
INFORME DE RESPUESTA ANTE INCIDENCIAS

Billionary LTD

Evaluación de Procesos, Capacidad de Respuesta y Gestión de Incidentes
Fecha: 28/05/2026
Elaborado por: Departamento de Ciberseguridad

---

1. Resumen Ejecutivo

El presente informe recoge el análisis del proceso de **gestión y respuesta ante incidencias de seguridad** en **Billionary LTD**, con el objetivo de evaluar la capacidad de detección, contención, análisis y recuperación frente a incidentes que puedan afectar a la disponibilidad, integridad o confidencialidad de los activos corporativos.

La revisión se ha basado en estándares internacionales como **NIST 800-61**, **ISO 27035** y buenas prácticas del sector.

Conclusión general:
El nivel de madurez del proceso de respuesta ante incidencias se considera **medio**, con procedimientos definidos pero con carencias en automatización, tiempos de reacción y documentación. Se identifican oportunidades de mejora en la coordinación interna, la monitorización y la comunicación durante incidentes.

---

2. Alcance del Proyecto

2.1 Objetivos

- Evaluar la capacidad de detección temprana de incidentes.
- Analizar la eficacia de los procedimientos de respuesta.
- Revisar la coordinación entre equipos técnicos y de negocio.
- Identificar brechas en comunicación, escalado y documentación.
- Proponer mejoras para aumentar la resiliencia operativa.

2.2 Áreas evaluadas

- Centro de Operaciones de Seguridad (SOC)
- Equipo de TI y soporte

- Sistemas críticos de negocio
- Herramientas de monitorización y alertado
- Procedimientos de escalado y comunicación interna

2.3 Exclusiones

- Sistemas industriales
- Infraestructura cloud gestionada por terceros sin acceso operativo

---

3. Metodología Aplicada

La evaluación se realizó siguiendo el ciclo de vida de gestión de incidentes definido por **NIST 800-61**:

1. **Preparación**
2. **Detección y análisis**
3. **Contención, erradicación y recuperación**
4. **Lecciones aprendidas**

Las actividades incluyeron entrevistas, revisión documental, análisis de logs, simulaciones controladas y evaluación de tiempos de respuesta.

---

4. Resultados del Análisis

4.1 Hallazgos Críticos

INC-001 – Falta de un procedimiento formal de escalado

- **Severidad:** Alta
- **Descripción:** No existe un protocolo documentado que defina niveles de severidad, responsables y tiempos de respuesta.
- **Impacto:** Retrasos en la toma de decisiones durante incidentes reales.
- **Riesgo:** Aumento del tiempo de exposición y del impacto operativo.
- **Recomendación:** Definir un plan de escalado con roles, tiempos y criterios claros.

INC-002 – Ausencia de un registro centralizado de incidentes

- **Severidad:** Alta

- **Descripción:** Los incidentes se registran de forma dispersa entre equipos.
- **Impacto:** Dificultad para analizar tendencias y mejorar procesos.
- **Recomendación:** Implementar una plataforma SIEM o ticketing centralizada.

4.2 Hallazgos de Severidad Media

INC-010 – Monitorización insuficiente en sistemas críticos

- **Severidad:** Media
- **Descripción:** Algunos servidores carecen de alertas de comportamiento anómalo.
- **Impacto:** Riesgo de detección tardía.
- **Recomendación:** Ampliar cobertura de monitorización y correlación de eventos.

INC-014 – Comunicación interna no estandarizada

- **Severidad:** Media
- **Descripción:** No existe un canal único para coordinar incidentes.
- **Impacto:** Mensajes duplicados o contradictorios.
- **Recomendación:** Crear un canal oficial de respuesta (Teams/Slack).

4.3 Hallazgos de Severidad Baja

INC-021 – Falta de simulacros periódicos

- **Severidad:** Baja
- **Descripción:** No se realizan ejercicios de respuesta ante incidentes.
- **Impacto:** Menor preparación del personal.
- **Recomendación:** Realizar simulacros semestrales.

---

5. Evaluación de la Capacidad de Respuesta

Durante las simulaciones realizadas se observó:

- **Tiempo medio de detección:** 47 minutos

- **Tiempo medio de contención:** 1 hora y 32 minutos
- **Tiempo medio de recuperación:** 3 horas y 15 minutos
- **Coordinación entre equipos:** Adecuada pero mejorable
- **Documentación generada:** Parcial e incompleta

Se identificaron retrasos principalmente en la fase de análisis y en la comunicación entre equipos.

---

6. Evaluación del Riesgo Global

Categoría	**Nivel**
Riesgo operativo	**Medio-Alto**
Riesgo técnico	**Medio**
Riesgo reputacional	**Medio**
Riesgo de cumplimiento	**Medio**

---

7. Recomendaciones Prioritarias

1. **Crear un Plan de Respuesta ante Incidentes (PRI)** formal y documentado.
2. **Establecer un sistema centralizado de registro y seguimiento de incidentes.**
3. **Ampliar la monitorización y correlación de eventos en sistemas críticos.**
4. **Definir un canal único de comunicación durante incidentes.**
5. **Realizar simulacros periódicos y sesiones de formación.**
6. **Implementar métricas y KPIs de respuesta.**
7. **Revisar y actualizar el PRI tras cada incidente relevante.**

---

8. Conclusiones

Billionary LTD presenta un nivel de madurez intermedio en la gestión de incidentes, con procedimientos básicos establecidos pero con carencias significativas en escalado, documentación y monitorización. La implementación

de las recomendaciones propuestas permitirá reducir los tiempos de respuesta, mejorar la coordinación interna y aumentar la resiliencia frente a incidentes reales.

El departamento de ciberseguridad queda disponible para acompañar en la implantación de mejoras y en la realización de simulacros futuros.

---

9. Anexos

- Plantilla de registro de incidentes
- Flujos de escalado propuestos
- Métricas de simulación
- Evidencias de monitorización
- Cronograma de actividades

Si quieres, puedo generarte también:

- **La portada corporativa**
- **La tabla de contenidos automática**
- **El documento con estilos de Word (H1, H2, H3)**
- **Una versión extendida con gráficos y diagramas de flujo**

¿Deseas que prepare la **versión final lista para maquetar en Word** con estilos aplicados?