Informe SOC (Service Organization Controls / Systems and Organization Controls) - ¿por qué es clave para la empresa?

Las empresas pueden demostrar que son responsables para llevar un adecuado control de la información financiera que gestiona, transmitiendo seguridad a clientes y proveedores.

- Otorga:
  - **Reputación**
  - **Seguridad**: Integridad, confidencialidad, disponibilidad y privacidad de la información.
  - **Confianza:** Implementación adecuada de medidas de seguridad y control.
  - **Cumplimiento:** De requerimientos de auditoría tanto interna como externa solicitada por los clientes.
  - **Ventaja competitiva:** Anticiparse a posibles requerimientos.
  - **Marco regulatorio**: Dr parte de órganos de gobierno corporativo en las empresas, reguladores nacionales y extranjeros.
- Las empresas invierten recursos para controlar los riesgos asociados al registro, el almacenamiento y el procesamiento de los datos a través de proveedores.
  - Deben garantizar la seguridad, la confidencialidad, la disponibilidad y la integridad de toda la información que se gestiona y se aloja en la Nube.

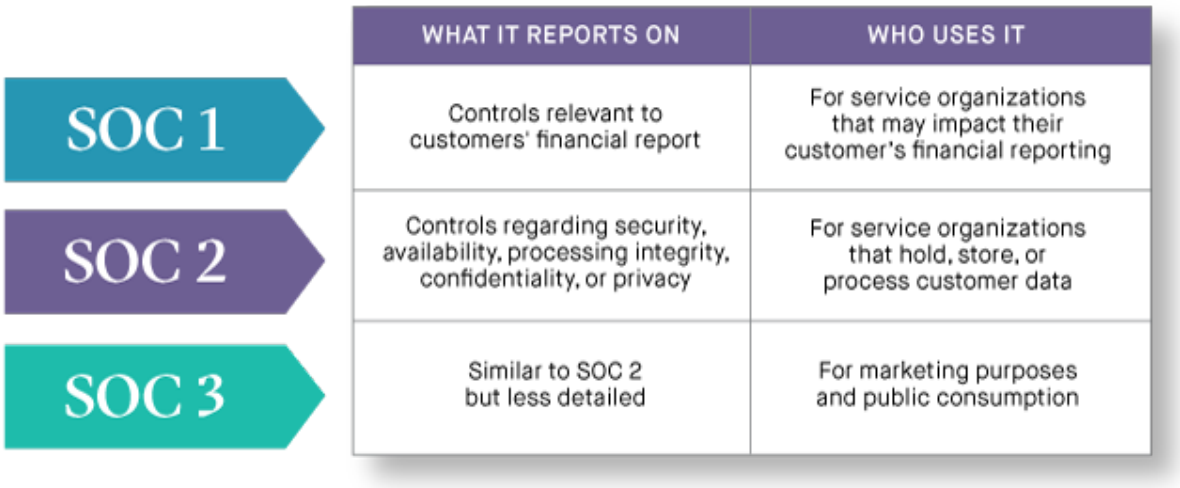
¿Quién realiza los informes SOC?

Los informes SOC son emitidos por una firma de auditoría **independiente** que tiene una certificación propia CPA (Certified Public Accountant).

- "Garantizan" ante el resto de *stakeholders*, sobre todo clientes, que "no existen grietas" por las que se pueda escapar información sensible ni comprometedora.
- Delimita el máximo control interno sobre la información financiera de otra empresa que maneja una entidad, evaluando el riesgo inherente que existe sobre el ejercicio de su actividad.

Categorías de informes SOC:

Existen tres categorías de informes SOC:



- **SOC 1**: Centrado en controles internos relacionados con la seguridad de los estados financieros y contables. La compañía está en condiciones de garantizar que desempeña las actividades de control suficientes para satisfacer las necesidades de sus clientes.
- **SOC 2**: Referente a los *controles operativos*, poniendo un especial énfasis en la *seguridad*, la *disponibilidad*, la *integridad* de los procesos, la *confidencialidad* y la *privacidad*. Suele incluir también una opinión del auditor acerca del diseño y el funcionamiento de los controles definidos por la compañía.
- **SOC 3**: Informe de cumplimiento de nivel superior que se puede compartir con los clientes pero sin revelar información confidencial (evaluación del diseño y de la efectividad operativa de los controles de seguridad). Es el análisis de protocolos de seguridad internos de la organización a nivel general y en dos formas: de manera permanente, o solo durante un periodo determinado, como, por ejemplo, durante la realización de un proyecto. Los informes SOC 3 suelen ser más breves y menos detallados que los SOC 2.

SOC 2 y los servicios en la Nube

Estándar internacional para evaluar las amenazas de ciberseguridad y los controles operativos e internos de un proveedor de servicios IT, *cloud* y *hosting*.

Su homologación internacional dentro de normas como la ISO/IEC 27001 le confieren una doble utilidad:

- Credencial para clientes de que el entorno virtual es seguro y confiable.
- Dentro de la organización:
  - Mayor comprensión de los riesgos por parte de los empleados.
  - Facilita la aceptación rutinaria de los controles internos.
  - Promueve un clima de gobernanza positivo.

Estos informes requieren de un esfuerzo externo coordinado durante un periodo de tiempo.

¿Qué beneficios aporta a una empresa el informe SOC?

- Minimiza el impacto de las auditorías, al realizar una evaluación de distintos ámbitos relacionados con la seguridad de manera periódica.
- Mejora la gestión de los riesgos:
  - Ventaja competitiva para la organización.
  - Optimiza los procesos y los controles comerciales.
- Valida la eficiencia y la seguridad de los procesos que tiene encomendados a terceros.
- Revelar la solidez de sus entornos a los clientes.

System and Organization Controls: SOC Suite of Services

SOC para organizaciones de servicios:

Reportes de control interno de servicios proveídos por una organización que brinda información valuable que los usuarios necesitan para evaluar y abordar los riesgos asociados a tercerizar un servicio.

SOC para ciberseguridad:

Un marco de trabajo para reportar información relevante y útil sobre la efectividad del programa de gestión de riesgos de la ciberseguridad, y reportes de CPA con información para alcanzar los requerimientos de un gran rango de partes interesadas.

SOC para la cadena de suministro:

Reporte de controles internos de una entidad en sistemas y controles para producir, fabricar o distribuir bienes para entender mejor los riesgos de ciberseguridad en su cadena de suministro.

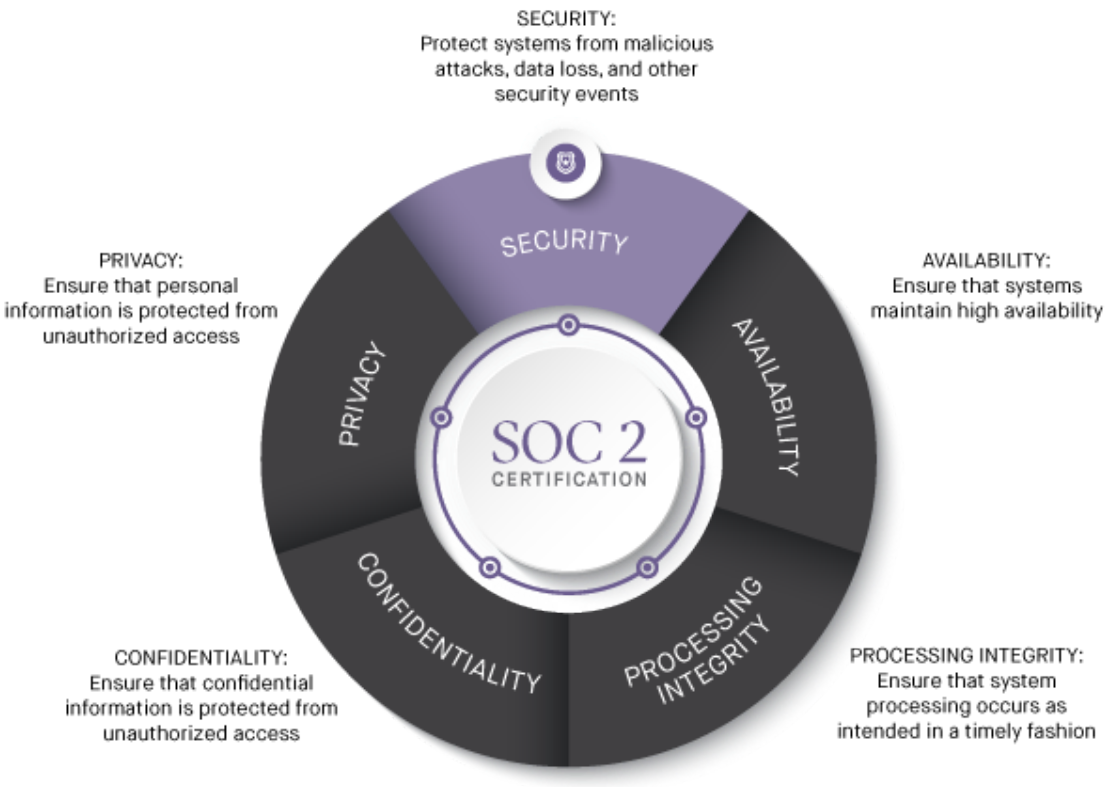
System and Organization Controls

Es el nombre de un conjunto de reportes producidos durante una auditoria. Utilizada por organizaciones que proveen sistemas de información como servicios para otras

organizaciones, para validar reportes brindados de controles internos de esos sistemas a sus clientes.
Los reportes se enfocan en controles agrupados en 5 categorías llamadas "Principios de Servicios de Confianza" (Trusted Services Principles), divididos en 2 niveles de reporte y 3 tipos.

Trust Service Principles:

5 categorías pseudo-superpuestas que soportan la tríada de la seguridad informática:



1. Seguridad:
    1. Firewalls.
    2. Detección de intrusiones.
    3. Autenticación de múltiples factores.
2. Disponibilidad:
    1. Monitoreo de rendimiento.
    2. Recuperación tras desastres.
    3. Manejo de incidentes.
3. Confidencialidad:
    1. Encriptación.
    2. Controles de acceso.
    3. Firewalls.
4. Integridad de procesos:
    1. Aseguramiento de calidad.

    2. Monitoreo de procesos.
5. Privacidad:
    1. Controles de acceso.
    2. Autenticación de múltiples factores.
    3. Encriptación.

Reportes:

Niveles:

También especificados por SSAE 18:

- ***Tipo I (Diseño)***: Describe el sistema de servicio de una organización y si su diseño de los controles especificados alcanzan los trust principales relevantes. ¿El diseño y la documentación están cerca de cumplir sus objetivos definidos en el reporte? En un momento especifico (cuando se hace la auditoria).
- ***Tipo II (Operatividad)***: También se enfoca en la efectividad operacional de los controles especificados sobre un periodo de tiempo (usualmente 9 a 12 meses). ¿Es la implementación apropiada?

Tipos:

- ***SOC 1*** - Controles internos sobre reportes financieros (ICFR).
- ***SOC 2*** - Trust Service Principles y criteria.
- ***SOC 3*** - Trust Service Principles y criteria para reportes de uso general.

Los reportes SOC 1 y SOC 2 están dirigidos a una audiencia limitada, específicamente, usuarios con un cierto entendimiento de los sistemas en cuestión. Los reportes SOC 3 contienen información menos específica y pueden ser distribuidos al público general.