# Lista de verificación de controles y cumplimiento

**Lista de comprobación de evaluación de controles**

|  |  |  |
| --- | --- | --- |
| **Sí** | **No** | **Control** |
|  | X | Privilegio mínimo |
|  | X | Planes de recuperación ante desastres |
|  | X | Políticas de contraseñas |
|  | X | Separación de funciones |
| X |  | Cortafuegos/Firewalls |
|  | X | Sistema de detección de intrusos (IDS) |
|  | X | Backups/Copias de seguridad |
| X |  | Software antivirus |
|  | X | Supervisión, mantenimiento e intervención manuales para sistemas heredados |
|  | X | Encriptación |
|  | X | Sistema de gestión de contraseñas |
| X |  | Cerraduras (oficinas, escaparate, almacén) |
| X |  | Vigilancia de circuito cerrado de televisión (CCTV) |
| X |  | Detección/prevención de incendios (alarma contra incendios, sistema de rociadores, etc.) |

**Lista de comprobación de cumplimiento**

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

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

Reglamento General de Protección de Datos (RGPD)

|  |  |  |
| --- | --- | --- |
| **Sí** | **No** | **Mejores prácticas** |
| X |  | Los datos de los clientes de la UE se mantienen privados / seguros. |
| X |  | Existe un plan para notificar a los clientes de la UE dentro de las 72 horas si sus datos se ven comprometidos o hay una violación. |
| X |  | Asegúrese de que los datos estén correctamente clasificados e inventariados. |
| X |  | Hacer cumplir las 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** |
|  | X | Se establecen políticas de acceso de usuarios. |
|  | X | Los datos confidenciales (PII/SPII) son confidenciales/privados. |
| X |  | La integridad de los datos garantiza que los datos sean consistentes, completos, precisos y hayan sido validados. |
| X |  | Los datos están disponibles para las personas autorizadas a acceder a ellos. |

Se recomienda a la Organización Botium Toys mejorar estos controles y prácticas para mantener la privacidad y la seguridad de sus datos:

* Ya que todos los empleados cuentan con el acceso a los datos PII y SPII, se recomienda implementar el control de privilegio mínimo, esto garantiza que la información sea accesible solamente al personal necesario y también trabajar bajo la separación de funciones
* Se recomienda la encriptación y el cifrado de la información de las tarjetas de crédito de los clientes
* Instalar un sistema de detección de intrusos (IDS) que esté en constante monitoreo en momento de una vulnerabilidad
* Es de suma importancia elaborar un plan de recuperación de desastres así como también crear copias de seguridad de la información y datos críticos; en dado caso de que haya una brecha, tener plan de recuperación y copias para que los daños no sean tan perjudiciales
* Implementar políticas de contraseñas que se ajusten a los requisitos mínimos actuales de complejidad de contraseña. También crear un sistema de gestión de contraseñas que agilice la productividad cuando envían solicitudes de recuperación de contraseñas o restablecerlas
* Actualizaciones en sistemas heredados