Auditoría de Seguridad de TI de Botium Toys

A continuación se muestra un resumen de toda la auditoría simplificando los cambios que se realizarán a fin de mejorar la seguridad y mitigar riesgos futuros.

Resumen

El objetivo de la auditoría fue evaluar la postura de seguridad actual de Botium Toys, identificar riesgos y recomendar controles para mitigar estos riesgos. Este proceso asegura la continuidad del negocio y el cumplimiento normativo a medida que la empresa crece.

Principales Hallazgos y Recomendaciones:

1. **Fortalecimiento de Políticas y Procedimientos (Controles Administrativos)**
    - **Principio de mínimo privilegio**: Limitar el acceso a la información solo a aquellos empleados que lo necesiten para sus funciones. Esto reduce significativamente el riesgo de acceso no autorizado.
    - **Planes de recuperación ante incidentes**: Desarrollar y probar regularmente para asegurar la continuidad del negocio durante incidentes críticos.
    - **Políticas de gestión de cuentas y control de acceso**: Implementar y hacer cumplir políticas robustas para gestionar el ciclo de vida de las cuentas y definir claramente quién puede acceder a qué información.
2. **Mejoras en la Infraestructura de Seguridad (Controles Técnicos)**
    - **Sistema de detección de intrusiones (IDS)**: Implementar un IDS para detectar actividades sospechosas en la red en tiempo real.
    - **Cifrado de datos**: Utilizar cifrado para proteger los datos sensibles, asegurando la confidencialidad de la información crítica.
    - **Copias de seguridad**: Realizar copias de seguridad regulares para asegurar la recuperación rápida de datos en caso de pérdida.
3. **Seguridad Física de los Activos (Controles Físicos)**
    - **Cerraduras y gabinetes seguros**: Instalar cerraduras en puertas y gabinetes de equipos de red para prevenir accesos no autorizados.
    - **Sistemas de detección y prevención de incendios**: Implementar estos sistemas para proteger los activos físicos de daños por incendios.

Plan de Implementación:

- **Corto Plazo (1-3 meses)**: Implementar políticas de control de acceso y gestión de cuentas, e instalar cerraduras en gabinetes de equipos de red.
- **Mediano Plazo (4-6 meses)**: Desarrollar y probar planes de recuperación ante incidentes, e implementar un IDS y cifrado de datos.
- **Largo Plazo (7-12 meses)**: Establecer la separación de funciones críticas y proveer capacitación en seguridad para empleados.

Beneficios Esperados:

- **Reducción de Riesgos**: Mitigación de riesgos asociados con accesos no autorizados, pérdida de datos y amenazas internas.
- **Cumplimiento Normativo**: Asegurar el cumplimiento con normativas relevantes, como el PCI DSS para pagos en línea y posibles regulaciones de protección de datos.
- **Mejora en la Resiliencia del Negocio**: Preparación adecuada para responder a incidentes, garantizando la continuidad del negocio.

Conclusión:

Implementar estos controles es esencial para fortalecer la seguridad de Botium Toys y garantizar su crecimiento sostenible. Estas medidas protegerán la infraestructura de la empresa, mantendrán la confianza de los clientes y socios comerciales, y asegurarán el cumplimiento normativo.