Auditoría de Seguridad

Lista de Verificación de Controles y Cumplimiento

Marque con una "X" en la columna correspondiente para responder a la pregunta: ¿Actualmente cuenta Botium Toys con este control?

Lista de Verificación para la Evaluación de Controles

Sí	No	Control	Explicación
	X	Privilegio mínimo	Actualmente, todos los empleados tienen acceso a la información de los clientes; es necesario restringir los privilegios para minimizar el riesgo de una violación de seguridad.
X		Planes de recuperación ante desastres	No se cuenta con planes de recuperación en caso de desastre. Es fundamental implementarlos para asegurar la continuidad de las operaciones.
X		Políticas de contraseñas	Las políticas de contraseñas son poco exigentes, lo cual podría facilitar que un atacante acceda a datos protegidos y otros activos a través de los dispositivos de los empleados o de la red corporativa.
X		Separación de funciones	Es importante aplicar esta medida para disminuir el riesgo de fraude y el acceso a información sensible, ya que el CEO actualmente gestiona tanto las operaciones diarias como la administración de la nómina.
X		Cortafuegos	El firewall actual bloquea el tráfico de acuerdo con reglas de seguridad adecuadamente definidas.
	X	Sistema de detección de intrusos (IDS)	El departamento de TI necesita un IDS para ayudar a identificar posibles intrusiones por parte de amenazas externas.
	X	Copias de seguridad	Es necesario que el departamento de TI mantenga copias de seguridad de los datos críticos, para garantizar la continuidad operativa en caso de una violación de datos.
X		Software antivirus	El departamento de TI supervisa y actualiza el software antivirus de forma regular.
	X	Supervisión, mantenimiento e intervención para sistemas heredados	Los activos incluyen sistemas heredados. Aunque estos sistemas son supervisados y mantenidos, no existe un calendario de mantenimiento regular ni

			políticas claras de intervención, lo cual podría aumentar su vulnerabilidad.
	X	Cifrado	Actualmente no se utiliza cifrado; su implementación mejoraría la protección de la información sensible.
	X	Sistema de gestión de contraseñas	No se cuenta con un sistema de gestión de contraseñas; implementarlo facilitaría la resolución de problemas de acceso, beneficiando tanto al departamento de TI como a otros empleados.
X		Cerraduras (oficinas, tienda, almacén)	Las instalaciones, que incluyen oficinas, tienda y almacén, cuentan con sistemas de cerraduras adecuados.
X		Vigilancia CCTV	El sistema de circuito cerrado de televisión está instalado y en funcionamiento en las instalaciones físicas de la tienda.
X		Detección/prevención de incendios (alarmas, rociadores, etc.)	Las instalaciones físicas de Botium Toys cuentan con sistemas funcionales de detección y prevención de incendios.

Lista de Verificación de Cumplimiento

Marque con una "X" en la columna correspondiente para indicar si Botium Toys actualmente cumple con esta mejor práctica.

Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS)

Sí	No	Mejores Prácticas	Explicación
	X	Solo los usuarios autorizados tienen acceso a la información de las tarjetas de crédito de los clientes.	Actualmente, todos los empleados pueden acceder a los datos internos de la empresa.
X		La información de las tarjetas de crédito se acepta, procesa, transmite y almacena en un entorno seguro.	La información de las tarjetas no está encriptada y todos los empleados pueden acceder a estos datos.
X		Implementar procedimientos de cifrado de datos para proteger puntos de contacto y transacciones con tarjetas de crédito.	La empresa no utiliza cifrado para proteger mejor la información financiera de sus clientes.
X		Adoptar políticas seguras de gestión de contraseñas.	Las políticas de contraseñas actuales son mínimas, y no se cuenta con un sistema de administración de contraseñas.

Reglamento General de Protección de Datos (RGPD)

Sí	No	Mejores Prácticas	Explicación
	X	Los datos de los clientes de la UE se mantienen privados y protegidos.	La empresa no emplea cifrado para asegurar la confidencialidad de la información financiera de los clientes.
X		Existe un plan para notificar a los clientes de la UE en un plazo de 72 horas si sus datos se ven comprometidos.	Existe un plan para informar a los clientes de la UE dentro de las 72 horas posteriores a una violación de datos.
	X	Asegurar que los datos estén clasificados e inventariados correctamente.	Los activos actuales están inventariados, pero no clasificados.
X		Aplicar políticas, procedimientos y procesos de privacidad para gestionar adecuadamente los datos.	Se han implementado políticas y procedimientos de privacidad en el equipo de TI y entre otros empleados, cuando es necesario.

Controles de Sistemas y Organizaciones (SOC tipo 1, SOC tipo 2)

Sí	No	Mejores Prácticas	Explicación
	X	Establecer políticas de acceso de usuarios.	No se han implementado controles de privilegios mínimos ni de separación de funciones, y todos los empleados tienen acceso a los datos internos.
X		Garantizar que los datos sensibles (PII/SPII) se mantengan confidenciales y privados.	Actualmente no se emplea cifrado para asegurar la confidencialidad de los datos PII/SPII.
X		Asegurar que la integridad de los datos se mantenga constante, completa, precisa y validada.	Se han implementado medidas para mantener la integridad de los datos.
	X	Asegurar la disponibilidad de los datos para usuarios autorizados.	Los datos están disponibles para todos los empleados, pero el acceso debe limitarse a quienes realmente lo necesiten para desempeñar sus funciones.

Recomendaciones (opcional):

Es fundamental implementar varios controles para mejorar la seguridad de Botium Toys y asegurar la confidencialidad de la información sensible, incluyendo privilegios mínimos, planes de recuperación ante desastres, políticas de contraseñas, separación de funciones, un IDS, mantenimiento continuo de sistemas heredados, cifrado y un sistema de gestión de contraseñas.

Para subsanar las brechas en el cumplimiento, Botium Toys debería implementar controles como el privilegio mínimo, la separación de funciones y el cifrado. Además, se debe clasificar correctamente los activos para identificar los controles adicionales necesarios que puedan fortalecer la seguridad y proteger mejor la información sensible.