Auditoría de Seguridad - Botium Toys

# 1. Evaluación de Controles de Seguridad

|  |  |  |
| --- | --- | --- |
| Control | ¿Está implementado? | Notas |
| Least Privilege | No | No se han implementado controles de acceso con el principio de privilegio mínimo. |
| Disaster Recovery Plans | No | No existen planes de recuperación ni copias de seguridad. |
| Password Policies | Parcialmente | Existe una política de contraseñas, pero no cumple con los requisitos mínimos de seguridad. |
| Separation of Duties | No | No se ha implementado la separación de funciones. |
| Firewall | Sí | Hay un firewall con reglas de seguridad adecuadas. |
| Intrusion Detection System (IDS) | No | No se ha instalado un IDS. |
| Backups | No | No existen copias de seguridad de datos críticos. |
| Antivirus Software | Sí | Hay software antivirus instalado y monitoreado. |
| Manual monitoring of legacy systems | No | No hay un cronograma definido ni procesos claros de mantenimiento. |
| Encryption | No | No se usa cifrado para proteger la información de las tarjetas de crédito. |
| Password Management System | No | No hay un sistema centralizado de gestión de contraseñas. |
| Locks (offices, storefront, warehouse) | Sí | Se cuenta con cerraduras físicas en las instalaciones. |
| CCTV Surveillance | Sí | Hay un sistema de vigilancia CCTV actualizado. |
| Fire Detection/Prevention | Sí | Existen alarmas contra incendios y sistemas de prevención. |

# 2. Evaluación de Cumplimiento Normativo

|  |  |  |
| --- | --- | --- |
| Regulación | ¿Cumple con la normativa? | Notas |
| PCI DSS | No | No hay cifrado ni control de acceso adecuado para la información de tarjetas. |
| GDPR | Parcialmente | Se notifican brechas de seguridad en 72 horas y hay políticas de privacidad, pero falta clasificación de datos y mayor seguridad en su almacenamiento. |
| SOC 1/SOC 2 | No | No hay controles adecuados para garantizar la confidencialidad e integridad de los datos. |

# 3. Recomendaciones para Mejorar la Seguridad

• Implementar controles de acceso (Least Privilege y Separation of Duties) para restringir el acceso a datos sensibles.

• Crear un plan de recuperación ante desastres y establecer un sistema de copias de seguridad para proteger los datos críticos.

• Actualizar la política de contraseñas para cumplir con estándares de seguridad y establecer un gestor de contraseñas centralizado.

• Implementar cifrado en los datos de tarjetas de crédito para cumplir con PCI DSS.

• Instalar un sistema de detección de intrusiones (IDS) para monitorear actividades sospechosas en la red.

• Mejorar la gestión de sistemas heredados estableciendo un cronograma claro de mantenimiento.