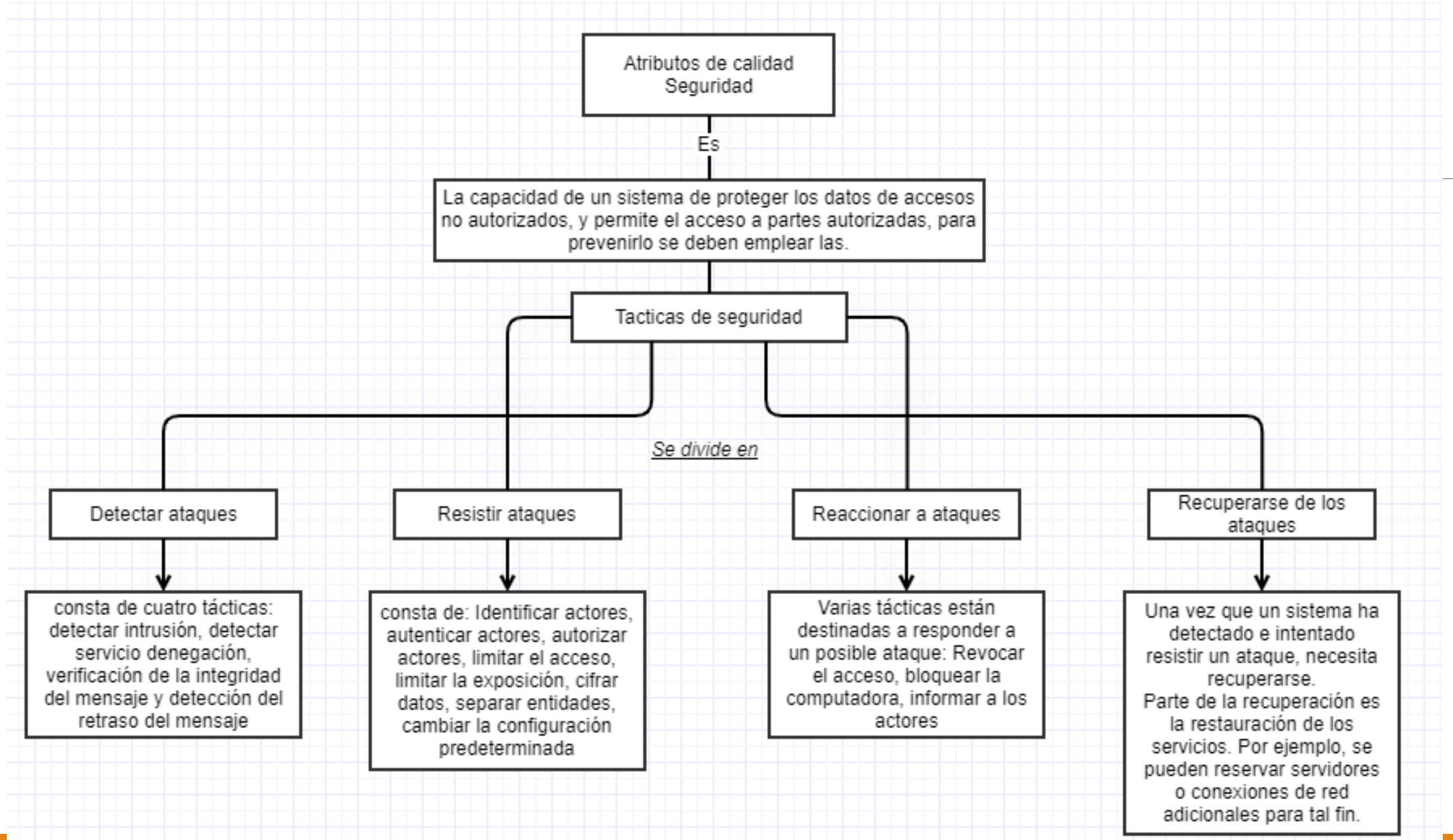
Atributo Seguridad

ATRIBUTO CALIDAD - SEGURIDAD

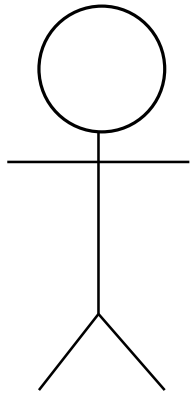
La capacidad de un sistema de proteger los datos de accesos no autorizados, y permitir el acceso a partes autorizadas


Atributos de calidad
Seguridad
Es
La capacidad de un sistema de proteger los datos de accesos no autorizados, y permite el acceso a partes autorizadas, para prevenirlo se deben emplear las.
Tacticas de seguridad
Se divide en
Detectar ataques
Resistir ataques
Reaccionar a ataques
Recuperarse de los ataques
consta de cuatro tácticas: detectar intrusión, detectar servicio denegación, verificación de la integridad del mensaje y detección del retraso del mensaje
consta de: Identificar actores, autenticar actores, autorizar actores, limitar el acceso, limitar la exposición, cifrar datos, separar entidades, cambiar la configuración predeterminada
Varias tácticas están destinadas a responder a un posible ataque: Revocar el acceso, bloquear la computadora, informar a los actores
Una vez que un sistema ha detectado e intentado resistir un ataque, necesita recuperarse.
Parte de la recuperación es la restauración de los servicios. Por ejemplo, se pueden reservar servidores o conexiones de red adicionales para tal fin.

Escenario

Ataque DDos

Una persona mal intencionada que realizando un ataque de denegación de servicio al sitio web – Ataque externo



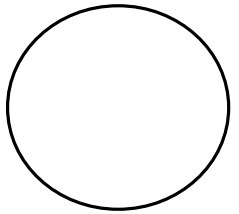
Recurso: Un hacker busca afectar la disponibilidad del sitio

Estimulo: Inunda de peticiones HTTP y consultas de DNS

Artefacto: Datos en el Sistema

Entorno: Externo, en línea.

Respuesta: Las herramientas correspondientes como blackhole o Web Application Firewall filtraran las solicitudes malintencionadas



Medidas de Respuesta: la disponibilidad de la pagina no se vera afectada y se tratara de trastear el ataque

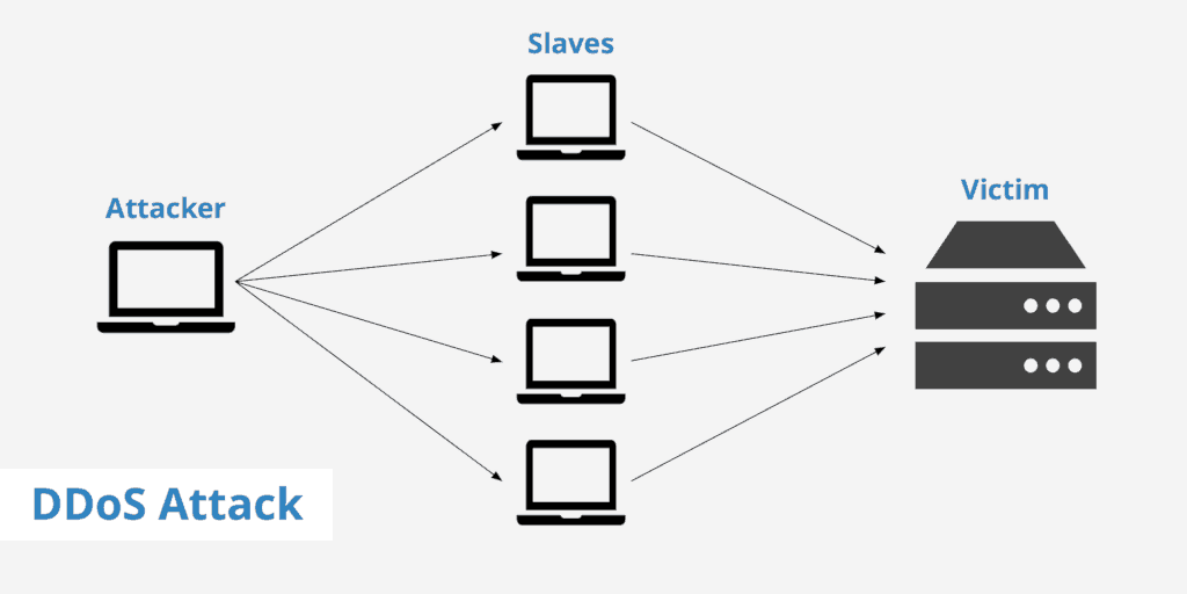
Detectar ataque

Detectar intrusión: Comportamiento malicioso en una base de datos

Detectar denegación servicio: trafico que ingresa con los perfiles históricos de ataques conocidos

Verificación de integridad mensaje: que los archivos o mensajes mantengan su integridad

Retraso del mensaje: una parte maliciosa está interceptando (y posiblemente modificando) los mensajes.



RESISTIR LOS ATAQUES

Identificar actores: Formas en que los usuarios pueden identificarse normalmente a través de ID

Autenticar actores: significa asegurarse de que un actor sea realmente quién pretende ser.

Autorizar a los actores: Ya autenticados tenga los privilegios correspondientes

Limitar el acceso: limitar el acceso a recursos como la memoria, las conexiones de

red o los puntos de acceso.

RESISTIR LOS ATAQUES

Cifrar datos: Los datos deben estar protegidos del acceso no autorizado. La confidencialidad se logra usualmente aplicando algún tipo de cifrado a los datos y a la comunicación.

Entidades separadas: Separación física

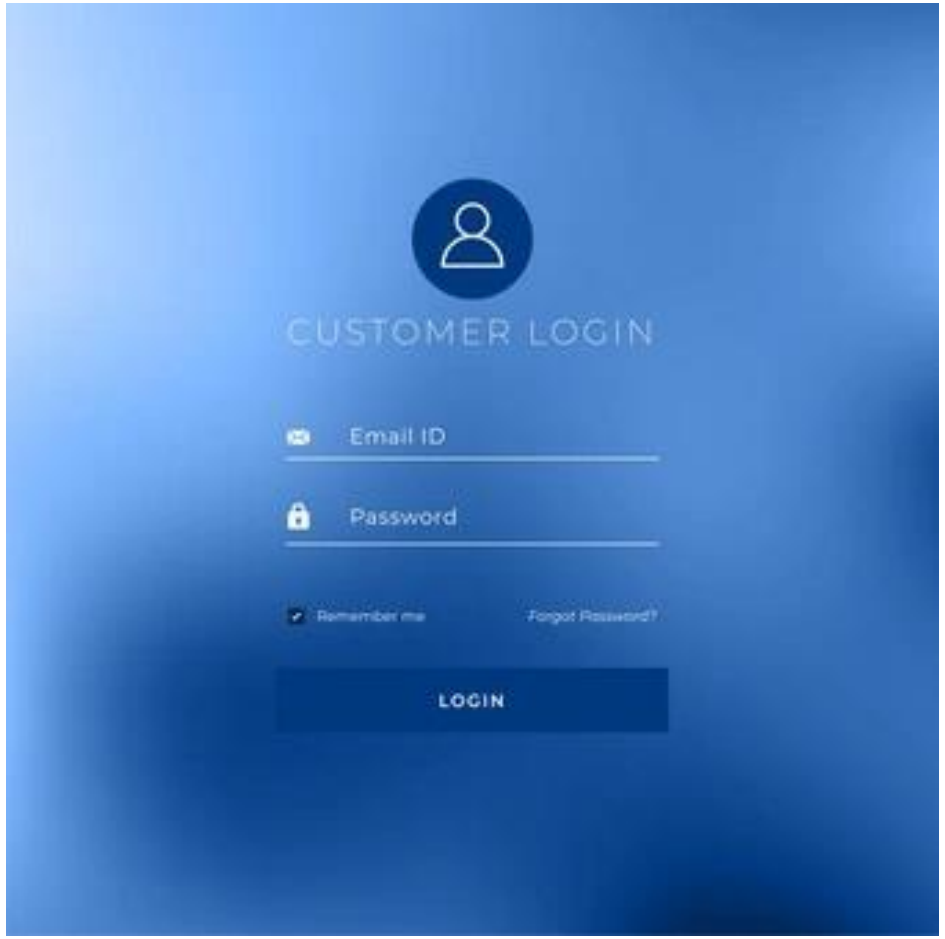
Cambiar la configuración predeterminada: Forzar al usuario a cambiar esa configuración evitará que los atacantes obtengan acceso al sistema a través de configuraciones que, en general, están disponibles al público.

REACCIONAR A LOS ATAQUES

Revocar el acceso: administrador del sistema cree que un ataque está en curso

Bloquear la computadora: Intento repetido de inicio de sesión fallidos

Informar a los actores: Los ataques continuos pueden requerir la acción de los operadores



RECUPERARSE DE LOS ATAQUES

Mantener la pista de auditoría: Mirar que fue lo que sucedió

Restaurar: Restaurar servidores, servicios

Ver Disponibilidad: evaluar si el sistema esta “bien”