INFORME DE AUDITORÍA INTERNA DE SEGURIDAD DE LA INFORMACIÓN

Empresa: Botium Toys
Tipo: Auditoría Interna de TI
Auditor responsable: Britanny Labraña
Fecha: 28-02-2026

1. Resumen Ejecutivo

Botium Toys es una empresa con crecimiento acelerado en comercio electrónico nacional e internacional. Este crecimiento incrementa su superficie de ataque y su exposición a riesgos regulatorios, particularmente en materia de procesamiento de pagos y protección de datos personales en la Unión Europea.

La auditoría fue realizada aplicando el marco del NIST CSF, con el objetivo de evaluar la postura actual de seguridad, identificar riesgos críticos y determinar el nivel de cumplimiento normativo.

Resultado general:
La organización presenta una postura de seguridad reactiva y no formalizada, con brechas significativas en gobernanza, monitoreo continuo y cumplimiento regulatorio.

Nivel de riesgo global estimado: Medio-Alto

2. Alcance de la Auditoría

La auditoría incluyó:

- Infraestructura tecnológica (servidores, estaciones de trabajo, red interna)
- Plataforma de comercio electrónico
- Sistemas de procesamiento de pagos

- Gestión de datos personales (clientes EE.UU. y UE)
- Controles de seguridad física en la sede única
- Políticas y procedimientos documentados

No se incluyó pentesting ni pruebas técnicas invasivas (evaluación documental y de controles).

3. Metodología

Se utilizó el **NIST CSF**, estructurado en sus cinco funciones:

1. Identificar
2. Proteger
3. Detectar
4. Responder
5. Recuperar

Se realizó:

- Revisión documental
- Identificación de activos críticos
- Evaluación cualitativa de riesgos
- Revisión de cumplimiento regulatorio

4. Identificación de Activos Críticos

Activos Tecnológicos

- Servidor web de e-commerce
- Base de datos de clientes
- Sistema de pagos en línea
- Red corporativa
- Equipos de empleados

Activos de Información

- Datos personales identificables (PII)
- Información financiera
- Datos de tarjetas de pago
- Información comercial estratégica

Activos Físicos

- Oficina principal
- Almacén
- Equipamiento tecnológico

5. Evaluación de Riesgos

Riesgo	Probabilidad	Impacto	Nivel
Phishing a empleados	Alta	Alto	Crítico
Fuga de datos de clientes	Media	Muy Alto	Crítico
Incumplimiento GDPR	Media	Muy Alto	Crítico
Ataque ransomware	Media	Alto	Alto
Fraude en pagos online	Media	Alto	Alto
Acceso no autorizado interno	Media	Medio	Medio

6. Evaluación por Función del NIST CSF

6.1 IDENTIFICAR

Hallazgos:

- No existe inventario formal de activos.
- No hay clasificación de información documentada.
- No se identifican formalmente los requisitos regulatorios (UE).

Riesgo: Falta de gobernanza estructurada.

6.2 PROTEGER

Hallazgos:

- No se evidencia uso obligatorio de MFA.
- No existe política formal de control de acceso basada en roles.
- No se confirma cifrado de datos en reposo.
- Capacitación en seguridad no formalizada.

Cumplimiento requerido:

- GDPR para clientes UE.
- PCI-DSS para pagos con tarjeta.

Riesgo: Exposición a multas regulatorias y brechas de datos.

6.3 DETECTAR

Hallazgos:

- No existe monitoreo continuo de seguridad.
- No se revisan logs de forma sistemática.
- No hay sistema IDS/IPS implementado.

Riesgo: Detección tardía de incidentes.

6.4 RESPONDER

Hallazgos:

- No existe plan formal de respuesta a incidentes.
- No se han definido roles ante crisis.
- No existe protocolo de notificación ante brechas (UE exige notificación en 72 horas).

Riesgo: Escalada del daño y sanciones regulatorias.

6.5 RECUPERAR

Hallazgos:

- No existe plan documentado de continuidad de negocio (BCP).
- No se evidencia pruebas periódicas de respaldo.
- No hay plan de recuperación ante desastres (DRP).

Riesgo: Interrupción prolongada del negocio.

7. Evaluación de Cumplimiento Normativo

Debido a operaciones en la UE, se debe cumplir con:

- Reglamento General de Protección de Datos (GDPR)
- PCI-DSS para procesamiento de pagos
- Normativa de comercio electrónico internacional

Estado actual:
Cumplimiento parcial / No verificado formalmente.

Riesgo legal: Elevado.

8. Conclusión Profesional

Botium Toys presenta una madurez de seguridad baja a intermedia.
El crecimiento digital no ha sido acompañado por una estrategia formal de ciberseguridad.

Las principales brechas se concentran en:

- Gobernanza y documentación
- Monitoreo continuo
- Gestión de incidentes
- Cumplimiento regulatorio internacional

Si no se implementan mejoras, la organización enfrenta:

- Multas regulatorias (UE)
- Pérdida de reputación
- Interrupción operativa
- Impacto financiero significativo

9. Recomendaciones Prioritarias (Orden Crítico)

1. Implementar programa formal de seguridad alineado a NIST CSF.
2. Adoptar autenticación multifactor (MFA).
3. Implementar cifrado completo (datos en tránsito y reposo).
4. Desarrollar plan formal de respuesta a incidentes.
5. Implementar monitoreo continuo (SIEM básico).
6. Evaluar cumplimiento GDPR y PCI-DSS con asesoría especializada.
7. Capacitación obligatoria en seguridad para empleados.
8. Implementar BCP y DRP documentados.

Evaluación Final del Auditor

Nivel de exposición actual: **MEDIO-ALTO**
Urgencia de remediación: **Alta**