Diligent

EVALUACIÓN DE SUS INDICADORES DE CIBERRIESGOS

Mejore la evaluación y el análisis de sus riesgos con el cuadro de indicadores de ciberriesgos

La importancia de la concienciación sobre los ciberriesgos

Las amenazas informáticas son dinámicas y cambian constantemente, y puede resultar difícil recuperarse de los daños financieros, reputacionales y estructurales provocados por un ciberataque. En el caso de los Consejos de Administración, es fundamental tener esta amenaza en cuenta.

Sin las herramientas adecuadas, puede ser casi imposible mantenerse al día. Independientemente del sector o la ubicación, la ciberseguridad es un problema clave para las empresas y será un asunto fundamental para los Consejos de Administración en los próximos meses y años.

De hecho, la encuesta de Gartner de 2020 sobre los Consejos de Administración prevé que alrededor del 40 % de los mismos tendrá una comisión específica para la ciberseguridad en 2025 (en comparación con menos del 10 % actual); se trata de un indicador claro de los cambios organizativos generales que ya están ocurriendo «en respuesta al aumento de riesgos creado por la mayor huella digital de las organizaciones durante la pandemia [de la COVID-19]».

Mientras las organizaciones avanzan por el camino hacia un futuro liderado por la tecnología digital, los Consejos de Administración deben dar los pasos correctos y definir las medidas adecuadas para garantizar que la transición sea lo más fluida posible. Los Consejos deben ser conscientes de las vulnerabilidades —desde las posibles filtraciones de datos hasta las asociaciones con terceros— que puedan suponer un riesgo si no se toman medidas preventivas.

El enfoque correcto de la gestión de los ciberriesgos exige una mejor comprensión de varios factores, entre ellos:

- La transformación digital, que implica un cambio hacia las operaciones basadas en la tecnología, así como un alejamiento simultáneo de los procesos del pasado manuales y en papel.
- Un aumento significativo del trabajo a distancia, lo que pone de manifiesto la importancia de la colaboración y la comunicación seguras en un entorno virtual.
- El control creciente de los inversores, las mayores expectativas de los consumidores y el número cada vez mayor de consideraciones de las partes interesadas que deben tenerse en cuenta.
- Un enfoque normativo sobre la supervisión de terceros.
- El efecto de los riesgos reputacionales y las repercusiones financieras asociadas a ellos.

Al fin y al cabo, prestar atención continua a los ciberriesgos es uno de los objetivos más urgentes para los Consejos de Administración actuales.

> «En el siglo XXI, no existe una sola decisión empresarial importante que no incluya consideraciones de ciberseguridad. La ciberseguridad debe integrarse en todo el proceso, desde la etapa de I+D hasta la de fabricación, pasando por las relaciones públicas. Eso es lo que debemos recordar sobre la ciberseguridad, que es cosa de todos».
>
> **Larry Clinton,**
> presidente de Internet Security Alliance

La supervisión eficaz de los riesgos comienza en la cúspide

Para que una estrategia de ciberriesgos sea eficaz, los consejeros deben tener acceso a los datos de ciberseguridad pertinentes, presentados en un formato intuitivo que permita una evaluación rápida y la toma de decisiones fundamentadas que mejoren la situación de la ciberseguridad.

Un cuadro de indicadores de ciberriesgos ofrece esta funcionalidad, especialmente cuando se incluye en el Portal para el Consejo de Administración con el que los consejeros ya están familiarizados. Los datos claros y concisos ayudan a los consejeros a identificar la información relevante y práctica, así como a aplicarla en la toma de decisiones futuras, ya sea para tomar medidas para mejorar la ciberseguridad o la preparación ante un ciberataque, o simplemente para generar consenso y conversaciones productivas en todos los niveles de la organización.

> «[Hoy en día] no existe una sola decisión empresarial importante que no incluya consideraciones de ciberseguridad. [La ciberseguridad] debe integrarse en todo el proceso».
>
> **Larry Clinton,**
> presidente de
> Internet Security Alliance

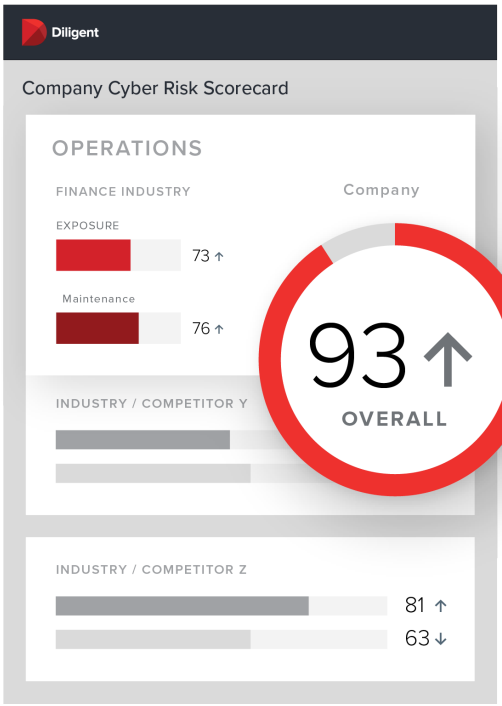
La lucha contra los ciberriesgos: prácticas recomendadas para los Consejos

- ☐ Facilitar la alineación en la organización, desde el Departamento Jurídico hasta el de Tecnología y Seguridad de los Datos. Un enfoque integrado en el Consejo de Administración y los niveles inferiores dará lugar a una respuesta más rápida y eficaz a las amenazas.
- ☐ Un buen Consejo predica con el ejemplo asegurándose de que sus propias comunicaciones sean seguras y estén protegidas. Al integrar la ciberseguridad en sus propios procesos, muestra la importancia de este enfoque al conjunto de la organización. La ciberseguridad debe considerarse como un problema de gestión de riesgos de toda la empresa, no solo del Departamento de TI.
- ☐ Implementar una solución para medir y comunicar con claridad los ciberriesgos. Este paso es clave en el paisaje actual de los riesgos, cada vez más complejo. La utilización de un cuadro de indicadores informativo, con todos los datos relacionados con los riesgos presentados juntos y de forma coherente, garantiza la claridad y permite la elaboración de informes fiables.
- ☐ Garantizar que existe un plan de reacción de ciberseguridad detallado, bien preparado y riguroso. Cuanto más rápida sea la respuesta, menos probable será el daño a largo plazo.
- ☐ Liderar desde la cúspide. A través de su propio gobierno corporativo y su atención a la ciberseguridad, el Consejo de Administración puede marcar la pauta para el resto de la organización. ¿La seguridad es un punto constante del orden del día o solo una preocupación pasajera? Dado que la estrategia y la gestión de riesgos ocupan un lugar destacado en las listas de prioridades de los Consejos de Administración, estos temas no deberían tratarse sin prestar atención a la tecnología y la seguridad.

Un cuadro de indicadores de ciberriesgos facilita la gestión de los mismos

Cuando hablamos de ciberseguridad, las calificaciones, los gráficos y los indicadores codificados por colores pueden actuar como ojos y oídos de los consejeros, y animarles a plantear las preguntas adecuadas:

- **¿Qué carencias tenemos en nuestro marco de ciberseguridad?**
- **¿El proveedor de servicios que estamos valorando sufre vulnerabilidades que podrían poner en riesgo a nuestra organización?**
- **¿Cuál es el nivel de riesgo de nuestros proveedores externos actuales?**
- **¿Cómo son nuestras capacidades en materia de ciberseguridad en comparación con las de la competencia?**
- **¿Cómo sabe el Consejo de Administración que la organización está mejorando en cuanto a ciberseguridad y cumplimiento?**
- **¿La empresa que vamos a adquirir sufre problemas de ciberseguridad que podrían afectar a la operación?**



Los riesgos de ciberseguridad están en constante evolución. Sin embargo, a efectos de elaboración de informes y planificación, el dato más útil suele ser una puntuación sencilla y de fácil comprensión. Una puntuación de ciberriesgos ofrece muchas ventajas: a través de un sencillo sistema de clasificación jerárquica, compuesto por letras o números, mejora la información de los directivos y los informes de ciberseguridad, que se alinean con las necesidades de la empresa. Gracias a esta puntuación y la visibilidad que proporciona, el Consejo de Administración está capacitado para tomar decisiones de ciberseguridad mejor fundamentadas y de manera más ágil.

Cuatro escenarios en los que se necesita un cuadro de indicadores de ciberriesgos

1 LA MEDICIÓN DEL CIBERRIESGO DE UNA ORGANIZACIÓN

Un cuadro de indicadores de ciberriesgos debe evaluar los riesgos de seguridad de una organización utilizando parámetros basados en datos y actualizados continuamente; asimismo, estos deben visibilizar las carencias en los controles de seguridad y las potenciales vulnerabilidades en todo el ecosistema de la cadena de suministro.

Con esta información, los Consejos de Administración pueden implementar cambios para corregir los puntos débiles. Asimismo, la supervisión continua de este sistema de puntuación permite a los Consejos de Administración ver en qué aspectos se ha progresado y medir los efectos de dicho progreso en el conjunto de la organización.

Un Consejo de Administración con la visibilidad que ofrece un cuadro de indicadores de ciberriesgos podrá gestionar y priorizar proactivamente los riesgos de seguridad, así como tomar decisiones empresariales fundamentadas y basadas en datos.

Las realidades de un ciberataque

Recientemente, SolarWinds, una importante empresa de TI que suministra software a entidades que van desde empresas de la lista Fortune 500 hasta el gobierno de EE. UU., fue víctima de un enorme ciberataque que se extendió a sus clientes y que pasó desapercibido durante meses. 18 000 clientes de SolarWinds instalaron involuntariamente actualizaciones de software que incluían código hackeado, ejecutado de forma tan discreta que puede que algunas víctimas no lleguen nunca a saber si sufrieron o no este ataque. Proteger de nuevo los sistemas afectados resultará astronómicamente caro y podría llevar años.

2 LA COMPARACIÓN CON ENTIDADES ANÁLOGAS

La capacidad de evaluar rápidamente la seguridad de las entidades análogas y los competidores del sector permite a los Consejos de Administración ver dónde se encuentran exactamente en comparación con otras organizaciones de su campo, lo que podría mejorarse y cuáles son sus ventajas frente a la competencia. La posibilidad de desglosar los problemas de seguridad específicos de un grupo de entidades análogas ofrece un método instantáneo de comparación y contraste en materia de ciberseguridad.

Las organizaciones analizan con regularidad los KPI de otras empresas en cuanto a ventas, beneficios o productividad para así mejorar su rendimiento interno reasignando recursos y priorizando determinados objetivos. Este mismo proceso puede ofrecer ventajas si se aplica al análisis de ciberriesgos, ya que conocer la situación de sus competidores no solo ayuda a cubrir las carencias de seguridad en su organización, sino también a impulsar el avance de la innovación y los procesos. Con estos datos pueden crearse un plan de actuación y unos objetivos a corto y largo plazo centrados en mejorar la ciberseguridad a un nivel igual o superior al de los competidores con mejores resultados.

3 LOS PROCESOS DE DILIGENCIA DEBIDA

El informe de Gartner «Innovation Insight for Security Rating Services» afirma que, en 2022, «Las evaluaciones de seguridad pasarán a ser tan importantes como las de crédito a la hora de analizar el riesgo de las relaciones comerciales». Un proceso exhaustivo de diligencia debida debe incluir información sobre el estado de salud digital de cualquier proveedor o empresa con los que la organización del Consejo de Administración prevea hacer negocios, ya se trate de socios o proveedores potenciales o actuales, o de posibles adquisiciones.

Para alcanzar el éxito, es fundamental ser capaz de identificar, supervisar y gestionar continuamente los riesgos en todo el ecosistema de proveedores. En definitiva, la ciberseguridad de una organización solo puede ser tan robusta como el eslabón más débil de su red: cualquier vulnerabilidad en la cadena de suministro no solo aumenta el riesgo de la empresa, sino que también pone en peligro su productividad, rentabilidad y reputación.

Del mismo modo, invertir, comprar o asociarse con otra empresa implica asumir sus operaciones digitales, lo que conlleva potenciales riesgos de ciberseguridad que podrían llegar a afectar al acuerdo. Si las ciberamenazas no se identifican y solucionan en una fase temprana del proceso, pueden poner en peligro el valor previsto de una operación.

Cuando un tercero sufre una filtración de datos, todas las organizaciones con las que está conectado sufren efectos devastadores. En 2018 se filtraron los datos de más de 2,65 millones de pacientes de Atrium Health cuando los servidores de su proveedor de facturación, AccuDoc Solutions, sufrieron un ataque. Del mismo modo, los datos personales de al menos 30 000 empleados del Departamento de Defensa estadounidense quedaron al descubierto cuando un proveedor externo de viajes fue hackeado.

> «[En 2022], las evaluaciones de seguridad pasarán a ser tan importantes como las de crédito a la hora de analizar el riesgo de las relaciones comerciales».
>
> «Innovation Insight for Security Rating Services»,
> Gartner

4 LA GESTIÓN DE LOS RIESGOS REPUTACIONALES

Probablemente, los riesgos reputacionales sean los más perjudiciales. Mientras que a menudo es posible gestionar y solucionar otros tipos de riesgos de forma interna, puede llevar años recomponer una imagen corporativa dañada. Por ello, es fundamental que las organizaciones gestionen su reputación con diligencia.

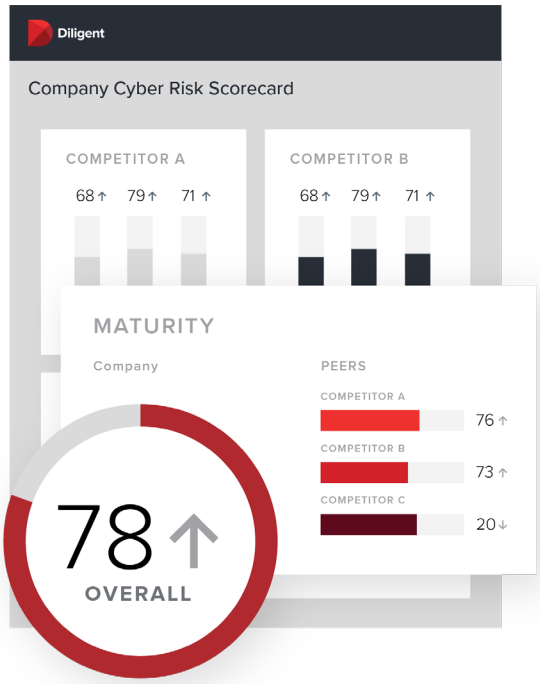
Un cuadro de indicadores de ciberriesgos visibiliza en todo momento las amenazas y vulnerabilidades potenciales que podrían afectar a las operaciones de la empresa. Esto permite a las organizaciones detectar posibles carencias de seguridad y, al mismo tiempo, asegurarse de que sus proveedores cumplen en todo momento la normativa vigente, lo que les permite enfrentarse a los riesgos reputacionales de terceros en tiempo real.

En 2017, Verizon pagó casi cuatro mil millones de euros por la compra de Yahoo, pero la operación estuvo a punto de cancelarse por dos escándalos de filtración de datos que salieron a la luz durante las negociaciones. Yahoo confesó que había sufrido dos filtraciones distintas de datos que no había hecho públicas y, aunque Verizon siguió adelante con la adquisición, consiguió una rebaja de casi 300 millones de euros sobre el precio de compra. Asimismo, Verizon se comprometió a compartir con Yahoo la responsabilidad legal por las filtraciones; esta herencia implicó un enorme coste que, junto con las repercusiones en cuanto a relaciones públicas, afectó al valor de la operación de incontables formas.

El cuadro de indicadores de ciberriesgos de Diligent ofrece una instantánea completa de su estado de salud digital

Para que una organización alcance un éxito sostenible, es indispensable contar con un enfoque proactivo de la gestión de los ciberriesgos.

El cuadro de indicadores de ciberriesgos de Diligent ofrece a los consejeros una visibilidad insuperable, ya que se actualiza constantemente y siempre está accesible, un aspecto crucial cuando hablamos de ciberriesgos. Asimismo, la información presentada es fácilmente asimilable, lo que ayuda en la comprensión, el análisis y la elaboración de informes. La manera en que mide la ciberseguridad resulta intuitiva, ya que obtiene los datos y la información de una serie de puntos de referencia y muestra las conclusiones en una presentación visual coherente. El cuadro de indicadores de ciberriesgos de Diligent proporciona evaluaciones de seguridad precisas que ayudan a detectar problemas importantes en la propia organización, con las entidades análogas, a lo largo del tiempo y en los factores clave en los que se basa la puntuación. Las organizaciones que lo deseen pueden profundizar más en la información sobre las relaciones con los proveedores, las transacciones de fusiones y adquisiciones, las operaciones de capital privado, la suscripción de créditos y las ventas y operaciones financieras.



Gracias al cuadro de indicadores de ciberriesgos de Diligent en colaboración con SecurityScorecard, empresa reconocida por el Foro Económico Mundial, los consejeros pueden desenvolverse en un paisaje digital cambiante y complejo:

- Accediendo a sus indicadores de ciberriesgos y comparándolos con los de entidades análogas y grupos competitivos gestionados con Diligent.
- Entendiendo su situación en materia de ciberseguridad en comparación con los puntos de referencia del sector, así como los tres principales factores de seguridad en los que se basan los indicadores.
- Priorizando las acciones e identificando la estructura y el software que deben revisarse.
- Gestionando los riesgos reputacionales, identificando tendencias y accediendo al historial de sus indicadores de ciberriesgos.

UNA VISIÓN DE LA ORGANIZACIÓN DESDE EL PUNTO DE VISTA EXTERNO

El cuadro de indicadores de ciberriesgos de Diligent ayuda a identificar las vulnerabilidades potenciales o activas, así como las ciberamenazas avanzadas, todo ello desde una perspectiva externa que ofrece a los Consejos de Administración la visión de un hacker. Gracias a la mayor visibilidad y al acceso directo a la información, los Consejos de Administración pueden mantenerse al día e informados.

El cuadro de indicadores de ciberriesgos puntúa a las empresas según una sencilla escala entre «A» y «F»; las organizaciones con una puntuación «F» tienen 7,7 más probabilidades de sufrir una filtración de datos que las que han recibido una «A». Cuando forman parte de una estrategia global de supervisión de riesgos, estas puntuaciones pueden poner de manifiesto eficazmente las vulnerabilidades de ciberseguridad y ayudar a evitar las filtraciones de datos.

Para ofrecer una visión lo más completa posible, las puntuaciones se basan en una multitud de factores, como el estado de los DNS, la reputación de las IP, la seguridad de las aplicaciones web, la seguridad de la red, la información filtrada, los foros de hackers, la seguridad de los puntos finales y la frecuencia de las revisiones. A pesar de la claridad y la sencillez visual de la información presentada en el cuadro de indicadores, este incluye una gran cantidad de datos, análisis humano y aprendizaje automático, por lo que puede evaluar a más de 1,6 millones de empresas.

El cuadro de indicadores de ciberriesgos de Diligent supervisa constantemente la seguridad de su organización y muestra los riesgos más importantes a los que se enfrenta su empresa, ordenados de más a menos graves. Asimismo, genera automáticamente una recomendación de plan de corrección según los objetivos y procedimientos de su organización, para ayudarle a implementar mejores procesos.

Glosario de ciberseguridad

- **Seguridad de red:** Algunos ejemplos de ataques a la seguridad de la red son el uso de vulnerabilidades, como los puntos de acceso abiertos y los certificados SSL inseguros o mal configurados, así como vulnerabilidades en las bases de datos o de seguridad derivadas de la ausencia de medidas de seguridad adecuadas.
- **Estado de los DNS:** Suele referirse a las mediciones de los ajustes del sistema de nombres de dominio, así como a la presencia de configuraciones recomendadas.
- **Frecuencia de las revisiones:** Mide cómo revisa la empresa sus sistemas operativos, servicios, aplicaciones, software y hardware, así como si lo hace cuando es necesario.
- **Seguridad de los puntos finales:** La seguridad de los puntos finales se refiere a la protección de los portátiles, ordenadores de sobremesa, dispositivos móviles y resto de dispositivos de los empleados que acceden a la red de la empresa.
- **Reputación de las IP:** El cuadro de indicadores de ciberriesgos recibe millones de señales de malware procedentes de infraestructuras de mando y control (C2) incautadas en todo el mundo. Las direcciones IP infectadas entrantes se procesan y se atribuyen a empresas corporativas mediante un algoritmo de atribución de IP. La cantidad y la duración de las infecciones de malware se utilizan como factor determinante en estos cálculos y ofrecen un punto de datos para la evaluación general de la reputación de las IP de una organización.
- **Foros de hackers:** El cuadro de indicadores de ciberriesgos recopila constantemente distintos flujos de conversaciones clandestinas, incluidas las de los foros de hackers de difícil acceso o privados, para identificar las IP y las organizaciones que se mencionan como posible objetivo.
- **Filtraciones de información:** El cuadro de indicadores de ciberriesgos identifica la información confidencial que queda al descubierto en filtraciones o pérdidas de datos, volcados de keylogger, volcados en Pastebin o de una base de datos, y a través de otros repositorios de información. A continuación, asigna esa información a las empresas propietarias de los datos.

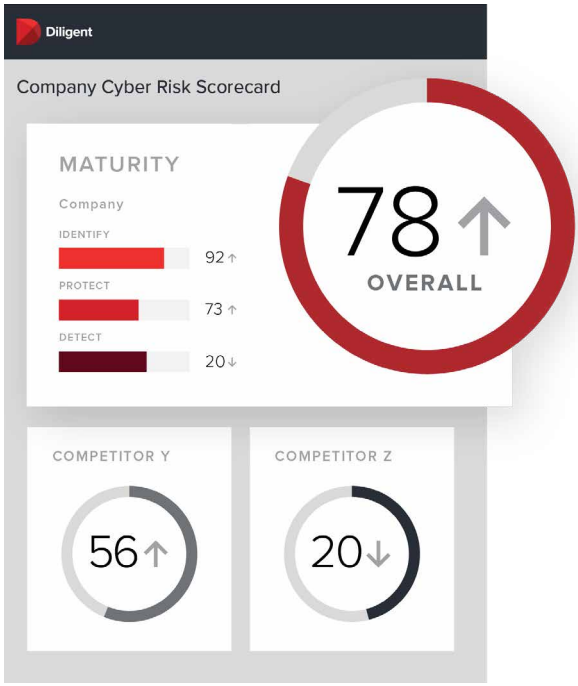
El cuadro de indicadores de ciberriesgos y el ecosistema general del gobierno corporativo

La buena gestión de una solución para las ciberamenazas presentes y futuras es solo una faceta del enfoque moderno del gobierno corporativo. La ciberseguridad, por su propia naturaleza, requiere una solución digital.

Asimismo, a medida que los Consejos de Administración van adoptando nuevos estilos de supervisión, también emplean nuevos canales de información. Aunque el concepto de «panel de riesgos» existe desde hace tiempo, ha llegado el momento de que los Consejos exijan el acceso al mismo. El cuadro de indicadores de ciberriesgos ofrece esta funcionalidad en un intuitivo panel.

El cuadro de indicadores de ciberriesgos funciona de forma sinérgica con el resto de la plataforma de gobierno corporativo moderno de Diligent para crear una organización más sólida, segura y digitalmente robusta, preparada para progresar. Con el cuadro de indicadores de ciberriesgos, las organizaciones obtienen:

- Seguridad constante y resiliencia digital.
- Mayor conocimiento sobre temas importantes, como la administración de datos o la seguridad de la cadena de suministro.
- Estabilidad de la organización.
- Potencial de inversión futuro.
- Prosperidad a largo plazo.



Los consejeros, directivos y profesionales del gobierno corporativo se enfrentan a los retos del gobierno corporativo moderno: deben sortear complejidades y tomar decisiones difíciles rápidamente. Para alcanzar la seguridad constante y la resiliencia digital, es fundamental contar con un paquete de soluciones que reduzca los riesgos, mejore las operaciones y mantenga informados a los líderes; asimismo, estas soluciones garantizan el potencial futuro y la estabilidad de la organización.

¿Está listo para ver el cuadro de indicadores de ciberriesgos de Diligent en acción? Programe una demostración.

SOLICITE UNA DEMOSTRACIÓN

Diligent

una empresa de
GOBIERNO
CORPORATIVO
MODERNO

Acerca de Diligent

Diligent es pionero en el ámbito del gobierno corporativo moderno. Nuestras reputadas aplicaciones basadas en la nube simplifican el trabajo diario de la gestión del Consejo de Administración y las comisiones, brindan soporte para una colaboración segura, gestionan datos de filiales y entidades y ofrecen perspectivas que capacitan a los líderes empresariales para tomar las mejores decisiones en el complejo entorno actual. Diligent reúne a la mayor red mundial de consejeros y directivos del ámbito corporativo y cuenta con el aval de más de 19 000 empresas y casi 700 000 líderes en más de 90 países.
Con un servicio mundial de atención al cliente merecedor de varios premios, Diligent presta asistencia a más del 50 % de las empresas integradas en la lista Fortune 1000, al 70 % de las que forman parte del índice FTSE 100 y al 65 % de las que conforman el ASX.

Socio de confianza de más de 700 000 líderes y 19 000 empresas de todo el mundo

mastercard · BARCLAYS · Marriott · General Mills · Domino's · Liberty Mutual

Los estándares de seguridad más estrictos.

- Cifrado de 256 bits
- Bloqueo a distancia
- Autorización de doble factor

Soporte técnico líder del sector

- Soporte técnico ininterrumpido
- Servicio especializado
- Formación ilimitada de los usuarios

Certificados de conformidad normativa

- Auditorías ASAE 18
- Certificación ISO
- Pruebas de seguridad de terceros

Póngase en contacto con nosotros para obtener más información o solicitar una demostración:

Teléfono: **+34 91 781 7048** • Correo electrónico: **lespinosa@diligent.com** • Sitio web: **www.diligent.com/es/**