📘 INFORME CORPORATIVO DE AUDITORÍA EN CIBERSEGURIDAD

Cibersecuritytech
Cliente: *Anubis Corp. LTD*
Fecha: *20/05/2026*

PORTADA

AUDITORÍA EN CIBERSEGURIDAD

Informe Ejecutivo y Técnico

Consultora: Cibersecuritytech
Confidencialidad: Alto
Versión: 1.0
Fecha: 01/05/2026 al 19/05/2026

ÍNDICE

---

1. RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada a *Anubis Corp. LTD* ha permitido evaluar el nivel de exposición, madurez y resiliencia frente a amenazas internas y externas.

Principales conclusiones

- **12 vulnerabilidades críticas** detectadas

- **23 vulnerabilidades medias**
- **Nivel de madurez global: 3,1 / 5**
- **Riesgo residual: Alto**
- **Prioridad de actuación:** Inmediata en sistemas expuestos y accesos privilegiados

Impacto potencial

- Compromiso de sistemas críticos
- Acceso no autorizado a datos sensibles
- Riesgo de ransomware
- Interrupción operativa

---

2. ALCANCE DE LA AUDITORÍA

2.1 Infraestructura

- Firewalls, routers, switches
- Servidores Windows y Linux
- Redes internas y externas
- Segmentación y VLANs

2.2 Sistemas y Aplicaciones

- Aplicaciones web
- APIs
- Bases de datos
- Servicios expuestos

2.3 Identidades y Accesos

- Active Directory
- Gestión de privilegios
- MFA
- Políticas de contraseñas

2.4 Procesos y Gobierno

- Políticas de seguridad
- Gestión de incidentes
- Gestión de vulnerabilidades
- Continuidad de negocio

---

3. METODOLOGÍA

3.1 Fases del proyecto

🔍 **Fase 1 — Revisión documental**
Políticas, procedimientos, inventario, arquitectura.

🛠️ **Fase 2 — Análisis técnico**
Escaneo, pruebas de configuración, análisis de logs.

👥 **Fase 3 — Entrevistas**
TI, seguridad, responsables de negocio.

📊 **Fase 4 — Evaluación de madurez**
Basada en NIST CSF e ISO 27001.

📑 **Fase 5 — Informe y recomendaciones**
Hallazgos priorizados y plan de acción.

---

4. HALLAZGOS CRÍTICOS

4.1 Exposición de servicios sensibles en Internet

Riesgo: Crítico
Impacto: Acceso no autorizado, explotación remota
Recomendación: Cerrar servicios, aplicar WAF, reforzar firewall

---

4.2 Credenciales débiles y sin MFA

Riesgo: Crítico
Impacto: Compromiso total del dominio
Recomendación: Activar MFA, rotación de contraseñas, implementar PAM

4.3 Segmentación de red insuficiente

Riesgo: Alto
Impacto: Movimiento lateral, propagación de malware
Recomendación: Microsegmentación, Zero Trust

4.4 Parches críticos pendientes

Riesgo: Alto
Impacto: Explotación de vulnerabilidades conocidas
Recomendación: Plan de parcheo mensual

---

5. HALLAZGOS DE RIESGO MEDIO

- Permisos excesivos en carpetas compartidas
- Falta de monitorización en sistemas clave
- Políticas de backup incompletas
- Ausencia de pruebas de restauración
- Aplicaciones web sin validación adecuada

---

6. EVALUACIÓN DE MADUREZ

Dominio	Nivel (0-5)	Estado
Identify	3.2	Aceptable
Protect	2.8	Mejorable
Detect	2.5	Insuficiente
Respond	3.0	Aceptable
Recover	3.1	Aceptable

Madurez global: 3,1 / 5

---

7. PLAN DE ACCIÓN PRIORITARIO

Prioridad 1 — Inmediata (0-30 días)

- Activar MFA
- Cerrar servicios expuestos
- Aplicar parches críticos
- Revisar accesos privilegiados

Prioridad 2 — Corto plazo (30-90 días)

- Implementar segmentación
- Revisar políticas de backup
- Activar SIEM
- Revisar permisos excesivos

Prioridad 3 — Medio plazo (90-180 días)

- Zero Trust
- Automatizar gestión de vulnerabilidades
- Formación en ciberseguridad

---

8. CONCLUSIONES

La organización presenta una base sólida, pero existen vulnerabilidades críticas que requieren atención inmediata.
La ejecución del plan de acción permitirá:

- Reducir el riesgo crítico en un **70%**
- Mejorar la madurez hasta **4,0 / 5**
- Aumentar la resiliencia ante ataques
- Cumplir con estándares regulatorios

---

9. ANEXOS

- Evidencias técnicas
- Capturas de configuraciones
- Listado de CVEs
- Inventario de activos
- Matriz de riesgos completa