# Botium Toys - Auditoría de Seguridad Interna

## Controls and Compliance Checklist

### Controls Assessment Checklist

|  |  |  |
| --- | --- | --- |
| Control | Implementado | Explicación |
| Least Privilege | No | Todos los empleados tienen acceso a datos internos, incluidas tarjetas y PII. Se debe restringir el acceso según roles. |
| Disaster recovery plans | No | No existen planes formales ni backups. Es esencial para garantizar la continuidad operativa. |
| Password policies | No | Las contraseñas actuales no cumplen requisitos mínimos (longitud, complejidad). |
| Separation of duties | No | No se aplica; funciones críticas están centralizadas. Esto aumenta el riesgo de errores o fraudes internos. |
| Firewall | Sí | Está activo y bien configurado, bloqueando tráfico no deseado. |
| Intrusion Detection System (IDS) | No | No se ha implementado ningún IDS; esto reduce la capacidad de detectar amenazas activas. |
| Backups | No | No existen copias de seguridad. |
| Antivirus software | Sí | Se encuentra instalado y actualizado por el departamento de TI. |
| Monitoreo manual de sistemas legacy | Parcial | Hay monitoreo, pero sin cronograma ni procedimientos documentados. |
| Encryption | No | No se usa cifrado para datos sensibles; esto expone información crítica. |
| Password management system | No | No hay sistema centralizado, lo que impacta la productividad ante olvidos. |
| Locks (oficinas, tienda, almacén) | Sí | Las instalaciones están aseguradas con cerraduras físicas. |
| CCTV | Sí | El sistema CCTV está en funcionamiento. |
| Detección y prevención de incendios | Sí | Sistemas de detección y extinción de incendios están operativos. |

### Compliance Checklist

#### PCI DSS

|  |  |  |
| --- | --- | --- |
| Buenas Prácticas | Cumple | Explicación |
| Solo usuarios autorizados acceden a tarjetas de clientes | No | Todos los empleados pueden acceder a los datos. |
| Información de tarjetas se procesa en entorno seguro | No | No hay cifrado ni control de acceso. |
| Cifrado de datos de tarjetas | No | No se ha implementado cifrado. |
| Políticas seguras de gestión de contraseñas | No | No hay políticas robustas ni gestor de contraseñas. |

#### GDPR

|  |  |  |
| --- | --- | --- |
| Buenas Prácticas | Cumple | Explicación |
| Protección de datos de clientes de la UE | No | No se usa cifrado ni controles de acceso. |
| Notificación en 72h ante brechas | Sí | Plan documentado por el equipo de TI. |
| Clasificación e inventario de datos | No | El inventario existe, pero no hay clasificación de datos. |
| Políticas de privacidad aplicadas | Sí | Se aplican en el equipo TI y otros empleados. |

#### SOC 1 / SOC 2

|  |  |  |
| --- | --- | --- |
| Buenas Prácticas | Cumple | Explicación |
| Políticas de acceso de usuarios | No | Todos los usuarios tienen acceso irrestricto. |
| Datos sensibles (PII/SPII) protegidos | No | No se aplica cifrado; todos tienen acceso. |
| Integridad de datos validada | Sí | Está asegurada por controles internos del departamento de TI. |
| Acceso a datos solo para personal autorizado | No | Actualmente, está disponible para todos los empleados. |