# Lista de verificación de controles y cumplimiento

Para completar la lista de verificación de evaluación de controles, consulte la información proporcionada en el [Informe de evaluación de alcance, objetivos y riesgos.](https://docs.google.com/document/d/1s2u_RuhRAI40JSh-eZHvaFsV1ZMxcNSWXifHDTOsgFc/template/preview#heading=h.evidx83t54sc). Para obtener más detalles sobre cada control, incluido el tipo y propósito, consulte la [categorías de control](https://docs.google.com/document/d/1btezuy_bMKWoK8pd97ZuzdWB9y6au_zfkrpkfVf8ktI/template/preview) documento.

Luego, seleccione “sí” o “no” para responder la pregunta: *¿Botium Toys cuenta actualmente con este control?*

**Lista de verificación de evaluación de controles**

| **Sí** | **No** | **Control** |
| --- | --- | --- |
|  |  | Mínimo privilegio |
|  |  | Planes de recuperación de desastres |
|  |  | Políticas de contraseña |
|  |  | Separación de funciones |
|  |  | Cortafuegos |
|  |  | Sistema de detección de intrusos (IDS) |
|  |  | Copias de seguridad |
|  |  | software antivirus |
|  |  | Monitoreo, mantenimiento e intervención manuales para sistemas heredados |
|  |  | Cifrado |
|  |  | Sistema de gestión de contraseñas |
|  |  | Cerraduras (oficinas, escaparate, almacén) |
|  |  | Vigilancia por circuito cerrado de televisión (CCTV) |
|  |  | Detección/prevención de incendios (alarma de incendios, sistema de rociadores, etc.) |

Para completar la lista de verificación de cumplimiento, consulte la información proporcionada en el [informe de evaluación de riesgos, objetivos y alcance](https://docs.google.com/document/d/1s2u_RuhRAI40JSh-eZHvaFsV1ZMxcNSWXifHDTOsgFc/template/preview). Para obtener más detalles sobre cada norma de cumplimiento, revise la [controles, marcos y cumplimiento](https://www.coursera.org/learn/foundations-of-cybersecurity/supplement/xu4pr/controls-frameworks-and-compliance) lectura.

Luego, seleccione “sí” o “no” para responder la pregunta: *¿Botium Toys cumple actualmente con estas mejores prácticas de cumplimiento?*

**Lista de verificación de cumplimiento**

Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS)

| **Sí** | **No** | **Mejores prácticas** |
| --- | --- | --- |
|  |  | Sólo los usuarios autorizados tienen acceso a la información de la tarjeta de crédito de los clientes. |
|  |  | La información de la tarjeta de crédito se almacena, acepta, procesa y transmite internamente, en un entorno seguro. |
|  |  | Implemente procedimientos de cifrado de datos para proteger mejor los datos y los puntos de contacto de las transacciones con tarjetas de crédito. |
|  |  | Adopte políticas seguras de gestión de contraseñas. |

Reglamento General de Protección de Datos (GDPR)

| **Sí** | **No** | **Mejores prácticas** |
| --- | --- | --- |
|  |  | UE. Los datos de los clientes se mantienen privados/seguros. |
|  |  | Existe un plan para notificar a la UE. clientes dentro de las 72 horas si sus datos se ven comprometidos/hay una violación. |
|  |  | Asegúrese de que los datos estén clasificados e inventariados adecuadamente. |
|  |  | Hacer cumplir políticas, procedimientos y procesos de privacidad para documentar y mantener adecuadamente los datos. |

Controles de sistemas y organizaciones (SOC tipo 1, SOC tipo 2)

| **Sí** | **No** | **Mejores prácticas** |
| --- | --- | --- |
|  |  | Se establecen políticas de acceso de usuarios. |
|  |  | Los datos confidenciales (PII/SPII) son confidenciales/privados. |
|  |  | La integridad de los datos garantiza que los datos sean coherentes, completos, precisos y hayan sido validados. |
|  |  | Los datos están disponibles para las personas autorizadas a acceder a ellos. |