
1
PREPARACIÓN
identificación de elementos críticos
2
PROTECCIÓN
3
DETECCIÓN
4
RESPUESTA
contención
remediación
5
ANÁLISIS FORENSE
6
MEJORA DEL SISTEMA
Servicio de Seguridad Gestionada

- Qué proteger (elementos críticos):

  - La estructura orgánica

  - Los objetivos de la organización

  - El impacto posible producido por una alteración

- Cómo, cuando....

Qué utilizar:

- **Técnicamente (aproximaciones diversas)**
- **Con que criterios**
- **Ámbito al que llegar**
- **SOC: la inteligencia**

Problemas:

- **SOC**
- **Falsos positivos**
- **Velocidad de cambio**
- **Caducidad – maduración del Conocimiento**
- **Tiempo de respuesta**

4. Respuesta

- **Contener**

- **Remediar**

- **Documentar:**
  - **Lucia**
  - **Personal cualificado**
  - **Catálogo de herramientas / caducidad**
  - **Guía 817**

5. Análisis Forense

Qué ocurre con los incidentes críticos, qué hay detrás de cada uno.

7. Mejora del sistema

- **La organización que aprende**

- **La cooperación necesaria**

- **La necesaria iniciativa concreta, continua y variable**