SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

3.2.1.MF0488_3. Capítulo 2
Parte 1

Proceso de notificación y gestión de intentos de intrusión

JOSÉ PABLO HERNÁNDEZ

1. INTRODUCCIÓN

Cuando se detecta un intento de intrusión es recomendable seguir un procedimiento definido claramente por las organizaciones para que la gestión de dicha intrusión se realice correctamente y se minimicen todo lo posible sus efectos negativos.

2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES

Intrusión: evento en el cual un usuario no autorizado intenta acceder a los equipos y/o dispositivos de una red para comprometer la integridad, confidencialidad y disponibilidad de la información.

2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES

Criterios en la elección de herramientas (cortafuegos/IDS/IPS):

- **Escalabilidad**
- **Firmas de ataque utilizadas**
- **Capacidad de administración y gestión**
- **Tipo de estructura de hardware utilizada**

2.1. RESPONSABILIDADES DE GESTIÓN Y NOTIFICACIÓN DE INTRUSIONES

La elección del correcto sistema de detección y prevención de intrusiones es fundamental para lograr una protección adecuada de la información contenida en los equipos de una organización.

Necesita un procedimiento adecuado de tratamiento del incidente.

2.1. RESPONSABILIDADES DE GESTIÓN Y NOTIFICACIÓN DE INTRUSIONES

Es necesaria la designación de responsables cuya función principal sea la de localizar las intrusiones detectadas por los sistemas de protección.

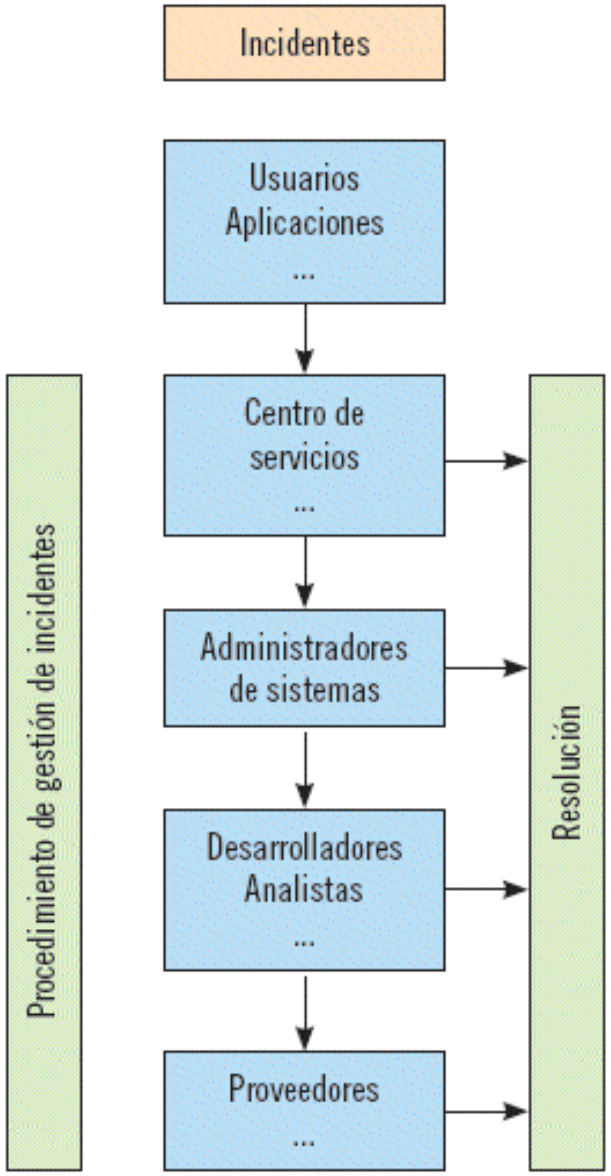
2.1. RESPONSABILIDADES DE GESTIÓN Y NOTIFICACIÓN DE INTRUSIONES

Las organizaciones deberán formar una estructura que:

- **Detecte cualquier alteración de los servicios ofrecidos por la organización.**
- **Registre y clasifique estos incidentes.**
- **Asigne al personal encargado de restaurar la situación al punto previo de la producción del incidente**

2.1. RESPONSABILIDADES DE GESTIÓN Y NOTIFICACIÓN DE INTRUSIONES

Estructura del proceso de gestión de incidentes



2.2. OBLIGACIONES LEGALES DE GESTIÓN Y NOTIFICACIÓN DE INCIDENTES

La LOPDGDD obliga ante un incidente de seguridad a registrar:

- **El tipo de incidencia.**
- **El momento en el que se ha producido la incidencia.**
- **La persona que realiza la notificación.**
- **A quién se le comunica.**
- **Los efectos que han derivado de la misma.**

3. CLASIFICACIÓN DE LOS INCIDENTES DE SEGURIDAD

- Categorización del incidente.
- Nivel de prioridad.
- Asignación de recursos.
- Monitorización del estado del incidente y del tiempo de respuesta esperado.

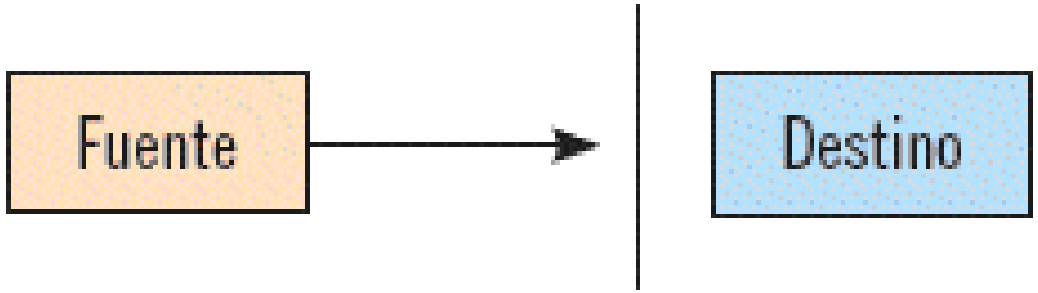
3.1. TIPOS DE ATAQUES

Antes de clasificar el incidente hay que saber qué tipo de ataque se está produciendo.

En una situación normal el flujo de información circula de origen a destino sin problemas de disponibilidad, integridad y accesibilidad.

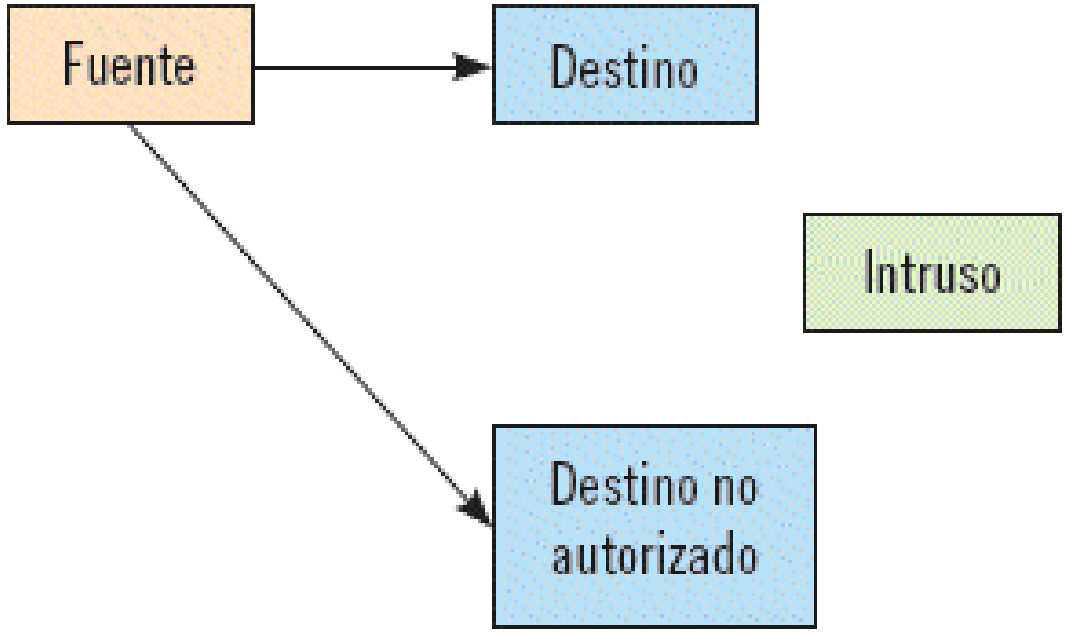
3.1. TIPOS DE ATAQUES

Ataques de interrupción



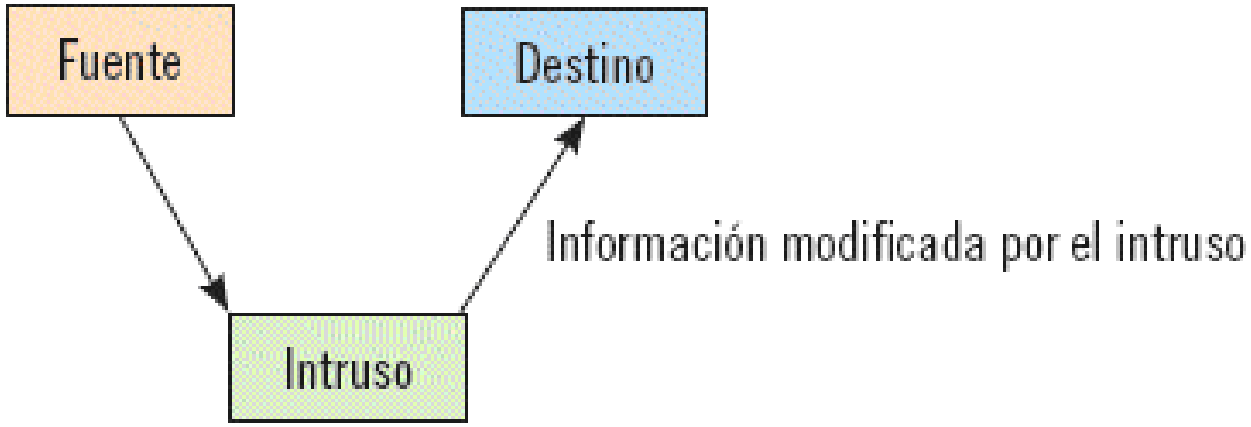
3.1. TIPOS DE ATAQUES

Ataques de intercepción



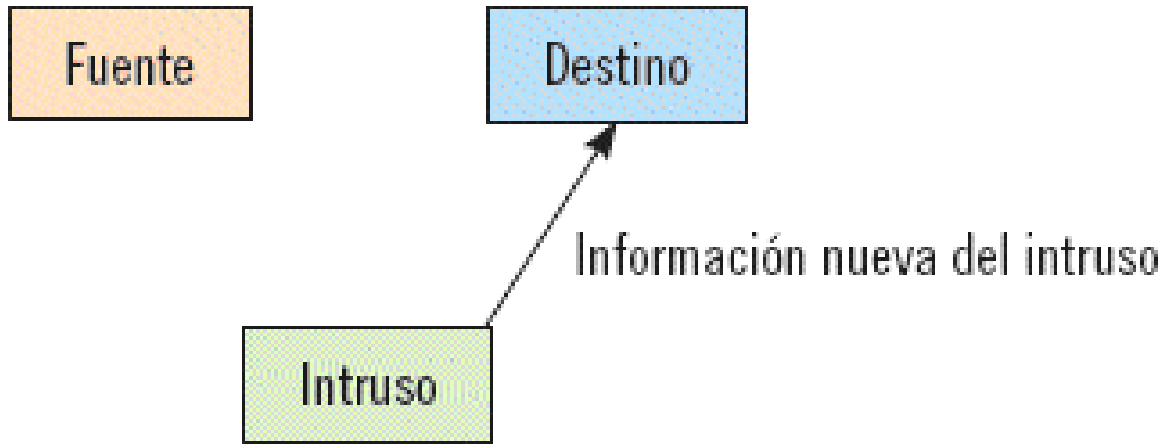
3.1. TIPOS DE ATAQUES

Ataques de modificación



3.1. TIPOS DE ATAQUES

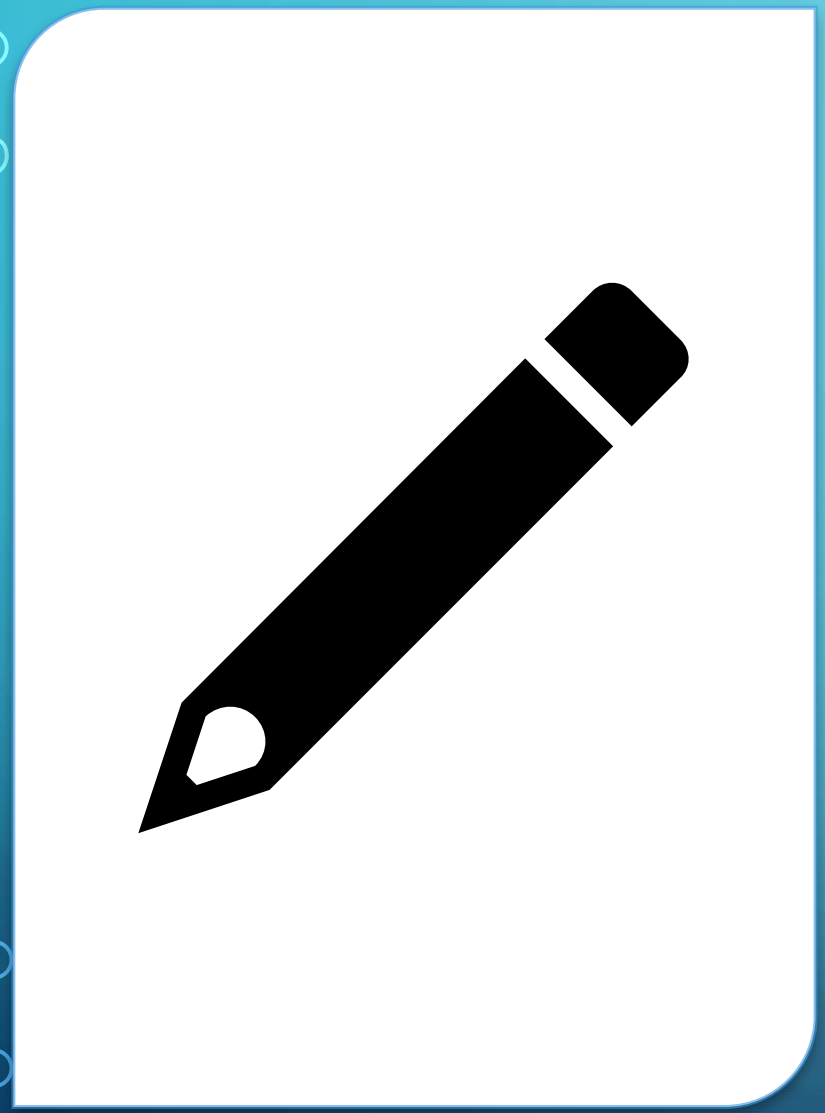
Ataques de fabricación



3.1. TIPOS DE ATAQUES

Clasificación de los distintos tipos de ataques atendiendo al grupo al que pertenecen:

Clasificación de los ataques	Tipos de ataques
Ataques pasivos	Ataques de intercepción
Ataques activos	Ataques de interrupción
	Ataques de modificación
	Ataques de fabricación



Ejemplo

INTENTANDO ACCEDER A LA PÁGINA WEB DE SU ENTIDAD BANCARIA SE DA CUENTA DE QUE HAY UNOS CAMBIOS EN LA MISMA QUE LE HACEN SOSPECHAR QUE PUEDA HABER ALGÚN ATAQUE DE SUPLANTACIÓN DE IDENTIDAD.

INDIQUE EN QUÉ CONSISTE LA SUPLANTACIÓN DE IDENTIDAD, RELACIÓNELO CON EL CASO DE SU ENTIDAD BANCARIA Y SEÑALE EN QUÉ TIPO DE ATAQUE SE CLASIFICA.

Ejemplo. Solución

LA SUPLANTACIÓN DE IDENTIDAD O PHISHING SON ATAQUES EN LOS QUE EL INTRUSO SIMULA SER OTRA ENTIDAD. EN EL CASO DE LA IDENTIDAD BANCARIA ES POSIBLE QUE UN INTRUSO HAYA SIMULADO SER DICHA ENTIDAD REALIZANDO MODIFICACIONES MÍNIMAS PARA ENGAÑAR AL USUARIO Y CONSEGUIR SUS CLAVES BANCARIAS.

LOS ATAQUES DE SUPLANTACIÓN DE IDENTIDAD ESTÁN CLASIFICADOS COMO ATAQUES ACTIVOS AL HABER ALTERACIÓN DE LOS DATOS TRANSFERIDOS EN LA RED.

3.2. CATEGORIZACIÓN DE LOS INCIDENTES

La categorización consistirá en calcular la prioridad del incidente atendiendo a su impacto y urgencia y teniendo en cuenta:

- **Los costes potenciales que se producirían si no se resuelve el incidente.**
- **El daño que puede causar a los distintos miembros de la organización y los costes implícitos que se pueden producir por una interrupción de la comunicación entre ellos.**
- **Las implicaciones legales que puede suponer.**

3.2. CATEGORIZACIÓN DE LOS INCIDENTES

Impacto	Definición	Ejemplos
ALTO	Tienen impacto elevado	Infecciones por software malintencionado como virus, troyanos, etc.
		Accesos no autorizados.
MEDIO	Tienen impacto significativo o potencialmente elevado	Intentos de modificación y obtención de contraseñas.
		Contraseñas desconocidas por los usuarios por alteraciones no autorizadas.
BAJO	Tienen impacto potencialmente significativo	Escaneos del tráfico de red.
		Bloqueos inesperados por la producción de varias denegaciones de accesos.

4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE

Una recomendación importante es la creación de una copia de seguridad en CD/DVD/pendrive/HD como herramienta básica para la respuesta a incidentes.

Revisar los logs de los diferentes sistemas de la red.

4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE

En Microsoft Windows se puede acceder al "Visor de eventos" a través de Inicio -> Herramientas administrativas -> Visor de eventos.

Otra herramienta de búsqueda de evidencias es "Servicios" en la que se accede seleccionando Inicio -> Panel de control -> Herramientas administrativas -> Servicios.

4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE

En Linux los archivos de registro más importantes son:

- **/var/log/messages: contiene los mensajes generales del sistema.**
- **/var/log/secure: almacena los sistemas de autenticación y seguridad.**
- **/var/log/wmtp: almacena un historial de los inicios y cierres de sesión acontecidos.**
- **/var/log/btmp: almacena los inicios de sesión fallidos o erróneos.**

Además de los archivos de registros mencionados también se pueden detectar evidencias de incidentes en archivos como:

- **/etc/passwd: contiene información de las claves del sistema.**
- **/etc/shadow: incluye información de los usuarios.**
- **/etc/group: incluye información sobre los grupos del sistema.**

4.1. CRITERIOS PARA LA RECOLECCIÓN DE EVIDENCIAS

Criterios de sensores basados en equipo o Host Based Sensors

Se encargan de obtener información de los eventos a nivel del sistema operativo (intentos de conexión, accesos al sistema operativo, etc.).

Como ventaja es importante destacar que la información que recogen es de calidad. Además se configuran con facilidad y suministran información con altos niveles de precisión.

Como inconveniente cabe decir que estos sensores pueden afectar considerablemente a la eficiencia del sistema en el que se ejecutan al consumir un elevado nivel de recursos.

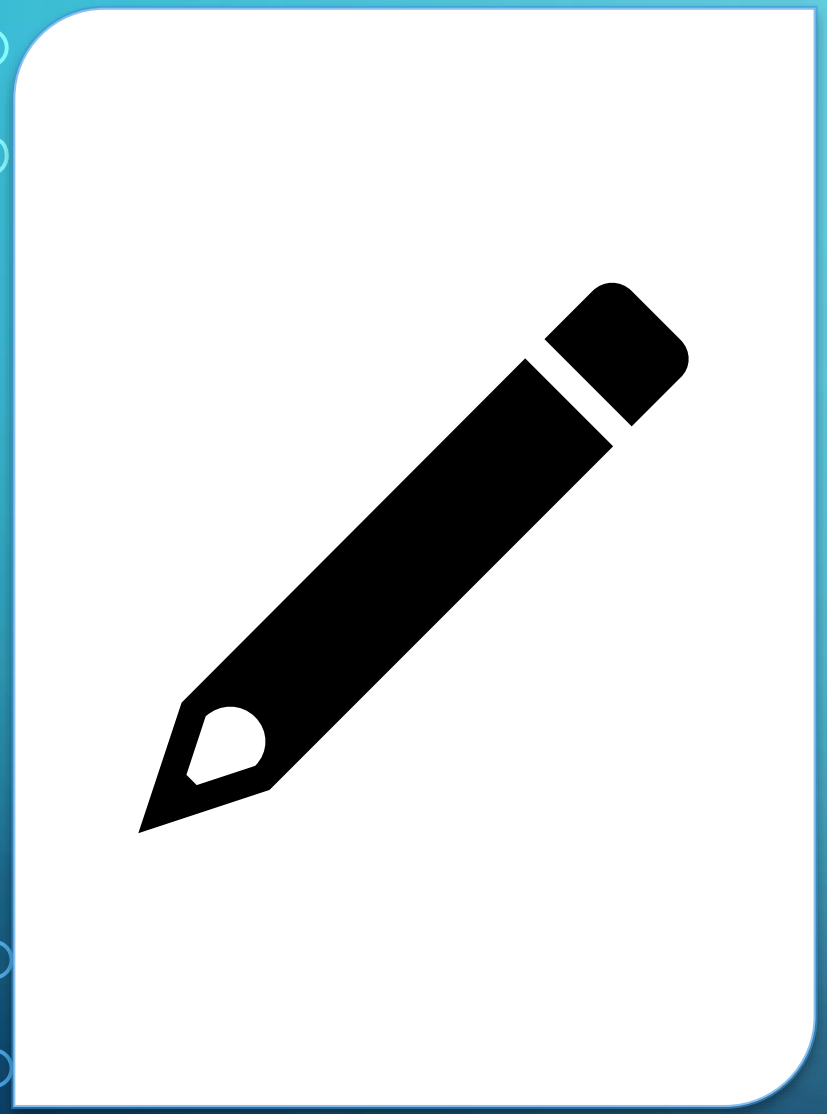
4.1. CRITERIOS PARA LA RECOLECCIÓN DE EVIDENCIAS

Criterios de sensores basados en red o Network Based Sensors

Recolectan información de los eventos que suceden en el tráfico de datos de la red.

Su nivel de seguridad es más elevado que los demás criterios, ya que no tienen que estar necesariamente instalados en el equipo que se pretende analizar y, por lo tanto, tienen más nivel de resistencia ante posibles ataques.

La ventaja principal, además de las comentadas, es la capacidad de obtener información que los otros sensores no ofrecen.



Ejemplo

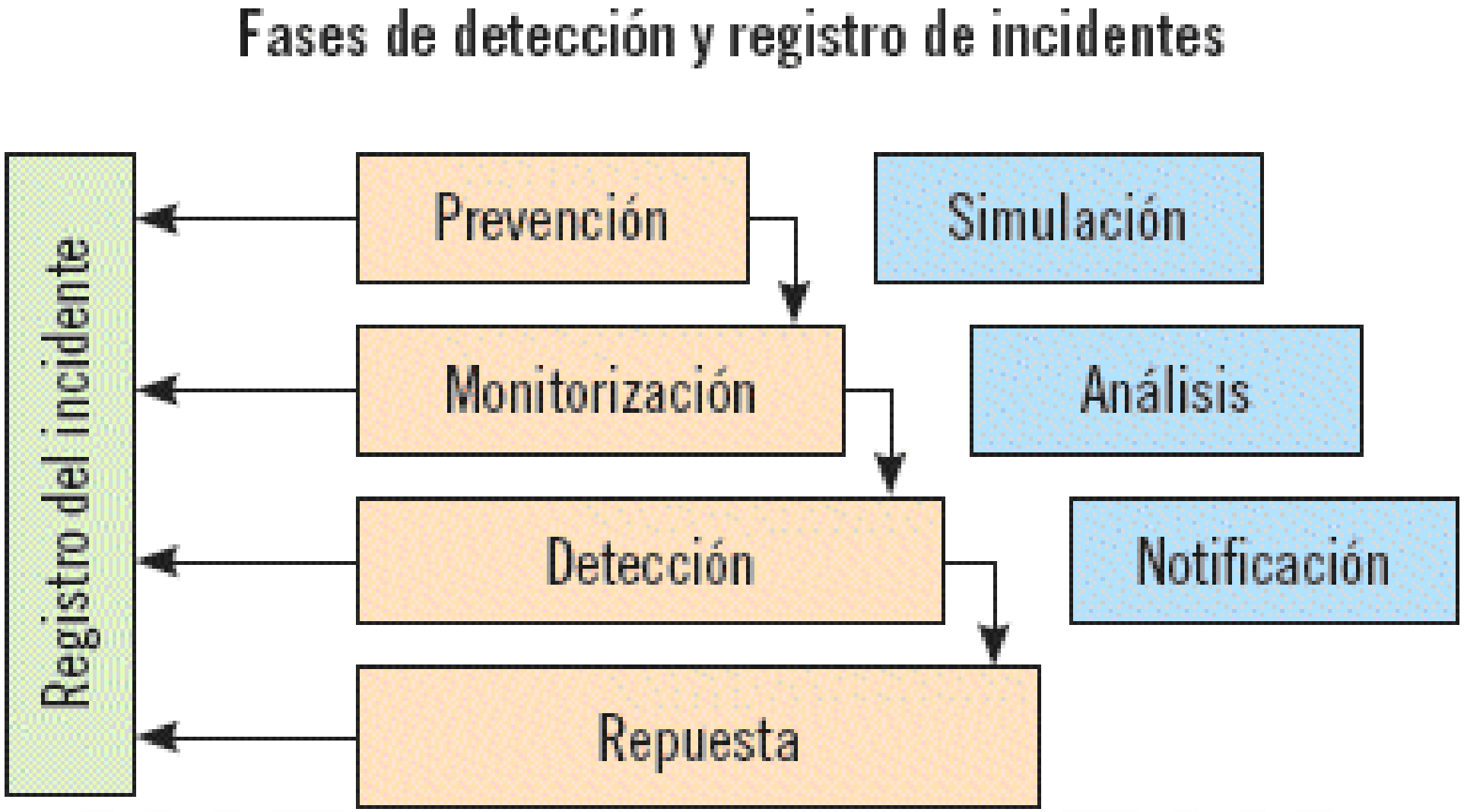
USTED, COMO RESPONSABLE DE LA GESTIÓN DE INCIDENTES, QUIERE IMPLANTAR UN SISTEMA DE RECOLECCIÓN DE EVIDENCIAS ANTE POSIBLES INCIDENTES QUE RECOJA INFORMACIÓN DEL TRÁFICO DE RED QUE CIRCULA ENTRE LOS EQUIPOS DE SU ORGANIZACIÓN. INDIQUE QUÉ CRITERIO (SENSOR) DEBERÍA IMPLANTAR PARA LOGRAR SU COMETIDO Y JUSTIFIQUE LA RESPUESTA.

Ejemplo. Solución

SI LO QUE SE PRETENDE ES OBTENER INFORMACIÓN SOBRE EL TRÁFICO DE DATOS DE UNA RED LA MEJOR OPCIÓN ES EL CRITERIO DE UTILIZACIÓN DE SENSORES EN RED. LOS SENSORES BASADOS EN EL SISTEMA O EN APLICACIONES SOLO RECOGEN INFORMACIÓN SOBRE EVENTOS OCURRIDOS DENTRO DEL EQUIPO SIN TENER EN CUENTA EL TRÁFICO DE RED, POR LO QUE NO SERÍAN ÚTILES EN ESTA OCASIÓN.

PARA UN NIVEL DE PROTECCIÓN MÁS COMPLETO SERÍA RECOMENDABLE UTILIZAR CRITERIOS DE SENSORES HÍBRIDOS QUE PERMITAN OBTENER INFORMACIÓN SOBRE LO QUE OCURRE EN LOS EQUIPOS Y SOBRE LA INFORMACIÓN QUE CIRCULA ENTRE ELLOS.

5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES



5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES

Criterios de sensores basados en red o Network Based Sensors

Tipos de detecciones	¿Cómo detectan?
Basadas en firmas	Buscan elementos reconocidos en su base de datos como intrusiones.
Basadas en políticas	Siguiendo directrices marcadas por la política de seguridad.
Basadas en anomalías	Buscan actividad anómala para su análisis y detección de intrusiones.
Honey pot o jarra de miel	Utilizan señuelos para atraer intrusiones.

5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES

Fase de monitorización de incidentes

En esta fase se monitoriza el tráfico de red del sistema con la finalidad de poder analizarlo y comprobar que todo funciona como se espera o, en caso contrario, incidir en el análisis para averiguar con profundidad los detalles de la actividad inusual.

5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES

Fase de detección de la intrusión

Con la monitorización del tráfico de red y de los procesos que se están ejecutando ya habrá indicios suficientes que determinarán si la actividad sospechosa es realmente una intrusión o no.

5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES

Respuesta

Los sistemas IDS, en general, no pueden combatir y eliminar la amenaza, simplemente se limitan a su detección y a la generación de alertas.

Las respuestas que pueden generar los sistemas IDS se pueden clasificar en:

- Respuestas pasivas
- Respuestas activas

5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES

Registro del incidente

Esta fase del proceso de gestión de incidentes no tiene un momento temporal específico, sino que se debe producir a lo largo de todo el incidente, desde la detección previa de posibles indicios de intrusión hasta el momento en el que se restaura la situación incluyendo el momento anterior de la entrada de la intrusión.