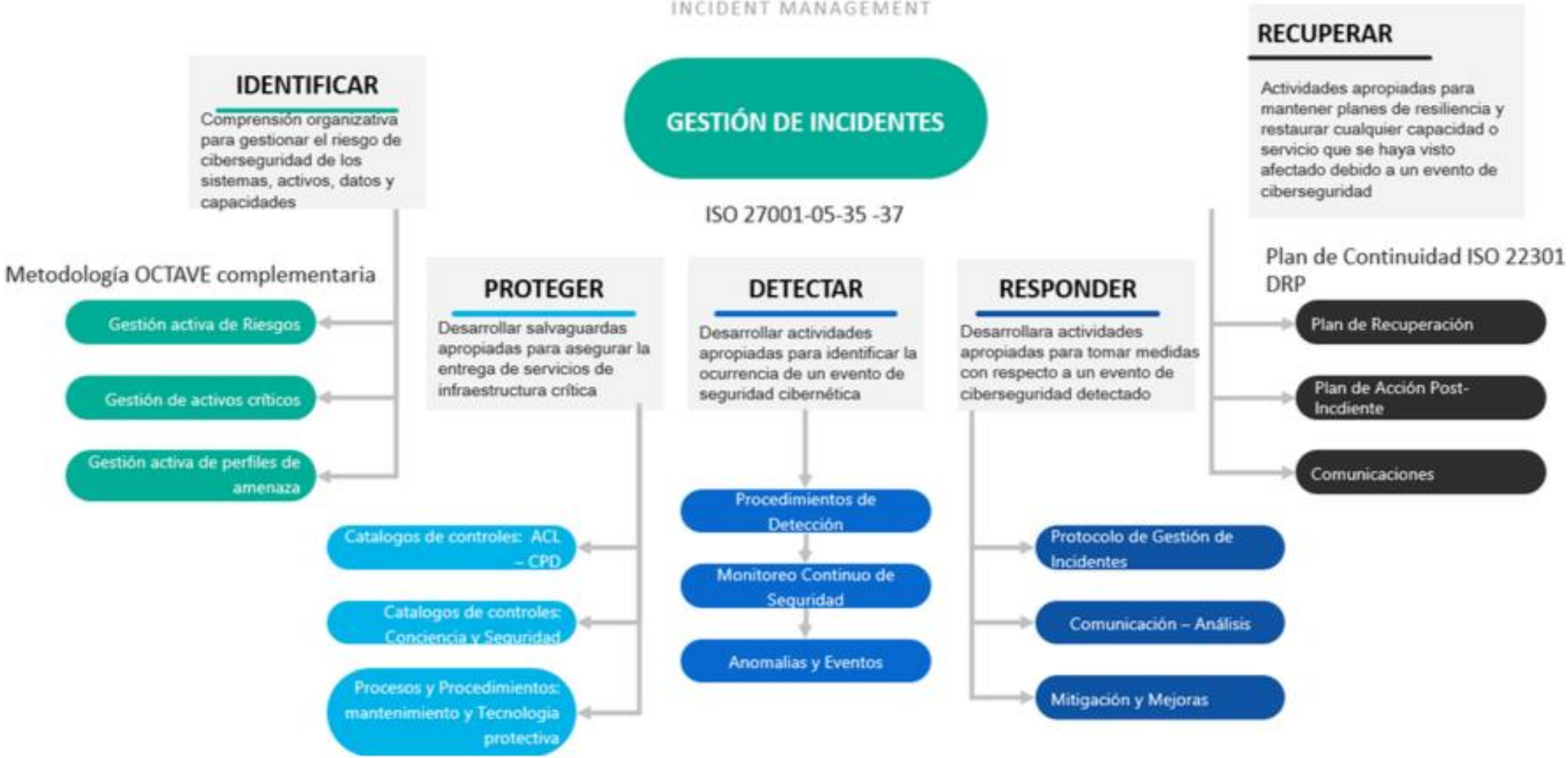
RESPUESTA INCIDENTES DE SEGURIDAD

Proceso de incidente

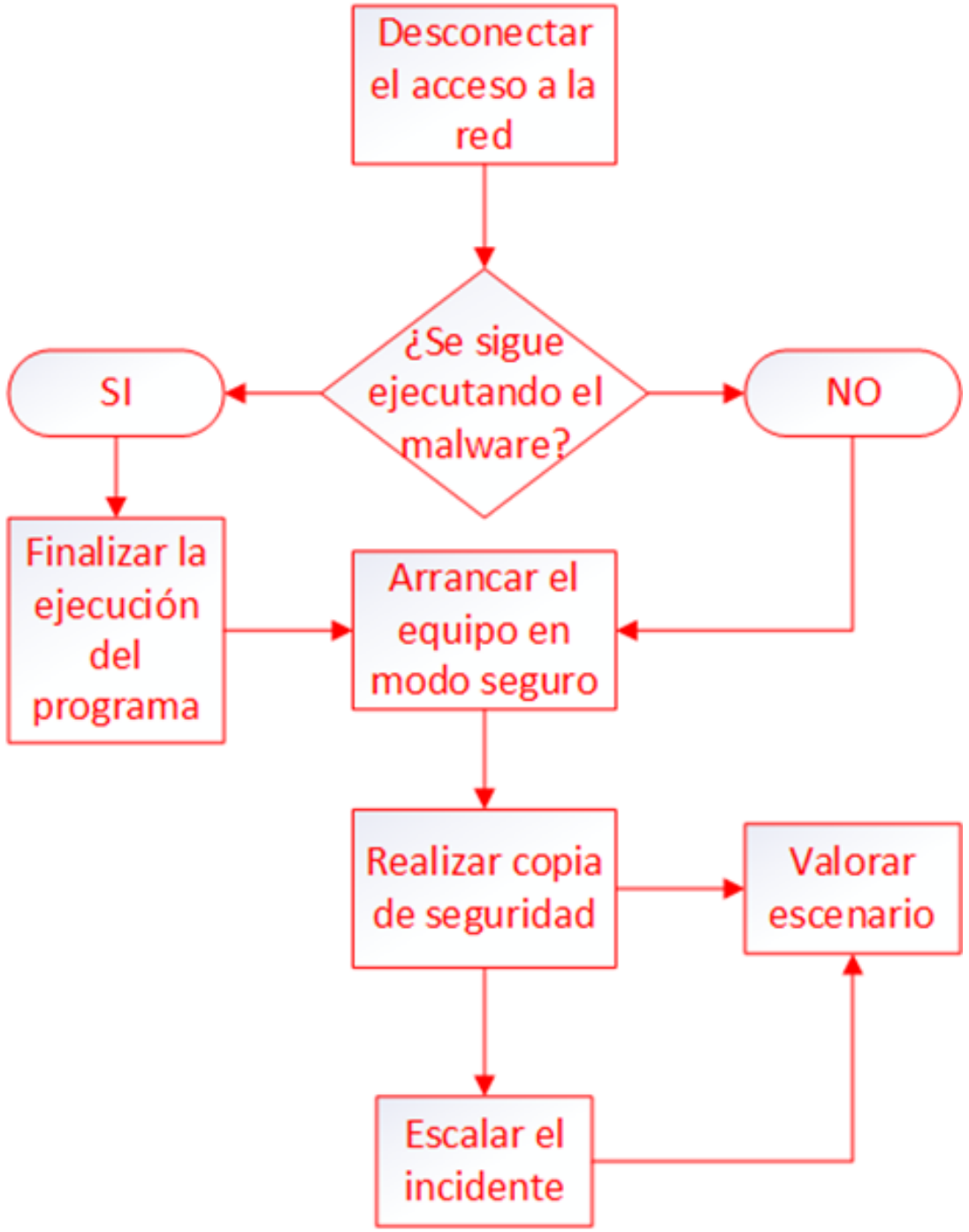
DIAGRAMA LINEA GUIA DE GESTIÓN NIST

INCIDENT MANAGEMENT

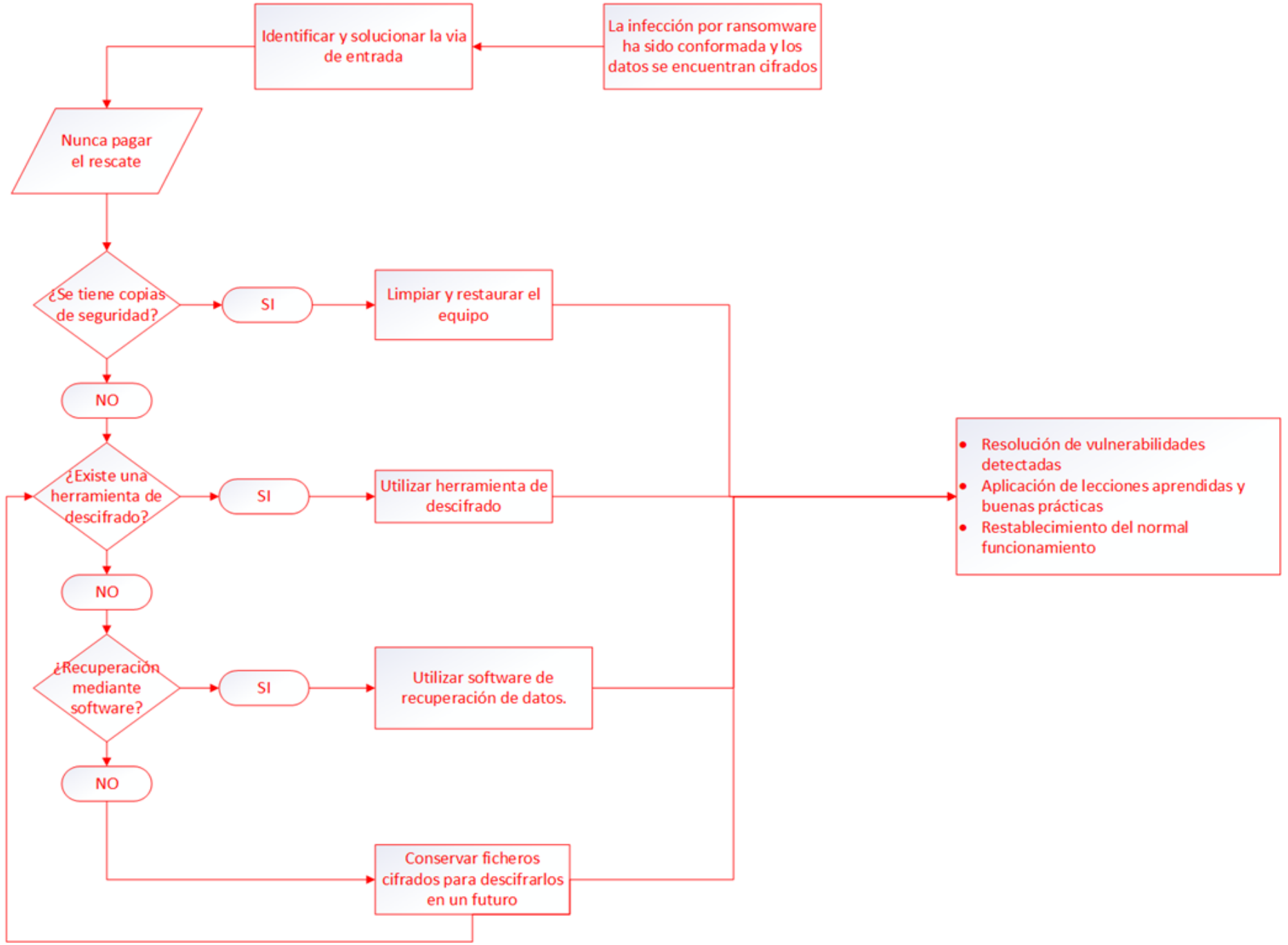


Elaboración Propia: Metodología de gestión de Incidentes: Línea base NIST CSF

Incidente Malware



Cifrado


La infección por ransomware ha sido conformada y los datos se encuentran cifrados
Identificar y solucionar la via de entrada
Nunca pagar el rescate
¿Se tiene copias de seguridad?
SI
Limpiar y restaurar el equipo
NO
¿Existe una herramienta de descifrado?
SI
Utilizar herramienta de descifrado
NO
¿Recuperación mediante software?
SI
Utilizar software de recuperación de datos.
NO
Conservar ficheros cifrados para descifrarlos en un futuro
Resolución de vulnerabilidades detectadas
Aplicación de lecciones aprendidas y buenas prácticas
Restablecimiento del normal funcionamiento

Verificaciones de incidentes

- Comprueba si la aplicación web puede identificar ataques de spam en los formularios de contacto utilizados en el sitio web.
- Servidor proxy: comprueba si el tráfico de red es monitoreado por dispositivos proxy. El servidor proxy dificulta que los piratas informáticos obtengan detalles internos de la red, protegiendo así el sistema de ataques externos.

- **Filtros de correo electrónico no deseado**: verifica si el tráfico de correo electrónico entrante y saliente se filtra y se bloquean los correos electrónicos no solicitados.
- Muchos clientes de correo electrónico vienen con filtros de spam incorporados que deben configurarse según sus necesidades. Estas reglas de configuración se pueden aplicar a encabezados de correo electrónico, asunto o cuerpo.
- **Cortafuegos**: asegúrate de que toda la red o las computadoras estén protegidas con cortafuegos. Un firewall puede ser software o hardware para bloquear el acceso no autorizado a un sistema. También puede evitar el envío de datos fuera de la red sin su permiso.
- Intenta explotar todos los servidores, sistemas de escritorio, impresoras y dispositivos de red.
- Verifica que todos los nombres de usuario y contraseñas estén encriptados y transferidos a través de conexiones seguras como https.

- Comprueba la información almacenada en las cookies del sitio web. No debe estar en un formato legible.
- Comprueba si no hay un puerto abierto en la red.
- Analiza todos los dispositivos telefónicos y la seguridad de la red WIFI.
- Verifica todos los métodos HTTP. Los métodos PUT y DELETE no deben habilitarse en un servidor web.
- Examina si la contraseña cumple con los estándares requeridos. La contraseña debe tener al menos 8 caracteres y contener al menos un número y un carácter especial.

- El nombre de usuario no debe ser «admin» o «administrador».
- La página de inicio de sesión de la aplicación debe bloquearse con algunos intentos fallidos de inicio de sesión.
- Los mensajes de error deben ser genéricos y no deben mencionar detalles de error específicos como «Nombre de usuario no válido» o «Contraseña no válida».
- Examina si los caracteres especiales, las etiquetas HTML y las secuencias de comandos se manejan correctamente como valor de entrada.
- Los detalles internos del sistema no deben revelarse en ninguno de los mensajes de error o alerta.

- Deben mostrarse mensajes de error personalizados a los usuarios finales en caso de un bloqueo de la página web.
- Analiza el uso de entradas de registro. La información confidencial no debe mantenerse en el registro.
- Todos los archivos deben analizarse antes de cargarlos en el servidor.
- Los datos confidenciales no deben pasarse en URL mientras se comunican con diferentes módulos internos de la aplicación web.
- No debe haber ningún nombre de usuario o contraseña codificados en el sistema.

- La funcionalidad de restablecimiento de contraseña debe ser segura.
- Prueba la aplicación para inyección SQL y la aplicación para Cross-Site Scripting .
- Las validaciones de entrada importantes se deben realizar en el lado del servidor en lugar de las comprobaciones de JavaScript en el lado del cliente.
- Los recursos críticos en el sistema deben estar disponibles solo para personas y servicios autorizados.
- Todos los registros de acceso deben mantenerse con los permisos de acceso adecuados.

- La sesión del usuario debe finalizar al cerrar sesión.
- La exploración del directorio debe estar deshabilitada en el servidor.
- Todas las aplicaciones y versiones de la base de datos deben estar actualizadas.
- Debes verificar la pérdida de memoria y el desbordamiento del búfer.
- El tráfico entrante de la red debe examinarse para encontrar ataques troyanos.

- El sistema debe estar a salvo de ataques de fuerza bruta, un método de prueba y error para encontrar información confidencial como contraseñas.
- El sistema o la red deben estar protegidos contra ataques DoS (denegación de servicio).
  - El ciberdelincuente puede apuntar a la red o un solo ordenador mediante solicitudes continuas ya que, al sobrecargarse los recursos en el sistema de destino, se produce la denegación de servicio para solicitudes legítimas.
- La aplicación debe estar protegido contra ataques de inyección de script HTML y contra ataques COM y ActiveX o similares…..

- Verificar contra ataques de suplantación de identidad. La suplantación de identidad puede ser de varios tipos:
  - suplantación de direcciones IP, suplantación de identidad de correo electrónico, falsificación de ARP, falsificación de referencias, falsificación de identificador de llamadas, envenenamiento de redes de intercambio de archivos, falsificación de GPS.
- Comprueba si hay un ataque de cadena de formato no controlado:
  - un ataque de seguridad que puede hacer que la aplicación se bloquee o ejecute el script dañino en él.