

Cómo generar confianza con cumplimiento continuo

Autora: **Eva Pittas**, miembro de los Consejos de Forbes. Cofundadora y directora de operaciones de heylaika.com. Anteriormente dirigió la gestión de cumplimiento y proveedores en Citigroup.

Si 2021 fue una indicación del futuro del cumplimiento de la seguridad de la información, podemos esperar una cantidad cada vez mayor de regulaciones, estándares, auditorías y debida diligencia. El año pasado estuvo plagado de historias de cumplimiento estricto , auditorías en profundidad y escrutinio sobre la gestión de cambios, la diligencia debida de los proveedores y el riesgo de conducta basado en las personas.

Si bien el mercado anteriormente funcionaba como un efecto cascada de la regulación de terceros, estamos viendo requisitos más altos para socios más distantes. A medida que aumenta la demanda de seguridad de la información demostrable, la industria de servicios se esfuerza por encontrar formas asequibles y eficientes de demostrar el cumplimiento continuo.

Beneficios del cumplimiento continuo

Las empresas que crecen rápidamente necesitan mantener su cumplimiento a lo largo del tiempo, no solo pasar la inspección en un momento único. Del mismo modo, a medida que crece un negocio, también aumenta la cantidad de riesgos, la probabilidad de una falla de control impactante y la cantidad de oportunidades de incumplimiento.

El monitoreo continuo reduce el riesgo comercial general al ayudar a mantener una sólida postura de seguridad y garantizar que se cumplan las obligaciones contractuales. Al mejorar la seguridad y el mantenimiento de registros y minimizar el tiempo de inactividad, el monitoreo continuo proporciona evidencia de que su negocio es un socio confiable y de confianza.

En un entorno con ataques cibernéticos cada vez mayores, habiendo alcanzado un récord de un solo año en 2021 por la cantidad de infracciones, es fundamental garantizar que los controles funcionen continuamente según lo previsto. Cualquier vulnerabilidad o brecha se puede marcar a través de la supervisión y corregirse rápidamente para evitar comprometer los datos o la disponibilidad de su producto.

El cumplimiento continuo permite que una empresa responda con confianza a los cuestionarios de seguridad, las revisiones anuales, las solicitudes ad-hoc y otros escrutinios regulares y crecientes. Además, notificar de manera proactiva a los clientes sobre violaciones de seguridad o privacidad garantiza que su empresa cumpla con las obligaciones reglamentarias.

Demostración de la seguridad de la información continua

Todo esto puede parecer bastante desalentador y por una buena razón. Las auditorías de seguridad de la información no son baratas, y las auditorías son el precio de hacer negocios. Las empresas quieren una verificación independiente de terceros de que las empresas mantienen el cumplimiento y los controles operativos de manera adecuada. Como era de esperar, la industria se está moviendo lentamente para ofrecer soluciones para el cumplimiento continuo.

Al aprovechar su pila tecnológica, la automatización, los monitores y están disponibles para las pequeñas y medianas empresas que no pueden permitirse aumentar los costos de auditoría que ya son elevados. Las principales categorías de seguimiento incluyen:

- **Entornos de aplicación, staging, desarrollo y live**. Este monitoreo puede recopilar datos sobre métricas como el tiempo de actividad, las respuestas de la API y el volumen de tráfico para evitar un colapso de la disponibilidad.
- **Infraestructura de red, incluidos centros de datos, hardware, software, servidores y otra infraestructura de TI aplicable.** Supervisar su red es más sencillo con una arquitectura de red que identifica las debilidades potenciales y puede mejorar el rendimiento del producto.
- **La disponibilidad de la infraestructura de la base de datos**, donde almacena y transmite información a través de su plataforma o aplicación, debe supervisarse, así como los permisos de usuario, la disponibilidad de almacenamiento, el estado general y las métricas de rendimiento.

Supervisión de controles de seguridad de la información y automatización de alertas

Mi primera recomendación: aproveche las alertas integradas dentro de sus herramientas y sistemas para marcar incidentes o actualizaciones no conformes. Hay muchas plataformas de software que pueden ayudar a integrarse con su stock de operaciones para hacer precisamente esto. Al asignar controles relevantes para las necesidades de su negocio a las alertas, puede monitorear su cumplimiento en tiempo real, evitando posibles situaciones embarazosas entre auditorías.

Estas alertas podrían incluir marcar el incumplimiento de:

- **La administración de acceso e identidad** se refiere a la implementación de MFA, administración de contraseñas, creación y deshabilitación de credenciales, controles de acceso basados en funciones, segregación de entornos y actividad de cuentas privilegiadas.
- **Seguridad de los datos**, incluido el uso adecuado de las soluciones de cifrado y gestión de claves dentro del proveedor de la nube.
- **Controles del sistema operativo**, como la configuración del sistema y la gestión de parches.
- **Controles de red**, como puertos abiertos, autenticación, conexión segura (VPN, SSL, SSH), encriptación.

Servicios de auditoría modernos

Como les digo a todos mis clientes que abordan por primera vez un informe de cumplimiento o una certificación: una auditoría no es una tarea insignificante. En mi amplia experiencia en el apoyo a empresas y nuevas empresas de tecnología, puedo garantizar que cualquier auditoría debe verse como una actividad seria que puede tener y tendrá consecuencias para su negocio.

En pocas palabras, una auditoría evalúa la validez de sus políticas y prácticas de cumplimiento. Si los auditores encuentran debilidades durante una auditoría, los problemas saldrán a la luz y se documentarán, y tendrán un impacto negativo en su negocio. Si es una empresa o una unidad de negocios dentro de una empresa, esto pone su negocio bajo el escrutinio de los reguladores, la gerencia ejecutiva y los clientes.

¿A qué se traduce esto?

Si bien hay una serie de impactos negativos, incluyen la reducción de los planes comerciales para expandirse, pausar la contratación hasta que se solucionen los problemas o soportar auditorías más frecuentes. Para una startup, podría significar perder ese gran trato frente a un competidor que tiene una postura de seguridad y un entorno de control más sólidos y lo demuestra regularmente.

Según mi experiencia, los evaluadores pueden pasar más de 200 horas probando los controles SOC 2. La falta de tecnología en el espacio de auditoría de seguridad de la información crea una experiencia minuciosa para el cliente. Esto ha creado un ciclo interminable entre el cliente y el auditor, y nadie intentó encontrar una solución centrada en la auditoría.

Elegir una firma de auditoría que esté bien versada en tecnología o soluciones en la nube es clave. Los auditores no técnicos necesitan dedicar más tiempo a comprender los sistemas y los flujos de trabajo. Cuando un auditor puede comprender las pilas de tecnología de vanguardia, es más probable que demuestre el cumplimiento continuo a través de pruebas de control innovadoras.

Además, mire el panorama tecnológico actual en busca de opciones para ayudar a eliminar o acortar una lista típica de solicitudes de auditoría a un puñado de solicitudes. Estas evaluaciones minimizan el elemento de error humano dentro de una auditoría y permiten resultados reproducibles. Cuando cualquier auditor puede examinar las pruebas y repetirlas, se puede demostrar el cumplimiento continuo en cualquier momento.

Fuente: Forbes