Ciberseguridad en ESG

Es hora de que ESG y ciberseguridad sean vistos a través del mismo lente.

KPMG Internacional | kpmg.com/cybersecurity

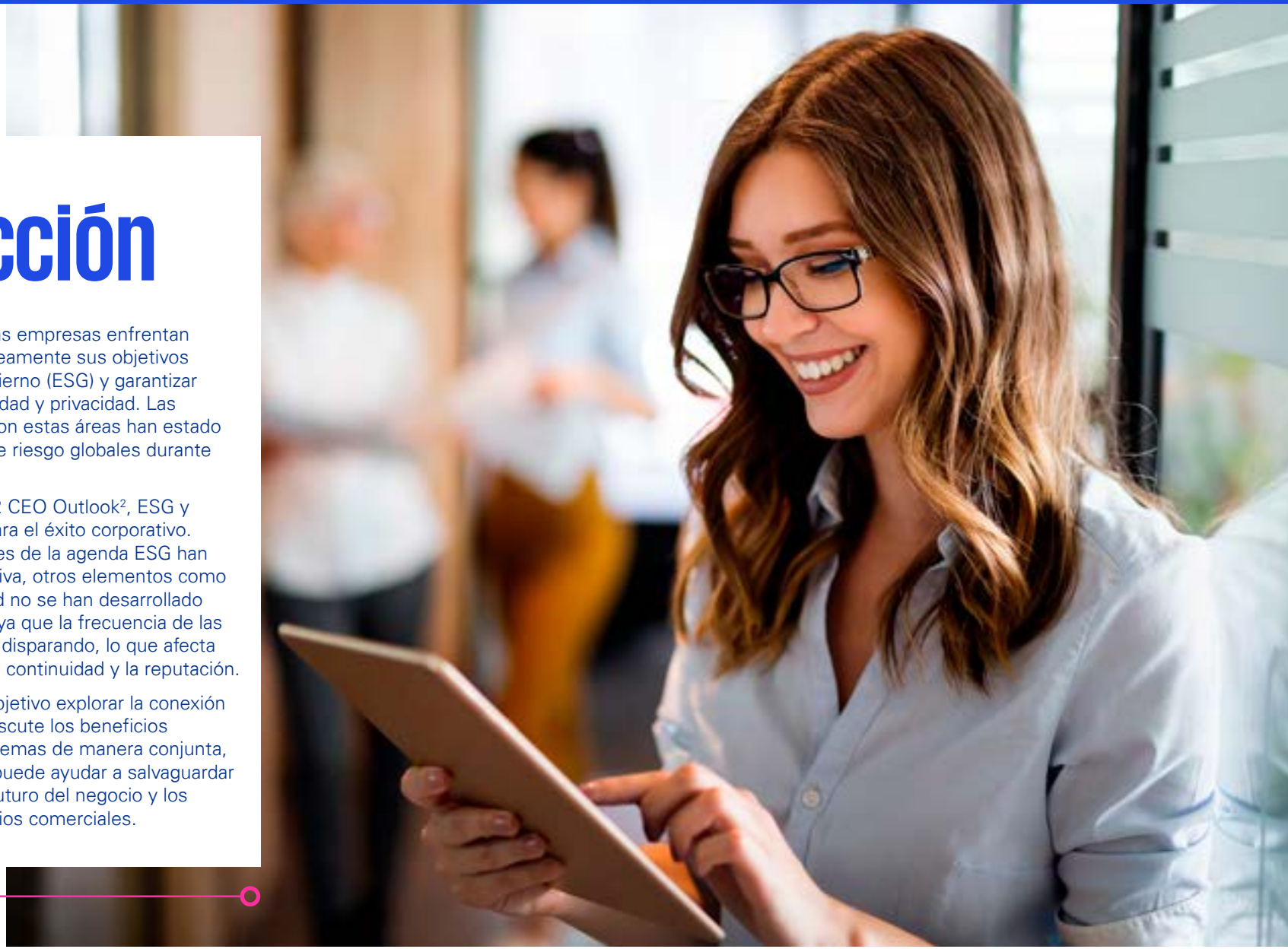
Contenido

Introducción

En la economía digital actual, las empresas enfrentan desafíos para cumplir simultáneamente sus objetivos ambientales, sociales y de gobierno (ESG) y garantizar medidas sólidas de ciberseguridad y privacidad. Las preocupaciones relacionadas con estas áreas han estado a la vanguardia en los mapas de riesgo globales durante varios años.[1]

Según la encuesta KPMG 2022 CEO Outlook[2], ESG y ciberseguridad son cruciales para el éxito corporativo. Si bien los aspectos ambientales de la agenda ESG han recibido una atención significativa, otros elementos como la ciberseguridad y la privacidad no se han desarrollado tan bien. Esto es preocupante ya que la frecuencia de las amenazas cibernéticas se está disparando, lo que afecta las operaciones comerciales, la continuidad y la reputación.

Este documento tiene como objetivo explorar la conexión entre ESG y ciberseguridad. Discute los beneficios esperados de gestionar estos temas de manera conjunta, y cómo un enfoque integrado puede ayudar a salvaguardar la salud de la organización, el futuro del negocio y los intereses de sus clientes y socios comerciales.



[1] www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf
[2] KPMG 2022 CEO Outlook 2022

Consideraciones medioambientales

La infraestructura crítica se enfrenta a nuevos riesgos significativos

Cuando se trata de ESG, los factores ambientales son una consideración clave. Sin embargo, el vínculo de ESG con la ciberseguridad, aunque menos obvio, se está convirtiendo en cada vez más importante. Según la encuesta de KPMG de 2022, el 64% de las empresas reconoce el cambio climático como un riesgo para su negocio.[3] Los profesionales de KPMG están empezando a considerar los ciberataques que ponen en peligro el medio ambiente al atacar infraestructuras críticas como centrales eléctricas e instalaciones de procesamiento de agua. Además, estos ataques a los sistemas de control industrial pueden causar mal funcionamiento de los equipos, daños ambientales y otros peligros. Las organizaciones necesitan una ciberseguridad sólida para proteger su infraestructura crítica contra las amenazas a su sofisticada e interconectada tecnología operativa. Como estos incidentes se vuelven más comunes, anticipamos un mayor enfoque regulatorio.

Conectar la seguridad con la descarbonización, la reducción de CO2 y la economía circular

La mayoría de los planes para la descarbonización y la reducción de CO2 se basan en la transformación digital y la aplicación de tecnologías inteligentes y sistemas automatizados que monitorean y gestionan la producción, distribución y consumo de energía. Sin embargo, estas soluciones pueden crear nuevas oportunidades para el cibercrimen y exigen un alto nivel de ciberseguridad y protección de datos.

Del mismo modo, la introducción de nuevas soluciones tecnológicas para apoyar la economía circular cuando esos sistemas implican transacciones financieras significativas para incentivar comportamientos ecológicos, puede generar preocupaciones sobre nuevos patrones de fraude.

La incorporación de la seguridad cibernética en estos programas puede ayudar a anticipar las amenazas y garantizar operaciones seguras. Al mismo tiempo, adherirse a los principios de protección de datos, como la minimización de datos, puede ayudar a reducir el riesgo de violaciones de datos y garantice el cumplimiento normativo.

La economía digital ha llevado a un aumento en el procesamiento de datos, lo que resulta en la construcción de centros de datos en todo el mundo. Los delincuentes han encontrado oportunidades para explotar las debilidades en la seguridad de los centros de datos y los servicios en la nube para robar recursos informáticos, incluida la minería de criptomonedas a escala. Desafortunadamente, el uso de estos sistemas tiene un impacto negativo en el consumo de energía y la huella de carbono; por ejemplo, implementar los controles cibernéticos requeridos o de mejores prácticas, como tener un centro de datos secundario para mejorar la resiliencia, puede conducir a un mayor uso de recursos y energía.

Las organizaciones de hoy deben considerar tanto los pros como los contras de la resiliencia cibernética, logrando un equilibrio con los objetivos de ciberseguridad y ESG.

[3] 'Grandes cambios, pequeños pasos'. Encuesta de informes de sostenibilidad, KPMG, 2022

Consideraciones sociales

Impactos en el panorama digital de la sociedad

Las consideraciones sociales también son un aspecto crítico de ESG, y el riesgo cibernético puede afectar significativamente a la sociedad, particularmente a medida que los ataques cibernéticos globales se vuelven más frecuentes e impactantes. Las aplicaciones y sistemas digitales ahora están integrados en todos los aspectos de nuestras vidas, desde los dispositivos personales en los que confiamos y las redes sociales con las que interactuamos hasta las sofisticadas plataformas y sistemas automatizados que respaldan los lugares de trabajo y estilos de vida digitales. La encuesta de KPMG de 2022 encontró que el 49% de las empresas reconocen los elementos sociales como un riesgo para su negocio.[4]

La protección de datos es fundamental

Esta integración puede hacerlo vulnerable a los riesgos cibernéticos que pueden conducir al robo de información personal y confidencial, lo que resulta en robo de identidad, fraude financiero y otros daños sociales. Los ataques cibernéticos también pueden interrumpir los servicios críticos de atención médica, transporte y emergencia. Para abordar estos riesgos, las organizaciones necesitan fuertes medidas de privacidad y ciberseguridad para proteger sus datos. Adicionalmente deben tener planes sólidos de respuesta a incidentes para minimizar el impacto de un ataque cibernético en los servicios críticos.

Los ataques de ransomware se disparan

Los ataques de ransomware lucrativos continúan aumentando a nivel mundial y pueden paralizar rápidamente las operaciones y la reputación de una organización. En medio de las graves consecuencias, muchas organizaciones se ven tentadas a pagar el rescate. Desafortunadamente, los pagos de ransomware solo fomentan más delitos y crean un ciclo costoso. Para combatir los ataques de ransomware, se deben implementar medidas modernas de ciberseguridad para minimizar su impacto social y financiero.

La libertad de expresión se enfrenta a nuevas amenazas

La privacidad y la ciberseguridad también desempeñan un papel vital en la protección de la libertad de expresión y en el aseguramiento de los canales digitales de comunicación actuales. Las protecciones legales, la promoción de la alfabetización digital y mediática, y el apoyo a la diversidad y la inclusión en los espacios en línea también son medidas importantes. Las tecnologías e encriptación pueden garantizar que solo los destinatarios previstos puedan acceder a la información sin temor a ser escuchados o vigilados. La ciberseguridad también puede ayudar a mitigar los efectos de los ataques disruptivos dirigidos a sitios web y plataformas en línea que facilitan la libertad de opinión y expresión.

Proteja la información del cliente para fomentar la confianza

Los controles de privacidad también pueden desempeñar un papel clave en la limitación de la explotación y el uso indebido de la información personal sin consentimiento o conocimiento. Esto es vital para mantener la confianza pública en las organizaciones.

Antes de regulaciones como el Reglamento General de Protección de Datos de la UE, muchas organizaciones creían que tenían la propiedad de los datos personales del público. Esto cambió con la introducción de estas regulaciones. Las personas ahora tienen derecho sobre sus propios datos personales, incluido el derecho a saber qué datos posee una empresa y el derecho a que se eliminen.

[4] 'Grandes cambios, pequeños pasos'. Encuesta de informes de sostenibilidad, KPMG, 2022

Nuevas preocupaciones sobre la IA y la ética de los datos

El uso de herramientas de inteligencia artificial (IA) puede acelerar la recopilación de datos, pero plantea nuevas preguntas sobre la ética en el uso que los algoritmos y el aprendizaje automático hacen de esa información. Los prejuicios pueden afectar injustamente a los individuos o a la sociedad en su conjunto.

Las organizaciones pueden tener un impacto positivo o negativo en la sociedad en función de cómo evalúan los riesgos y protegen los datos que procesan. Las nuevas regulaciones, como la Ley de IA de la UE, tienen como objetivo garantizar que la IA se use de manera que no genere daños

Aumentar la conciencia cibernética y la alfabetización

Muchas organizaciones están enfatizando su propósito y responsabilidad social. Reconocen que tienen un papel que desempeñar en la promoción de la alfabetización y la conciencia en materia de ciberseguridad, ya sea en su base de clientes o en el ecosistema de proveedores. Estas acciones pueden ayudar a prevenir el fraude, fomentar la lealtad a la marca y reducir la exposición a los ataques en la cadena de suministro.

Algunas organizaciones también persiguen objetivos altruistas de crear conciencia social sobre las amenazas cibernéticas, ayudar a desarrollar habilidades y promover la ciberseguridad como profesión, al tiempo que apoyan a otras organizaciones, como las benéficas, que pueden no tener la capacidad de proteger completamente sus propios sistemas. Octubre es el mes de Concientización sobre Ciberseguridad, una campaña anual destinada a crear conciencia sobre la ciberseguridad y proporcionar recursos para que las personas y las organizaciones mejoren sus prácticas de ciberseguridad. KPMG, entre otras organizaciones, está participando activamente en esta campaña para mejorar la seguridad para todos.

Consideraciones de gobernanza

Mantener las regulaciones en el foco en medio del cambio

La gobernanza es el tercer aspecto de ESG. Los riesgos cibernéticos pueden tener implicaciones significativas para la gobernanza. Existen varias regulaciones cibernéticas específicas de la industria o del mercado, como la regulacion de los EE.UU. para la Gestión de Riesgos Cibernéticos para los Asesores de Inversión, Estrategia, Gobierno y Divulgación de Incidentes, la Divulgación de Nombres de Compañias de Inversión, y la Regla de Diversidad de la Nasdaq. En la UE las regulaciones incluyen el Reglamento General de Protección de Datos (GDPR), la Ley de Resiliencia Operativa Digital (DORA) y la Directiva revisada de Redes y Sistemas de Información (NIS2).

Las regulaciones relacionadas con ESG incluyen el Reglamento de Divulgación de Finanzas Sostenibles de la Unión Europea (SFDR) y la Directiva de Informes de Sostenibilidad Corporativa (CSRD). En los Estados Unidos, las regulaciones de divulgación obligatorias incluyen la orientación de la comisión con respecto a la divulgación relacionada al cambio climático, la mejora y estandarización de las divulgaciones relacionadas con el clima, enmiendas a las reglas de los artículos 101, 103, 105 del reg S-K, y divulgaciones mejoradas por parte de ciertos asesores de inversión y compañías de inversión sobre prácticas de inversión ambientales, sociales y de gobernanza.

Medir la efectividad de las prácticas de privacidad, ciberseguridad y gestión de datos de una organización puede ayudar a determinar qué tan bien gobierna los datos que procesan y comparten tanto internamente como a través de las fronteras.

Los datos e informes de ESG deben ser precisos

Los datos ESG provienen de cuatro fuentes principales: de terceros, informados, derivados y funcionales, y los que son propiedad de la empresa. Se están realizando esfuerzos significativos en los informes ESG y asegurar su presentación, pero ¿puede confiarse en que los datos son precisos y confiables? La ciberseguridad es un factor crítico para garantizar informes ESG confiables. Trabaja para proteger los datos en sus orígenes mientras se recopilan, en tránsito y después de que se han analizados e informados. Además, también se requiere el cumplimiento de la privacidad de datos cuando los datos personales se procesan en la generación de informes ESG.

Los modelos de compensación ESG, los informes y la recopilación de datos pueden implicar procesos automatizados, así como modelos y análisis de datos. Es vital que estos procesos no sean manipulados o sesgados para garantizar informes precisos.

La ciberseguridad es relevante para las tres dimensiones ESG, por lo que las organizaciones en cualquier etapa de su viaje ESG deben considerar informar sobre su postura en este aspecto como parte de sus informes ESG. Esto ayuda a desarrollar y mantener la confianza con sus clientes, empleados y partes interesadas externas.

SASB y otras normas se centran en la transparencia

El Consejo de Normas de Contabilidad de Sostenibilidad (SASB) proporciona estándares específicos de la industria para informar sobre factores de sostenibilidad, incluídos los medio ambientales, sociales y de gobernanza. Las normas son importantes desde el punto de vista financiero, y tienen como objetivo aumentar la transparencia y la comparabilidad en la presentación de informes corporativos, lo que puede ayudar a los inversores a tomar decisiones de inversión más informadas. Sin embargo, menos de la mitad de las empresas tienen representación a nivel de liderazgo para la sostenibilidad.[5]

[5] 'Grandes cambios, pequeños pasos'. Encuesta de informes de sostenibilidad, KPMG, 2022

Uno de los factores de sostenibilidad que cubre SASB es el riesgo cibernético, que cae dentro de la industria de la tecnología y las comunicaciones, pero muchos otros sectores también lo mencionan. El riesgo cibernético es un factor que las empresas deben considerar divulgar en sus presentaciones públicas y se incluye en el tema de divulgación de seguridad de datos, este tema cubre una variedad de amenazas cibernéticas que podrían comprometer información confidencial, y proporciona orientación sobre la gestión de riesgos cibernéticos.

Un estándar similar, la Global Reporting Initiative (GRI), es ampliamente utilizado para la presentación de informes de sostenibilidad. Los estándares GRI incluyen orientación sobre cómo las empresas deben divulgar su gestión de la ciberseguridad y los problemas de privacidad de datos.

Al incluir el riesgo cibernético como un factor de sostenibilidad material, SASB y GRI reconocen que las amenazas cibernéticas pueden afectar significativamente el rendimiento financiero, la reputación y la sostenibilidad a largo plazo de una empresa. Las empresas que divulgan sus prácticas de gestión de riesgos cibernéticos y proporcionan información sobre sus políticas y procedimientos de seguridad de datos pueden mejorar su transparencia y responsabilidad ante las partes interesadas, incluidos los inversores, los clientes y los reguladores.

Sin embargo, menos de la mitad de las empresas tienen representación a nivel de liderazgo para la sostenibilidad.[6]

Los clientes esperan servicios confiables

Es más probable que los clientes hagan negocios con una empresa en la que confían para proteger su información personal y financiera. Esto es especialmente cierto para los clientes corporativos, que valoran la protección de sus datos confidenciales y propiedad intelectual. Muchas industrias tienen requisitos regulatorios para la ciberseguridad, y las organizaciones que cumplen con estas regulaciones son preferidas por las partes interesadas. La encuesta de KPMG encontró que menos de la mitad de las empresas revelan sus riesgos de gobernanza.[7]

Tanto los clientes privados como los corporativos quieren asegurarse de que los servicios que compran cumplan con sus expectativas de ESG y ciberseguridad. El compromiso de una empresa con ESG puede ser un facilitador de ventas: mejorar su reputación, impulsar la innovación, gestionar los riesgos, garantizar el cumplimiento y mejorar el acceso al capital. Por lo tanto, es importante considerar qué tan sostenibles son las prácticas de privacidad y ciberseguridad de una empresa al hacer negocios.

Al abordar los riesgos cibernéticos en el contexto de ESG, las empresas pueden salvaguardar sus operaciones, clientes y reputación mientras cumplen con sus obligaciones sociales y ambientales más amplias.

[6-7] 'Grandes cambios, pequeños pasos'. Encuesta de informes de sostenibilidad KPMG, 2022

Conclusión — creación de nuevos vínculos entre ESG y seguridad

Las organizaciones pueden beneficiarse enormemente al explorar la estrecha conexión entre los riesgos cibernéticos y ESG. Ambas áreas se centran en identificar y gestionar riesgos y oportunidades, lo que lleva a productos y soluciones mejorados y a una mejor sociedad. Esta conexión está siendo cada vez más reconocida por los mercados, incluidos los proveedores de calificación ESG que se esfuerzan por lograr una mayor transparencia y equidad en la medición y comparación de las organizaciones.

Para proteger su infraestructura crítica, sistemas de control industrial y datos de clientes, las empresas deben contar con medidas sólidas de privacidad y ciberseguridad. La buena noticia es que muchas empresas ya lo hacen, lo que debería tener un impacto positivo en su desempeño ESG. Además, las empresas deben invertir en tecnología con socluciones sostenibles para ayudar a reducir el impacto ambiental y minimizar la exposición a riesgos cibernéticos.

Finalmente, las empresas deben tener estructuras de gobierno sólidas para supervisar la gestión de riesgos a la privacidad y ciberseguridad, y garantizar el cumplimiento de los requisitos legales y reglamentarios. Al abordar los riesgos cibernéticos en el contexto de ESG, las empresas pueden salvaguardar sus operaciones, clientes y reputación al tiempo que cumplen con sus obligaciones sociales y ambientales.

Cómo pueden ayudar los profesionales de KPMG

Existe una creciente presión para que las empresas sean transparentes en sus actividades de compromiso corporativo en ciberseguridad y ESG. La ciberseguridad está en la agenda de muchos reguladores que demandan la notificación oportuna y completa de los incidentes y la divulgación de la madurez de los controles de seguridad cibernética. Y su conexión con la agenda ESG está jugando un papel muy importante en el futuro de la responsabilidad social corporativa.
Las empresas de KPMG tienen experiencia en todos los aspectos necesarios, desde la sala del board hasta el centro de datos. Además de evaluar su ciberseguridad y alinearla con las prioridades de su negocio, los profesionales de KPMG pueden ayudarlo a desarrollar soluciones digitales avanzadas, implementar y monitorear riesgos, ayudándole a responder de manera efectiva a los incidentes cibernéticos. No importa cómo se involucre, puede esperar trabajar con personas que entiendan su negocio y su tecnología.

Y ya sea que esté ingresando a un nuevo mercado, lanzando productos y servicios, o interactuando con los clientes de una nueva manera, el crecimiento sostenible es la única forma de construir un negocio exitoso y resiliente.

Los profesionales de KPMG se comprometen a trabajar con usted para mejorar la confianza, mitigar el riesgo y desbloquear un nuevo valor a medida que construye un negocio resiliente para lograr un futuro más sostenible. Con acceso a experiencia líder en la industria, tecnología basada en datos y alianzas globales, puede convertir la información en una oportunidad para su negocio, su gente y el planeta. Los profesionales de KPMG pueden ayudarle a anticipar el mañana, moverse más rápido y obtener una ventaja con tecnología segura y confiable.

Contactos

Mika Laaksonen
Líder y socio global
de ESG en ciberseguridad
KPMG en Finlandia
mika.laaksonen@kpmg.fi

Prasad Jayaraman
Líder y Director de Seguridad
Cibernética de las Américas
KPMG in the US
prasadjayaraman@kpmg.com

Matt O'Keefe
Líder y socio de seguridad
cibernética de ASPAC
KPMG España
mokeefe@kpmg.com.au

Akhilesh Tuteja
Global Cyber Security Leader
KPMG International and Partner
KPMG in India
atuteja@kpmg.com

Dani Michaux
Líder y socio de seguridad
cibernética de EMA
KPMG en Irlanda
dani.michaux@kpmg.ie

Nadine Hönighaus
Líder y socio global
de gobernanza de ESG
KPMG en Alemania
nhoenighaus@kpmg.com

Algunos o todos los servicios descritos en este documento pueden no ser permitidos para los clientes de auditoría de KPMG y sus afiliados o entidades relacionadas.

kpmg.com/socialmedia

Diseñado por Evalueserve.

Nombre de la publicación:Ciberseguridad en ESG | Número de publicación: 138862-G | Fecha de publicación: Julio 2023