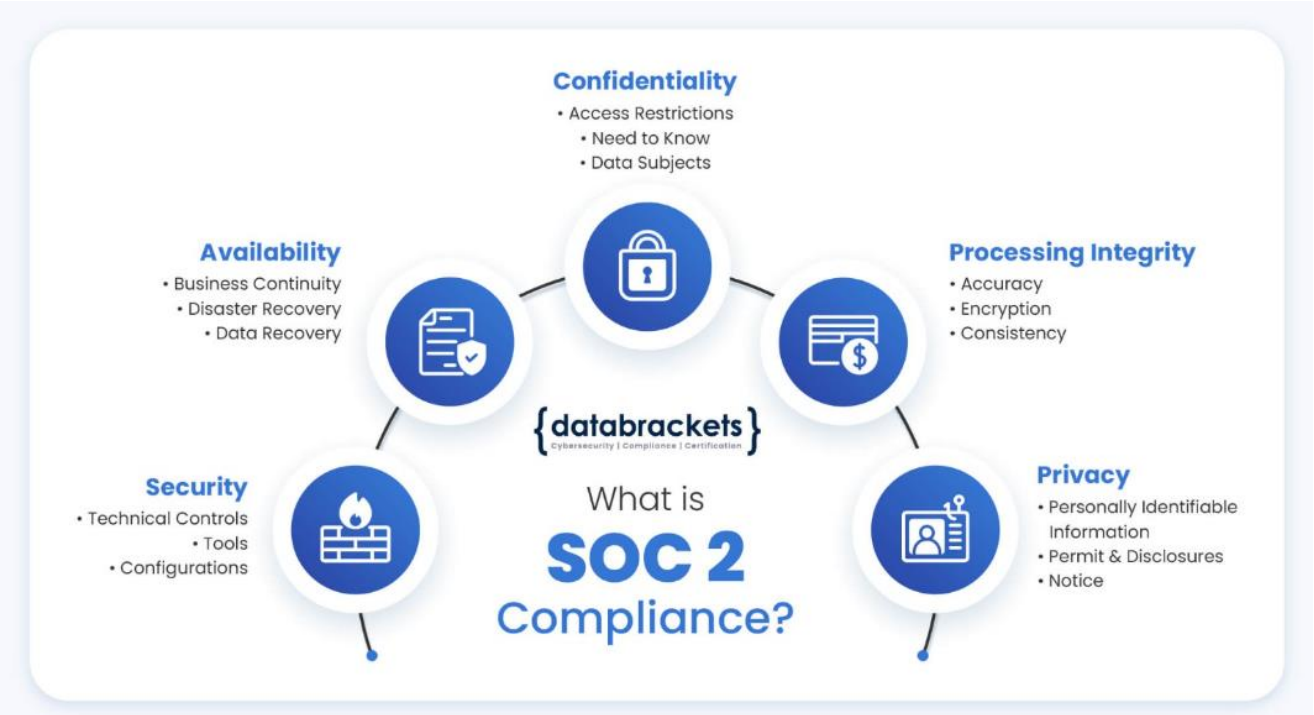
SOC 2

SYSTEM AND ORGANIZATION CONTROLS 2



SOC 2 (System and Organization Controls 2) es un estándar desarrollado por el American Institute of CPAs (AICPA) para evaluar la efectividad de los controles relacionados con:

1. La seguridad,
2. Disponibilidad,
3. Integridad del procesamiento,
4. Confidencialidad
5. Privacidad de los datos en las organizaciones de servicios.

Es especialmente relevante para empresas que almacenan o procesan información del cliente, ya que asegura a los clientes y stakeholders que la organización ha implementado controles adecuados para proteger la información.

INFORME SOBRE CUMPLIMIENTO SOC 2

Principios de Confianza de SOC 2

1. SEGURIDAD:

- Protege contra el acceso no autorizado, tanto físico como lógico.
- Implementa controles para prevenir y detectar actividades maliciosas.
- Utiliza firewalls, sistemas de detección de intrusiones y medidas de autenticación estrictas.

2. DISPONIBILIDAD:

- Garantiza que los sistemas estén operativos y disponibles según los compromisos o acuerdos establecidos.
- Incluye controles para monitorear y mantener la infraestructura de TI, minimizar el tiempo de inactividad y gestionar la capacidad.

3. INTEGRIDAD DEL PROCESAMIENTO:

- Asegura que los sistemas de procesamiento funcionen correctamente, de manera completa, precisa y autorizada.
- Implementa controles para validar la entrada de datos, el procesamiento y la salida para prevenir errores.

4. CONFIDENCIALIDAD:

- Protege la información clasificada como confidencial según acuerdos o compromisos.
- Utiliza cifrado y controles de acceso para garantizar que solo el personal autorizado tenga acceso a la información confidencial.

5. PRIVACIDAD:

- Maneja la información personal de acuerdo con los principios de privacidad establecidos.
- Implementa políticas para la recolección, uso, retención, divulgación y eliminación de información personal.

PROCESO DE CUMPLIMIENTO SOC 2

1. DEFINICIÓN DEL ALCANCE Y OBJETIVOS:

- Determina qué sistemas y servicios serán evaluados.
- Identifica los principios de confianza relevantes para la organización.

2. PREPARACIÓN:

- Documenta las políticas, procedimientos y controles existentes.
- Realiza una evaluación de brechas para identificar áreas de mejora.

3. EVALUACIÓN DE RIESGOS:

- Identifica y evalúa los riesgos potenciales que puedan afectar la seguridad, disponibilidad, integridad del procesamiento, confidencialidad y privacidad.

4. IMPLEMENTACIÓN DE CONTROLES:

- Establece controles para mitigar los riesgos identificados.
- Documenta y prueba los controles para asegurar su efectividad.

5. AUDITORÍA INTERNA:

- Realiza una auditoría interna para verificar que los controles están funcionando correctamente.

- Documenta los hallazgos y realiza ajustes según sea necesario.

6. AUDITORÍA EXTERNA:

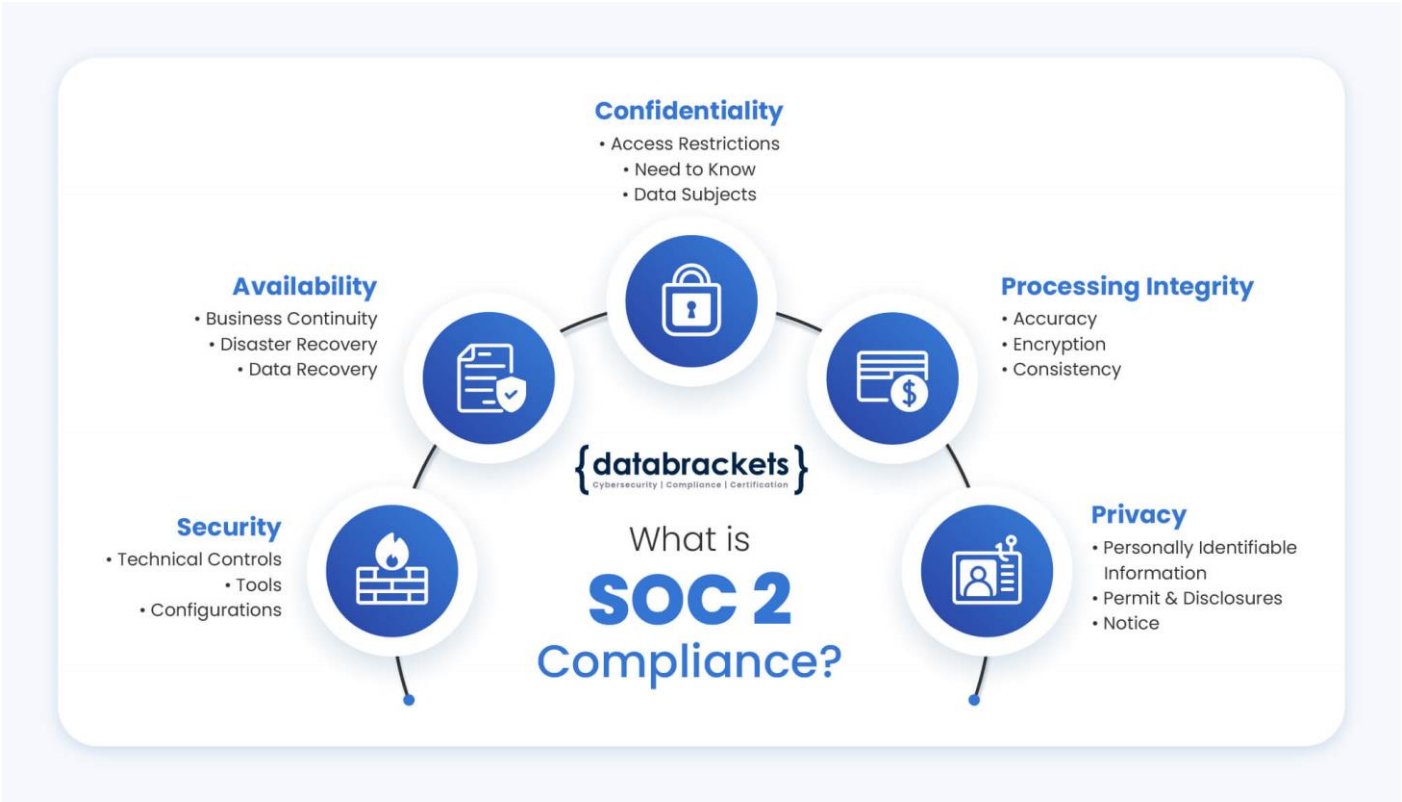
- Un auditor externo independiente realiza una evaluación formal.
- El auditor emite un informe SOC 2 detallando la efectividad de los controles implementados.

BENEFICIOS DEL CUMPLIMIENTO SOC 2

- Confianza del Cliente: Asegura a los clientes que su información está protegida adecuadamente.
- Ventaja Competitiva: Diferencia a la organización en el mercado.
- Cumplimiento Normativo: Ayuda a cumplir con diversas regulaciones y requisitos legales.
- Mejora de Procesos: Fomenta la mejora continua de los procesos de seguridad y gestión de riesgos.

CONCLUSIÓN

El cumplimiento de SOC 2 es esencial para organizaciones que manejan datos sensibles de clientes, proporcionando una estructura robusta para la gestión de la seguridad, disponibilidad, integridad del procesamiento, confidencialidad y privacidad de la información. Implementar y mantener un programa de cumplimiento SOC 2 puede proporcionar a las organizaciones una ventaja competitiva significativa, garantizar la confianza de los clientes y mejorar la postura general de seguridad.



CUESTIONARIO DE ELEMENTOS EMPRESARIALES

REQUERIMIENTOS	Descripción	Estado
Misión		
Visión		
Sedes	Sedes o branches en Colombia u otros paises	
# de empleados		
Normograma o leyes que deben cumplir	Leyes y entes reguladores a quienes deben reportar o cumplir normas	
Análisis de contexto	Clientes Interno y externos	
Mapa de procesos		
Procesos		
Organigrama		
Politicas SI		
Procedimientos		
Gobierno de TI	Estructura organizacional en el area de TI, con roles y responsables	
Informe de Auditorias Previas	Si existen	
Matriz de gestion de riesgos TI	Si existe	
Planes de tratamiento	Si existen	
Inventario de activos de información	Requiero el listado o inventarios de activos de información. Por ejemplo: Aplicaciones, servidores, switches, pc, impresoras, discos duros, etc.	
Diagrama de Red de alto nivel	Diagrama que refleje el esquema de interconexión de las redes o comunicaciones en la empresa.	
Listado de proveedores críticos que tengan acceso a información o infraestructura	Listado de proveedores que tengan acceso a la info de la empresa.	