Botium Toys: Evaluación de riesgos

Activo circulante

Los activos administrados por el Departamento de TI incluyen:

1. Equipos locales para las necesidades empresariales en la oficina
2. Equipos de los empleados: dispositivos de usuario final (ordenadores de sobremesa/portátiles, smartphones), estaciones de trabajo remotas, auriculares, cables, teclados, ratones, estaciones de acoplamiento, cámaras de vigilancia, etcétera.
3. Gestión de sistemas, software y servicios: contabilidad, telecomunicaciones, bases de datos, seguridad, comercio electrónico y gestión de inventarios
4. Acceso a Internet
5. Red interna
6. Gestión de acceso de proveedores
7. Servicios de alojamiento de centros de datos
8. Retención y almacenamiento de datos
9. Lectores de credenciales
10. Mantenimiento de sistemas heredados: sistemas al final de su vida útil que requieren supervisión humana

Descripción del riesgo

En la actualidad, existe una gestión inadecuada de los activos. Además, Botium Toys no cuenta con los controles adecuados y es posible que no cumpla con las regulaciones y estándares estadounidenses e internacionales.

Prácticas recomendadas de control

La primera de las cinco funciones del CSF del NIST es Identificar. Botium Toys tendrá que dedicar recursos a la gestión de los activos. Además, deberán determinar el impacto de la pérdida de activos existentes, incluidos los sistemas, en la continuidad del negocio.

Puntuación de riesgo

En una escala del 1 al 10, la puntuación de riesgo es 8, que es bastante alta. Esto se debe a la falta de controles y al cumplimiento de las normas y reglamentos de cumplimiento necesarios.

Comentarios adicionales

El impacto potencial de la pérdida de un activo se califica como medio, porque el departamento de TI no sabe qué activos se perderían. La probabilidad de que se pierda un activo o de que se impongan multas por parte de los órganos de gobierno es alta porque Botium Toys no cuenta con todos los controles necesarios y no cumple con las regulaciones y normas requeridas relacionadas con la privacidad de los datos de los clientes.