🧩 **Reto: "El Ransomware del viernes en Innovatech S.A.S."**

Contexto general

La empresa **Innovatech S.A.S.**, dedicada al desarrollo de software financiero, cuenta con 150 empleados. Tiene servicios críticos en la nube (Microsoft 365, GitHub y AWS) y una VPN corporativa para acceso remoto.

El **equipo de SOC** detecta un comportamiento anómalo justo antes del cierre de jornada el **viernes a las 5:42 p.m.**:

- Se reciben múltiples alertas del **EDR** indicando **cifrado masivo de archivos** en tres estaciones de trabajo del área de contabilidad.
- En los logs de red se observa **tráfico hacia una IP de Europa del Este** usando el puerto 445.
- En los escritorios afectados aparece una nota de rescate con el mensaje:

"Sus archivos han sido cifrados por **BlackSnakeLocker**. Pague 0.5 BTC en 48 horas o sus datos serán publicados."

Además, el **servidor de archivos contables** comienza a responder de forma errática y varios empleados reportan imposibilidad de acceder a documentos compartidos.
El **back-up diario** estaba programado a las 22:00, pero **no se sabe si se ejecutará correctamente**.

Tu misión 🧠

Los participantes deben **diseñar un playbook de respuesta a incidentes tipo ransomware**, siguiendo el enfoque del material:

1. **Activación (gatillo):** ¿Qué evento o alerta dispara la ejecución del playbook?
2. **Objetivo:** ¿Qué se busca lograr (ej. aislar el ransomware, preservar evidencia, restaurar servicios)?
3. **Alcance:** Qué cubre (servidores, estaciones de trabajo, nube) y qué no.
4. **Roles (RACI):** Qué equipos y personas intervienen (SOC, IT, Legal, Comunicaciones, etc.).
5. **Plantillas y comunicación:** mensajes internos y externos (ej. aviso a dirección y usuarios).

6. **Checklist de cierre:** validaciones técnicas y administrativas antes de cerrar el ticket.

Entregable 💡

Cada participante debe presentar:

- 📃 **Playbook documentado (1–2 páginas)** con estructura clara, siguiendo el ejemplo del PDF.
- 🛠️ **Diagrama o flujo del proceso de respuesta.**
- 📈 **Métricas de efectividad** simuladas (tiempo de detección, contención y recuperación).
- 🎯 **Lección aprendida:** una mejora que la organización podría implementar tras el incidente.