

# **IFCT0109. SEGURIDAD INFORMÁTICA MF0488\_3 GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA**



## **UD02**

**UNIDAD 02. IMPLANTACIÓN Y  
PUESTA EN PRODUCCIÓN DE  
SISTEMAS IDS/IPS**

# CONTENIDOS

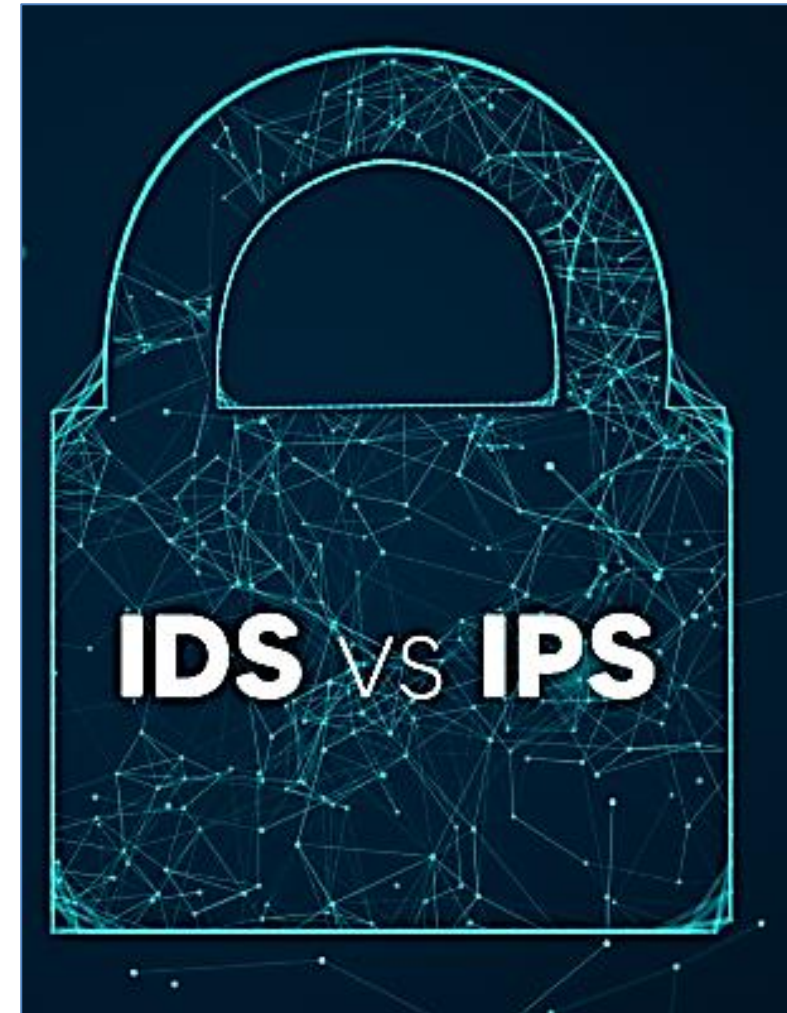
## 1. INTRODUCCIÓN

2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO
3. DEFINICIÓN DE POLÍTICAS DE CORTE DE INTENTOS DE INTRUSIÓN EN LOS IDS/IPS
4. ANÁLISIS DE LOS EVENTOS REGISTRADOS POR EL IDS/IPS PARA DETERMINAR FALSOS POSITIVOS Y CARACTERIZARLOS EN LAS POLÍTICAS DE CORTE DEL IDS/IPS
5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN
6. ESTABLECIMIENTO DE LOS NIVELES REQUERIDOS DE ACTUALIZACIÓN, MONITORIZACIÓN Y PRUEBAS DEL IDS/ IPS

## 1. INTRODUCCIÓN

CUANDO UNA ORGANIZACIÓN DECIDE IMPLANTAR UN SISTEMA IDS/IPS DEBE REALIZAR UNA SERIE DE **ANÁLISIS Y COMPROBACIONES PREVIAS** PARA GARANTIZAR QUE LA IMPLEMENTACIÓN SE REALICE CORRECTAMENTE.

SE DEBE TOMAR LA DECISIÓN DE **UBICACIÓN DEL SISTEMA, EQUIPOS QUE VAN A FUNCIONAR Y SE VAN A UTILIZAR BAJO LOS IDS/IPS Y LOS PROTOCOLOS Y SERVICIOS QUE EMPLEA EN SU ACTIVIDAD DIARIA Y EN LA TRANSFERENCIA Y UTILIZACIÓN DE DATOS.**

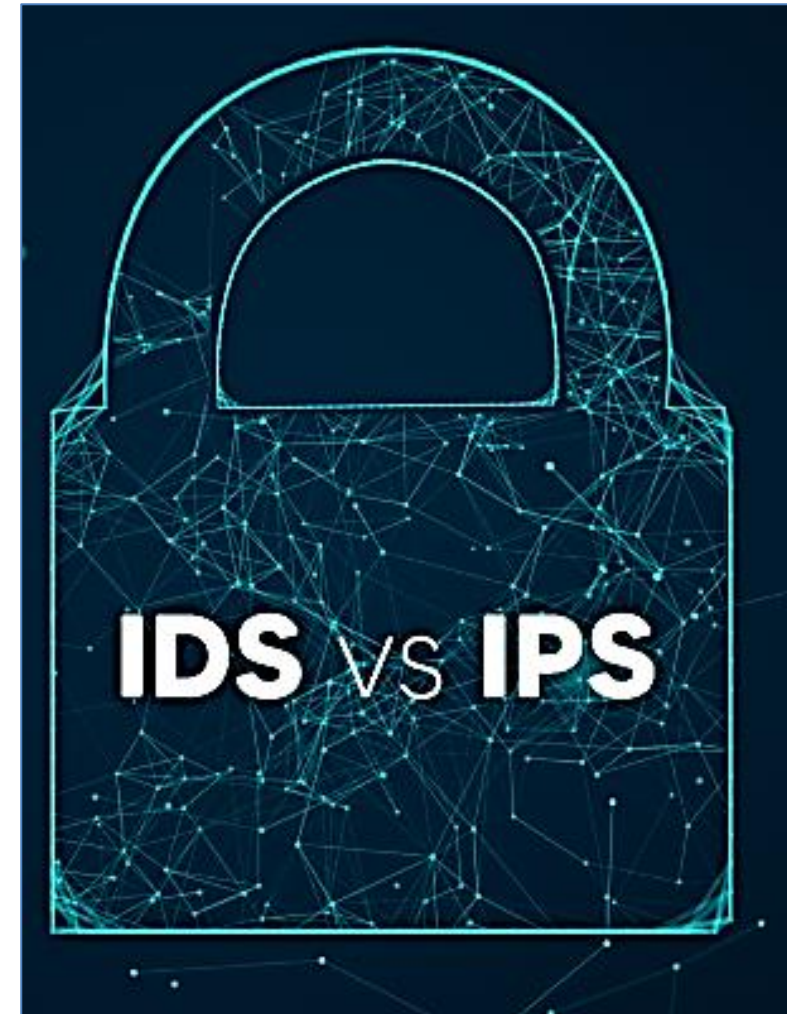


## 1. INTRODUCCIÓN

SE MENCIONAN ALTERNATIVAS DE **POLÍTICAS DE SEGURIDAD** QUE PUEDEN UTILIZARSE EN EL MOMENTO EN EL QUE SE DETECTA ALGÚN TIPO DE ACTIVIDAD SOSPECHOSA.

***NO TODAS LAS INTRUSIONES DETECTADAS TIENEN QUE SER INTRUSIONES REALES Y QUE TAMBIÉN PUEDE SER QUE HAYA ALGUNA INTRUSIÓN NO DETECTADA.***

SE FORMULAN RECOMENDACIONES QUE PERMITAN CONFIGURAR LOS SISTEMAS IDS/IPS PARA REDUCIR LAS INTRUSIONES NO DETECTADAS Y LAS FALSAS DETECCIONES.

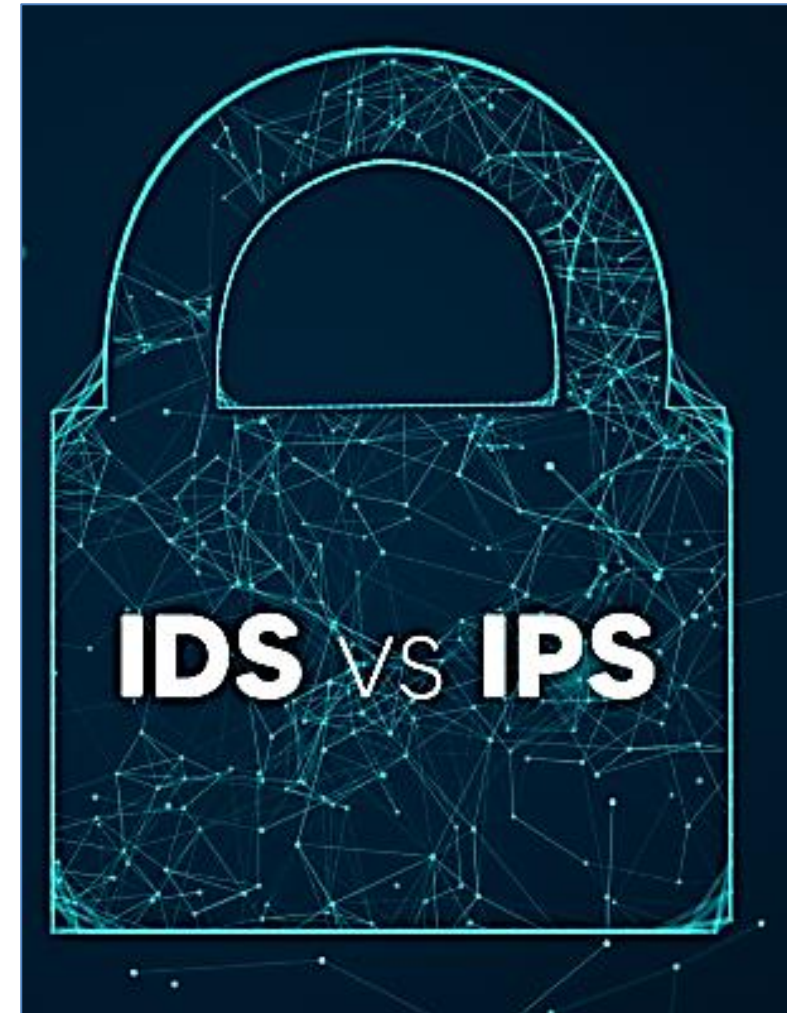




## 1. INTRODUCCIÓN

TAMBIÉN SE DESCRIBEN LAS INFORMACIONES DETALLADAS QUE DEBEN FACILITAR LOS SISTEMAS IDS/IPS CUANDO DETECTAN ALGUNA INTRUSIÓN PARA REALIZAR LA MONITORIZACIÓN DE LOS EVENTOS Y COMPROBAR EL FUNCIONAMIENTO CORRECTO DEL EQUIPO Y SUS DISPOSITIVOS.

POR ÚLTIMO, SE FORMULAN RECOMENDACIONES PARA DEFINIR LOS NIVELES ADECUADOS DE MONITORIZACIÓN, ACTUALIZACIÓN Y PRUEBAS A REALIZAR ANTES DE LA IMPLANTACIÓN Y UNA VEZ IMPLANTADO EL SISTEMA IDS/IPS.



# CONTENIDOS

1. INTRODUCCIÓN
2. **ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO**
3. DEFINICIÓN DE POLÍTICAS DE CORTE DE INTENTOS DE INTRUSIÓN EN LOS IDS/IPS
4. ANÁLISIS DE LOS EVENTOS REGISTRADOS POR EL IDS/IPS PARA DETERMINAR FALSOS POSITIVOS Y CARACTERIZARLOS EN LAS POLÍTICAS DE CORTE DEL IDS/IPS
5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN
6. ESTABLECIMIENTO DE LOS NIVELES REQUERIDOS DE ACTUALIZACIÓN, MONITORIZACIÓN Y PRUEBAS DEL IDS/ IPS

## 2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO

LOS SISTEMAS IDS/IPS CADA VEZ RESULTAN **MÁS IMPRESCINDIBLES** PARA CUALQUIER EMPRESA QUE TRABAJE CON ALGUNA INFRAESTRUCTURA DE RED.

LOS **INTENTOS DE INTRUSIÓN** Y DE UTILIZACIÓN MALINTENCIONADA DE LOS DATOS DE UNA ORGANIZACIÓN **SIGUEN AUMENTANDO** A NIVELES CADA VEZ MÁS ELEVADOS.



## 2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO

AUNQUE ESTOS SISTEMAS RESULTAN MUY ÚTILES PARA EVITAR POSIBLES INTRUSIONES, NO SON SUFICIENTES: LAS ORGANIZACIONES DEBEN ESTABLECER UNA SERIE DE MEDIDAS DE SEGURIDAD ADICIONALES QUE SIRVAN DE APOYO EN EL MOMENTO QUE OCURRA CUALQUIER FALLO DE SEGURIDAD.





## 2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO

ES NECESARIO QUE LAS ORGANIZACIONES REALICEN PREVIAMENTE UN ESTUDIO DE SUS INFRAESTRUCTURAS, SERVICIOS, EQUIPOS, ZONAS Y PROTOCOLOS, ENTRE OTROS MUCHOS ELEMENTOS, PARA QUE LA IMPLANTACIÓN DEL SISTEMA **IDS/IPS** Y DE LAS DEMÁS MEDIDAS DE SEGURIDAD SE REALICEN DE UN MODO CORRECTO Y EFECTIVO.



## 2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO

ESTO REQUIERE UN PROCESO PREVIO DE PLANIFICACIÓN, PREPARACIÓN, PRUEBAS Y FORMACIÓN ESPECIALIZADA DE LOS ADMINISTRADORES DE MODO QUE SE PUEDA FUNCIONAR A PLENO RENDIMIENTO Y CON LA CERTEZA DE QUE EL NIVEL DE SEGURIDAD DE LA INFRAESTRUCTURA DE LA ORGANIZACIÓN ES EL ADECUADO.



## 2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO

LA IMPLEMENTACIÓN DE LOS SISTEMAS IDS/IPS DEPENDEN EN MAYOR PARTE DE LOS RECURSOS Y POLÍTICAS DE LA ORGANIZACIÓN Y **DEBE REALIZARSE ESCALONADAMENTE** PARA QUE EL PROCESO DE APRENDIZAJE DE LOS ADMINISTRADORES SEA PROFUNDO Y BASADO EN LA EXPERIENCIA QUE VAYA ADQUIRIENDO A MEDIDA QUE SE COMPLETA LA IMPLEMENTACIÓN.

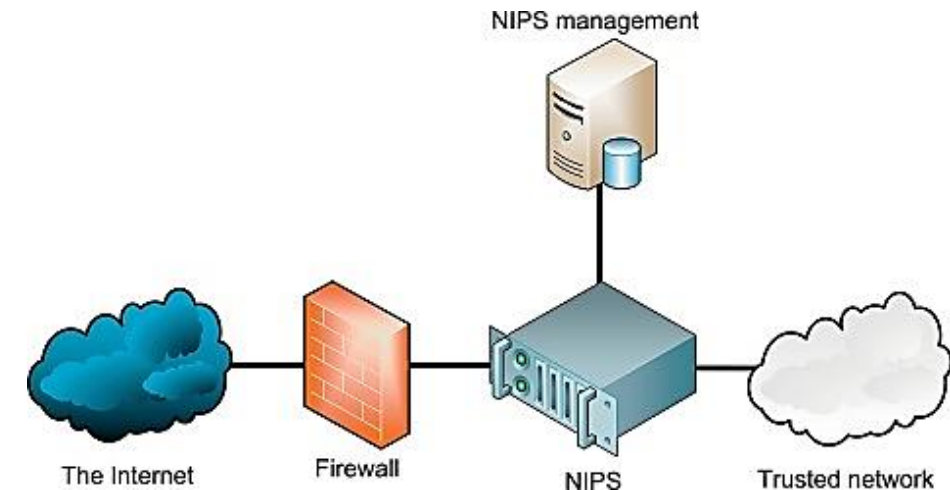


## 2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO

### SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES EN RED O NIPS

LOS **NIPS** MONITORIZAN LOS DATOS QUE CIRCULAN EN UNA RED, PARA BUSCAR POSIBLES ACCESOS NO AUTORIZADOS Y FILTRAR EL TRÁFICO.

**SON MUY ÚTILES PORQUE PROPORCIONAN ALERTAS CUANDO SE PRODUCE UN ATAQUE EN LA RED Y PUEDEN REACCIONAR PARA EVITARLA O PARA INTENTAR QUE LOS DAÑOS SEAN MÍNIMOS.**



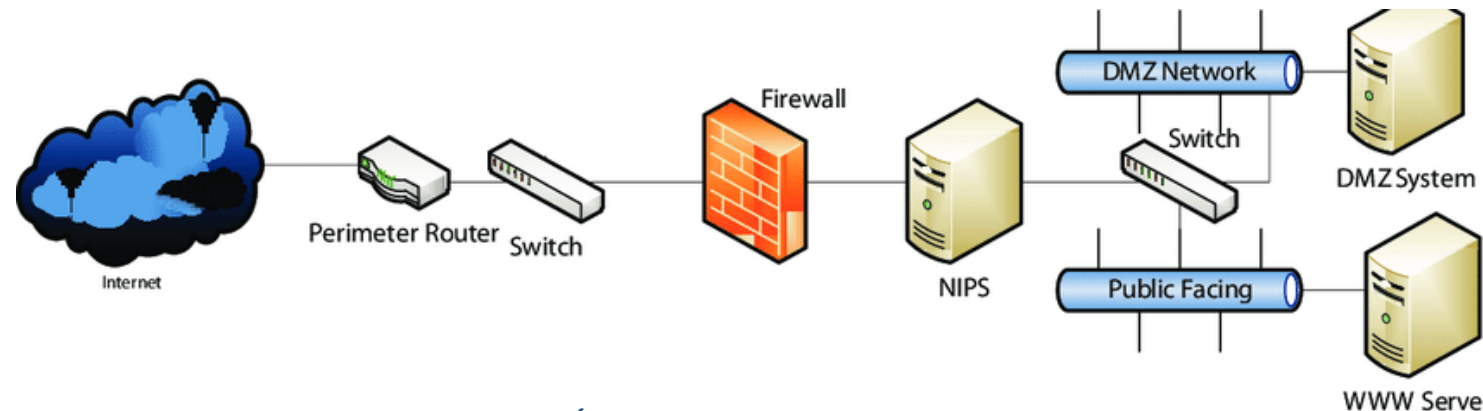


## 2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO

### SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES EN RED O NIPS

ADEMÁS, FACILITAN UN ANÁLISIS DE LAS INTRUSIONES EXITOSAS, LO QUE AYUDA A LAS ORGANIZACIONES A PREVENIR ESTAS INTRUSIONES EN MOMENTOS FUTUROS.

NO OBSTANTE, NUNCA DEBEN SER SUSTITUTOS DE UNA POLÍTICA DE SEGURIDAD, SINO QUE DEBEN SER ACCESORIOS.



## **2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO**

### **SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES EN RED O NIPS**

ESTOS SISTEMAS PUEDEN COLOCARSE EN VARIAS UBICACIONES DE LA  
INFRAESTRUCTURA DE RED DE UNA ORGANIZACIÓN

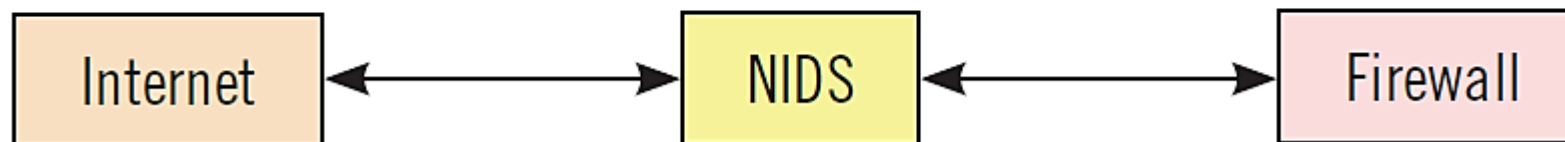
- **DELANTE DEL FIREWALL**
- **DETRÁS DEL FIREWALL**
- **DELANTE Y DETRÁS DEL FIREWALL**

## 2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO

### SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES EN RED O NIPS DELANTE DEL FIREWALL

LA COLOCACIÓN DELANTE DEL CORTAFUEGOS EXTERNO PERMITE UNA MONITORIZACIÓN DE LOS ATAQUES (TANTO EN TIPO COMO EN NÚMERO DE ATAQUES) CONTRA LA INFRAESTRUCTURA DE UNA ORGANIZACIÓN Y DETECTA **PRINCIPALMENTE AQUELLOS ATAQUES QUE VAN DIRIGIDOS CONTRA EL FIREWALL DE LA RED.**

Delante del cortafuegos



## **2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO**

### **SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES EN RED O NIPS DELANTE DEL FIREWALL**

ESTA UBICACIÓN TAMBIÉN IMPLICA UNA SERIE DE **DESVENTAJAS**:

- NO DETECTA ATAQUES CON INFORMACIÓN ENCRIPTADA.
- EL NIPS, SI ESTÁ MAL DISEÑADO, SE PUEDE SATURAR DEBIDO AL ELEVADO TRÁFICO DE RED QUE ACONTECE EN ESTA ZONA DE LA INFRAESTRUCTURA DE LA RED.
- EL EXCESO DE INFORMACIÓN PRODUCIDO POR EL ELEVADO TRÁFICO DE RED PUEDE SER CONTRAPRODUCENTE, YA QUE PUEDE SER MÁS DIFÍCIL LOCALIZAR LA INFORMACIÓN IMPORTANTE Y, POR LO TANTO, LOS ATAQUES EFECTIVOS.
- NO OFRECE UN ELEVADO GRADO DE PROTECCIÓN YA QUE SI ALGÚN INTRUSO LO LOCALIZA PUEDE DIRIGIR SUS ATAQUES DIRECTAMENTE A ÉL.

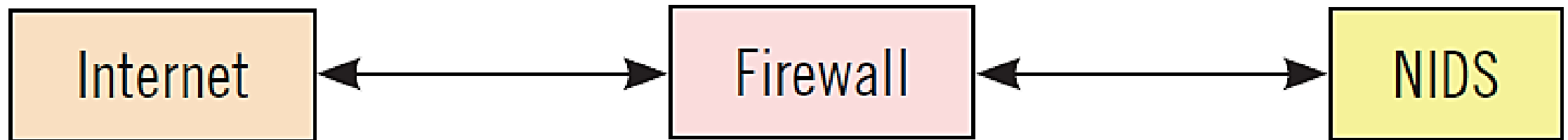


## 2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO

### SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES EN RED O NIPS DETRÁS DEL FIREWALL

EL SISTEMA **NIPS** SE SITÚA ENTRE LA RED EXTERNA Y LA RED INTERNA EN UNA ZONA LLAMADA **DMZ** (ZONA DESMILITARIZADA).

ESTA LOCALIZACIÓN PERMITE COMPROBAR LA TOTALIDAD DE LOS ATAQUES QUE SE PRODUCEN EN LA RED DE LA ORGANIZACIÓN, TANTO EXITOSOS COMO NO EXITOSOS.



## **2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO**

### **SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES EN RED O NIPS DETRÁS DEL FIREWALL**

COMO VENTAJAS DE LOCALIZAR LOS SISTEMAS EN ESTA ZONA DESTACAN:

- EN ESTA UBICACIÓN SE MONITORIZAN AQUELLAS INTRUSIONES QUE CONSIGUEN ATRAVESAR EL CORTAFUEGOS O FIREWALL.
- LOS ATAQUES DETECTADOS SON POTENCIALMENTE MUCHO MÁS PELIGROSOS QUE LOS DETECTADOS EN OTRAS UBICACIONES, POR LO QUE EL RIESGO DE ATAQUES EXITOSOS DISMINUYE CONSIDERABLEMENTE.
- AL PODER IDENTIFICAR LOS ATAQUES MÁS COMUNES PERMITE UNA CONFIGURACIÓN MÁS EFECTIVA DEL CORTAFUEGOS PRINCIPAL.
- LA CANTIDAD DE LOGS ES INFERIOR, PERO LA INFORMACIÓN FACILITADA POR ESTOS SISTEMAS ESTÁ MEJOR SELECCIONADA Y ES MÁS RELEVANTE.

## **2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO**

### **SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES EN RED O NIPS DETRÁS DEL FIREWALL**

NO TODO SON VENTAJAS, TAMBIÉN HAY QUE TENER EN CUENTA UNA SERIE DE **DESVENTAJAS**:

- SOLO SE MONITORIZA EL TRÁFICO QUE HAYA ENTRADO REALMENTE EN LA RED. AL ESTAR SITUADO POSTERIORMENTE AL CORTAFUEGOS, LOS DATOS QUE LE LLEGAN HAN SIDO PREVIAMENTE FILTRADOS POR LA BARRERA DEL FIREWALL.
- EN ESTA UBICACIÓN TAMPOCO SE PUEDEN IDENTIFICAR LOS ATAQUES CON INFORMACIÓN ENCRIPTADA.
- AUNQUE LA SEGURIDAD DEL NIPS MEJORA CONSIDERABLEMENTE AL ESTAR SITUADO A CONTINUACIÓN DEL CORTAFUEGOS, ESTA SIGUE SIN SER SUFICIENTE: HAY QUE UTILIZAR MEDIDAS DE SEGURIDAD ADICIONALES.

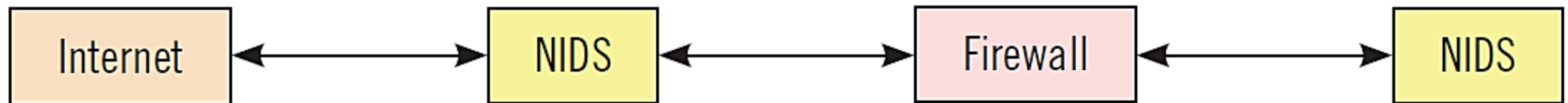
## 2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO

### SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES EN RED O NIPS

### COMBINACIÓN DE LOS DOS ANTERIORES

UNA OPCIÓN MUY VÁLIDA QUE CONTRARRESTA LAS DESVENTAJAS DE LA UBICACIÓN DEL SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES ANTES O DESPUÉS DEL CORTAFUEGOS ES LA COMBINACIÓN DE AMBAS: SITUAR SISTEMAS ANTES Y DESPUÉS DEL CORTAFUEGOS.

Delante y detrás del cortafuegos





## **2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO**

### **SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES EN RED O NIPS COMBINACIÓN DE LOS DOS ANTERIORES**

ESTA COMBINACIÓN REÚNE LAS **VENTAJAS** DE LAS DOS UBICACIONES Y, ADEMÁS, PROPORCIONA OTRAS ADICIONALES:

- HAY UN MAYOR CONTROL DE LAS POSIBLES INTRUSIONES EN LA RED.
- EN EL SUPUESTO DE QUE SE DEJE PASAR TRÁFICO QUE NO SE DEBE, ESTA COMBINACIÓN PERMITE IR MEJORANDO LA SEGURIDAD A TRAVÉS DEL APRENDIZAJE.
- PERMITE UNA CORRELACIÓN ENTRE LOS ATAQUES DETECTADOS ANTES Y DESPUÉS DEL CORTAFUEGOS.

COMO **DESVENTAJA** PRINCIPAL DESTACA EL COSTE DE DOS MÁQUINAS PARA IMPLEMENTAR ESTOS SISTEMAS EN DOS UBICACIONES.

## 2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO

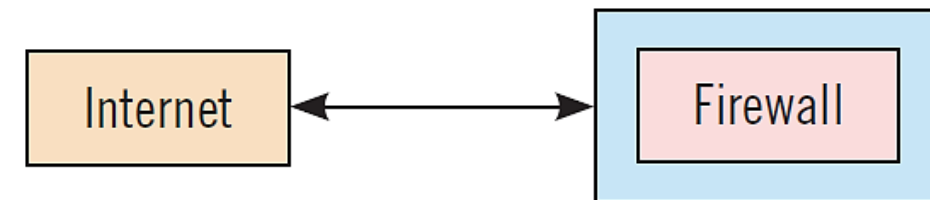
### SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES EN RED O NIPS

#### COMBINACIÓN FIREWALL/NIDPS

CUANDO LA ORGANIZACIÓN NO DISPONE DE MÁQUINAS SUFICIENTES PARA QUE HAYA UNA DE ELLAS DESTINADA EXCLUSIVAMENTE A IPS, UNA ALTERNATIVA ES UTILIZAR **UN EQUIPO QUE FUNCIONE COMO CORTAFUEGOS Y NIPS A LA VEZ.**

SE MONITORIZA TODO EL TRÁFICO DE LA RED CON VENTAJAS Y DESVENTAJAS, PERO SE REDUCE EL GASTO.

Equipo utilizado como cortafuegos y NIDS



## **2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO**

**SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES EN RED O NIPS**

**UBICACIÓN EN LAS REDES PRINCIPALES DE LA ORGANIZACIÓN**

MONITORIZA UNA CANTIDAD MÁS ELEVADA DE TRÁFICO, LO QUE  
**AUMENTA LAS POSIBILIDADES DE ENCONTRAR POSIBLES ATAQUES.**

ADEMÁS, TAMBIÉN PERMITE DETECTAR AQUELLOS ATAQUES QUE SE  
**PRODUCEN DENTRO DE LA MISMA RED INTERNA DE LA ORGANIZACIÓN.**

AUN ASÍ, TAMBIÉN PRESENTA UNA SERIE DE **DESVENTAJAS:**

- TAMPOCO SE DETECTAN ATAQUES CON INFORMACIÓN ENCRIPTADA.
- LOS SISTEMAS SITUADOS EN LAS REDES GENERALES PUEDEN HACERLAS MÁS VULNERABLES ANTE ATAQUES INTERNOS PRODUCIDOS DENTRO DE LA MISMA RED.

## **2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO**

### **SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES EN RED O NIPS**

### **UBICACIÓN EN LAS REDES CRÍTICAS DE LA ORGANIZACIÓN**

LA UBICACIÓN DE LOS IDS/IPS EN ESTAS REDES PERMITE LA DETECCIÓN Y PREVENCIÓN DE LOS ATAQUES REALIZADOS ESPECÍFICAMENTE CONTRA LOS DATOS CRÍTICOS Y AÑADEN UN NIVEL DE SEGURIDAD ADICIONAL A LOS MISMOS, MINIMIZANDO AÚN MÁS LOS POSIBLES RIESGOS DE ATAQUES.

AUN ASÍ, NO EVITAN LOS ATAQUES CONTRA LAS REDES GENERALES Y SERÁN NECESARIAS MÁS MEDIDAS ADICIONALES QUE PROTEJAN A LA INFRAESTRUCTURA DE RED GENERAL DE LA ORGANIZACIÓN.



## **2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO**

### **SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES EN HIPS**

LOS SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES BASADOS EN HOSTS SON LOS **QUE RESIDEN EN EL MISMO EQUIPO QUE MONITORIZAN Y SOLO SE PREOCUPAN DE PROTEGER A DICHO EQUIPO** SIN NECESIDAD DE MONITORIZAR TODO EL TRÁFICO DE LA RED DE UNA ORGANIZACIÓN.

CONSUMEN MENOS RECURSOS QUE LOS **NIDS** O **NIPS** Y NO IMPIDEN UN BUEN RENDIMIENTO DEL SISTEMA.

AUNQUE IMPLICAN UN MEJOR RENDIMIENTO DEL SISTEMA, ESTOS TIPOS DE SISTEMA **COMBATEN LAS INTRUSIONES UNA VEZ QUE EL EQUIPO YA ESTÁ EN PELIGRO**, LO QUE EL RIESGO ES BASTANTE MAYOR.

## **2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO**

### **SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES EN HIPS**

**ADEMÁS, IMPLICA UNAS MAYORES MEDIDAS DE SEGURIDAD EN EL EQUIPO PARA COMBATIR LOS ATAQUES.**

LOS **HIPS** MONITORIZAN CON MÁS PROFUNDIDAD LOS DATOS DEL EQUIPO QUE LOS **NIPS** COMO: EL TRÁFICO INALÁMBRICO, EL TRÁFICO DE RED, LOS ACCESOS A LOS ARCHIVOS, LOS CAMBIOS DE CONFIGURACIÓN EN EL EQUIPO O EN ALGUNA APLICACIÓN, ETC.

AUN ASÍ, Y DEL MISMO MODO QUE EN LOS DEMÁS SISTEMAS MENCIONADOS, TAMPOCO DETECTA LOS ATAQUES CON INFORMACIÓN ENCRIPTADA.

## **2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO IDS/IPS EN AMBIENTES VIRTUALES**

LA UTILIZACIÓN SERVICIOS EN **LA NUBE** ES MAYOR DEBIDO A SUS  
NUMEROSAS VENTAJAS:

- HAY UN AHORRO DE ENERGÍA AL SER NECESARIA UNA INFRAESTRUCTURA MENOR EN LA ORGANIZACIÓN PARA ALMACENAR DATOS.
- SUPONEN UN COSTE MENOR DE MANTENIMIENTO, LOS EQUIPOS PUEDEN TENER MAYOR CAPACIDAD DE ALMACENAMIENTO Y REDUCIR EL ESPACIO FÍSICO Y COSTES (ELECTRICIDAD, MENOS GASTOS DE ALQUILER DE LOCAL, ETC.).

## **2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO IDS/IPS EN AMBIENTES VIRTUALES**

EL NIVEL DE SEGURIDAD EN ESTE TIPO DE SISTEMAS ES BASTANTE ELEVADO AL ESTAR LAS ESTRUCTURAS FÍSICAS SITUADAS FUERA DE LA ORGANIZACIÓN.

ADEMÁS, AL UTILIZAR SOLUCIONES DE DETECCIÓN Y PREVENCIÓN DE ATAQUES FACILITADAS POR PROVEEDORES QUE OFRECEN SERVICIO A MUCHAS OTRAS ORGANIZACIONES, **LA BASE DE DATOS DE POSIBLES VULNERABILIDADES Y ATAQUES ES MUCHO MAYOR Y HAY MÁS POSIBILIDAD DE DETECCIÓN Y REACCIÓN.**

## **2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO**

### **IDS/IPS INALÁMBRICOS O WIRELESS IDS/IPS**

ESTE TIPO DE SISTEMAS ANALIZAN LOS PROTOCOLOS INALÁMBRICOS PARA DETECTAR LAS ACTIVIDADES SOSPECHOSAS.

SU FUNCIONAMIENTO ES IGUAL A LOS **NIPS**, CON SERVIDOR, CONSOLA Y BASE DE DATOS Y PERMITE LA MONITORIZACIÓN DEL TRÁFICO DE RED QUE CIRCULA POR LA RED INALÁMBRICA DE LA ORGANIZACIÓN.

COMO DESVENTAJA PRINCIPAL CABE SEÑALAR QUE **LOS ANÁLISIS DE ESTOS SISTEMAS SE LIMITAN A UN SOLO CANAL**, POR LO QUE SI LA ORGANIZACIÓN UTILIZA VARIOS CANALES INALÁMBRICOS NO PODRÁN REALIZARSE ANÁLISIS DE TODOS LOS CANALES SIMULTÁNEAMENTE.



## **2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO**

### **DECISIONES DE LA ORGANIZACIÓN PARA UBICAR UN SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES**

EN EL MOMENTO DE DECIDIR QUE SISTEMA IDS/IPS IMPLANTAR EN LA ORGANIZACIÓN, ES NECESARIO REALIZAR UN ANÁLISIS PREVIO Y PROFUNDO QUE INCLUYA VARIOS ASPECTOS:

- **ANÁLISIS DE LOS PROCESOS DE NEGOCIO** E IDENTIFICACIÓN DE LA INFORMACIÓN VALIOSA EN CADA UNO DE LOS PROCESOS.
- **ANÁLISIS DE LOS PROTOCOLOS DE RED** UTILIZADOS PARA TRANSFERIR DATOS ENTRE LOS EQUIPOS DE LA ORGANIZACIÓN Y AL EXTERIOR.
- **ANÁLISIS DE LOS PROTOCOLOS Y POLÍTICAS DE LA ORGANIZACIÓN** PARA SER COHERENTES CON SU POLÍTICA DE SEGURIDAD Y SU POLÍTICA DE COSTES EN EL MOMENTO DE IMPLANTAR EL SISTEMA IDS/IPS APROPIADO.

## **2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO**

### **DECISIONES DE LA ORGANIZACIÓN PARA UBICAR UN SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES**

- **ANÁLISIS DE LAS DISTINTAS ZONAS** QUE FORMAN PARTE DE LA ORGANIZACIÓN Y LA UBICACIÓN DE SUS EQUIPOS Y SERVIDORES PARA VER QUÉ UBICACIÓN DEL IDS/ IPS PUEDE SER MÁS CONVENIENTE SEGÚN SUS CARACTERÍSTICAS.
- **ANÁLISIS DE LOS SERVICIOS** QUE OFRECE LA ORGANIZACIÓN PARA AVERIGUAR CUÁLES DE ELLOS NECESITAN UN NIVEL DE SEGURIDAD ESPECIAL DEBIDO A LA TIPOLOGÍA DE INFORMACIÓN CON LA QUE TRABAJAN.

## **2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO**

### **DECISIONES DE LA ORGANIZACIÓN PARA UBICAR UN SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES**

**NO OBSTANTE, LOS SISTEMAS IDS/IPS NO DEBEN SER LOS ÚNICOS  
SISTEMAS DE SEGURIDAD IMPLANTADOS SIENDO NECESARIAS OTRAS  
MEDIDAS COMO ANTIVIRUS, FIREWALLS, ETC.**

# CONTENIDOS

1. INTRODUCCIÓN
2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO
3. **DEFINICIÓN DE POLÍTICAS DE CORTE DE INTENTOS DE INTRUSIÓN EN LOS IDS/IPS**
4. ANÁLISIS DE LOS EVENTOS REGISTRADOS POR EL IDS/IPS PARA DETERMINAR FALSOS POSITIVOS Y CARACTERIZARLOS EN LAS POLÍTICAS DE CORTE DEL IDS/IPS
5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN
6. ESTABLECIMIENTO DE LOS NIVELES REQUERIDOS DE ACTUALIZACIÓN, MONITORIZACIÓN Y PRUEBAS DEL IDS/ IPS

### **3. DEFINICIÓN DE POLÍTICAS DE CORTE DE INTENTOS DE INTRUSIÓN EN LOS IDS/IPS**

UNA VEZ TOMADA LA DECISIÓN SOBRE EL SISTEMA IDS/IPS QUE SE VA A IMPLANTAR EN LA ORGANIZACIÓN **HAY QUE DEFINIR UNA SERIE DE POLÍTICAS SOBRE EL TIPO DE RESPUESTA** QUE DEBE TOMAR CUANDO HAYA ALGÚN INTENTO DE INTRUSIÓN O ATAQUE.

VEAMOS LOS TIPOS DE ANÁLISIS QUE REALIZAN ESTOS SISTEMAS.

SEGÚN EL **PROCEDIMIENTO DE ANÁLISIS DE LOS DATOS**, HAY DOS TIPOS FUNDAMENTALES DE ANÁLISIS:

- **DETECCIÓN DE USOS INDEBIDOS (MISUSE)**
- **DETECCIÓN DE ANOMALÍAS**



### **3. DEFINICIÓN DE POLÍTICAS DE CORTE DE INTENTOS DE INTRUSIÓN EN LOS IDS/IPS**

#### **DETECCIÓN DE USOS INDEBIDOS (MISUSE)**

LOS IDS/IPS UTILIZAN UNA BASE DE DATOS PARA **ENCONTRAR USOS INDEBIDOS MEDIANTE LA COMPARACIÓN DE LAS FIRMAS** DE LA BASE DE DATOS CON LA INFORMACIÓN RECOGIDA PREVIAMENTE.

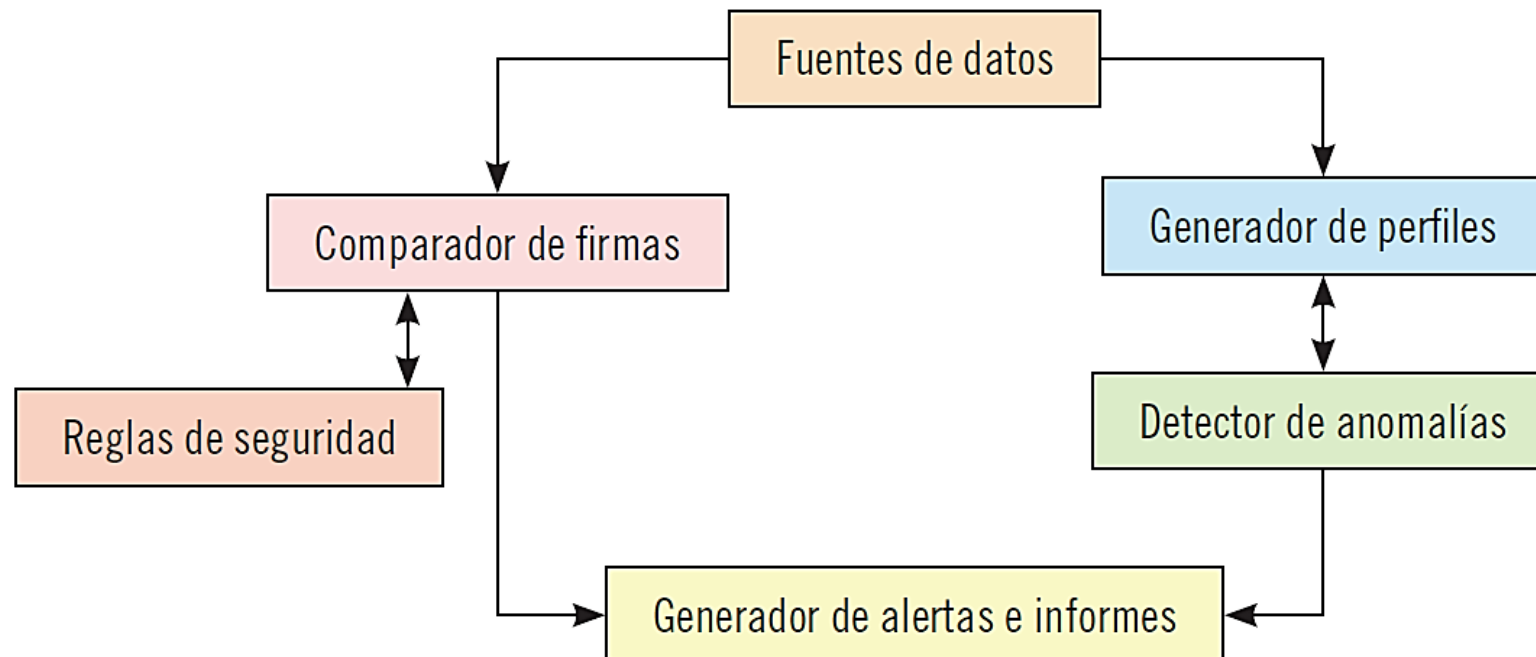
#### **DETECCIÓN DE ANOMALÍAS**

EN ESTE CASO NO SE UTILIZA UNA BASE DE DATOS COMO ELEMENTO DE COMPARACIÓN, SINO QUE **SE EMPLEAN TÉCNICAS ESTADÍSTICAS PARA DEFINIR Y APROXIMAR LOS PATRONES** QUE SE CORRESPONDEN CON UN COMPORTAMIENTO NORMAL.

### 3. DEFINICIÓN DE POLÍTICAS DE CORTE DE INTENTOS DE INTRUSIÓN EN LOS IDS/IPS

EN LA SIGUIENTE FIGURA SE PUEDE OBSERVAR EL FUNCIONAMIENTO DE LOS DOS TIPOS DE ANÁLISIS EN LOS SISTEMAS DE DETECCIÓN DE INTRUSIONES.

Tipos de análisis de detección de intrusiones



### **3. DEFINICIÓN DE POLÍTICAS DE CORTE DE INTENTOS DE INTRUSIÓN EN LOS IDS/IPS**

OTRA MANERA DE DISTINGUIR LOS TIPOS DE ANÁLISIS DE LOS SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES ES TENIENDO EN CUENTA **EL TIEMPO DE REALIZACIÓN DE LOS ANÁLISIS**, DISTINGUIENDO ENTRE:

- **ANÁLISIS POR LOTES (BATCH MODE)**
- **ANÁLISIS EN TIEMPO REAL**

### **3. DEFINICIÓN DE POLÍTICAS DE CORTE DE INTENTOS DE INTRUSIÓN EN LOS IDS/IPS**

#### **ANÁLISIS POR LOTES (BATCH MODE)**

**EL ANÁLISIS DE LOS DATOS PARA DETECTAR INTRUSIONES SE REALIZA CADA CIERTO INTERVALO DE TIEMPO DEFINIDO.**

**AL FINALIZAR CADA PERÍODO DE TIEMPO EL SISTEMA REALIZA EL ANÁLISIS DE LOS DATOS RECIBIDOS EN ESE PERÍODO.**

**TIENE COMO INCONVENIENTE PRINCIPAL QUE LAS POSIBLES ALARMAS DE LAS INTRUSIONES SUCEDIDAS NO SE HACEN EN TIEMPO REAL, SINO QUE SE ORIGINAN DESPUÉS DE HABERSE PRODUCIDO LAS INTRUSIONES.**

### **3. DEFINICIÓN DE POLÍTICAS DE CORTE DE INTENTOS DE INTRUSIÓN EN LOS IDS/IPS**

- **ANÁLISIS EN TIEMPO REAL**

**EN ESTE TIPO DE ANÁLISIS SE EXAMINAN LOS DATOS CONFORME SE VAN RECIBIENDO A TIEMPO REAL O CON UN RETARDO MÍNIMO DE TIEMPO.**

**SON MÁS UTILIZADOS YA QUE POSIBILITAN RESPONDER A LAS POSIBLES INTRUSIONES A LA MISMA VEZ QUE SE VAN DETECTANDO.**



### 3. DEFINICIÓN DE POLÍTICAS DE CORTE DE INTENTOS DE INTRUSIÓN EN LOS IDS/IPS

#### Análisis de los datos obtenidos por los IDS/IPS

Clasificación del análisis	Tipo de análisis
Según el procedimiento de análisis de los datos	Detección de usos indebidos
	Detección de anomalías
Según el tiempo del análisis	Análisis por lotes
	Análisis a tiempo real

### 3. DEFINICIÓN DE POLÍTICAS DE CORTE DE INTENTOS DE INTRUSIÓN EN LOS IDS/IPS

EL SIGUIENTE PASO CONSISTE EN DEFINIR LAS POLÍTICAS DE ACTUACIÓN DEL SISTEMA **IDS/IPS** CUANDO SE DETECTA ALGÚN INTENTO DE INTRUSIÓN. SE PUEDE DISTINGUIR ENTRE DOS LÍNEAS ACTUACIÓN EN CUANTO A POLÍTICAS DE SEGURIDAD:

- **POLÍTICA PROHIBITIVA:** SE PROHÍBE TODO LO QUE NO SE HA DEFINIDO COMO PERMITIDO EXPRESAMENTE.
- **POLÍTICA PERMISIVA:** SE DEFINE TODO LO QUE SE VA A PROHIBIR Y TODO LO DEMÁS SE CONSIDERA PERMITIDO.

LO MÁS HABITUAL ES UTILIZAR POLÍTICAS PERMISIVAS, YA QUE LAS PROHIBITIVAS SON DEMASIADO RESTRICTIVAS Y PUEDEN OCASIONAR BLOQUEOS DE ACCIONES RUTINARIAS O BÁSICAS QUE SE PUEDEN HABER PASADO POR ALTO EN LA DEFINICIÓN DE LAS PERMISIONES.

### **3. DEFINICIÓN DE POLÍTICAS DE CORTE DE INTENTOS DE INTRUSIÓN EN LOS IDS/IPS**

## **POLÍTICAS DE CORTE DE INTRUSIONES EN SISTEMAS IDS/IPS**

EN CUANTO A LOS SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES, CUANDO SE DETECTA ALGUNA INTRUSIÓN SE PUEDEN DEFINIR DOS TIPOS DE **POLÍTICAS DE CORTE DE INTRUSIONES**:

- **POLÍTICAS DE RESPUESTA PASIVA**
- **POLÍTICAS DE RESPUESTA ACTIVA**

### **3. DEFINICIÓN DE POLÍTICAS DE CORTE DE INTENTOS DE INTRUSIÓN EN LOS IDS/IPS**

## **POLÍTICAS DE CORTE DE INTRUSIONES EN SISTEMAS IDS/IPS**

### **POLÍTICAS DE RESPUESTA PASIVA**

CUANDO SE DETECTA UNA INTRUSIÓN, EL SISTEMA SE LIMITA A REGISTRAR Y A EMITIR UNA ALARMA DEL ATAQUE DETECTADO.

NO SE REALIZA NINGUNA ACCIÓN PARA CAMBIAR EL CURSO DEL ATAQUE.

ALGUNOS EJEMPLOS SON LOS SIGUIENTES:

- **ENVÍO DE UN CORREO ELECTRÓNICO A UNO O VARIOS USUARIOS:** CUANDO SE DETECTA UNA INTRUSIÓN SE ENVÍA UN CORREO ELECTRÓNICO A UNO O VARIOS USUARIOS INFORMANDO DE ESTA INTRUSIÓN.
- **REGISTRO DEL ATAQUE:** SE ALMACENAN LOS DETALLES DE LA ALERTA (FECHA DEL ATAQUE, HORA, IP DEL INTRUSO, IP DEL DESTINO, PROTOCOLO UTILIZADO, ETC.) EN UNA BASE DE DATOS.

### **3. DEFINICIÓN DE POLÍTICAS DE CORTE DE INTENTOS DE INTRUSIÓN EN LOS IDS/IPS**

## **POLÍTICAS DE CORTE DE INTRUSIONES EN SISTEMAS IDS/IPS**

## **POLÍTICAS DE RESPUESTA PASIVA**

- **ALMACENAMIENTO DE PAQUETES SOSPECHOSOS:** SE ALMACENAN TODOS LOS PAQUETES DE DATOS QUE ORIGINARON LA ALERTA.
- **APERTURA DE UNA APLICACIÓN:** CUANDO HAY ALGÚN INTENTO DE INTRUSIÓN SE ABRE UNA APLICACIÓN QUE REALIZA UNA ACCIÓN ESPECÍFICA COMO EL ENVÍO DE MENSAJES DE TEXTO O LA EMISIÓN DE ALGÚN SONIDO, ENTRE OTRAS.
- **NOTIFICACIÓN VISUAL:** CUANDO SE PRODUCE UN INTENTO DE INTRUSIÓN SE EMITE UNA NOTIFICACIÓN VISUAL EN LAS CONSOLAS DE ADMINISTRACIÓN.
- **ENVÍO DE UNA TRAMPA SNMP A UN HIPERVISOR EXTERNO:** SE EMITE UN MENSAJE DE ALERTA (TRAMPA) EN PROTOCOLO SNMP A UNA CONSOLA EXTERNA.



### **3. DEFINICIÓN DE POLÍTICAS DE CORTE DE INTENTOS DE INTRUSIÓN EN LOS IDS/IPS**

## **POLÍTICAS DE CORTE DE INTRUSIONES EN SISTEMAS IDS/IPS**

### **POLÍTICAS DE RESPUESTA ACTIVA**

EL SISTEMA CUANDO DETECTA UNA INTRUSIÓN, ADEMÁS DE GENERAR UNA ALARMA Y REMITIRLA AL RESPONSABLE, MODIFICA EL ENTORNO PARA EVITAR QUE LA INTRUSIÓN TENGA ÉXITO.

ALGUNOS EJEMPLOS SE DESCRIBEN A CONTINUACIÓN:

- **ENVÍO DE UN RESETKILL:** EN EL MOMENTO DE LA DETECCIÓN DE LA INTRUSIÓN SE ENVÍA UN PAQUETE DE ALERTA QUE FUERZA LA FINALIZACIÓN DE LA CONEXIÓN EVITANDO QUE EL ATACANTE CONSIGA ENTRAR EN EL EQUIPO.
- **RECONFIGURACIÓN DE DISPOSITIVOS EXTERNOS:** AL DETECTARSE EL ATAQUE SE ENVÍA UN COMANDO PARA QUE EL DISPOSITIVO EXTERNO SE RECONFIGURE DE INMEDIATO Y PUEDA BLOQUEAR EL INTENTO DE ATAQUE.

### 3. DEFINICIÓN DE POLÍTICAS DE CORTE DE INTENTOS DE INTRUSIÓN EN LOS IDS/IPS

## POLÍTICAS DE CORTE DE INTRUSIONES EN SISTEMAS IDS/IPS

Políticas de corte de intrusiones	
<b>Políticas de respuesta pasiva:</b> se limitan a registrar los datos del intento de intrusión.	<b>Políticas de respuesta activa:</b> registran los datos del intento de intrusión e intentan evitarlo.
Envío de correo electrónico.	Envío de un <i>ResetKill</i> .
Envío de trampas SNMP a consolas externas.	Reconfiguración de los dispositivos externos.
Registro del ataque.	
Almacenamiento de los paquetes de datos sospechosos.	
Apertura de una aplicación.	
Notificación visual de una alerta.	

# CONTENIDOS

1. INTRODUCCIÓN
2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO
3. DEFINICIÓN DE POLÍTICAS DE CORTE DE INTENTOS DE INTRUSIÓN EN LOS IDS/IPS
4. **ANÁLISIS DE LOS EVENTOS REGISTRADOS POR EL IDS/IPS PARA DETERMINAR FALSOS POSITIVOS Y CARACTERIZARLOS EN LAS POLÍTICAS DE CORTE DEL IDS/IPS**
5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN
6. ESTABLECIMIENTO DE LOS NIVELES REQUERIDOS DE ACTUALIZACIÓN, MONITORIZACIÓN Y PRUEBAS DEL IDS/ IPS

#### **4. ANÁLISIS DE LOS EVENTOS REGISTRADOS POR EL IDS/IPS PARA DETERMINAR FALSOS POSITIVOS Y CARACTERIZARLOS EN LAS POLÍTICAS DE CORTE DEL IDS/IPS**

EL ANÁLISIS DE LOS DISTINTOS EVENTOS REGISTRADOS EN EL SISTEMA POR LOS IDS/IPS NO ES IMPECABLE.

PUEDE QUE LA BASE DE DATOS DE FIRMAS ESTÉ DESACTUALIZADA Y QUE LOS MÉTODOS ESTADÍSTICOS DE DETECCIÓN DE COMPORTAMIENTOS INDEBIDOS NO SEAN PERFECTOS.

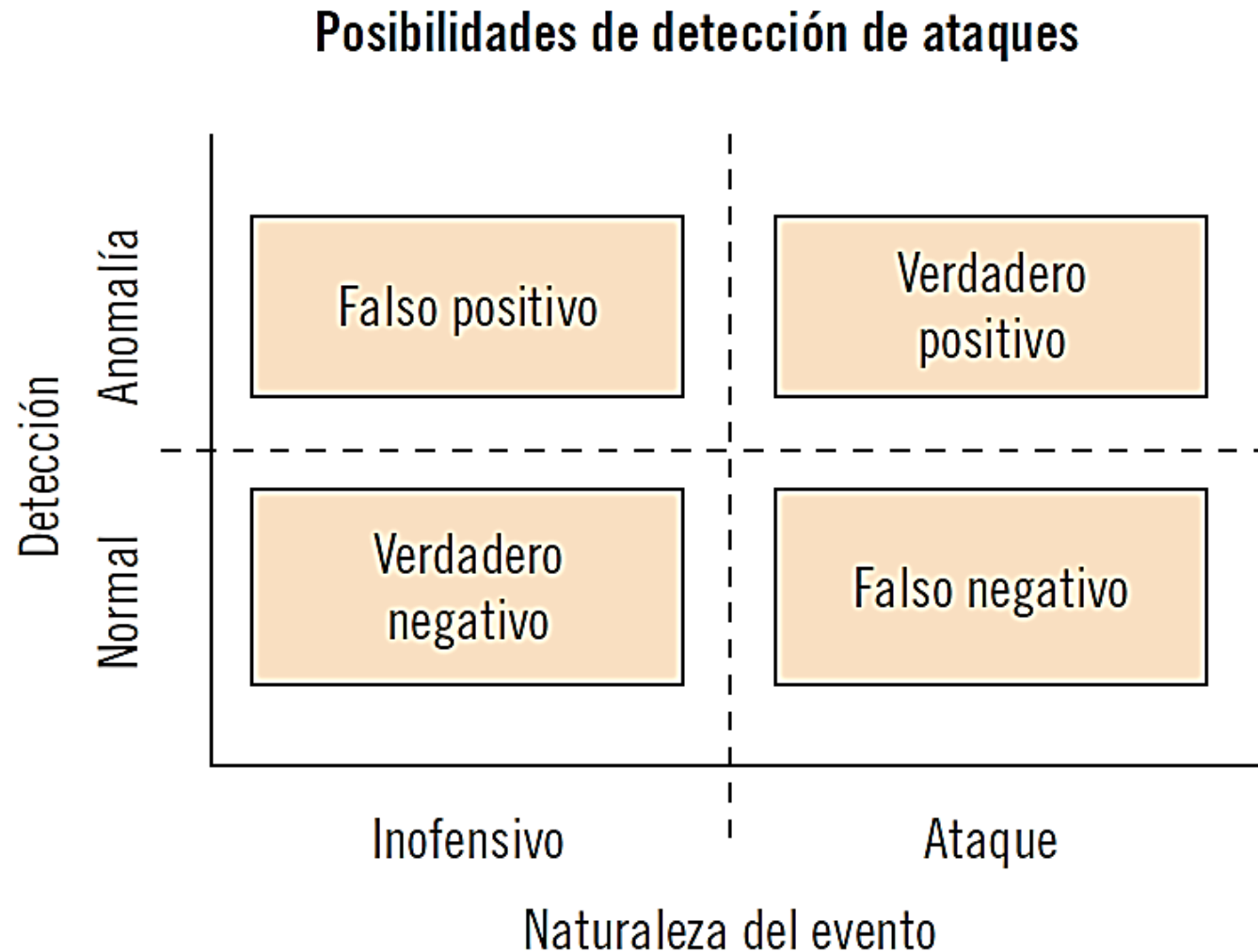
POR ELLO, CUANDO **LOS SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES** TOMAN DECISIONES SOBRE SI UN EVENTO DEBE CONSIDERARSE O NO UN ATAQUE, **PUEDEN EQUIVOCARSE.**

#### **4. ANÁLISIS DE LOS EVENTOS REGISTRADOS POR EL IDS/IPS PARA DETERMINAR FALSOS POSITIVOS Y CARACTERIZARLOS EN LAS POLÍTICAS DE CORTE DEL IDS/IPS**

EN EL MOMENTO DE LA TOMA DE DECISIÓN DE SI UN EVENTO ES EFECTIVAMENTE UN ATAQUE O NO PUEDE HABER **CUATRO POSIBILIDADES:**

- **FALSO POSITIVO O FALSA ALARMA:** CUANDO EL IDS/IPS DETECTA COMO ATAQUE EL TRÁFICO DE DATOS QUE EN VERDAD ES INOFENSIVO.
- **FALSO NEGATIVO:** ATAQUE QUE NO ES DETECTADO POR EL IDS/IPS.
- **VERDADERO NEGATIVO:** EVENTO INOFENSIVO QUE EL IDS/IPS HA DETECTADO COMO TRÁFICO DE RED NORMAL.
- **ATAQUE DETECTADO CORRECTAMENTE** POR EL IDS/IPS.

#### 4. ANÁLISIS DE LOS EVENTOS REGISTRADOS POR EL IDS/IPS PARA DETERMINAR FALSOS POSITIVOS Y CARACTERIZARLOS EN LAS POLÍTICAS DE CORTE DEL IDS/IPS





#### **4. ANÁLISIS DE LOS EVENTOS REGISTRADOS POR EL IDS/IPS PARA DETERMINAR FALSOS POSITIVOS Y CARACTERIZARLOS EN LAS POLÍTICAS DE CORTE DEL IDS/IPS**

ANTE ESTAS POSIBILIDADES EL OBJETIVO QUE DEBE ESTABLECERSE EN UN IDS/IPS ES **MINIMIZAR EL NÚMERO DE ERRORES EN LA DETECCIÓN Y MAXIMIZAR EL NÚMERO DE ACIERTOS** POR VARIOS MOTIVOS:

- UN ELEVADO NIVEL DE FALSOS POSITIVOS Y NEGATIVOS PUEDE DIFUMINAR LOS MOTIVOS POR LOS QUE SE IMPLANTÓ EL IDS/IPS, OBTENIENDO BAJOS NIVELES DE EFECTIVIDAD DEL SISTEMA.
- LOS FALSOS POSITIVOS OCUPAN TIEMPO Y RECURSOS CUANDO EL IDS/IPS GENERA ALARMAS CUANDO NO DEBE.
- LA NO DETECCIÓN DE ATAQUES (FALSOS NEGATIVOS) PUEDE TENER GRAVES CONSECUENCIAS EN LA INFORMACIÓN DE LA ORGANIZACIÓN.

#### **4. ANÁLISIS DE LOS EVENTOS REGISTRADOS POR EL IDS/IPS PARA DETERMINAR FALSOS POSITIVOS Y CARACTERIZARLOS EN LAS POLÍTICAS DE CORTE DEL IDS/IPS**

ASÍ, VIENDO LOS EFECTOS QUE TIENE LA CONFIGURACIÓN ESTABLECIDA EN EL SISTEMA IDS/IPS Y **VIENDO LOS FALSOS POSITIVOS Y LOS FALSOS NEGATIVOS** QUE SE GENERAN, **SE PUEDEN REALIZAR MODIFICACIONES EN LA CONFIGURACIÓN** PARA CONSEGUIR LA MÁS ADECUADA Y QUE TRABAJE CON UN MAYOR RENDIMIENTO.

HAY QUE REALIZAR VARIAS PRUEBAS DE REFERENCIA SOBRE DISTINTAS CONFIGURACIONES PARA QUE SE PUEDAN HACER COMPARACIONES DE LOS RESULTADOS.

CON EL ANÁLISIS DE LAS DIFERENCIAS DE LOS RESULTADOS OBTENIDOS CON LAS DIVERSAS CONFIGURACIONES SE PUEDE DETECTAR Y ELIMINAR LA CAUSA QUE PROVOCA LOS FALSOS POSITIVOS Y NEGATIVOS.

## 4. ANÁLISIS DE LOS EVENTOS REGISTRADOS POR EL IDS/IPS PARA DETERMINAR FALSOS POSITIVOS Y CARACTERIZARLOS EN LAS POLÍTICAS DE CORTE DEL IDS/IPS

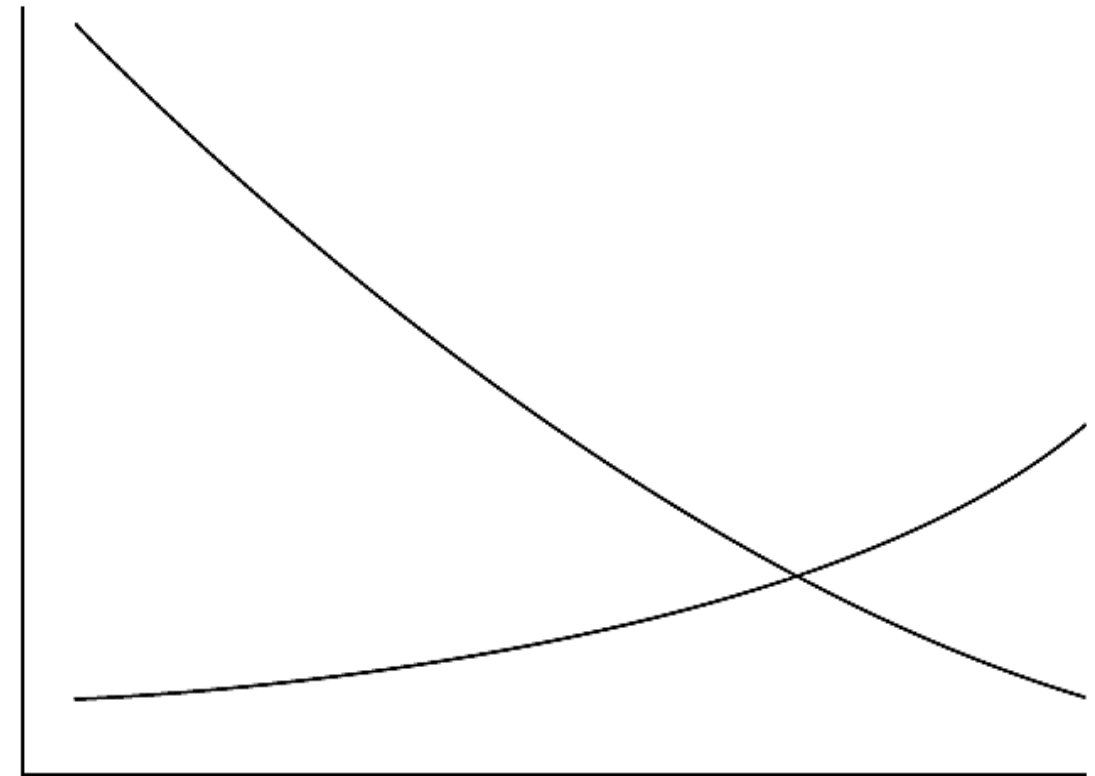
EL OBJETIVO A PERSEGUIR CON LA CONFIGURACIÓN DEL IDS/IPS ES CONSEGUIR UN EQUILIBRIO ENTRE LOS FALSOS POSITIVOS Y LOS FALSOS NEGATIVOS, CONSIGUIENDO LOCALIZARSE EN EL CRUCE DE LAS TASAS DE FALSOS POSITIVOS Y NEGATIVOS MOSTRADO EN EL GRÁFICO SIGUIENTE:

EL GRÁFICO DE LA IMAGEN ES UN MODELO DE LA TASA DE ERROR EN UN IDS/IPS, REPRESENTANDO LO QUE OCURRE CUANDO SE REDUCE LA SENSIBILIDAD DEL SISTEMA PARA EMITIR ALERTAS Y CUANDO SE INCREMENTA LA CANTIDAD DE PAQUETES INSPECCIONADOS:

- A MAYOR SENSIBILIDAD DEL SISTEMA, MAYOR POSIBILIDAD DE DETECCIÓN DE FALSOS POSITIVOS Y MENOR APARICIÓN DE FALSOS NEGATIVOS.
- A MENOR SENSIBILIDAD, MENOR DETECCIÓN DE FALSOS POSITIVOS Y MAYOR APARICIÓN DE FALSOS NEGATIVOS.
- A MAYOR CANTIDAD DE PAQUETES INSPECCIONADOS, MAYOR POSIBILIDAD DE DETECTAR FALSOS POSITIVOS Y MENOR APARICIÓN DE FALSOS NEGATIVOS.
- A MENOR CANTIDAD DE PAQUETES INSPECCIONADOS, MENOR POSIBILIDAD DE DETECCIÓN DE FALSOS POSITIVOS Y MAYOR APARICIÓN DE FALSOS NEGATIVOS.

EN CONCLUSIÓN, EN EL MOMENTO DE DECIDIR LA CONFIGURACIÓN DE UN IDS/IPS HAY QUE ENCONTRAR A TRAVÉS DE VARIAS PRUEBAS EL EQUILIBRIO ENTRE LA SENSIBILIDAD DEL SISTEMA Y LA CANTIDAD DE DATOS A INSPECCIONAR, ATENDIENDO A LAS NECESIDADES DE CADA ORGANIZACIÓN E INTENTANDO CONSEGUIR EL MAYOR RENDIMIENTO POSIBLE.

Falsos positivos



Falsos negativos

#### **4. ANÁLISIS DE LOS EVENTOS REGISTRADOS POR EL IDS/IPS PARA DETERMINAR FALSOS POSITIVOS Y CARACTERIZARLOS EN LAS POLÍTICAS DE CORTE DEL IDS/IPS**

COMO RECOMENDACIÓN, EN EL MOMENTO DE REALIZAR LAS PRUEBAS DE CONFIGURACIÓN HAY QUE TENER EN CUENTA ALGUNAS DE LAS **CAUSAS MÁS FRECUENTES DE FALSOS POSITIVOS**:

1. **ACTIVIDAD DEL SISTEMA DE SUPERVISIÓN DE RED:** EN OCASIONES, LAS EMPRESAS UTILIZAN SISTEMAS DE SUPERVISIÓN DE REDES PARA OBTENER REGISTROS DE LA ACTIVIDAD QUE HAY EN SUS SISTEMAS. MUCHOS SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS SUELEN CLASIFICAR ESTA ACTIVIDAD COMO HOSTIL O SOSPECHOSA CUANDO EN VERDAD ES INOFENSIVA. COMO SOLUCIÓN *SE RECOMIENDA CONFIGURAR EL IDS/IPS ELIMINANDO LAS ALERTAS DE ESTE TIPO DE LA BASE DE DATOS.*
2. **ESCANEEO DE VULNERABILIDAD Y ESCÁNERES DE PUERTOS DE RED:** CUANDO SE PRETENDE REALIZAR UNA PRUEBA DE VULNERABILIDAD DE LA RED O UN ESCÁNER DE SUS PUERTOS EL IDS/IPS LO SUELE DETECTAR COMO ATAQUE, YA QUE SU FUNCIONAMIENTO ES MUY SIMILAR AL UTILIZADO POR LOS PIRATAS INFORMÁTICOS EN SUS ATAQUES. *SE RECOMIENDA DESACTIVAR EL IDS/IPS MOMENTÁNEAMENTE CUANDO SE REALIZA ESTE TIPO DE ACTIVIDADES.*

#### **4. ANÁLISIS DE LOS EVENTOS REGISTRADOS POR EL IDS/IPS PARA DETERMINAR FALSOS POSITIVOS Y CARACTERIZARLOS EN LAS POLÍTICAS DE CORTE DEL IDS/IPS**

3. **ACTIVIDAD DEL USUARIO:** EN MUCHOS IDS/IPS VIENE CONFIGURADO POR DEFECTO LA EMISIÓN DE ALARMAS ANTE COMPORTAMIENTOS DEL USUARIO QUE CONSIDERA COMO “PELIGROSAS”: COMPARTIR ARCHIVOS PUNTO A PUNTO O UTILIZACIÓN DE MENSAJERÍA INSTANTÁNEA, ENTRE OTRAS. PARA EVITAR QUE SE GENEREN ESTAS ALERTAS *ES RECOMENDABLE CONFIGURAR ESPECÍFICAMENTE LAS ALARMAS* ELIMINANDO ESTAS CASUÍSTICAS.
4. **COMPORTAMIENTOS SIMILARES A TROYANOS O GUSANOS:** EN OCASIONES, LA MISMA ORGANIZACIÓN REALIZA ACCIONES QUE SON SIMILARES A LAS QUE EJECUTAN LOS GUSANOS O LOS TROYANOS Y EMITE ALARMAS CUANDO REALMENTE SON ACCIONES INOFENSIVAS. EN ESTE CASO *NO SE RECOMIENDA DESACTIVAR LAS ALARMAS*, YA QUE DEJARÍA AL EQUIPO DESPROVISTO DE MECANISMOS DE DETECCIÓN DE ATAQUES REALES DE TROYANOS Y GUSANOS.

#### **4. ANÁLISIS DE LOS EVENTOS REGISTRADOS POR EL IDS/IPS PARA DETERMINAR FALSOS POSITIVOS Y CARACTERIZARLOS EN LAS POLÍTICAS DE CORTE DEL IDS/IPS**

5. **CADENAS LARGAS DE REGISTRO WEB:** HAY ALERTAS QUE SE GENERAN POR LA DETECCIÓN DE CADENAS DE REGISTRO WEB LARGAS, YA QUE ALGUNOS ATAQUES LAS UTILIZAN PARA DESBORDAR LA MEMORIA DEL EQUIPO Y ASÍ PODER ACCEDER A SU SISTEMA. AUNQUE EN LA ACTUALIDAD HAY MUCHAS WEBS QUE UTILIZAN CADENAS LARGAS DE UN MODO HABITUAL *NO SE RECOMIENDA DESACTIVAR LAS ALERTAS DE SU DETECCIÓN, YA QUE PERMITIRÍA EL ACCESO DE ATAQUES POTENCIALMENTE DAÑINOS.*
6. **ACTIVIDAD DE AUTENTICACIÓN DE BASE DE DATOS:** LOS SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES SUELEN ANALIZAR LA ACTIVIDAD ADMINISTRATIVA DE LAS BASES DE DATOS PORQUE CONSIDERAN QUE UNA ELEVADA ACTIVIDAD PUEDE SER UN INDICIO DE ESTAR SUFRIENDO ALGÚN ATAQUE. SI LA ORGANIZACIÓN UTILIZA BASES DE DATOS EN CONTINUA ACTUALIZACIÓN Y CON UN ELEVADO NIVEL DE ACTIVIDAD ADMINISTRATIVA, *SE RECOMIENDA DESACTIVAR ESTAS ALERTAS PARA REDUCIR EL NÚMERO DE FALSOS NEGATIVOS.*



#### **4. ANÁLISIS DE LOS EVENTOS REGISTRADOS POR EL IDS/IPS PARA DETERMINAR FALSOS POSITIVOS Y CARACTERIZARLOS EN LAS POLÍTICAS DE CORTE DEL IDS/IPS**

**HAY DOS METODOLOGÍAS DE LIBRE CONFIGURACIÓN QUE SE UTILIZAN PARA EVALUAR Y REALIZAR TEST DE LOS DISTINTOS ELEMENTOS DE SEGURIDAD DE UNA ORGANIZACIÓN, ENTRE ELLOS LOS SISTEMAS IDS/IPS:**

- **METODOLOGÍA OSSTM (OPEN SOURCE SECURITY TESTING METHODOLOGY):** LA METODOLOGÍA DE TESTEO DE SEGURIDAD DE CÓDIGO ABIERTO HA SIDO ELABORADA POR EL INSTITUTO PARA LA SEGURIDAD Y CÓDIGO ABIERTO (**ISECOM**) Y OFRECE UNA *METODOLOGÍA DE EVALUACIÓN DE SISTEMAS DE SEGURIDAD, SOBRE TODO DE CORTAFUEGOS E IDS/IPS.*
- **METODOLOGÍA OSEC (OPEN SECURITY EVALUATION CRITERIA):** EL CRITERIO DE EVALUACIÓN DE CÓDIGO ABIERTO ES SIMILAR AL **OSSTM** PERO ESTÁ CONCENTRADO *FUNDAMENTALMENTE EN ESTANDARIZAR PRODUCTOS DE SEGURIDAD RELATIVOS A LOS NIDS Y A LOS CORTAFUEGOS.*

# CONTENIDOS

1. INTRODUCCIÓN
2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO
3. DEFINICIÓN DE POLÍTICAS DE CORTE DE INTENTOS DE INTRUSIÓN EN LOS IDS/IPS
4. ANÁLISIS DE LOS EVENTOS REGISTRADOS POR EL IDS/IPS PARA DETERMINAR FALSOS POSITIVOS Y CARACTERIZARLOS EN LAS POLÍTICAS DE CORTE DEL IDS/IPS
5. **RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN**
6. ESTABLECIMIENTO DE LOS NIVELES REQUERIDOS DE ACTUALIZACIÓN, MONITORIZACIÓN Y PRUEBAS DEL IDS/ IPS

## **5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN**

**LOS REGISTROS DE AUDITORÍA DEL IDS/IPS SON AQUELLOS EN LOS QUE SE REGISTRAN LAS ACCIONES REALIZADAS POR LOS USUARIOS EN UN SISTEMA.**

ESTOS REGISTROS SON VITALES, YA QUE CUANDO SE PRODUCE UN INCIDENTE DE SEGURIDAD FACILITAN INFORMACIÓN SOBRE EL USUARIO QUE HAYA PODIDO COMETER LA INFRACCIÓN.

EL REGISTRO DE AUDITORÍA NO SOLO CONTIENE INFORMACIÓN DE LOS USUARIOS, SINO QUE TAMBIÉN **CONTIENE INFORMACIÓN IMPORTANTE SOBRE LAS INFRACCIONES DE SEGURIDAD SUCEDIDAS EN EL SISTEMA.**

## **5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN**

**LOS ADMINISTRADORES DE SEGURIDAD DEBEN REALIZAR ANÁLISIS PERIÓDICOS DE LOS REGISTROS DE AUDITORÍA.**

DE ESTE MODO SE PUEDEN IR AJUSTANDO LOS NIVELES DE SEGURIDAD E IR DETECTANDO LOS DEFECTOS DE SEGURIDAD QUE SUCEDEN EN EL EQUIPO.

**HAY QUE REMARCAR QUE NO TODOS LOS REGISTROS DE AUDITORÍA PONEN DE MANIFIESTO FALLOS DE SEGURIDAD.**

**LA GRAN MAYORÍA DE ESTOS SON MERAMENTE INFORMATIVOS.**

EN EL MOMENTO DE ESTABLECER LA POLÍTICA DE AUDITORÍA HAY QUE REALIZAR UN ANÁLISIS PREVIO PARA QUE LA POLÍTICA IMPLANTADA SEA LA ADECUADA.

## **5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN**

**SI SE AUDITAN DEMASIADOS TIPOS DE EVENTOS PUEDE SOBRECARGARSE EL SISTEMA Y REDUCIR SU RENDIMIENTO.**

**PARA LA DEFINICIÓN DE LA POLÍTICA DE AUDITORÍA SE PLANTEAN UNA SERIE DE RECOMENDACIONES:**

- DETERMINAR LOS EQUIPOS Y DISPOSITIVOS EN LOS QUE SE VA A CONFIGURAR LA AUDITORÍA.
- DETERMINAR LOS EVENTOS QUE SE QUIEREN AUDITAR (POR EJEMPLO, LOS ACCESOS A ARCHIVOS Y CARPETAS, EL INICIO DE SESIÓN DE LOS USUARIOS, EL ENCENDIDO DEL SERVIDOR, ETC.).
- DETERMINAR SI SE QUIERE AUDITAR EL ÉXITO DEL EVENTO, EL FALLO DEL EVENTO O AMBOS CASOS.
- DETERMINAR LA NECESIDAD REAL DE AUDITAR LAS TENDENCIAS DE USO DEL SISTEMA.
- DETERMINAR LA PERIODICIDAD DE LAS REVISIONES DE LOS REGISTROS DE SEGURIDAD.

## 5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN

UN REGISTRO DE AUDITORÍA PUEDE CLASIFICARSE EN UNA DE LAS CATEGORÍAS MOSTRADAS EN LA TABLA SIGUIENTE:

Categoría del registro	Descripción
Error	Para eventos de seguridad importantes.
Advertencia	Para eventos que no son importantes pero que pueden causar algún problema en un futuro.
Información	Para operaciones realizadas con éxito.
Auditoría correcta	En eventos ocurridos cuando la auditoría se ha realizado correctamente.
Auditoría incorrecta	En eventos ocurridos cuando ha habido algún fallo de auditoría.



## **5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN**

SEA DE LA CATEGORÍA QUE SEA, UN EVENTO EN EL REGISTRO DE AUDITORÍA CONTIENE INFORMACIÓN SOBRE:

- LA ACCIÓN REALIZADA.
- EL USUARIO QUE HA REALIZADO LA ACCIÓN.
- EL ÉXITO O FRACASO DEL EVENTO.
- CUANDO SE HA PRODUCIDO EL EVENTO.
- INFORMACIÓN ADICIONAL COMO, POR EJEMPLO, EL SISTEMA DESDE EL QUE SE REALIZA LA ACCIÓN.

## 5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN

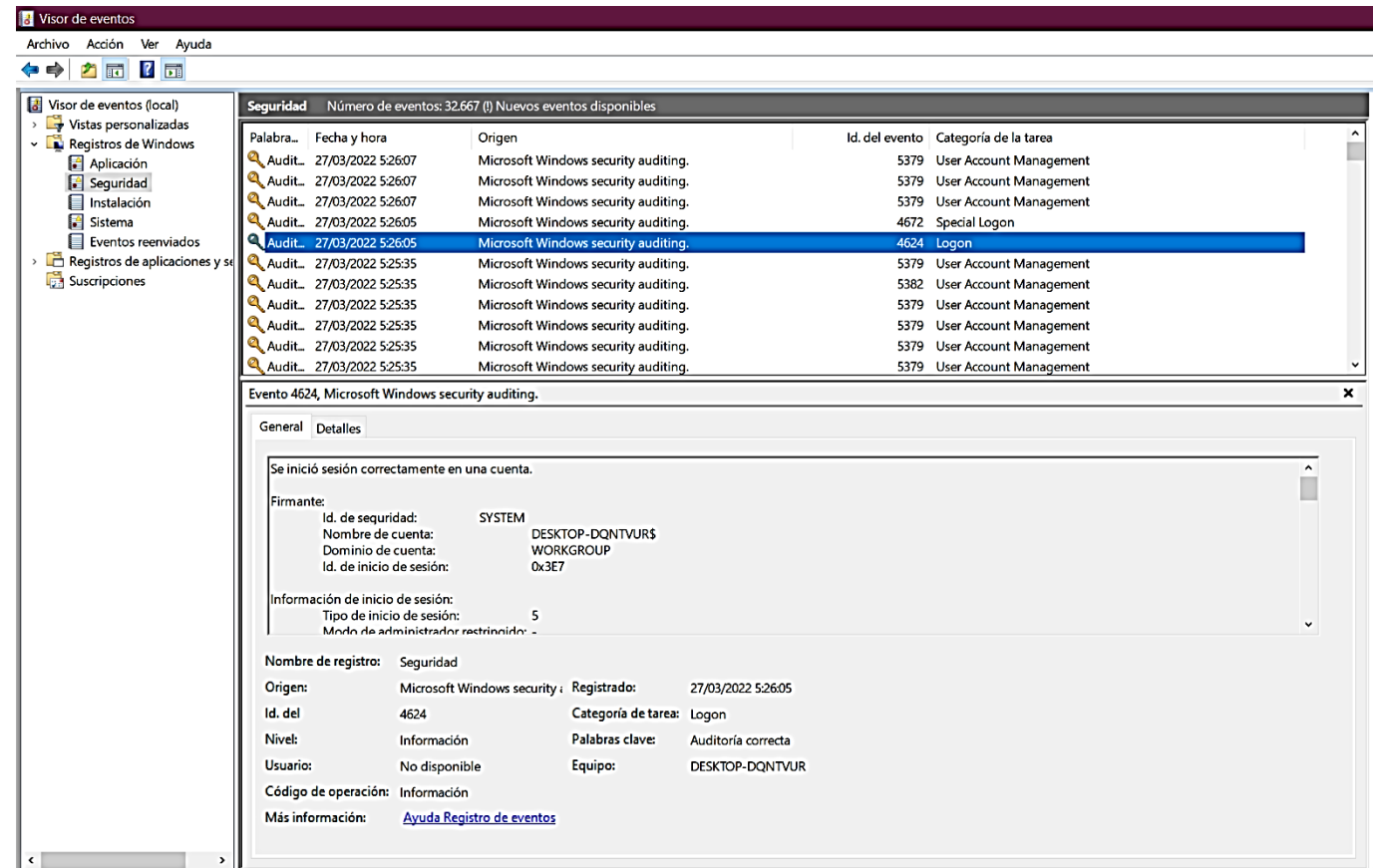
EL ACCESO A LOS REGISTROS DEL SISTEMA EN **LINUX** SE HACE A TRAVÉS DE VARIOS COMANDOS DEPENDIENDO DEL TIPO DE INFORMACIÓN DEL EVENTO QUE SE PRETENDE OBTENER.

PARA VER LOS REGISTROS DE SEGURIDAD DEL SISTEMA HAY QUE ACCEDER AL ARCHIVO DE REGISTRO DE SEGURIDAD CON EL COMANDO **tail -f** (SI SOLO SE QUIEREN VER LAS ÚLTIMAS LÍNEAS DEL REGISTRO) O CON EL COMANDO **less +F** (SI SE QUIERE VER EL ARCHIVO DE REGISTRO COMPLETO).

EN **WINDOWS** ESTA INFORMACIÓN SE OBTIENE A TRAVÉS DEL “**VISOR DE EVENTOS**” ACCEDIENDO A INICIO -> PANEL DE CONTROL -> HERRAMIENTAS ADMINISTRATIVAS -> VISOR DE EVENTOS.

## 5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN

EN LA PESTAÑA SEGURIDAD DENTRO DE VISOR DE EVENTOS DE WINDOWS SE PUEDEN VER ESPECÍFICAMENTE LOS REGISTROS DE SEGURIDAD CON TODA LA INFORMACIÓN DETALLADA.



**Visor de eventos**

Archivo Acción Ver Ayuda

Visor de eventos (local)

- Vistas personalizadas
- Registros de Windows
  - Aplicación
  - Seguridad
  - Instalación
  - Sistema
  - Eventos reenviados
- Registros de aplicaciones y servicios
- Suscripciones

Palabra clave	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Audit...	27/03/2022 5:26:07	Microsoft Windows security auditing.	5379	User Account Management
Audit...	27/03/2022 5:26:07	Microsoft Windows security auditing.	5379	User Account Management
Audit...	27/03/2022 5:26:07	Microsoft Windows security auditing.	5379	User Account Management
Audit...	27/03/2022 5:26:05	Microsoft Windows security auditing.	4672	Special Logon
Audit...	27/03/2022 5:26:05	Microsoft Windows security auditing.	4624	Logon
Audit...	27/03/2022 5:25:35	Microsoft Windows security auditing.	5379	User Account Management
Audit...	27/03/2022 5:25:35	Microsoft Windows security auditing.	5382	User Account Management
Audit...	27/03/2022 5:25:35	Microsoft Windows security auditing.	5379	User Account Management
Audit...	27/03/2022 5:25:35	Microsoft Windows security auditing.	5379	User Account Management
Audit...	27/03/2022 5:25:35	Microsoft Windows security auditing.	5379	User Account Management
Audit...	27/03/2022 5:25:35	Microsoft Windows security auditing.	5379	User Account Management

**Evento 4624, Microsoft Windows security auditing.**

General Detalles

Se inició sesión correctamente en una cuenta.

Firmante:

Id. de seguridad: SYSTEM

Nombre de cuenta: DESKTOP-DQNTVUR\$

Dominio de cuenta: WORKGROUP

Id. de inicio de sesión: 0x3E7

Información de inicio de sesión:

Tipo de inicio de sesión: 5

Método de administración restringido: ...

Nombre de registro: Seguridad

Origen: Microsoft Windows security auditing Registrado: 27/03/2022 5:26:05

Id. del: 4624 Categoría de tarea: Logon

Nivel: Información Palabras clave: Auditoría correcta

Usuario: No disponible Equipo: DESKTOP-DQNTVUR

Código de operación: Información

Más información: [Ayuda Registro de eventos](#)

## **5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN**

### **RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/IPS NECESARIOS PARA UN CORRECTO CONTROL DE INTRUSIONES**

UNA VEZ VISTO EL MODO EN EL QUE ESTÁN MONITORIZADOS LOS EVENTOS DE AUDITORÍA ES IMPRESCINDIBLE **CONOCER CUÁLES SON LOS EVENTOS FUNDAMENTALES QUE LAS ORGANIZACIONES DEBEN AUDITAR PARA QUE LA DETECCIÓN Y PREVENCIÓN DE INTRUSIONES EN UN IDS/IPS SEA LO MÁS EFICIENTE POSIBLE.**

A CONTINUACIÓN, SE DESCRIBEN LOS **ELEMENTOS IMPRESCINDIBLES QUE DEBEN SER SOMETIDOS A AUDITORÍA.**

## **5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN**

### **RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/IPS NECESARIOS PARA UN CORRECTO CONTROL DE INTRUSIONES SUCEOS DE INICIO DE SESIÓN DE CUENTA**

ES NECESARIO CONFIGURAR LOS IDS/IPS PARA QUE AUDITEN LOS INTENTOS DE INICIO DE SESIÓN DE CUENTA, TANTO EXITOSOS COMO NO EXITOSOS.

ESO SÍ, EN EL MOMENTO DE SU CONFIGURACIÓN HAY QUE DECIDIR EN LA POLÍTICA DE CORTE DE ATAQUES SI SE QUIEREN AUDITAR SOLO LOS INTENTOS EXITOSOS, LOS INTENTOS FRACASADOS, AMBOS O SI DIRECTAMENTE SE DECIDE OMITIR ESTA AUDITORÍA.

## **5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN**

### **RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/IPS NECESARIOS PARA UN CORRECTO CONTROL DE INTRUSIONES SUCEOS DE INICIO DE SESIÓN DE CUENTA**

*LAS AUDITORÍAS DE INICIOS DE SESIÓN CON ÉXITO SIRVEN PARA COMPROBAR QUÉ HA REALIZADO CADA USUARIO Y DESCUBRIR QUIÉN ES EL RESPONSABLE DE CUALQUIER INCIDENTE DE SEGURIDAD: QUIÉN ACCEDIÓ, CÓMO CONSIGUIÓ ACCEDER Y EN QUÉ EQUIPO ACCEDIÓ.*

*LAS AUDITORÍAS DE INICIOS DE SESIÓN SIN ÉXITO RESULTAN MUY ÚTILES PARA DETECTAR INTENTOS DE INTRUSIONES Y PREVENIR FUTUROS INTENTOS.*



## **5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN**

### **RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/IPS NECESARIOS PARA UN CORRECTO CONTROL DE INTRUSIONES ADMINISTRACIÓN DE CUENTAS**

EN ESTOS REGISTROS DE AUDITORÍA SE REFLEJAN LOS DISTINTOS SUCESOS DE ADMINISTRACIÓN DE CUENTAS DE UN EQUIPO COMO, POR EJEMPLO:

- CUANDO SE CREA, MODIFICA O SE ELIMINA ALGUNA CUENTA DE USUARIO.
- CUANDO SE MODIFICA ALGUNA CONTRASEÑA.
- CUANDO SE ACTIVA O DESACTIVA ALGUNA CUENTA DE USUARIO.
- CUANDO SE MODIFICA EL NOMBRE DE ALGUNA CUENTA DE USUARIO.

## **5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN**

### **RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/IPS NECESARIOS PARA UN CORRECTO CONTROL DE INTRUSIONES ADMINISTRACIÓN DE CUENTAS**

SE PUEDE DECIDIR QUE EL IDS/IPS ELABORE REGISTROS SOBRE LOS INTENTOS EXITOSOS, NO EXITOSOS O AMBOS.

LAS AUDITORÍAS DE SUCESOS EXITOSOS DE ADMINISTRACIÓN DE CUENTAS SON MUY ÚTILES PARA *COMPROBAR TODOS LOS CAMBIOS PRODUCIDOS EN LAS CUENTAS DE USUARIO DEL SISTEMA Y DEBERÍAN ESTAR SIEMPRE HABILITADOS* PARA LLEVAR UN SEGUIMIENTO DE LA EVOLUCIÓN DE LAS CUENTAS Y DE LOS USUARIOS RESPONSABLES.

## **5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN**

### **RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/IPS NECESARIOS PARA UN CORRECTO CONTROL DE INTRUSIONES SUCEOS DE INICIO DE SESIÓN**

LA DECISIÓN DE REGISTRAR *LOS EVENTOS DE INICIO DE SESIÓN EXITOSOS* PUEDE SER DE GRAN UTILIDAD, YA QUE SE OBTIENE INFORMACIÓN SOBRE EL USUARIO QUE CONSIGUE REGISTRARSE EN CADA EQUIPO EN EL MOMENTO DE INVESTIGAR ALGÚN INCIDENTE DE SEGURIDAD.

*LOS REGISTROS DE INICIOS DE SESIÓN SIN ÉXITO TAMBIÉN SON ÚTILES (AL IGUAL QUE EN LOS SUCEOS DE INICIO DE SESIÓN DE CUENTA) PARA DETECTAR INTENTOS DE ACCESO DE INTRUSOS.*

## **5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN**

### **RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/IPS NECESARIOS PARA UN CORRECTO CONTROL DE INTRUSIONES ACCESO A OBJETOS**

CONTIENEN INFORMACIÓN SOBRE LOS ACCESOS DE UN USUARIO A CUALQUIER TIPO DE OBJETO DEL SISTEMA (COMO CARPETAS, ARCHIVOS, DISPOSITIVOS, ETC.) QUE ESTÉ INCLUIDO EN UNA LISTA DE CONTROL PREDEFINIDA POR EL ADMINISTRADOR.

LA ORGANIZACIÓN TAMBIÉN PUEDE DECIDIR SI REGISTRAR LOS ACCESOS CON ÉXITO, LOS INTENTOS FRACASADOS, AMBOS O, DIRECTAMENTE, NO AUDITAR ESTE TIPO DE SUCESOS.

## **5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN**

### **RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/IPS NECESARIOS PARA UN CORRECTO CONTROL DE INTRUSIONES USO DE PRIVILEGIOS**

CONTIENEN INFORMACIÓN DE CADA EVENTO SUCEDIDO CUANDO UN USUARIO REALIZA ALGUNA ACCIÓN BAJO UNOS PRIVILEGIOS QUE LE HAN SIDO OTORGADOS PREVIAMENTE. ALGUNOS EJEMPLOS PUEDEN SER:

- CUANDO UN ADMINISTRADOR REALIZA COPIAS DE SEGURIDAD DE ALGÚN ARCHIVO O DIRECTORIO.
- CUANDO UN USUARIO SIN PRIVILEGIOS INTENTA REALIZAR ALGUNA ACCIÓN PARA LA QUE NO TIENE PERMISO (SE GENERA UN REGISTRO DE ERROR).
- CUANDO EL USUARIO CON PRIVILEGIOS DE ADMINISTRADOR RESTAURA ALGÚN ARCHIVO O DIRECTORIO.

## **5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN**

### **RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/IPS NECESARIOS PARA UN CORRECTO CONTROL DE INTRUSIONES SEGUIMIENTO DE PROCESOS**

CONTIENEN INFORMACIÓN DETALLADA DE LOS SUCESOS OCURRIDOS EN EL SISTEMA COMO PUEDEN SER: LA ACTIVACIÓN DE ALGUNA APLICACIÓN, EL ACCESO O SALIDA A UN PROCESO, ETC.

*NO SE RECOMIENDA LA ACTIVACIÓN DE ESTE TIPO DE REGISTRO DE AUDITORÍA, YA QUE DEBIDO AL ELEVADO NÚMERO DE PROCESOS QUE ACONTECEN EN EL SISTEMA PUEDE SER DIFÍCIL LOCALIZAR LA INFORMACIÓN DE LOS SUCESOS MÁS VALIOSOS.*



## **5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN**

### **RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/IPS NECESARIOS PARA UN CORRECTO CONTROL DE INTRUSIONES SUCESOS DEL SISTEMA**

FACILITAN INFORMACIÓN SOBRE EL REINICIO O CIERRE DE UN EQUIPO POR PARTE DE UN USUARIO O GENERADO POR ALGÚN SUCESO QUE HAYA AFECTADO A LA SEGURIDAD DEL SISTEMA.

*ES DE GRAN UTILIDAD ACTIVAR LA GENERACIÓN DE ESTE TIPO DE REGISTROS, YA QUE LOS SUCESOS QUE ACONTECEN SON POCOS Y LA INFORMACIÓN QUE SE PUEDE OBTENER PUEDE SER DE GRAN VALOR.*

## 5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN

### RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/IPS NECESARIOS PARA UN CORRECTO CONTROL DE INTRUSIONES

Registro de auditoría	Breve descripción
Sucesos de inicio de sesión de cuenta	En eventos de inicio o cierre de sesión de cuenta a través de la red.
Administración de cuentas	En eventos de modificaciones de las cuentas de usuario.
Sucesos de inicio de sesión	En eventos de inicio o cierre de sesión en equipos locales.
Acceso a objetos	En eventos de acceso a objetos predefinidos en una lista de control.
Uso de privilegios	En eventos de acciones de un usuario bajo unos privilegios asignados.
Seguimiento de procesos	En eventos referentes a cualquier proceso ejecutado en el sistema.
Sucesos del sistema	En eventos de reinicio o cierre de sesión provocados por algún usuario o por algún fallo de seguridad.

# CONTENIDOS

1. INTRODUCCIÓN
2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO
3. DEFINICIÓN DE POLÍTICAS DE CORTE DE INTENTOS DE INTRUSIÓN EN LOS IDS/IPS
4. ANÁLISIS DE LOS EVENTOS REGISTRADOS POR EL IDS/IPS PARA DETERMINAR FALSOS POSITIVOS Y CARACTERIZARLOS EN LAS POLÍTICAS DE CORTE DEL IDS/IPS
5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN
6. ESTABLECIMIENTO DE LOS NIVELES REQUERIDOS DE ACTUALIZACIÓN, MONITORIZACIÓN Y PRUEBAS DEL IDS/ IPS

## 5. ESTABLECIMIENTO DE LOS NIVELES REQUERIDOS DE ACTUALIZACIÓN, MONITORIZACIÓN Y PRUEBAS DEL IDS/ IPS

LOS SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES SIGUEN UNA SERIE DE **FASES** EN SUS PROCESOS:

- **PREVENCIÓN:** EN UN MOMENTO INICIAL, LOS IDS/IPS INTENTAN EVITAR LOS ATAQUES MEDIANTE MECANISMOS QUE DIFICULTEN EL ACCESO DE INTRUSOS.
- **MONITORIZACIÓN DE LA INTRUSIÓN:** SI, A PESAR DE TODAS LAS MEDIDAS PREVENTIVAS HA HABIDO UNA INTRUSIÓN O ACTIVIDAD SOSPECHOSA, LOS IDS/IPS DETECTAN ESTA ACTIVIDAD Y MONITORIZAN EL TRÁFICO DE DATOS SOSPECHOSO PARA QUE PUEDA SER ANALIZADO Y REVISADO POR EL ADMINISTRADOR DEL SISTEMA.

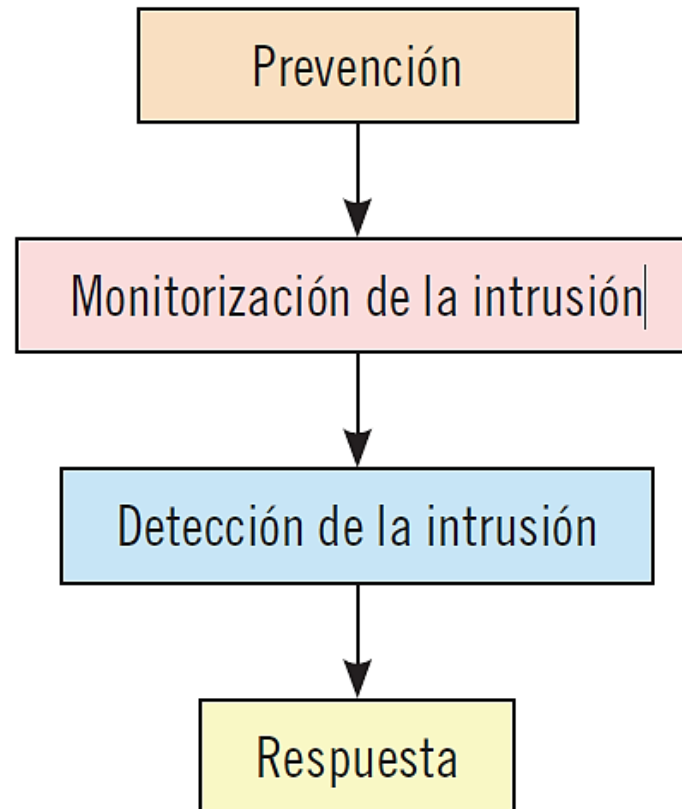
## 5. ESTABLECIMIENTO DE LOS NIVELES REQUERIDOS DE ACTUALIZACIÓN, MONITORIZACIÓN Y PRUEBAS DEL IDS/ IPS

### FASES:

- **DETECCIÓN DE LA INTRUSIÓN:** CUANDO SE HA ANALIZADO EL TRÁFICO, SI EL IDS/IPS DETERMINA QUE LA ACTIVIDAD SOSPECHOSA ES EFECTIVAMENTE UNA INTRUSIÓN, EL SISTEMA GENERA UNA ALARMA PARA NOTIFICAR ESTA INTRUSIÓN AL ADMINISTRADOR.
- **RESPUESTA:** DETERMINADA LA INTRUSIÓN COMO ATAQUE LOS SISTEMAS IDS/IPS PUEDEN ADOPTAR UNA SERIE DE MEDIDAS QUE INTENTEN BLOQUEAR EL ACCESO DEL ATACANTE AL SISTEMA.

## 5. ESTABLECIMIENTO DE LOS NIVELES REQUERIDOS DE ACTUALIZACIÓN, MONITORIZACIÓN Y PRUEBAS DEL IDS/ IPS

Fases de los procesos de detección y prevención de intrusiones





## **5. ESTABLECIMIENTO DE LOS NIVELES REQUERIDOS DE ACTUALIZACIÓN, MONITORIZACIÓN Y PRUEBAS DEL IDS/ IPS**

**ES NECESARIA LA INCLUSIÓN DE UNA BASE DE DATOS DE FIRMAS QUE PERMITA LA MONITORIZACIÓN DE LOS EVENTOS Y SU CLASIFICACIÓN ENTRE ACTIVIDADES SOSPECHOSAS, ACTIVIDADES NO SOSPECHOSAS E INTRUSIONES REALES.**

**ES POSIBLE QUE EL FUNCIONAMIENTO DEL SISTEMA NO SEA EL ADECUADO DEBIDO AL ELEVADO NÚMERO DE FALSOS POSITIVOS O FALSOS NEGATIVOS.**

**HAY QUE REALIZAR UNA SERIE DE PRUEBAS QUE PERMITAN COMPARAR LOS RESULTADOS DE VARIAS CONFIGURACIONES Y ASÍ CONSEGUIR DEFINIR LA CONFIGURACIÓN MÁS ADECUADA A LAS NECESIDADES DE SEGURIDAD DE LA ORGANIZACIÓN.**

## **5. ESTABLECIMIENTO DE LOS NIVELES REQUERIDOS DE ACTUALIZACIÓN, MONITORIZACIÓN Y PRUEBAS DEL IDS/ IPS**

**NO HAY QUE OLVIDAR REALIZAR COMPROBACIONES Y ACTUALIZACIONES PERIÓDICAS PARA DETECTAR LA POSIBLE OBSOLESCENCIA DE LA BASE DE DATOS DE INTRUSIONES O LA PÉRDIDA DE EFECTIVIDAD DEL SISTEMA IMPLANTADO.**

**PARA MEDIR LA EFICIENCIA DEL SISTEMA IDS/IPS Y ESTABLECER ESTOS NIVELES SE DEBEN TENER EN CUENTA LAS CARACTERÍSTICAS SIGUIENTES:**

- **PRECISIÓN**
- **RENDIMIENTO**
- **COMPLETITUD**
- **TOLERANCIA A FALLOS**
- **TIEMPO DE RESPUESTA**

## 5. ESTABLECIMIENTO DE LOS NIVELES REQUERIDOS DE ACTUALIZACIÓN, MONITORIZACIÓN Y PRUEBAS DEL IDS/ IPS

### PRECISIÓN

ES LA CAPACIDAD DEL SISTEMA IDS/IPS PARA DETECTAR ATAQUES Y DIFERENCIARLOS DEL TRÁFICO NORMAL DE UNA RED. SE UTILIZA LA FÓRMULA SIGUIENTE:

$$\textit{Precisión} = \frac{\textit{Ataques reales detectados}}{\textit{Ataques reales detectados} + \textit{falsos positivos}}$$

LO IDEAL ES ENCONTRAR EL EQUILIBRIO ENTRE FALSOS POSITIVOS Y FALSOS NEGATIVOS.

LA PRECISIÓN SERÁ MAYOR CUANDO EL RATIO OBTENIDO SEA 1 O LO MÁS CERCANO A 1 POSIBLE, LO QUE SIGNIFICARÁ QUE LA GRAN MAYORÍA DE ATAQUES REALES DETECTADOS SON REALMENTE ATAQUES.

## **5. ESTABLECIMIENTO DE LOS NIVELES REQUERIDOS DE ACTUALIZACIÓN, MONITORIZACIÓN Y PRUEBAS DEL IDS/ IPS**

### **RENDIMIENTO**

**CONSISTE EN LA CANTIDAD DE EVENTOS QUE EL SISTEMA PUEDE ANALIZAR**

AUNQUE LO IDEAL SERÍA QUE EL SISTEMA PUDIESE ANALIZAR TODO EL TRÁFICO DE LA RED HABRÁ QUE LIMITAR SU RENDIMIENTO A LO QUE PERMITA LA CAPACIDAD DE PROCESAMIENTO DEL EQUIPO.

DE ESTE MODO LAS ORGANIZACIONES DEBERÁN BUSCAR UN EQUILIBRIO ENTRE LA CANTIDAD DE TRÁFICO DE RED A ANALIZAR Y LA CANTIDAD DE RECURSOS QUE QUIEREN O PUEDEN UTILIZAR PARA ESTE ANÁLISIS.

## 5. ESTABLECIMIENTO DE LOS NIVELES REQUERIDOS DE ACTUALIZACIÓN, MONITORIZACIÓN Y PRUEBAS DEL IDS/ IPS

### COMPLETITUD

SE CONSIGUE CUANDO DETECTA TODOS LOS TIPOS DE ATAQUES SUCEDIDOS EN EL EQUIPO. LA FÓRMULA DE LA PLENITUD DE UN SISTEMA SE DEFINE A CONTINUACIÓN:

$$\text{Compleitud} = \frac{\text{Ataques reales detectados}}{\text{Ataques reales detectados} + \text{falsos negativos}}$$

SE DEBE CONSEGUIR UN EQUILIBRIO ENTRE LA COMPLETITUD DE UN SISTEMA Y SU PRECISIÓN PARA QUE ASÍ SE DETECTE EL MAYOR NÚMERO POSIBLE DE ATAQUES SIN QUE HAYA UN EXCESO DE FALSOS POSITIVOS O FALSAS ALARMAS.

## **5. ESTABLECIMIENTO DE LOS NIVELES REQUERIDOS DE ACTUALIZACIÓN, MONITORIZACIÓN Y PRUEBAS DEL IDS/ IPS**

### **TOLERANCIA A FALLOS**

**ES LA CAPACIDAD DEL IDS/IPS PARA RESISTIR A LOS ATAQUES Y A LOS FALLOS DEL SISTEMA (CORTES DE ELECTRICIDAD, ETC.).**

*UN IDS DEBE SER SÓLIDO Y SEGURO PARA QUE UN ATAQUE NO PUEDA INUTILIZARLO Y DEJAR EL SISTEMA EXPUESTO A TODO TIPO DE RIESGOS.*

**ADEMÁS, UN IDS/IPS TAMBIÉN DEBE SER CAPAZ DE RECUPERAR LA CONFIGURACIÓN ESTABLECIDA, LOS PATRONES PARA DETECTAR INTRUSIONES Y LOS REGISTROS Y ALARMA GENERADOS ANTERIORMENTE.**



## **5. ESTABLECIMIENTO DE LOS NIVELES REQUERIDOS DE ACTUALIZACIÓN, MONITORIZACIÓN Y PRUEBAS DEL IDS/ IPS**

### **TIEMPO DE RESPUESTA**

**CONSISTE EN EL PERÍODO DE TIEMPO QUE TARDA EN REACCIONAR EL  
IDS/IPS CUANDO SE PRODUCE UN ATAQUE.**

ESTA REACCIÓN PUEDE SER TANTO LA GENERACIÓN DE ALARMAS COMO EL  
ESTABLECIMIENTO DE MEDIDAS DE CORTE DEL ATAQUE.

ESTÁ CLARO QUE LAS ORGANIZACIONES DEBEN CONFIGURAR ESTOS  
SISTEMAS PARA QUE EL TIEMPO DE RESPUESTA SEA LO MÁS REDUCIDO  
POSIBLE, PUES ASÍ SE CONSEGUIRÁ UNA MAYOR EFECTIVIDAD.

# CONTENIDOS

1. INTRODUCCIÓN
2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO
3. DEFINICIÓN DE POLÍTICAS DE CORTE DE INTENTOS DE INTRUSIÓN EN LOS IDS/IPS
4. ANÁLISIS DE LOS EVENTOS REGISTRADOS POR EL IDS/IPS PARA DETERMINAR FALSOS POSITIVOS Y CARACTERIZARLOS EN LAS POLÍTICAS DE CORTE DEL IDS/IPS
5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN
6. ESTABLECIMIENTO DE LOS NIVELES REQUERIDOS DE ACTUALIZACIÓN, MONITORIZACIÓN Y PRUEBAS DEL IDS/ IPS

## RESUMEN

**LOS SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES SON UNA POTENTE HERRAMIENTA PARA EVITAR POSIBLES ATAQUES QUE PUEDEN PRODUCIRSE EN LA INFRAESTRUCTURA DE RED DE LA ORGANIZACIÓN.**

**SON SISTEMAS COMPLEJOS Y MUY ESPECIALIZADOS, POR LO QUE ES VITAL QUE LAS ORGANIZACIONES REALICEN UN ANÁLISIS PREVIO DE SUS INFRAESTRUCTURAS, SERVICIOS, EQUIPOS, ZONAS Y PROTOCOLOS UTILIZADOS PARA DETERMINAR EL SISTEMA A IMPLANTAR, SUS CARACTERÍSTICAS Y CONFIGURACIONES Y SU LOCALIZACIÓN DENTRO DE SUS INSTALACIONES O A TRAVÉS DE ENTORNOS VIRTUALES.**

## RESUMEN

UNA VEZ YA TOMADA LA DECISIÓN SOBRE EL SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES QUE SE VA A IMPLANTAR EN UNA ORGANIZACIÓN **DEBEN DECIDIRSE QUÉ POLÍTICAS DE CORTE DE ATAQUES SE VAN A APLICAR** CUANDO SE DETECTE ALGUNA INTRUSIÓN DISTINGUIENDO ENTRE **POLÍTICAS DE RESPUESTA PASIVA** (CUANDO EL SISTEMA SE LIMITA A INFORMAR DE LOS DETALLES DE LA INTRUSIÓN) Y **POLÍTICAS DE RESPUESTA ACTIVA** (CUANDO EL SISTEMA ADEMÁS DE INFORMAR TOMA MEDIDAS QUE FRENE EL ATAQUE).

LA SIGUIENTE FASE EN LA DETECCIÓN Y PREVENCIÓN DE INTRUSIONES CONSISTE EN **ANALIZAR LOS EVENTOS QUE HA REGISTRADO EL IDS/IPS Y QUE HA CALIFICADO COMO ATAQUES.**

## RESUMEN

ESTOS SISTEMAS NO SON PERFECTOS Y PUEDE SER QUE HAYA FALSOS POSITIVOS Y FALSOS NEGATIVOS. POR ELLO, LAS ORGANIZACIONES **DEBEN CONFIGURAR SUS SISTEMAS** PARA QUE EL NÚMERO DE ERRORES SEA EL MÍNIMO POSIBLE **CONSIGUIENDO UN EQUILIBRIO ENTRE LA SENSIBILIDAD DEL SISTEMA Y LA CANTIDAD DE DATOS A INSPECCIONAR** SEGÚN SUS REQUERIMIENTOS Y NECESIDADES.

**LOS REGISTROS DE AUDITORÍA EN UN IDS/IPS** SON AQUELLOS EN LOS QUE SE REGISTRAN EVENTOS REALIZADOS POR LOS USUARIOS EN UN SISTEMA Y FACILITAN INFORMACIÓN TANTO DE LOS USUARIOS COMO DE LOS DEMÁS DETALLES DEL EVENTO REALIZADO.

## RESUMEN

UNA VEZ DEFINIDAS LAS POLÍTICAS DE ACTUACIÓN Y ANALIZADOS LOS REGISTROS DE AUDITORÍA, LOS ADMINISTRADORES DE LA ORGANIZACIÓN YA TIENEN SUFICIENTE INFORMACIÓN PARA COMPROBAR LA EFICACIA DEL SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES.

AUN ASÍ, SIEMPRE SERÁ NECESARIO EL ESTABLECIMIENTO **DE PRUEBAS Y ACTUALIZACIONES PERIÓDICAS DEL SISTEMA IMPLANTADO** QUE GARANTICEN QUE NO HAY NINGUNA MERMA DE EFICACIA MEDIANTE LA COMPROBACIÓN DE UNA SERIE DE INDICADORES **COMO EL RENDIMIENTO, LA COMPLETITUD, LA PRECISIÓN, LA TOLERANCIA A FALLOS Y EL TIEMPO DE RESPUESTA DEL SISTEMA.**



