Alumno: Rodrigo Vila

# Ejercicio Número 2 Unidad 1

**Crear un documento (DOC/PDF), en el cual este explicado con sus propias palabras, de acuerdo a lo leído en esta unidad, si las medidas son ¿suficientes o no?**

**Desarrollar: si son suficientes las políticas, justificar el porqué de cada una (no más de 1 página).**

**Si son insuficientes: explicar que agregaría y justificar el porqué de cada una (no más de 2 páginas).**

**También se pueden aportar nuevas ideas de medidas.**

**Comienzo** respondiendo con mis palabras la primer pregunta. ¿Las medidas son suficientes o no? Mas que a la cuestión práctica debo apelar a una respuesta casi filosófica... Creo que las medidas nunca son suficientes. Podemos implementar prácticas que nos ayuden a mantener la seguridad de la información, pero siempre debemos innovar, explorar, analizar, curiosear. Chusmear nuestro tráfico de red. "Esta IP recurrente me resulta sospechosa, ¿que está haciendo? ¿a que recursos quiere acceder? ¿A quien corresponde? ¿Los necesita?".

Tenemos que realizar auditorias periódicas. Analisis, laboratorios, atacar (pentesting), identificar puntos debiles, revisar el trafico. Renovarnos cuando haga falta. Mantenernos actualizados, y sobre todo, inquietos. Jamas sentarnos en los laureles porque una red aparentemente segura en un parpadeo lo puede dejar de ser.

**Continúo** enumerando las políticas de seguridad a analizar:

1. Que haya responsables en el área de desarrollo, implementación y gestión de la política a imponer.
2. Proteger equipos y dispositivos en uso.
3. Proteger la red.
4. Proteger los servidores.
5. Proteger los datos.
6. Protección de las aplicaciones y recursos.

**Son suficientes?:** No.

**Que agregaría?:**

- Simulación exacta de la red en laboratorio: Una simulación logica de la red completa

que nos permita realizar prácticas, ataques y simulacros para identificar puntos débiles, deficiencias y posibles optimizaciones.

- Un equipo de Pentesting: Un equipo dedicado a encontrar vulnerabilidades y listarlas, para luego reportarlas y mitigarlas.
- Simulacros periódicos (Drills): Organizar diferentes prácticas de desastres en la red para evaluar la efectividad de los planes de contingencia. Capacitar un equipo "blue team" de respuesta y blindeo tanto post-ataque como en tiempo real.

Todo esto suponiendo que ya tenemos implementadas las politicas de las cuales ya hemos hablado y leido tanto en este modulo como en los anteriores y en las clases, como la de mantener la concientización de los usuarios, controlar los privilegios de usuarios, analisis de IDSs, IPSs, Firewalls, ACLs, autentificaciónes controladas, VPNs para el cifrado del tráfico, backups en la nube y demás temas que se desprenden de los puntos listados al principio de éste documento.

*Rodrigo Vila.-*