Diligent

10 PREGUNTAS

que formular al evaluar la seguridad de un portal para Consejos de Administración

Cuando las empresas contratan los servicios de un proveedor de portales para Consejos de Administración, están confiándole la tarea de salvaguardar los documentos confidenciales y de ofrecer un sistema destinado a administrar el acceso a dichos documentos. Esta confianza va más allá de las especificaciones técnicas. Por este motivo, resulta esencial que los Consejos de Administración, secretarías corporativas, asesores generales y directores de sistemas de información se sientan cómodos y confíen en la seguridad del proveedor de su portal para Consejos de Administración.

Con este propósito, a continuación encontrará 10 preguntas que las empresas deben formularse acerca de cualquier posible proveedor de portales para Consejos de Administración:

1 ¿Realiza el proveedor inversiones importantes en investigación y desarrollo en materia de ciberseguridad?

Las amenazas de ciberseguridad están en constante evolución, no solamente debido a los avances en lo que a tecnología se refiere, sino también debido a los cambios en el mundo cibernético. Los piratas solitarios han dado paso a empresas sofisticadas que pueden provocar interrupciones a escala mundial. Un proveedor de portales para Consejos de Administración debe ser capaz de demostrar las capacidades de investigación y desarrollo que le permitan mantenerse a la vanguardia de las nuevas amenazas.

2 ¿Es el proveedor transparente acerca de sus procesos de seguridad?

El proveedor debe explicar claramente sus controles de seguridad física (protección de los servidores, enrutadores y otros equipos), los procesos de selección para los nuevos empleados, los controles internos, la supervisión del sistema (si tuvieran un ataque de piratas informáticos, ¿cómo lo sabrían?) y cualquier histórico de vulneraciones de seguridad, así como su resolución.

3 ¿Cumple el proveedor con los más altos estándares de seguridad?

Como prestadores terceros de información confidencial, los portales de los Consejos de Administración deben cumplir con normas de seguridad exigentes comparables a las de los departamentos de TI pertenecientes a varios sectores. Las acreditaciones principales incluyen un histórico impecable de auditorías SOC/SSAE 16 anuales (que cubren el modo en que los proveedores informan sobre sus controles internos) y la certificación de seguridad ISO 27001 (cumplimiento de los sistemas de seguridad de información del proveedor de software real con las normas internacionales, en vez de limitarse únicamente al cumplimiento de sus centros de alojamiento de datos).

4 ¿Permite el proveedor pruebas de intrusión externa?

La mayoría de los proveedores de portales para Consejos de Administración realizan pruebas de intrusión como parte de su control de calidad. Los portales con altos estándares de seguridad realizarán pruebas de manera casi continua en lugar de anualmente, con el fin de mantenerse al día respecto a las amenazas en constante evolución. Además, deben permitir a los clientes y posibles clientes realizar sus propias pruebas de seguridad (o a contratar a terceros de su elección) para ejecutar pruebas independientes. Esto significaría una clara prueba de confianza (así como un reconocimiento de que la seguridad es, en última instancia, un esfuerzo de equipo).

5 ¿Confía el proveedor en las plataformas o software de terceros?

Muchos de los portales para Consejos de Administración se construyen en función de las plataformas disponibles a nivel comercial o utilizan componentes conectables y listos para usar en ciertos elementos de su software. Sin embargo, esos elementos de terceros cuentan sus propias vulnerabilidades de seguridad, que pueden resultar atractivas para los hackers precisamente por el uso tan generalizado de dichas plataformas y porque éstas no han sido diseñadas para satisfacer las exigencias de un portal para Consejos de Administración. Por el contrario, dichos portales para los Consejos de Administración deben crearse a partir de cero, incorporando características de seguridad diseñadas para todas y cada una de las aplicaciones .

6 ¿Qué nivel de seguridad física proporciona el proveedor?

Si bien a menudo la información digital se considera intangible, ésta, de hecho, se almacena en servidores muy reales. Esas instalaciones de alojamiento de datos deben protegerse mediante elementos de protección *in situ*, así como televisión de circuito cerrado y múltiples capas de seguridad perimetral. Los propios servidores deben estar alojados en cubículos de seguridad y los datos almacenados de cada empresa deben estar físicamente separados. Además, las claves criptográficas de estos servidores deben protegerse mediante dispositivos resistentes y a prueba de manipulaciones.

Consíguelo en el App Store | Consíguelo de Microsoft | DISPONIBLE EN Google Play | AICPA SOC | ISO 27001 CERTIFICADO por BRIGHTLINE

7 ¿Qué grado de redundancia de datos se proporciona?

¿Están los datos respaldados y los centros de datos principales dotados de procedimientos de fallo seguro hacia centros de datos de recuperación de desastres? Los proveedores de portales para Consejos de Administración deben ofrecer ubicaciones remotas y dispersas a nivel geográfico para garantizar que cualquier evento que impacte en una ubicación no afecte a uno secundario. Además, la redundancia de datos debe respaldarse con inteligencia permanente, en tiempo real, sobre el rendimiento de los datos.

8 ¿Puede restringirse el acceso al portal r a un dispositivo específico?

La seguridad de sus dispositivos es de suma importancia ya que los miembros de los Consejos de Administración se encuentran repartidos por todo el mundo y viajan con mucha frecuencia. ¿Puede el acceso al portal de un usuario restringirse a un dispositivo específico que está registrado en el portal para Consejos de Administración? ¿Existe también una opción para desactivar el acceso por navegador? Las soluciones de autorización de dispositivos permiten a las empresas evitar el acceso a dispositivos desconocidos y no fiables. El resultado es un mayor control de los derechos de acceso y de ubicaciones.

9 ¿Le permite el proveedor asignar el nivel adecuado de seguridad del portal?

Cada solución de seguridad implica una relación de compromiso entre conveniencia y seguridad. Por consiguiente, está claro que la misma solución no es válida para todas las empresas. En cambio, un portal para Consejos de Administración debe adaptar las funciones con el fin de ajustarse a las necesidades de seguridad específicas de cada empresa, por ejemplo, debe disponer de contraseñas con diferentes niveles de seguridad, políticas de bloqueo y opciones para exportar e imprimir documentos del Consejo de Administración desde los portales.

10 ¿Están respaldadas las características de seguridad del portal mediante un soporte al cliente?

Con independencia del alto nivel de seguridad que ofrezca un portal, es necesaria la supervisión humana para garantizar la celeridad en lo que respecta a la resolución de cualquier problema. Por ejemplo, un consejero que escribe mal la contraseña de forma reiterada y al que se le bloquea el acceso al sistema. debe recibir, de forma inmediata, una llamada de teléfono de soporte al cliente, tanto para proporcionarle ayuda, como para comprobar la causa de sus intentos fallidos.

Para obtener más información o solicitar una demostración, póngase en contacto con nosotros hoy mismo:

Correo electrónico: info@diligent.com

Llame al: +34 91 781 70 48

Visite: www.diligent.com