con la productividad personal. Así explicó que, a veces, las personas llegamos a lo que él denomina "puntos de bloqueo" que impiden actuar o que provocan una reacción emocional exagerada. ¿Cómo se puede mejorar?

En su opinión, con tres pilares básicos:

1. *Foco*: Prestar atención a una sola cosa. Si se tienen demasiados frentes abiertos, el cerebro se realentiza.
2. *Cambios de contexto*: Si se tienen muchas tareas a la vez cada vez le cuesta más al cerebro pasar de una a otra. Recomienda elaborar una lista, empezar una tarea y terminarla y no ir saltando de tarea en tarea; de esta manera no solo evitamos que el cerebro se bloquee sino que cada tarea cerrada, cada tarea tachada de la lista, provoca un efecto recompensa en el cerebro en forma de dopamina.
3. *Inhibición*: Se trata de una respuesta consciente que requiere de cierto entrenamiento por nuestra parte. Consiste en pensar en las consecuencias de una determinada acción e inhibirse de realizarla.

En su opinión, las reuniones de planificación, priorización, etc. tienen el efecto contrario al que se consigue con una lista de tareas. Con la lista lo que se logra es liberar al cerebro traspasando las tareas al papel; por el contrario, con la planificación se hace justo lo inverso, se traspasan las tareas del papel al cerebro de modo que este se "carga".

Respecto al estrés, señala que éste no siempre es malo; solo lo es si se cronifica o se mantiene a un nivel elevado. De hecho, sin un mínimo de estrés las personas no funcionamos ni aprendemos y cometemos los denominados "errores no forzados". No obstante, un cerebro estresado (un cerebro cansado) será incapaz de generar respuestas creativas porque se pone en "modo ahorro de energía" (ya no puede más).

Una fuente enorme de estrés es la incertidumbre. El cerebro humano, ante una situación de incertidumbre, está programado para asumir entre un rango de posibilidades aquellas más negativas porque son las que han ayudado a la especie a sobrevivir.

Por tanto, la gestión de la incertidumbre es una habilidad que hay que educar (en el fondo es una inhibición). La idea: relajarse y gestionarla.

Por último, ofreció tres pautas para mejorar la conectividad neuronal y, por ende, el rendimiento cognitivo:

- Desconecta
- Descansa
- Diversifica, porque refuerza las redes neuronales y ayuda a vivir mejor.

Sesión 12: Entender el *blokchain*

En primer lugar, Luz Parrondo explicó diversos conceptos relacionados con lo que es el *blockchain* y como nos puede afectar en el futuro.

Si bien Internet democratizó la información, *blockchain* lo que va a hacer es democratizar la creación de valor. Es decir, además de facilitar el acceso a la información, *blockchain* va a permitir que la creación de valor esté al alcance de todo el mundo y que todos aquellos que aportan valor tengan una recompensa por ello.

Blockchain es una cadena de bloques, cada uno de los cuales incluye información sobre una transacción. Estos bloques no contienen datos, sino información sobre la transacción mediante códigos numéricos, por lo que se precisa que cada uno de los objetos de la transacción este *"tokenizado*": es decir, que cada uno de ellos este identificado por un código numérico univoco. Esto permitirá establecer una trazabilidad perfecta de todos los elementos de la transacción.

Algunas de las características que presenta *blockchain* son que está totalmente descentralizada (todos los nodos que conforman la red *blockchain* tiene la misma información al mismo momento), es persistente (no se borra), es inmutable y es público y auditable.

Blockchain va a permitir que haya ecosistemas en los que las fronteras entre las empresas o las instituciones se van a derretir, porque todos tendrán la misma información en el mismo momento. Esta tecnología cambia la forma tradicional de hacer transferencias y va a afectar a los intermediarios, pero no se van a eliminar de manera total.

Es una tecnología DLT (*Distributed Ledger Technology*), aunque no nos debe preocupar como funciona esta tecnología sino como afecta a la manera en que nos relacionamos y las cosas que nos permite realizar.

A nuestros efectos *blockchain e*s como una gran base de datos en la que participan todos los actores que pertenecen a la misma. Es como estar en el ordenador, en el ERP de otra empresa.

Podíamos asimilarla a las vías del tren (la plataforma), sobre la cual circulan diferentes cosas (*bitcoins*, etc.). Hay diferentes vías de tren: la primera fue la de Bitcoin, pero posteriormente se fueron creando otras como Ethereum y otras que añadían a estas vías aplicaciones y accesorios ("*Smart contracts*") para darles mayor funcionalidad.

Uno de los aspectos fundamentales es cómo se realiza la validación de estas transacciones. La primera forma de validación fue a través de los denominados "mineros", quienes se llamaban así porque al validar las transacciones recibían a cambio *bitcoins* nuevos que ponían en circulación en el mercado (al igual que hace un minero cuando coge oro y lo pone en el mercado, como un medio de pago sin la intervención de ninguna institución financiera). Posteriormente se han ido creando otras maneras de validación. Al final, todo esto supone un "Banco Central de Internet", que las fronteras se diluyan y que las regulaciones deban tener un ámbito supranacional.

Todavía esta tecnología se encuentra en la prehistoria, pero todos los grandes quieren apropiarse de ella. Los primeros que han empezado a utilizarla son las entidades financieras y luego en el mundo empresarial las cadenas logísticas y los transportistas.

En el tema contable se habla de la triple contabilidad: p.e. en el momento en que una mercancía entre por tu puerta, al estar en un *ledger* compartido (en un *blockchain* que traspasa las fronteras de la empresa), la transacción estará enlazada automáticamente con tu contabilidad, pero habrá una tercera contabilidad que una las dos empresas involucradas.

Esta tecnología afectará de manera general a la gobernanza de las empresas, a su administración, a su fiscalidad, etc., pero donde ha tomado la delantera es en la financiación, abriendo nuevas formas de financiar a las empresas, como son las *Initial Coin Offering* (ICOs).

Lanzar una ICO es vender "*tokens*" (monedas de plástico) que circulan por un *blockchain*, dentro del cual se delimita cuáles son los limites por donde pueden circular y lo que se puede hacer con ellos. Estos *tokens* se emitían a cambio de una promesa futura (p.e. de un servicio), pero sin nada real en la actualidad, eso sí con un rendimiento importante, lo que llevo a una euforia de ICOs, debido a que los grandes inversores apostaron por ellos ante las bajas rentabilidades que se daban en otros mercados. Este fervor inicial de las ICOs está empezando a bajar, y también los fraudes que se producían con ellas, porque todo el mundo está más informado sobre estas operaciones y se están controlando más por los organismos reguladores de los países.

En algunos países (como Suiza) se ha comenzado a poner algo de orden en la gran diversidad de *tokens* que se han emitido y las consecuencias que tienen. Así, por ejemplo, desde el punto de vista de sus consecuencias legales se podrían clasificar en tres categorías: "*Utility Tokens*" (sirven para utilizar un servicio), "*Security Tokens*" (con derechos similares a los de las acciones o bonos) y "*Cryptomonedas*" (de pago). El problema es que, a veces, es difícil diferenciar cuales son unos u otros y la regulación es diferente para cada uno de ellos.

Para finalizar la sesión, Borja Sánchez comentó algunas reflexiones planteadas desde la Comisión de Jóvenes del Col·legi en relación con el mundo de la tecnología y la auditoría, basada en el impacto de la tecnología en tres ámbitos: en nosotros mismos, en los clientes y en las firmas de auditoría.

En primer lugar, respecto a nosotros mismos, aunque tenemos claro que no somos ingenieros debemos ser conscientes del entorno tecnológico y conocernos mejor.

Respecto a las empresas que auditamos, cada vez los procesos y los controles están más automatizados y las empresas están absolutamente informatizadas. Hay que reflexionar hasta qué punto le estamos dando la importancia que esto tiene y estamos considerando la necesidad de equipos especializados.

El tercer punto es sobre nuestras propias firmas de auditoría y debemos plantearnos si estamos informatizados.