Botium Toys: Gestión de riesgos

Activos actuales

Entre los activos administrados por el departamento de TI se encuentran los siguientes:

- Equipos en las instalaciones para las necesidades comerciales en la oficina.
- Equipos del personal: dispositivos de usuario final (computadoras de escritorio/portátiles, teléfonos inteligentes), estaciones de trabajo remotas, auriculares, cables, teclados, mouse, estaciones de acoplamiento, cámaras de vigilancia, etc.
- Gestión de sistemas, software y servicios: contabilidad, telecomunicaciones, bases de datos, seguridad, comercio electrónico y gestión de inventario.
- Acceso a Internet.
- Red interna.
- Gestión de acceso a proveedores.
- Servicios de alojamiento del centro de datos.
- Retención y almacenamiento de datos.
- Lectores de tarjetas de identificación.
- Mantenimiento de sistemas heredados: sistemas obsoletos que requieren supervisión humana.

Descripción del riesgo

Actualmente, existe una gestión insuficiente de los activos. Además, Botium Toys no ha implementado los controles adecuados y es posible que no cumpla con las regulaciones y los estándares estadounidenses e internacionales.

Prácticas recomendadas de control

La primera de las cinco funciones del Marco de Ciberseguridad del NIST es la identificación. Botium Toys deberá asignar recursos para gestionar los activos. Además, tendrá que determinar el impacto de la pérdida de los activos existentes, incluidos los sistemas, en la continuidad del negocio.

Puntuación de riesgo

En una escala de 1 a 10, la puntuación de riesgo es de 8, lo cual es bastante alto. Esto se debe a la falta de controles y cumplimiento de las regulaciones y los estándares necesarios.

Comentarios adicionales

El impacto potencial por la pérdida de un activo se califica como medio, debido a que el departamento de TI no sabe qué activos se perderían. La probabilidad de pérdida de un activo o de multas por parte de órganos reguladores es alta, ya que Botium Toys no tiene todos los controles necesarios implementados y no cumple con las normativas y estándares requeridos para mantener la privacidad de los datos de laslos clientes.