# Ejemplo de memorando de partes interesadas

PARA: Gerente de TI, partes interesadas

DE: (Su nombre)   
FECHA: (Fecha de hoy)   
ASUNTO: Hallazgos y recomendaciones de auditoría interna de TI

Estimados colegas,

Revise la siguiente información sobre el alcance de la auditoría interna, los objetivos, los hallazgos críticos, el resumen y las recomendaciones de Botium Toys.

**Alcance:**

* Los siguientes sistemas están incluidos en el alcance: contabilidad, detección de puntos finales, cortafuegos, sistema de detección de intrusiones y herramienta SIEM. Los sistemas se evaluarán en cuanto a:
  + Permisos de usuario actuales
  + Controles implementados actualmente
  + Procedimientos y protocolos actuales
* Asegúrese de que los permisos de usuario, controles, procedimientos y protocolos actuales estén alineados con los requisitos de cumplimiento de PCI DSS y GDPR.
* Asegúrese de que se tenga en cuenta la tecnología actual tanto para el hardware como para el acceso al sistema.

**Objetivos:**

* Adherirse al NIST CSF.
* Establecer un mejor proceso para sus sistemas para garantizar que cumplan con las normas.
* Fortalecer los controles del sistema.
* Adaptarse al concepto de permisos mínimos cuando se trata de la gestión de credenciales de usuario.
* Establecer sus políticas y procedimientos, incluidos sus manuales de estrategias.
* Asegúrese de que cumplan con los requisitos de cumplimiento.

**Hallazgos críticos** (deben abordarse de inmediato):

* Es necesario desarrollar e implementar múltiples controles para cumplir los objetivos de auditoría, entre ellos:
  + Control de privilegios mínimos y separación de funciones
  + Planes de recuperación ante desastres
  + Políticas de contraseñas, control de acceso y gestión de cuentas, incluida la implementación de un sistema de gestión de contraseñas
  + Cifrado (para transacciones seguras en sitios web)
  + Identificación
  + Copias de seguridad
  + Software antivirus
  + Circuito cerrado de televisión
  + Cabellos
  + Monitoreo, mantenimiento e intervención manual para sistemas heredados
  + Sistemas de detección y prevención de incendios
* Es necesario desarrollar e implementar políticas para cumplir con los requisitos de cumplimiento de PCI DSS y GDPR.
* Es necesario desarrollar e implementar políticas que se alineen con las pautas SOC1 y SOC2 relacionadas con las políticas de acceso de los usuarios y la seguridad general de los datos.

**Hallazgos** (deberían abordarse, pero no hay necesidad inmediata):

* Se deben implementar los siguientes controles cuando sea posible:
  + Caja fuerte controlada por tiempo
  + Iluminación adecuada
  + Armarios con cerradura
  + Señalización que indica el proveedor del servicio de alarma

**Resumen/Recomendaciones:** Se recomienda abordar de inmediato los hallazgos críticos relacionados con el cumplimiento de PCI DSS y GDPR, ya que Botium Toys acepta pagos en línea de clientes de todo el mundo, incluida la UE. Además, dado que uno de los objetivos de la auditoría es adaptarse al concepto de permisos mínimos, se deben utilizar las pautas SOC1 y SOC2 relacionadas con las políticas de acceso de los usuarios y la seguridad general de los datos para desarrollar políticas y procedimientos adecuados. Tener planes de recuperación ante desastres y copias de seguridad también es fundamental porque respaldan la continuidad del negocio en caso de un incidente. La integración de un software de IDS y AV en los sistemas actuales respaldará nuestra capacidad de identificar y mitigar riesgos potenciales, y podría ayudar con la detección de intrusiones, ya que los sistemas heredados existentes requieren monitoreo e intervención manuales. Para proteger aún más los activos alojados en la ubicación física única de Botium Toys, se deben usar cerraduras y CCTV para proteger los activos físicos (incluido el equipo) y para monitorear e investigar las amenazas potenciales. Si bien no es necesario de inmediato, el uso de cifrado y tener una caja fuerte controlada por tiempo, iluminación adecuada, gabinetes con cerradura, sistemas de detección y prevención de incendios y señalización que indique el proveedor de servicios de alarma mejorarán aún más la postura de seguridad de Botium Toys.