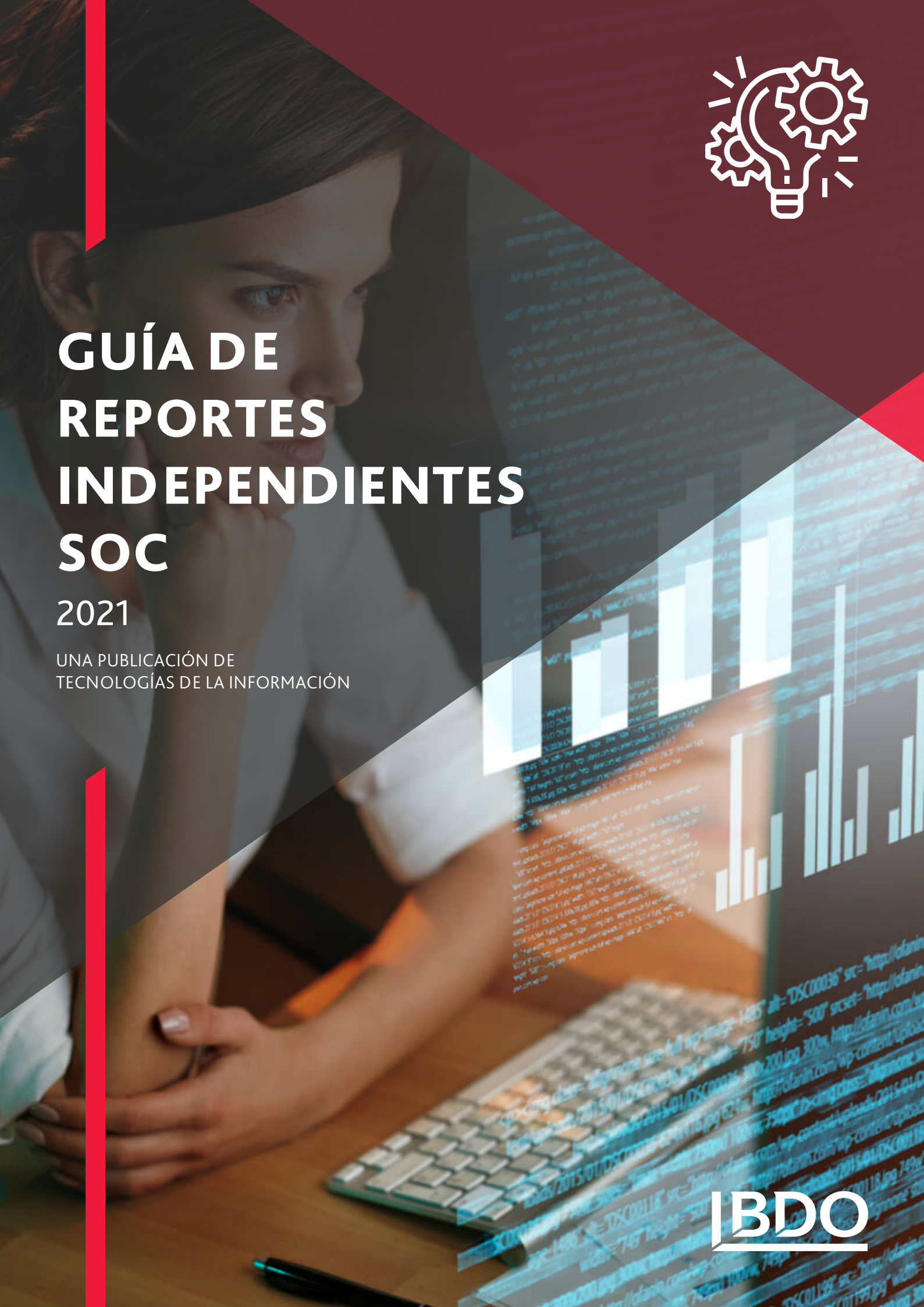


GUÍA DE REPORTES INDEPENDIENTES SOC

2021

UNA PUBLICACIÓN DE
TECNOLOGÍAS DE LA INFORMACIÓN

BDO

En esta edición

El proceso de transformación digital que las empresas están llevando a cabo requiere el uso de nuevas tecnologías para mejorar la eficiencia y crear valor para los clientes y/o ciudadanos. Para ello, es cada vez más común que las organizaciones y/o empresas tercericen el soporte tecnológico y el almacenamiento de su información a empresas especializadas utilizando tecnologías como la nube. Sin embargo, ello plantea retos en términos de confidencialidad y privacidad de la información de la organización (referido a datos institucionales/empresariales o personales) que ahora es cedida a un tercero para su administración.

Garantizar que la gestión de la información clave esté protegida adecuadamente y que es tratada para los fines contratados es el rol de un proveedor de servicios de tecnología especializado. En tal sentido y para fortalecer la confianza requerida para este tipo de labor, es importante que un auditor evalúe los procesos tecnológicos de los proveedores de servicios de tecnología a fin de contar con una opinión independiente sobre las medidas que han adoptado los mismos para gestionar el soporte tecnológico (infraestructura, plataformas, bases de datos, aplicaciones, entre otros) de sus clientes.

La importancia de evaluar el procesamiento de datos por terceros

La pandemia COVID-19 ha obligado a muchas compañías a adoptar nuevas formas de trabajo y a aprovechar las tecnologías existentes en el mercado para continuar con sus operaciones en esta coyuntura. Una de las tecnologías que ha resaltado más en este contexto es el Cloud Computing (nube) cuyo principal beneficio es el acceder a una gran cantidad de información procesada desde cualquier parte del mundo sin necesidad de contar con una gran infraestructura para ello.

Una muestra de que esta tecnología está siendo consumida con mayor intensidad es que los ingresos de las principales empresas que brindan servicio en la nube como Amazon (AWS), Microsoft (Azure) y Google (Google Cloud) ha crecido en 34%, 59% y 52% respectivamente.

El uso más intensivo de esta tecnología obliga a tener un mayor control de los riesgos de asociados al registro, almacenamiento y procesamiento de datos a través de terceros (proveedores), por lo que, se requieren establecer controles adecuados para resguardar la seguridad, disponibilidad, integridad del procesamiento, confidencialidad y privacidad de la información que se almacena y procesa en la nube. Es por ello que, el Instituto Estadounidense de Contadores Públicos Certificados (AICPA) introduce los reportes de Control de Organización de Servicios (SOC), conocidos como SOC 1, SOC 2 o SOC 3, que son marcos establecidos para informar sobre los controles internos implementados en organizaciones de servicios (organizaciones que proveen servicios de procesamiento de información a sus clientes).

Las empresas que contraten a una organización de servicios para proveerles servicios relacionados con el registro, almacenamiento y procesamiento de datos pueden solicitarle a esta entidad un Reporte SOC, con la finalidad de asegurarse que se han implementado controles para administrar la información empresarial de manera segura.

El reporte SOC es emitido por una empresa independiente (firma de auditoria) en la cual evalúa los controles internos de la organización de servicios en términos de seguridad, disponibilidad, integridad del procesamiento, confidencialidad y privacidad.

¿QUÉ REPORTE ES EL ADECUADO PARA MI ORGANIZACIÓN?

En la actualidad, las organizaciones de servicios deben contar con reportes SOC independientes para mantenerse vigentes en el mercado y brindar confianza a sus clientes. Por ende, es importante seleccionar el reporte SOC más adecuado según la naturaleza del servicio que se brinda, los requisitos solicitados por los reguladores, entre otros.

A continuación, la explicación de cada tipo de reporte SOC:

Reporte SOC 1

El reporte SOC 1 se centra en la evaluación independiente de los controles internos relacionados con la seguridad de los estados financieros. Las compañías están obligadas a definir sus propias actividades de control, objetivos y actividades que respondan a las necesidades de sus clientes. Esta evaluación se lleva a cabo de conformidad con la Declaración de Normas de Tareas de Atestación Nº 18 (SSAE 18) y la Norma Internacional de Compromisos de Certificación Nº 3402 (ISAE 3402).

Reporte SOC 2

El reporte SOC 2 se centra en la evaluación independiente de los controles de operación, basado en la evaluación de los principios de servicios de confianza desarrollados por el AICPA. Este reporte emite opinión sobre los siguientes aspectos de una organización de servicios:

- Seguridad
- Disponibilidad
- Integridad del procesamiento
- Confidencialidad
- Privacidad

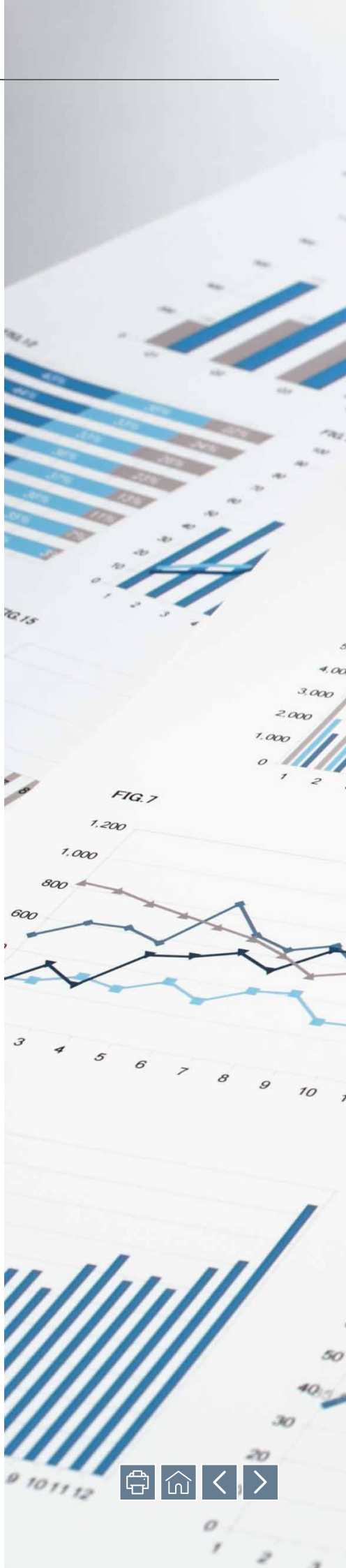
También incluye la opinión del auditor independiente acerca del diseño y del funcionamiento de los controles definidos por la compañía; asimismo, los procedimientos de prueba del auditor y los resultados de cada control. Las organizaciones que forman parte de los reportes SOC 2 son las que se encargan de administrar datos altamente sensibles, gestionar transacciones o información clasificada, entre otros. Es preciso mencionar que para los reportes tipo SOC 2 existen también dos tipos:

- **SOC 2 Tipo 1:** Evalúa solo el diseño de controles en un momento del tiempo especifico.
- **SOC 2 Tipo 2:** Evalúa el diseño y efectividad de los controles durante el período de tiempo cubierto.

Reporte SOC 3

El reporte SOC 3 abarca los cinco principios de servicios de confianza en materia de seguridad, disponibilidad, integridad de procesamiento, confidencialidad y privacidad. El reporte es un resumen ejecutivo del reporte de SOC 2 e incluye la opinión de un auditor independiente sobre el diseño y funcionamiento de los controles de la compañía.

Finalmente, si bien es cierto que el rubro financiero regulado por la Superintendencia de Banca, Seguros y AFP (SBS) obliga las entidades del sector contar con reportes SOC en caso realicen un procesamiento significativo de datos (reglamento SBS N.º 504-2021), cualquier empresa u organización puede solicitar este tipo de reportes a las organizaciones de servicios (proveedores de nube u otros) a fin de conocer como está siendo administrada su información empresarial.



Evaluación de servicios de información y tecnología tercerizados

Los reportes de control de organizaciones de servicios (SOC) son informes emitidos por entidades independientes (firmas de auditoría) a fin de asegurar que la información de las empresas que contratan servicios de información y tecnología a terceros está siendo administrada de manera segura y con los controles apropiados. Contar con reportes SOC puede proveer múltiples beneficios a las organizaciones de servicios como:

- **CONFIANZA Y CREDIBILIDAD EN LA GESTIÓN DE LA INFORMACIÓN**
- **NUEVOS NEGOCIOS POR UTILIZACIÓN DE PRÁCTICAS INTERNACIONALES DE SEGURIDAD DE LA INFORMACIÓN**
- **FORTALECIMIENTO DEL GOBIERNO CORPORATIVO**
- **IDENTIFICACIÓN Y ADMINISTRACIÓN DE RIESGOS TECNOLÓGICOS**
- **FORTALECIMIENTO DEL CONTROL INTERNO**

El Instituto Americano de Contadores Públicos Certificados (AICPA) es la organización que provee los lineamientos para emitir los reportes SOC, dentro de los cuales considera los siguientes:

SEGURIDAD	DISPONIBILIDAD	INTEGRIDAD DE PROCESAMIENTO	CONFIDENCIALIDAD	PRIVACIDAD
Protección el acceso no autorizado, integridad de los datos y gestión de cambios e incidentes.	Uso según lo acordado en los niveles de servicio.	Completo, preciso, oportuno y autorizado.	Proteger la transmisión y procesamiento de datos confidenciales.	Requisitos de privacidad de la organización y normativa legal.

Para emitir un reporte SOC se debe efectuar una metodología basada en los lineamientos del AICPA. En ese sentido, nuestra metodología permite evaluar los servicios de tecnología y procesamiento de datos y considera, de manera general, los pasos presentados a continuación:

PASO 1
Determinar el alcance de la evaluación

PASO 2
Entendimiento del entorno tecnológico

PASO 3
Identificación de riesgos y controles

PASO 4
Evaluación del diseño

PASO 5
Evaluación de la efectividad

PASO 6
Presentación de hallazgos

PASO 7
Elaboración del reporte SOC de acuerdo a la sección 101 del AT de AICPA

Aplicabilidad de la evaluación de servicios de información y tecnología tercerizados

La tercerización de servicios como los de tecnología, permite a las organizaciones dedicarse a sus operaciones estratégicas y actividades claves, mejorando la eficiencia y flexibilidad. Sin embargo, tercerizar servicios de tecnología puede significar la transferencia o gestión de datos por terceros, lo cual implica ciertos riesgos que deben ser mitigados con reportes independientes.

¿QUÉ EMPRESAS DEBEN SOLICITAR UN REPORTE INDEPENDIENTE (P.E. REPORTE SOC) A SU PROVEEDOR DE TECNOLOGÍA?

Empresas que contratan servicios en la nube	Empresas que contratan la infraestructura tecnológica a un tercero	Empresas que contratar servicios de procesamiento de datos (sistema de información y datos) a terceros	Empresas filiales cuya casa matriz en el exterior les brinda el servicio de procesamiento de datos (sistemas de información y datos)

RIESGOS MÁS COMUNES QUE SE MITIGAN CON UN REPORTE INDEPENDIENTE (REPORTE SOC)

Las empresas necesitan que los proveedores de tecnología que brindan servicios de procesamiento de datos, proporcionen garantías sobre las tareas y la información que se les confía.

SEGURIDAD

Accesos no autorizados a información sensible y robo de la información

RESPALDO Y RESTAURACIÓN

Datos críticos no respaldados regularmente y fallas en la restauración

CAMBIOS A PROGRAMAS

Cambios en las aplicaciones internas y la infraestructura sin autorización

SEGURIDAD FÍSICA

Data Center sin mecanismos de seguridad perimetral ante siniestros

ACCESOS LÓGICOS

Creación y modificación de cuentas de usuario sin autorización

El Reporte SOC 2 (tipo de reporte SOC) es una forma en que las empresas supervisan el cumplimiento de las buenas prácticas para el manejo adecuado de la información y las tareas por parte del proveedor de tecnología.

Novedades asociadas a la aplicabilidad del reporte SOC tipo 2 en el sector bancario

La Resolución SBS N°504-2021, publicada el 23 de febrero del 2021, aprueba el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, en el cual obliga a las empresas que cuenten con servicios en la nube, evidenciar anualmente que su proveedor de tecnología mantiene vigente las certificaciones ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018, y que cuenta con un reporte SOC 2 tipo 2 u otros equivalentes.

Cómo puede ayudar BDO

BDO cuenta con un equipo especializado y con experiencia ayudando a empresas de diferentes sectores en la evaluación de los controles de tecnología asociados a servicios provistos por terceros. Nuestro equipo puede ayudarlo de la siguiente manera:

- Diseño e implementación de controles de seguridad de la información y ciberseguridad basado en prácticas de referencia (ISO 27001, NIST 800-53, NIST CSF)
- Evaluación especializada de servicios de tecnología de la información y procesamiento de datos brindados por terceros, con la finalidad de emitir los reportes de Control de Organización de Servicios (SOC) de AICPA (SOC2 Tipo I, SOC2 Tipo II y SOC3) bajo el estándar AT101
- Diagnóstico y adecuación de los procesos de tecnología de la información y seguridad de la información, de acuerdo a la circular G-140 (modificado por la Resolución SBS N° 504-2021)
- Diseño e implementación del Modelo de Gobierno y gestión de tecnología de acuerdo al marco de referencia COBIT 2019
- Evaluación del área de tecnología de información considerando prácticas de referencia (COBIT2019, ISO27001, ITIL)

PARA MAYOR INFORMACIÓN:

VICTOR VERA TUDELA
Socio de Consultoría de Negocios
vveratudela@bdo.com.pe

www.bdo.com.pe

AUDITORÍA | TAX & LEGAL | CONSULTORÍA DE NEGOCIOS | OUTSOURCING