# Stakeholder memorandum

Complete each section of the stakeholder memorandum template to communicate your audit results and recommendations to stakeholders:

* Scope
* Goals
* Critical findings (must be addressed immediately)
* Findings (should be addressed, but no immediate need)
* Summary/Recommendations

Use information from the following documents:

* [Botium Toys: Audit scope and goals](https://docs.google.com/document/d/1bA-J96jzDVFi9XjNOKd4w2bCR7X7ZTs3_szPElOkyFM/template/preview)
* Controls assessment (completed in “Conduct a security audit, part 1”)
* Compliance checklist (completed in “Conduct a security audit, part 1”)

### *[Use the following template to create your memorandum]*

TO: IT Manager, Stakeholders

FROM: José Escamilla

DATE: July 15, 2024

SUBJECT: Internal IT Audit Findings and Recommendations

Dear Colleagues,

Please review the following information regarding the Botium Toys internal audit scope, goals, critical findings, summary, and recommendations.

Scope:

The internal IT audit of Botium Toys encompassed a comprehensive assessment of the entire security program, including user permissions, implemented controls, procedures, and compliance alignment across critical systems such as accounting, endpoint detection, firewalls, intrusion detection systems, and the Security Information and Event Management (SIEM) tool. The audit also included an inventory of current technology assets, both hardware and system access.

Goals:

The goals of the internal IT audit were:

1. Adherence to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).
2. Establishment of robust processes to ensure system compliance.
3. Strengthening of system controls.
4. Implementation of least privilege principles in user credential management.
5. Establishment of comprehensive security policies, procedures, and playbooks.
6. Assurance of compliance with regulatory requirements.

Critical findings (must be addressed immediately):

1. Inadequate User Permission Management: Immediate implementation of least privilege principles to restrict user access to only necessary resources.
2. Insufficient Security Controls: Urgent establishment and reinforcement of security controls across critical systems, including multi-factor authentication and continuous security event monitoring.
3. Lack of Formalized Security Policies: Immediate development and implementation of comprehensive security policies, operational playbooks, and incident response plans to enhance organizational resilience.

Findings (should be addressed, but no immediate need):

1. Asset Management: Improvement needed in inventory and management of technological assets, including end-user devices and critical systems.
2. Compliance Issues: Address potential gaps in compliance with U.S. and international regulations related to data privacy and online payment acceptance.

Summary/Recommendations: In summary, Botium Toys faces critical vulnerabilities in user permission management, security controls, and formalized security policies that require immediate attention to mitigate risks effectively. Addressing these issues promptly will enhance the organization's security posture and ensure compliance with regulatory standards. It is recommended to allocate resources and prioritize these initiatives to safeguard company assets and maintain customer trust.

Please let me know if you require further details or clarification on any aspect of the audit findings.

Best regards,

José Escamilla

### *[Use the following template to create your memorandum] Spanish*

TO: Gerente de TI, Partes Interesadas  
DE: José Escamilla   
FECHA: 15 de julio de 2024  
ASUNTO: Resultados y Recomendaciones de la Auditoría Interna de TI

Estimados colegas,

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

**Alcance:**

La auditoría interna de TI de Botium Toys abarcó una evaluación integral del programa de seguridad, incluyendo permisos de usuario, controles implementados, procedimientos y alineación de cumplimiento en sistemas críticos como contabilidad, detección de puntos finales, firewalls, sistemas de detección de intrusiones y la herramienta de Gestión de Información y Eventos de Seguridad (SIEM). La auditoría también incluyó un inventario de activos tecnológicos actuales, tanto hardware como acceso a sistemas.

**Objetivos:**

Los objetivos de la auditoría interna de TI fueron:

* Adherencia al Marco de Ciberseguridad del Instituto Nacional de Normas y Tecnología (NIST CSF).
* Establecimiento de procesos robustos para garantizar el cumplimiento del sistema.
* Fortalecimiento de los controles del sistema.
* Implementación de principios de privilegio mínimo en la gestión de credenciales de usuario.
* Establecimiento de políticas, procedimientos y playbooks de seguridad integrales.
* Aseguramiento del cumplimiento de requisitos normativos.

Hallazgos Críticos (deben abordarse inmediatamente):

1. **Gestión Inadecuada de Permisos de Usuario:** Implementación inmediata de principios de privilegio mínimo para restringir el acceso de los usuarios solo a los recursos necesarios.
2. **Controles de Seguridad Insuficientes:** Establecimiento urgente y refuerzo de controles de seguridad en sistemas críticos, incluyendo autenticación multifactor y monitoreo continuo de eventos de seguridad.
3. **Falta de Políticas de Seguridad Formalizadas:** Desarrollo e implementación inmediata de políticas de seguridad integrales, playbooks operativos y planes de respuesta a incidentes para mejorar la resiliencia organizacional.

Hallazgos (deben abordarse, pero no hay necesidad inmediata):

1. **Gestión de Activos:** Se necesita mejorar el inventario y la gestión de activos tecnológicos, incluidos dispositivos de usuarios finales y sistemas críticos.
2. **Problemas de Cumplimiento:** Abordar posibles brechas de cumplimiento con regulaciones nacionales e internacionales relacionadas con la privacidad de datos y la aceptación de pagos en línea.

**Resumen/Recomendaciones:**

En resumen, Botium Toys enfrenta vulnerabilidades críticas en la gestión de permisos de usuario, controles de seguridad y políticas de seguridad formalizadas que requieren atención inmediata para mitigar los riesgos de manera efectiva. Abordar estos problemas de manera oportuna mejorará la postura de seguridad de la organización y garantizará el cumplimiento de estándares regulatorios. Se recomienda asignar recursos y priorizar estas iniciativas para proteger los activos de la empresa y mantener la confianza del cliente.

Por favor, háganme saber si necesitan más detalles o aclaraciones sobre algún aspecto de los hallazgos de la auditoría.

Atentamente,

José Escamilla

### 