**Manual de estrategias:** manual que proporciona detalles sobre cualquier acción operativa, también aclara que herramientas deben usarse en respuesta a un incidente de Seguridad

Urgencia, eficiencia y precisión son necesarias para identificar y mitigar rápidamente una amenaza para reducir el riesgo potencial. Los manuales garantizan que se siga una lista coherente de acciones de una manera prescrita, uno de los manuales más utilizados comúnmente es el *manual de respuestas a incidentes.* Respuesta ante incidentes es el intento rápido de una organización de identificar un ataque, contener el daño y corregir los efectos, este manual es una guía con seis fases utilizado para ayudar a mitigar y gestionar los incidentes de seguridad de principio a fin

1. **Fase de preparación:** las organizaciones deben prepararse para mitigar la probabilidad, el riesgo y el impacto de un incidente documentando procedimientos, estableciendo planes de personal y educando a los usuarios, ya que esto sienta las bases para una respuesta exitosa a los incidentes
2. **Fase de detección y análisis:** su objetivo es detectar y analizar eventos utilizando procesos y tecnología definidos. Usar herramientas y estrategias adecuadas durante esta fase ayuda a los analistas de seguridad a determinar si se produjo una violación y analizar su posible magnitud
3. **Fase de contención:** el objetivo es evitar daños mayores y reducir el impacto inmediato de un incidente. Los profesionales de seguridad toman medidas para contener un incidente y minimizar los daños. La contención es una alta prioridad para las organizaciones porque ayuda a prevenir los riesgos continuos para los activos y datos críticos
4. **Fase de erradicación y la recuperación:** implica la eliminación completa de los artefactos de un incidente para que la organización pueda volver a sus operaciones normales, durante esta fase, los profesionales de seguridad eliminan los artefactos del incidente al eliminar el código malicioso y mitigar las vulnerabilidades
5. **Fase de actividad posterior al incidente:** incluye documentar el incidente, informar a los lideres de la organización y aplicar las lecciones aprendidas para garantizar que la organización este mejor preparada para gestionar futuros incidentes
6. **Fase de coordinación:** implica denunciar los incidentes y compartir información durante todo el proceso de respuesta a los incidentes, según los estándares establecidos por la organización, la misma es importante ya que garantiza que las organizaciones cumplan con los requisitos de cumplimiento y permite una respuesta y resolución coordenadas

Los manuales crean estructuras, garantizan el cumplimiento y describen los procesos de comunicación y documentación, y las organizaciones pueden usar diferentes tipos de guías de respuesta a incidentes según la situación. Para empezar, analicemos como un analista de seguridad podría usar un manual para abordar una alerta de SIEM. En la situación de un ataque de software malicioso, un manual de estrategias tiene un valor incalculable para guiar a un analista a través de las acciones necesarias para abordar la alerta de manera adecuada, la primera acción es evaluar la alerta, lo que significa determinar si es realmente valida identificando por que el SIEM genero la alerta. Luego el manual describe acciones y herramientas a utilizar para contener el software y reducir el daño adicional. Tras contener el incidente, se describen las formas de eliminar todo rastro y restaurar los sistemas afectados. Por último, el cuarto paso indica al analista que lleve a cabo varias actividades posteriores al incidente y esfuerzos de coordinación con el equipo de seguridad, como crear un informe final

**Herramientas SOAR:** son similares a las SIEM en el sentido de que se utilizan para la supervisión de amenazas. SOAR es una pieza de software utilizada para automatizar tareas repetitivas generadas por herramientas como un SIEM o una detección y respuesta gestionadas. Por ejemplo, si un usuario intenta iniciar sesión en su computadora demasiadas veces con una contraseña incorrecta, un SOAR bloquearía automáticamente su cuenta para detener una posible intrusión. A continuación, los analistas consultarían un Manual de estrategias para dar los pasos necesarios para resolver el Problema.