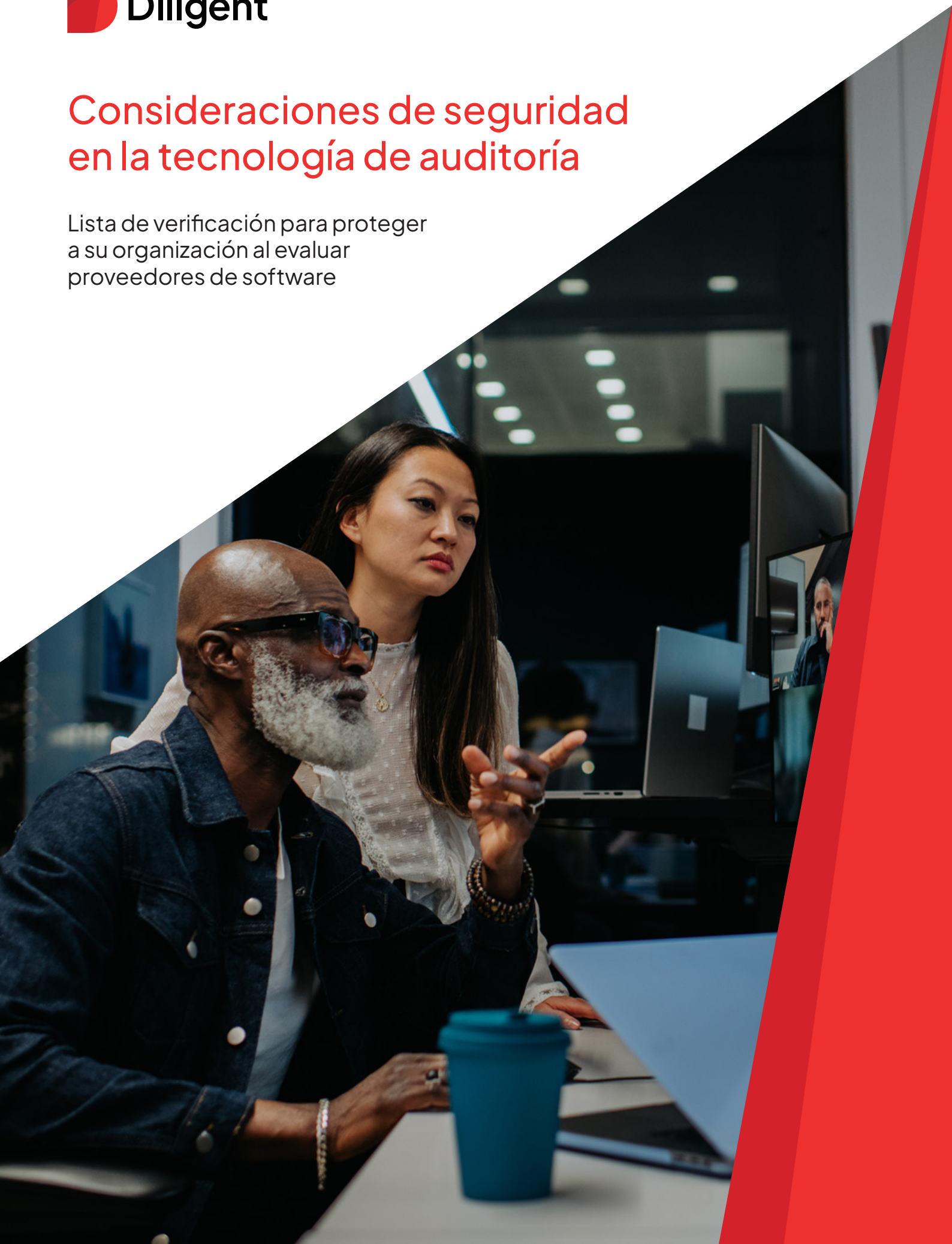
Diligent

Consideraciones de seguridad en la tecnología de auditoría

Lista de verificación para proteger a su organización al evaluar proveedores de software



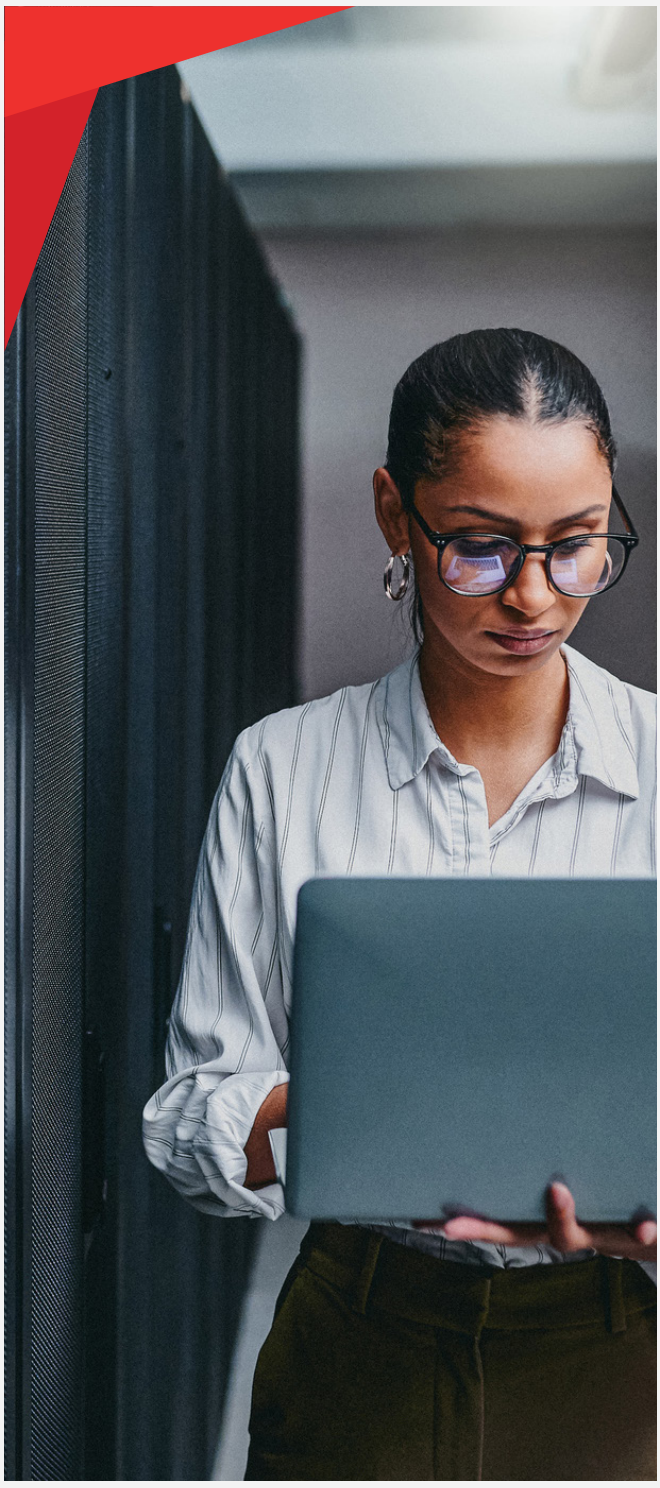
Invertir en software para ayudar a aumentar la eficacia de su equipo de auditoría es una decisión clave

Cada centavo de su inversión o del dinero público cuenta, y es fundamental proteger la reputación de su organización. Cuando se trata de garantizar la integridad y la eficacia de las operaciones financieras, tanto en el sector privado como en el público, el rol del software de auditoría es esencial.

No importa si su organización es pequeña, mediana o grande: una brecha de seguridad puede ser catastrófica. Podría tener que incurrir en costos gigantescos, como pagar un rescate por sus datos, sufrir daños en su reputación, dedicar tiempo del personal a intentar recuperar y regenerar datos y reportes y posibles multas normativas, además de los días, o semanas, de tiempo de inactividad.

Contar con software de auditoría adecuado puede mejorar mucho la seguridad, la precisión y la transparencia de los procesos financieros, y permitir a las organizaciones cumplir con sus obligaciones normativas y salvaguardar sus ingresos o los fondos públicos.

Use esta lista de verificación de preguntas clave para realizar a los proveedores de software de auditoría durante el proceso de compra para asegurarse de cubrir todos los requisitos de seguridad de su organización.



Preguntas clave sobre consideraciones de seguridad de software de auditoría

Seguridad de los datos

- ☐ ¿Le podemos enviar nuestro cuestionario sobre seguridad?
- ☐ ¿Qué solución de cifrado de datos ofrece su software para datos almacenados y durante la transmisión?
- ☐ ¿Puede confirmar el nivel de cifrado que proporciona para los datos almacenados y la transmisión de datos?

Una evaluación exhaustiva de un proveedor de seguridad comienza con un cuestionario sobre seguridad. Este paso le permite comprender mejor los riesgos potenciales relacionados con el software y la red del proveedor.

Asegúrese de que el software de auditoría ofrezca una funcionalidad de cifrado de datos robusta tanto para los datos almacenados como durante la transmisión de datos. Esto incluye el cifrado en bases de datos, copias de seguridad y durante la comunicación entre los dispositivos de los usuarios y los servidores del software. Se deben implementar algoritmos de cifrado fuertes, como AES-256, para proteger la información confidencial.

Controles de acceso

- ☐ ¿Qué mecanismos de control de acceso proporciona el software?
- ☐ ¿Cómo se procesan la autenticación y el inicio de sesión?
- ☐ ¿Cómo se procesa el acceso remoto?
- ☐ ¿Cómo hace la tecnología para procesar los controles de acceso basados en roles (RBAC)?

Evalúe los mecanismos de control de acceso que proporciona el software. Busque características como la autenticación multifactor (MFA) que requieran que los usuarios proporcionen varias formas de identificación para acceder al sistema, así como compatibilidad con el inicio de sesión único (SSO) o SAML. Los controles de acceso basados en roles (RBAC) también son importantes, ya que permiten a los administradores asignar diferentes niveles de acceso a los usuarios en función de sus roles y responsabilidades.

> "[El software de auditoría] nos permite mirar nuestra propia situación y ver con facilidad si hay algo extraño o que no cuadre. Nos permite detectar los problemas antes de que sea demasiado tarde".
>
> **Jewell Freeman**
> Directora de auditoría,
> Departamento de Correccionales de Luisiana

Cumplimiento y certificaciones

- ☐ ¿Qué certificaciones y estándares de la industria cumple que serían relevantes para nuestra organización del sector público y ubicación?
- ☐ ¿El software cumple con FedRAMP y/o NIST?

Pregunte si el software cumple con los estándares y las normativas de la industria relevantes para su organización. Por ejemplo, ISO 27001 (gestión de seguridad de la información), GDPR (Reglamento General de Protección de Datos), HIPAA (Ley de Portabilidad y Responsabilidad del Seguro de Salud) y SOC 2 (Control de Organizaciones de Servicios). Las auditorías y las certificaciones de terceros pueden proporcionar aseguramiento respecto a las prácticas y los controles de seguridad del software.

Preguntas clave sobre consideraciones de seguridad de software de auditoría (cont.)

Residencia y privacidad de datos

- ☐ ¿Cómo trata la tecnología el procesamiento de datos y la política de privacidad?
- ☐ ¿Se cumplen los requisitos de residencia de datos de regiones específicas sobre el alojamiento de datos?
- ☐ ¿Cómo respeta las normativas de protección de datos?
- ☐ ¿Cómo se recopilan, almacenan, procesan y comparten los datos de los usuarios?
- ☐ ¿Puede confirmar que su organización no vende los datos ni los usa indebidamente?

Lea la política de privacidad y las prácticas de tratamiento de datos del proveedor de software y, si tiene datos específicos que no puedan salir de la región, asegúrese de que se cumplan los requisitos de residencia. Asegúrese de que respete las normativas de protección de datos y defina con claridad cómo se recopilan, almacenan, procesan y comparten los datos de los usuarios. Verifique que el proveedor de software no venda ni use indebidamente los datos de los usuarios.

Gestión de vulnerabilidades

- ☐ ¿Cuál es su enfoque respecto de la gestión de vulnerabilidades?
- ☐ ¿Cuáles son sus procesos para identificar, evaluar y corregir las vulnerabilidades de seguridad en su software?

Las actualizaciones de seguridad periódicas y las revisiones de seguridad a tiempo son esenciales para mitigar las posibles amenazas. Averigüe cómo es el enfoque del proveedor respecto de la gestión de vulnerabilidades. Pregunte cuáles son sus procesos para identificar, evaluar y corregir las vulnerabilidades de seguridad en el software.

Copia de seguridad y recuperación de datos

- ☐ ¿Con qué frecuencia se hacen copias de seguridad de los datos?
- ☐ ¿Dónde se almacenan los datos de las copias de seguridad?
- ☐ ¿Qué objetivos de tiempo de recuperación y punto de recuperación puede garantizar?
- ☐ ¿Qué otras medidas tiene implementadas para recuperación ante desastres?

El uso de mecanismos adecuados de copia de seguridad y recuperación de datos protege contra la pérdida de datos debido a acontecimientos imprevistos o fallos del sistema. Evalúe las capacidades de copia de seguridad y recuperación de datos del sistema. Pregunte acerca de la frecuencia de las copias de seguridad, la ubicación de almacenamiento de los datos de las copias de seguridad y los objetivos de tiempo de recuperación (RTO) y punto de recuperación (RPO) que pueden garantizar.

Respuesta ante incidentes y monitoreo

- ☐ ¿Cómo funciona su respuesta ante incidentes y monitoreo?
- ☐ ¿Qué procesos tiene para detectar y monitorear incidentes de seguridad?

El monitoreo proactivo, los sistemas de detección de intrusiones (IDS) y las soluciones de gestión de eventos e incidentes de seguridad (SIEM) son componentes valiosos para la detección temprana y una respuesta eficaz a los incidentes. Indague acerca de la respuesta ante incidentes y las capacidades de monitoreo del software del proveedor. Pregunte por los procesos utilizados para detectar y responder a incidentes de seguridad.

Preguntas clave sobre consideraciones de seguridad de software de auditoría (cont.)

Viabilidad, prácticas de seguridad y riesgo de terceros del proveedor

- ☐ ¿Cuáles son sus políticas de seguridad internas?
- ☐ ¿Cómo capacita a sus empleados sobre temas de seguridad y riesgo?
- ☐ ¿Qué controles de antecedentes realiza?
- ☐ ¿Usa algún otro proveedor de infraestructura o procesador secundario?

Un proveedor que tenga implementadas medidas de seguridad robustas es más probable que priorice la seguridad de su software. Además, haga lo mismo para evaluar el riesgo asociado a terceros —qué proveedores de infraestructura o procesadores secundarios se usan para procesar o almacenar los datos— y asegúrese de que la cadena de suministro del proveedor sea tan sólida como el proveedor en sí.

Propiedad y portabilidad de los datos

- ☐ ¿Qué sucede con nuestros datos si decidimos dejar de usar su software?
- ☐ ¿Puede confirmar que no conservará ni usará nuestros datos si se termina nuestro contrato?

Pida información clara acerca de los derechos de propiedad y portabilidad de sus datos. Asegúrese de que pueda exportar sus datos o conectarse a ellos con facilidad desde el software si decide cambiar de proveedor o dejar de usar el servicio. Verifique que el proveedor no retenga ni use los datos después de la finalización del servicio.

Acuerdos de nivel de servicio (SLA)

- ☐ ¿Cuáles son los acuerdos de nivel de soporte?
- ☐ ¿Hay alguna cláusula en los SLA relacionada con la seguridad que debamos tener en cuenta?

Lea los SLA que le proporcione el proveedor del software. Preste atención a las cláusulas relacionadas con la seguridad, la disponibilidad y los tiempos de respuesta en caso de incidentes. Con SLA claros es más fácil establecer expectativas y garantizar la responsabilidad del proveedor de mantener un servicio seguro y confiable.

Evaluación independiente de la seguridad

- ☐ ¿Usa algún proveedor externo para evaluar sus controles y prácticas de seguridad?

Este proveedor externo podría proporcionar una evaluación imparcial de la postura de seguridad del software y así brindar mayor confianza en cuanto a la seguridad.

¿Cuál es el nivel de seguridad de la infraestructura digital de su equipo de auditoría?

Una lista de verificación meticulosa de la seguridad del software es una herramienta fundamental para garantizar la solidez de su infraestructura digital. Una evaluación rigurosa de cada aspecto, desde los controles de acceso hasta el cifrado de los datos, le puede ayudar a garantizar que sus sistemas puedan resistir posibles vulnerabilidades.

También destaca la importancia de buscar un socio colaborativo que tenga la experiencia de responder a sus consultas y aclararle las dudas de manera integral. Elegir un socio que conozca de forma integral los diferentes aspectos de la seguridad no solo mejora la eficacia de su equipo y sus procesos de auditoría, sino que prepara el terreno para un futuro seguro.

¿Está listo para descubrir de qué forma Diligent puede ayudarle a agregar valor, gestionar mejor su flujo de trabajo de auditoría y aportar conocimientos estratégicos? Programe hoy mismo una reunión.

Diligent

Acerca de Diligent

Diligent es el líder internacional en gobernanza moderna que proporciona soluciones de SaaS de gobernanza, riesgo, cumplimiento, auditoría y ESG. Asistimos a más de un millón de usuarios y 700 000 miembros y líderes de juntas directivas con una visión holística de las prácticas de GRC de sus organizaciones para que puedan tomar mejores decisiones al instante, sin importar el desafío.

Para obtener más información o solicitar una demostración:

info@diligent.com | diligent.com/es-mx

1199129948