

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



## **UD01**

### **SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDS/IPS)**

# CONTENIDOS

1. INTRODUCCIÓN
2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN
3. IDENTIFICACIÓN Y CARACTERIZACIÓN DE LOS DATOS DE FUNCIONAMIENTO DEL SISTEMA
4. ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS
5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD
6. CRITERIOS DE SEGURIDAD PARA EL ESTABLECIMIENTO DE LA UBICACIÓN DE LOS IDS/IPS

# 1. INTRODUCCIÓN

LAS ORGANIZACIONES DEBEN **DEFINIR POLÍTICAS DE SEGURIDAD MÁS EXHAUSTIVAS EN SUS SISTEMAS DE INFORMACIÓN PARA EVITAR EL ACCESO A ELLOS POR PERSONAL NO AUTORIZADO Y PARA IMPEDIR UN USO MALINTENCIONADO DE SUS DATOS.**

HAY NUMEROSAS MOTIVACIONES POR LAS QUE UN ATACANTE PUEDE ACTUAR EN UNA ORGANIZACIÓN: *DESDE MOTIVOS ECONÓMICOS, POR SIMPLE DIVERSIÓN, POR DISCONFORMIDAD CON SUS DIRECTRICES O VALORES O POR LA MERA AUTORREALIZACIÓN PERSONAL*, ENTRE MUCHAS OTRAS.

# 1. INTRODUCCIÓN

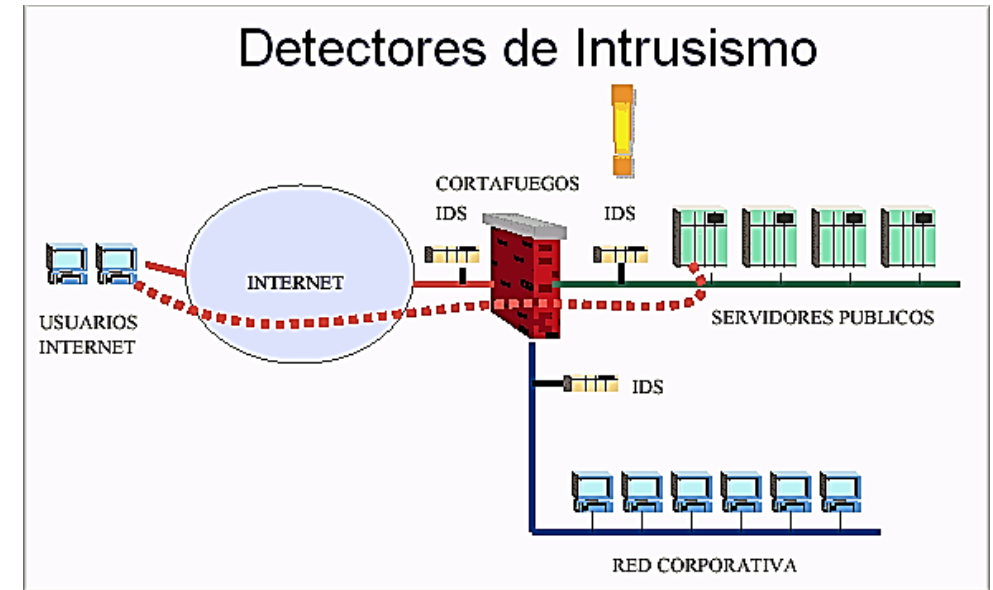
SE VAN A IDENTIFICAR Y CARACTERIZAR LOS DISTINTOS DATOS DE FUNCIONAMIENTO DEL SISTEMA *DONDE LOCALIZAR LAS INCIDENCIAS QUE LE SUCEDEN.*

TAMBIÉN SE VAN A DESCRIBIR Y ANALIZAR VARIAS TÉCNICAS PARA DETECTAR Y PREVENIR EL ATAQUE DE INTRUSOS MEDIANTE UNA SERIE DE HERRAMIENTAS COMO SON LOS **SISTEMAS DE PREVENCIÓN DE INTRUSIONES (IPS)** Y LOS **SISTEMAS DE DETECCIÓN INTRUSIONES (IDS)**



# 1. INTRODUCCIÓN

UNA VEZ QUE YA SE HAN DESCRITO LAS HERRAMIENTAS NECESARIAS PARA DECIDIR QUÉ SISTEMA DE PREVENCIÓN O DETECCIÓN DE INTRUSOS VAN A IMPLANTAR LAS ORGANIZACIONES EN SUS SISTEMAS DE INFORMACIÓN, SE APORTAN UNA SERIE DE **PAUTAS A TENER EN CUENTA EN EL MOMENTO DE ELEGIR LA UBICACIÓN DE ESTOS IDS Y/O IPS** ATENDIENDO A LAS NECESIDADES CONCRETAS DE CADA ORGANIZACIÓN.



# CONTENIDOS

1. INTRODUCCIÓN
2. **CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN**
3. IDENTIFICACIÓN Y CARACTERIZACIÓN DE LOS DATOS DE FUNCIONAMIENTO DEL SISTEMA
4. ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS
5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD
6. CRITERIOS DE SEGURIDAD PARA EL ESTABLECIMIENTO DE LA UBICACIÓN DE LOS IDS/IPS

## **2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN**

ANTES DE DEFINIR LOS CONCEPTOS DE GESTIÓN DE INCIDENTES Y SUS RELACIONES ES IMPRESCINDIBLE CONOCER TRES CONCEPTOS BÁSICOS REFERENTES A LA INFORMACIÓN:

### **CONFIDENCIALIDAD**

GARANTIZA EL ACCESO A LA MISMA SOLO A USUARIOS AUTORIZADOS.

### **INTEGRIDAD**

GARANTIZA QUE NO HA SIDO ALTERADA Y QUE SOLO PUEDE SER MODIFICADA POR LOS USUARIOS AUTORIZADOS.

### **DISPONIBILIDAD**

GARANTIZA QUE ESTÉ DISPONIBLE PARA LOS USUARIOS CUANDO ESTOS LO REQUIERAN.



## **2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN**

**PARA QUE LA INFORMACIÓN CUMPLA UNOS ESTÁNDARES DE SEGURIDAD ADECUADOS DEBE CONTENER LAS TRES PROPIEDADES: *INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD*.**

**UN INCIDENTE DE SEGURIDAD ES CUALQUIER EVENTO QUE PUEDE AFECTAR A LA INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN.**

**ATENDIENDO A LA NORMA ISO 27001, UN INCIDENTE DE SEGURIDAD ES UN EVENTO NO DESEADO O NO ESPERADO QUE PUEDE COMPROMETER SIGNIFICATIVAMENTE LAS OPERACIONES DE NEGOCIO Y AMENAZAR LA SEGURIDAD DE LA INFORMACIÓN.**



## **2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN**

### **TIPOS DE INCIDENTES DE SEGURIDAD**

SON NUMEROSOS LOS TIPOS DE INCIDENTES DE SEGURIDAD QUE PUEDEN OCURRIR EN UN SISTEMA. UNA POSIBLE CLASIFICACIÓN SERÍA LA SIGUIENTE:

- **ACCESOS NO AUTORIZADOS**
- **CÓDIGO MALICIOSO O MALWARE**
- **DENEGACIÓN DEL SERVICIO**
- **PRUEBAS, ESCANEOS O INTENTOS DE OBTENCIÓN DE INFORMACIÓN DE UN SISTEMA DE INFORMACIÓN**
- **MAL USO DE LOS RECURSOS TECNOLÓGICOS**

## 2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN

### TIPOS DE INCIDENTES DE SEGURIDAD

#### ACCESOS NO AUTORIZADOS

SON ***INGRESOS Y OPERACIONES NO AUTORIZADAS A LOS SISTEMAS***, CON ÉXITO O NO. FORMAN PARTE DE ESTA CATEGORÍA:

- ROBO DE INFORMACIÓN
- BORRADO DE INFORMACIÓN
- ACCESOS NO AUTORIZADOS EXITOSOS
- ALTERACIÓN DE LA INFORMACIÓN
- INTENTOS RECURRENTES Y NO RECURRENTES DE ACCESO NO AUTORIZADO
- ABUSO O MAL USO DE LOS SERVICIOS INFORMÁTICOS (TANTO INTERNOS COMO EXTERNOS) QUE REQUIERAN AUTENTICACIÓN

## 2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN

### TIPOS DE INCIDENTES DE SEGURIDAD CÓDIGO MALICIOSO O MALWARE

SON INCIDENTES QUE *SE INFILTRAN EN UN SISTEMA DE INFORMACIÓN SIN AUTORIZACIÓN DEL PROPIETARIO*. SON INCIDENTES DE CÓDIGO MALICIOSO LOS SIGUIENTES:

- **VIRUS** INFORMÁTICOS.
- **TROYANOS**: SE INTRODUCE EN EL SISTEMA INFORMÁTICO COMO UN PROGRAMA APARENTEMENTE INOFENSIVO, PERO AL EJECUTARLO PERMITE EL ACCESO REMOTO NO AUTORIZADO AL SISTEMA A USUARIOS.
- **GUSANOS**: CÓDIGO MALICIOSO QUE, UNA VEZ HA ACCEDIDO AL SISTEMA, SE VA DUPLICANDO A SÍ MISMO. NO ALTERA LOS ARCHIVOS YA INSTALADOS, PERO SUPONE UN CONSUMO DE RECURSOS IMPORTANTE.

## 2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN

### TIPOS DE INCIDENTES DE SEGURIDAD

#### DENEGACIÓN DEL SERVICIO

EVENTOS QUE ***PRODUCEN LA PÉRDIDA DE UN SERVICIO EN PARTICULAR***, IMPIDIENDO SU EJECUCIÓN NORMAL.

SUELEN SER INCIDENTES DE DENEGACIÓN DEL SERVICIO CUANDO EN EL SISTEMA SE NOTA QUE HAY TIEMPOS DE RESPUESTA MUY BAJOS Y SERVICIOS INTERNOS Y EXTERNOS INACCESIBLES SIN MOTIVOS APARENTES.

## 2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN

### TIPOS DE INCIDENTES DE SEGURIDAD

**PRUEBAS, ESCANEOS O INTENTOS DE OBTENCIÓN DE INFORMACIÓN DE UN SISTEMA DE INFORMACIÓN**

SON EVENTOS QUE *INTENTAN OBTENER INFORMACIÓN SOBRE LAS ACCIONES QUE SE PRODUCEN EN UN SISTEMA INFORMÁTICO.*

ALGUNOS DE ESTOS EVENTOS SON:

- **SNIFFERS:** APLICACIONES CUYA FUNCIÓN ES OBTENER LA INFORMACIÓN QUE ENVÍAN LOS DISTINTOS EQUIPOS DE UNA RED.
- **DETECCIÓN DE VULNERABILIDADES:** APLICACIONES QUE BUSCAN LAS VULNERABILIDADES DE UN SISTEMA DE INFORMACIÓN PARA APROVECHARSE DE ELLO MALICIOSAMENTE.

## 2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN

### TIPOS DE INCIDENTES DE SEGURIDAD

#### MAL USO DE LOS RECURSOS TECNOLÓGICOS

EVENTOS QUE ***ATACAN A LOS RECURSOS TECNOLÓGICOS DE UN SISTEMA DE INFORMACIÓN*** A CAUSA DE UN MAL USO DE LOS MISMOS.

FORMAN PARTE DE ESTE TIPO DE EVENTOS:

- VIOLACIÓN DE LA NORMATIVA DE ACCESO A INTERNET.
- ABUSO O MAL USO DE LOS SERVICIOS INFORMÁTICOS EXTERNOS O INTERNOS.
- ABUSO O MAL USO DEL CORREO ELECTRÓNICO.
- VIOLACIÓN DE LAS POLÍTICAS, NORMAS Y PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA DE UNA ORGANIZACIÓN.

## 2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN

### GESTIÓN Y MEDIDAS DE INCIDENTES DE SEGURIDAD

ANTE LA POSIBILIDAD DE QUE HAYA ALGÚN TIPO DE INCIDENTE DE SEGURIDAD EN LA ORGANIZACIÓN HAY QUE TOMAR UNA SERIE DE MEDIDAS QUE PUEDEN SER:

- **MEDIDAS PREVENTIVAS:** AQUELLAS MEDIDAS QUE SE APLICAN ***PARA EVITAR LA OCURRENCIA*** DE INCIDENTES DE SEGURIDAD. ALGUNOS EJEMPLOS SON: UTILIZACIÓN DE CONTRASEÑAS, CIFRADO DE INFORMACIÓN, ESTABLECIMIENTO DE FIREWALLS, ETC.
- **MEDIDAS DE DETECCIÓN:** MEDIDAS QUE SIRVEN ***PARA DETECTAR Y CONTROLAR*** LOS INCIDENTES DE SEGURIDAD. POR EJEMPLO: AUDITORÍAS DE SEGURIDAD, REVISIONES DE SEGURIDAD, ETC.



## 2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN

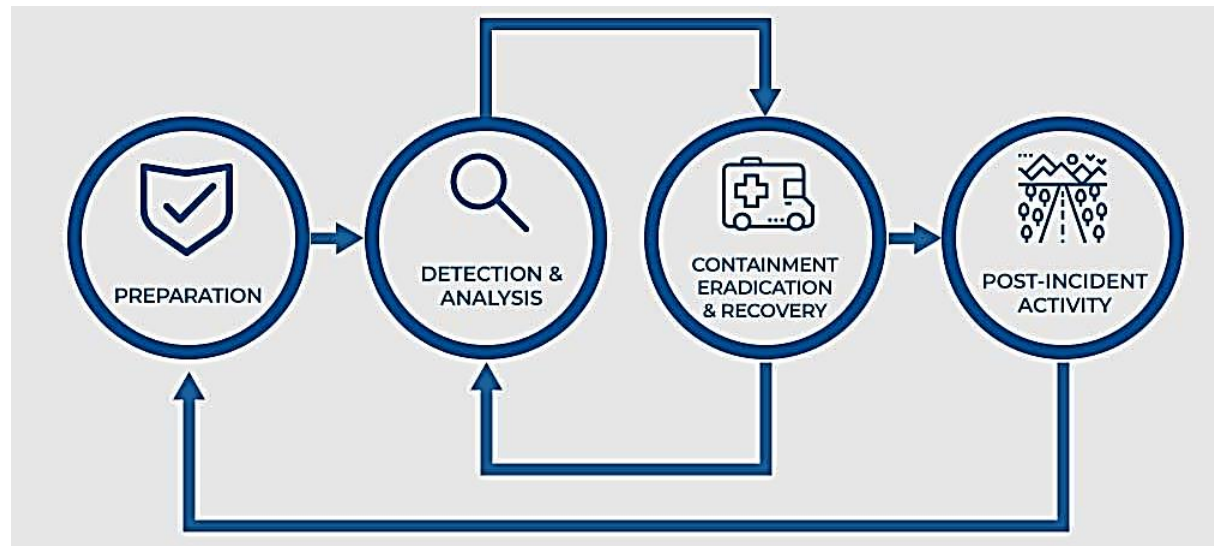
### GESTIÓN Y MEDIDAS DE INCIDENTES DE SEGURIDAD

- **MEDIDAS CORRECTIVAS:** MEDIDAS IMPLEMENTADAS UNA VEZ YA HA SUCEDIDO EL INCIDENTE DE SEGURIDAD QUE *SIRVEN PARA EVITAR QUE VUELVAN A OCURRIR Y PARA RESTAURAR LA SITUACIÓN INICIAL* ANTES DE LA INCIDENCIA. SUELEN SER PROCEDIMIENTOS DE RESTAURACIÓN, ELIMINACIÓN DE CÓDIGO MALICIOSO Y AUDITORÍA FORENSE.

## 2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN

### GESTIÓN Y MEDIDAS DE INCIDENTES DE SEGURIDAD

LA **GESTIÓN DE INCIDENTES** TIENE COMO OBJETIVO *CALCULAR Y UTILIZAR ADECUADAMENTE LOS RECURSOS NECESARIOS PARA APLICAR CORRECTAMENTE ESTAS MEDIDAS DE PREVENCIÓN, DETECCIÓN Y CORRECCIÓN DE INCIDENTES DE SEGURIDAD.*



## **2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN**

### **GESTIÓN Y MEDIDAS DE INCIDENTES DE SEGURIDAD**

SE ESTABLECEN UNAS PAUTAS GENERALES A SEGUIR PARA QUE ESTA GESTIÓN ESTÉ BIEN EJECUTADA:

- **PREVENCIÓN DE LOS INCIDENTES**
- **DETECCIÓN Y REPORTE DE LOS INCIDENTES**
- **CLASIFICACIÓN DEL INCIDENTE**
- **ANÁLISIS DEL INCIDENTE**
- **RESPUESTA AL INCIDENTE**
- **REGISTRO DE INCIDENTES**
- **APRENDIZAJE**

## **2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN**

### **GESTIÓN Y MEDIDAS DE INCIDENTES DE SEGURIDAD**

#### **PREVENCIÓN DE LOS INCIDENTES**

APLICACIÓN DE LAS *MEDIDAS PREVENTIVAS* QUE EVITEN LA PRODUCCIÓN DE LOS INCIDENTES.

#### **DETECCIÓN Y REPORTE DE LOS INCIDENTES**

EN CASO DE PRODUCIRSE EL INCIDENTE HAY QUE *DETECTARLO Y REPORTAR* EL MISMO A LOS RESPONSABLES DE SU GESTIÓN.

#### **CLASIFICACIÓN DEL INCIDENTE**

*DEFINICIÓN DEL TIPO DE INCIDENTE* QUE HA OCURRIDO (ACCESO NO AUTORIZADO, ROBO DE INFORMACIÓN, ETC.).

## 2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN

### GESTIÓN Y MEDIDAS DE INCIDENTES DE SEGURIDAD

#### ANÁLISIS DEL INCIDENTE

*ANÁLISIS DE CÓMO SE HA PRODUCIDO EL INCIDENTE Y DE LOS DAÑOS QUE HA CAUSADO.*

#### RESPUESTA AL INCIDENTE

*APLICACIÓN DE LAS MEDIDAS CORRECTIVAS PARA RESTAURAR EL SISTEMA A LA SITUACIÓN INICIAL ANTES DE PRODUCIRSE EL INCIDENTE.*

## **2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN**

### **GESTIÓN Y MEDIDAS DE INCIDENTES DE SEGURIDAD**

#### **REGISTRO DE INCIDENTES**

REGISTRO DEL INCIDENTE SUCEDIDO Y DE LAS MEDIDAS APLICADAS PARA *OBTENER UN HISTORIAL Y UN CONTROL DE TODOS LOS REGISTROS QUE HAN IDO OCURRIENDO.*

#### **APRENDIZAJE**

ANÁLISIS DE LOS POSIBLES ERRORES CAUSANTES DE LA INCIDENCIA PARA *EVITAR QUE SE VUELVAN A PRODUCIR.*

## 2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN

### GESTIÓN Y MEDIDAS DE INCIDENTES DE SEGURIDAD

SIGUIENDO ESTAS FASES DE GESTIÓN DE INCIDENTES, LAS ORGANIZACIONES PUEDEN OBTENER NUMEROSOS **BENEFICIOS**, ENTRE ELLOS:

- RÁPIDA, EFICIENTE Y SISTEMÁTICA RESPUESTA ANTE LA APARICIÓN DE INCIDENTES.
- RÁPIDA RESTAURACIÓN DEL SISTEMA INFORMÁTICO GARANTIZANDO LA MÍNIMA PÉRDIDA DE INFORMACIÓN POSIBLE.
- GENERACIÓN DE UNA BASE DE DATOS CON EL HISTÓRICO DE LOS INCIDENTES Y DE LAS MEDIDAS TOMADAS PARA UNA MAYOR RAPIDEZ ANTE PRÓXIMOS INCIDENTES.



## **2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN**

### **GESTIÓN Y MEDIDAS DE INCIDENTES DE SEGURIDAD**

#### **BENEFICIOS:**

- MEJORA CONTINUA DE LA GESTIÓN Y TRATAMIENTO DE INCIDENTES.
- ELIMINACIÓN DE LA APARICIÓN DE INCIDENTES REPETITIVOS (GRACIAS AL REGISTRO HISTÓRICO).
- OPTIMIZACIÓN DE LOS RECURSOS DISPONIBLES.
- MAYOR PRODUCTIVIDAD DE LOS USUARIOS.
- MAYOR CONTROL DE LOS PROCESOS DEL SISTEMA DE INFORMACIÓN Y DEL PROCESO DE MONITORIZACIÓN DEL MISMO.

## **2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN**

### **GESTIÓN Y MEDIDAS DE INCIDENTES DE SEGURIDAD**

**SIN EMBARGO, UNA GESTIÓN DE INCIDENTES DEFICIENTE PUEDE LLEVAR A EFECTOS ADVERSOS IMPORTANTES:**

- DESPERDICIO Y BAJO RENDIMIENTO DE LOS RECURSOS.
- PÉRDIDA DE INFORMACIÓN VALIOSA PARA LA ORGANIZACIÓN.
- PÉRDIDA DE PRODUCTIVIDAD EN LOS SERVICIOS Y PEOR CALIDAD DE SERVICIO A LOS CLIENTES.

## **2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN**

### **DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN**

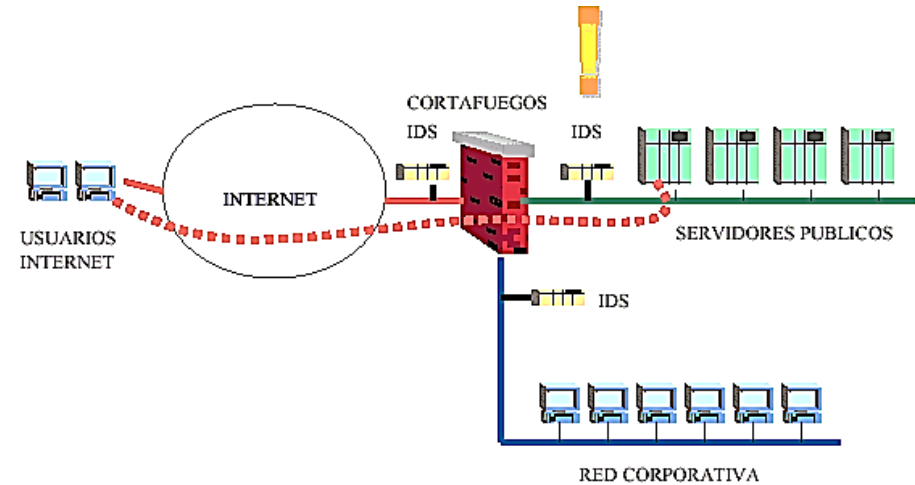
**LOS INTENTOS DE INTRUSIÓN SON AQUELLOS INTENTOS QUE PUEDEN AFECTAR NEGATIVAMENTE A LA SEGURIDAD DE LA INFORMACIÓN DE UN EQUIPO O QUE INTENTAN EVITAR LOS MECANISMOS DE SEGURIDAD QUE HAY ESTABLECIDOS.**

**ESTAS INTRUSIONES PUEDEN PRODUCIRSE DE VARIOS MODOS: DESDE *USUARIOS NO AUTORIZADOS* QUE ACCEDEN AL SISTEMA A TRAVÉS DE INTERNET, *USUARIOS QUE SÍ ESTÁN AUTORIZADOS* PERO QUE INTENTAN ACCEDER A PRIVILEGIOS PARA LOS QUE NO TIENEN AUTORIZACIÓN, HASTA *USUARIOS AUTORIZADOS QUE UTILIZAN MALINTENCIONADAMENTE LOS PRIVILEGIOS* QUE LES HAN SIDO OTORGADOS.**

## 2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN

**DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN**  
PARA EVITAR ESTE TIPO DE INTRUSIONES ESTÁN LOS **SISTEMAS DE PREVENCIÓN DE INTRUSIONES O IDS.**

SON SISTEMAS QUE PERMITEN ESTABLECER UNA PROTECCIÓN ADICIONAL A LOS EQUIPOS Y REDES DE UNA ORGANIZACIÓN ANTE LAS POSIBLES AMENAZAS QUE PUEDEN APARECER DEBIDO AL USO EXHAUSTIVO DE LAS REDES Y DE LOS SISTEMAS DE INFORMACIÓN EXTERNOS.



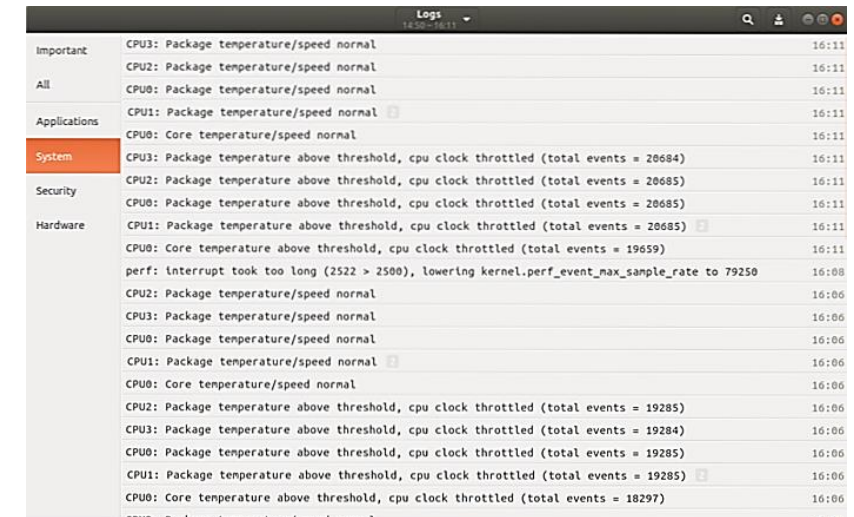
# CONTENIDOS

1. INTRODUCCIÓN
2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN
- 3. IDENTIFICACIÓN Y CARACTERIZACIÓN DE LOS DATOS DE FUNCIONAMIENTO DEL SISTEMA**
4. ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS
5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD
6. CRITERIOS DE SEGURIDAD PARA EL ESTABLECIMIENTO DE LA UBICACIÓN DE LOS IDS/IPS

### 3. IDENTIFICACIÓN Y CARACTERIZACIÓN DE LOS DATOS DE FUNCIONAMIENTO DEL SISTEMA

UN LOG ES UN REGISTRO OFICIAL DE LOS EVENTOS DEL SISTEMA PRODUCIDOS A LO LARGO DE UN PERÍODO DE TIEMPO DETERMINADO. EN LOS LOGS SE REGISTRAN DATOS DE EVENTOS REFERENTES A:

- QUÉ TIPO DE EVENTO HA OCURRIDO
- QUIÉN HA ORIGINADO EL EVENTO
- CUANDO SE HA PRODUCIDO EL EVENTO
- DÓNDE SE HA PRODUCIDO EL EVENTO
- POR QUÉ SE HA PRODUCIDO EL EVENTO



Category	Event Description	Time
Important	CPU3: Package temperature/speed normal	16:11
	CPU2: Package temperature/speed normal	16:11
All	CPU0: Package temperature/speed normal	16:11
	CPU1: Package temperature/speed normal	16:11
Applications	CPU0: Core temperature/speed normal	16:11
System	CPU3: Package temperature above threshold, cpu clock throttled (total events = 20684)	16:11
	CPU2: Package temperature above threshold, cpu clock throttled (total events = 20685)	16:11
Security	CPU0: Package temperature above threshold, cpu clock throttled (total events = 20685)	16:11
Hardware	CPU1: Package temperature above threshold, cpu clock throttled (total events = 20685)	16:11
	CPU0: Core temperature above threshold, cpu clock throttled (total events = 19659)	16:11
	perf: Interrupt took too long (2522 > 2500), lowering kernel.perf_event_max_sample_rate to 79250	16:08
	CPU2: Package temperature/speed normal	16:06
	CPU3: Package temperature/speed normal	16:06
	CPU0: Package temperature/speed normal	16:06
	CPU1: Package temperature/speed normal	16:06
	CPU0: Core temperature/speed normal	16:06
	CPU2: Package temperature above threshold, cpu clock throttled (total events = 19285)	16:06
	CPU3: Package temperature above threshold, cpu clock throttled (total events = 19284)	16:06
	CPU0: Package temperature above threshold, cpu clock throttled (total events = 19285)	16:06
	CPU1: Package temperature above threshold, cpu clock throttled (total events = 19285)	16:06
	CPU0: Core temperature above threshold, cpu clock throttled (total events = 18297)	16:06

### **3. IDENTIFICACIÓN Y CARACTERIZACIÓN DE LOS DATOS DE FUNCIONAMIENTO DEL SISTEMA**

PARA COMPROBAR EL CORRECTO FUNCIONAMIENTO DEL SISTEMA E IDENTIFICAR LOS DISTINTOS EVENTOS SUCEDIDOS **SE RECOMIENDA EVALUAR LOS LOGS DE LOS EQUIPOS**, YA QUE SE PODRÁN DETECTAR FALLOS Y EVENTOS COMO:

- INCIDENTES DE SEGURIDAD.
- FUNCIONAMIENTOS ANÓMALOS.
- CAMBIOS DE CONFIGURACIÓN DE APLICACIONES O DISPOSITIVOS.
- UTILIZACIÓN Y RENDIMIENTO DE LOS RECURSOS.
- INTENTOS FALLIDOS DE ACCESO DE USUARIOS NO AUTORIZADOS.

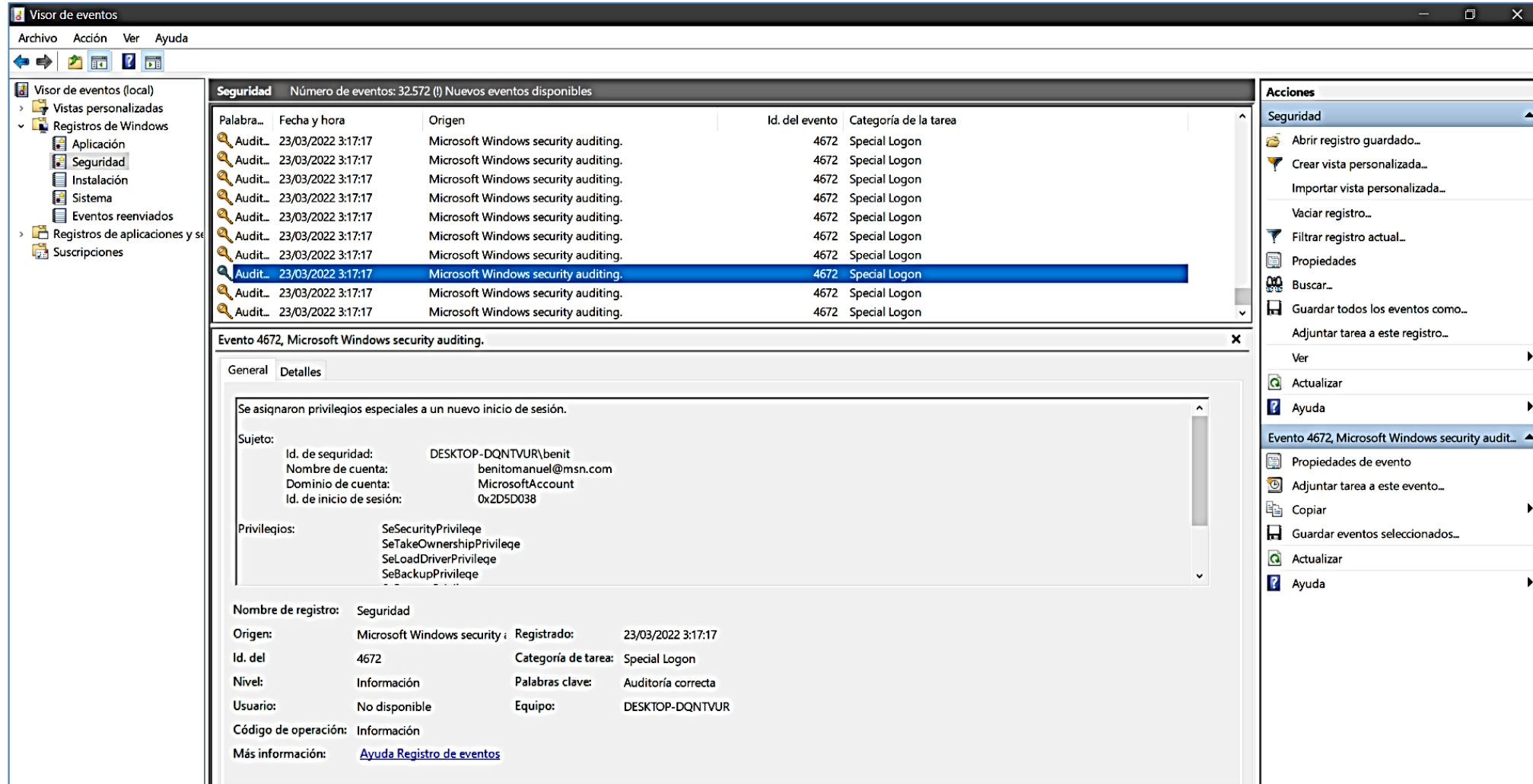


### 3. IDENTIFICACIÓN Y CARACTERIZACIÓN DE LOS DATOS DE FUNCIONAMIENTO DEL SISTEMA

EN **WINDOWS** SE PUEDE UTILIZAR EL **VISOR DE EVENTOS**. CON ESTA HERRAMIENTA SE PUEDEN VISUALIZAR DISTINTOS TIPOS DE EVENTOS SUCEDIDOS:

- **REGISTROS DE APLICACIÓN:** REGISTRADOS POR APLICACIONES O PROGRAMAS.
- **REGISTROS DE SEGURIDAD:** OCURRIDOS EN LOS ACCESOS DEL SISTEMA COMO LOS INTENTOS DE INICIO DE SESIÓN (TANTO EXITOSOS COMO FALLIDOS), LAS INTRODUCCIONES DE CONTRASEÑAS ERRÓNEAS, LA UTILIZACIÓN DE LOS RECURSOS, ETC.
- **REGISTROS DE INSTALACIÓN:** HACEN REFERENCIA A LA INSTALACIÓN DE APLICACIONES EN EL EQUIPO. SE SUELEN UTILIZAR PARA COMPROBAR SI SE HA INSTALADO ALGÚN CÓDIGO MALICIOSO EN EL EQUIPO.
- **REGISTROS DE EVENTOS REENVIADOS:** SE HAN REENVIADO A ESTE REGISTRO DESDE OTROS EQUIPOS.

### 3. IDENTIFICACIÓN Y CARACTERIZACIÓN DE LOS DATOS DE FUNCIONAMIENTO DEL SISTEMA



**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

**Seguridad** Número de eventos: 32.572 (0) Nuevos eventos disponibles

Palabra...	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Audit...	23/03/2022 3:17:17	Microsoft Windows security auditing.	4672	Special Logon
Audit...	23/03/2022 3:17:17	Microsoft Windows security auditing.	4672	Special Logon
Audit...	23/03/2022 3:17:17	Microsoft Windows security auditing.	4672	Special Logon
Audit...	23/03/2022 3:17:17	Microsoft Windows security auditing.	4672	Special Logon
Audit...	23/03/2022 3:17:17	Microsoft Windows security auditing.	4672	Special Logon
Audit...	23/03/2022 3:17:17	Microsoft Windows security auditing.	4672	Special Logon
Audit...	23/03/2022 3:17:17	Microsoft Windows security auditing.	4672	Special Logon
Audit...	23/03/2022 3:17:17	Microsoft Windows security auditing.	4672	Special Logon
Audit...	23/03/2022 3:17:17	Microsoft Windows security auditing.	4672	Special Logon

**Evento 4672, Microsoft Windows security auditing.**

General Detalles

Se asignaron privilegios especiales a un nuevo inicio de sesión.

Sujeto:

- Id. de seguridad: DESKTOP-DQNTVUR\benit
- Nombre de cuenta: benitomanuel@msn.com
- Dominio de cuenta: MicrosoftAccount
- Id. de inicio de sesión: 0x2D5D038

Privilegios:

- SeSecurityPrivilege
- SeTakeOwnershipPrivilege
- SeLoadDriverPrivilege
- SeBackupPrivilege

Nombre de registro: Seguridad

Origen: Microsoft Windows security Registrado: 23/03/2022 3:17:17

Id. del: 4672 Categoría de tarea: Special Logon

Nivel: Información Palabras clave: Auditoría correcta

Usuario: No disponible Equipo: DESKTOP-DQNTVUR

Código de operación: Información

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

**Acciones**

Seguridad

- Abrir registro guardado...
- Crear vista personalizada...
- Importar vista personalizada...
- Vaciar registro...
- Filtrar registro actual...
- Propiedades
- Buscar...
- Guardar todos los eventos como...
- Adjuntar tarea a este registro...
- Ver
- Actualizar
- Ayuda

**Evento 4672, Microsoft Windows security audit...**

- Propiedades de evento
- Adjuntar tarea a este evento...
- Copiar
- Guardar eventos seleccionados...
- Actualizar
- Ayuda

### 3. IDENTIFICACIÓN Y CARACTERIZACIÓN DE LOS DATOS DE FUNCIONAMIENTO DEL SISTEMA

UTILIZANDO **LINUX** NO HAY UNA APLICACIÓN GRÁFICA QUE PERMITA VISUALIZAR LOS EVENTOS DE UN EQUIPO. PARA ELLO SERÁ NECESARIO ACCEDER A LOS ARCHIVOS DE REGISTRO INICIANDO LA SESIÓN COMO USUARIO “**ROOT**” Y UTILIZAR UNA SERIE DE COMANDOS:

- CON EL COMANDO **TAIL -F** SE VEN LAS ÚLTIMAS LÍNEAS DE UN ARCHIVO Y SUS ACTUALIZACIONES.
- CON EL COMANDO **LESS +F** EN LUGAR DE ACCEDER A LAS ÚLTIMAS LÍNEAS DE UN ARCHIVO DE REGISTRO SE ACCEDE A SU TOTALIDAD, PUDIÉNDOSE VER, INCLUSO, LAS ACTUALIZACIONES DEL MISMO A TIEMPO REAL.

### 3. IDENTIFICACIÓN Y CARACTERIZACIÓN DE LOS DATOS DE FUNCIONAMIENTO DEL SISTEMA

LOS PRINCIPALES ARCHIVOS DE REGISTRO QUE SE UTILIZAN PARA COMPROBAR EL FUNCIONAMIENTO DEL SISTEMA Y SUS PROBLEMAS DE SEGURIDAD SE PUEDEN OBSERVAR EN LA TABLA SIGUIENTE (ALGUNOS DIFIEREN SEGÚN LA DISTRIBUCIÓN):

Nombre de archivo	Funcionalidad
/var/log/auth.log	Eventos de autenticación de usuarios y permisos.
/var/log/boot.log	Eventos y servicios empezados cuando se inicia el sistema.
/var/log/daemon.log	Mensajes sobre permisos o servicios corriendo en el sistema.
/log/dmesg.log	Mensajes del núcleo Linux.
/var/log/errors.log	Errores del sistema.
/var/log/everything.log	Mensajes misceláneos no cubiertos por los otros archivos.
/var/log/httpd.log	Mensajes y errores de Apache.
/var/log/mail.log	Mensajes del servidor de correo electrónico.
/var/log/messages.log	Alertas generales del sistema.
/var/log/secure	Registro de seguridad.
/var/log/syslog.log	Registro del sistema de registro.
/var/log/user.log	Muestra información acerca de los procesos usados por el usuario.

### **3. IDENTIFICACIÓN Y CARACTERIZACIÓN DE LOS DATOS DE FUNCIONAMIENTO DEL SISTEMA**

**MEDIANTE LAS HERRAMIENTAS DE VISUALIZACIÓN DE LOGS Y DE EVENTOS SE PUEDEN COMPROBAR Y EVALUAR LOS DISTINTOS PARÁMETROS DE FUNCIONAMIENTO DE UN SISTEMA O DE UN EQUIPO.**

**SE PODRÁN DETECTAR LAS DISTINTAS DEFICIENCIAS DE LA GESTIÓN DE RECURSOS E INCIDENTES DE UN SISTEMA Y ANALIZAR DE DÓNDE PROVIENEN Y PODER ESTABLECER UNA SERIE DE MEDIDAS CORRECTIVAS QUE PERMITAN UNA EFICIENTE GESTIÓN DEL EQUIPO.**

**MEDIANTE EL HISTORIAL DE LOGS Y EVENTOS TAMBIÉN SE PUEDEN OBSERVAR LOS EVENTOS REPETIDOS PERJUDICIALES PARA EL EQUIPO Y ENCONTRAR AQUELLAS MEDIDAS QUE EVITEN QUE VUELVAN A SUCEDER MEJORANDO SIGNIFICATIVAMENTE EL RENDIMIENTO DEL EQUIPO Y AUMENTANDO LA SEGURIDAD DEL MISMO.**

# CONTENIDOS

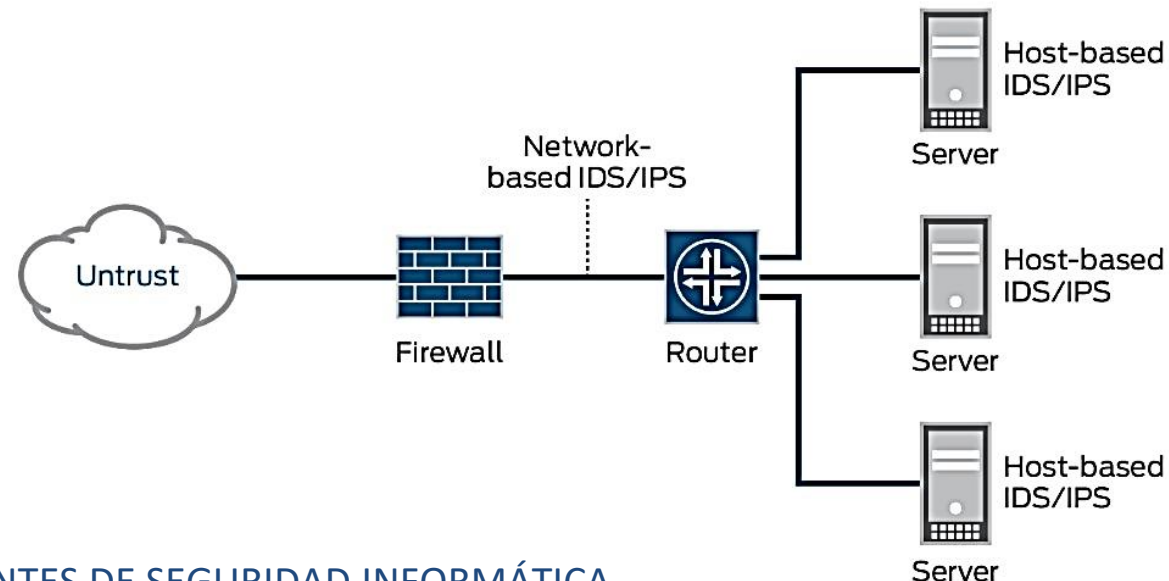
1. INTRODUCCIÓN
2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN
3. IDENTIFICACIÓN Y CARACTERIZACIÓN DE LOS DATOS DE FUNCIONAMIENTO DEL SISTEMA
4. **ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS**
5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD
6. CRITERIOS DE SEGURIDAD PARA EL ESTABLECIMIENTO DE LA UBICACIÓN DE LOS IDS/IPS



## 4. ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS

LOS SISTEMAS DE DETECCIÓN DE INTRUSOS O IDS (INTRUSION DETECTION SYSTEM) SON PROGRAMAS CUYA UTILIDAD ES DETECTAR LAS INTRUSIONES QUE SE PUEDEN PRODUCIR EN LA RED O EN UN EQUIPO.

SE ENCARGAN DE MONITORIZAR LOS EVENTOS DEL EQUIPO PARA BUSCAR INTENTOS DE INTRUSIÓN.

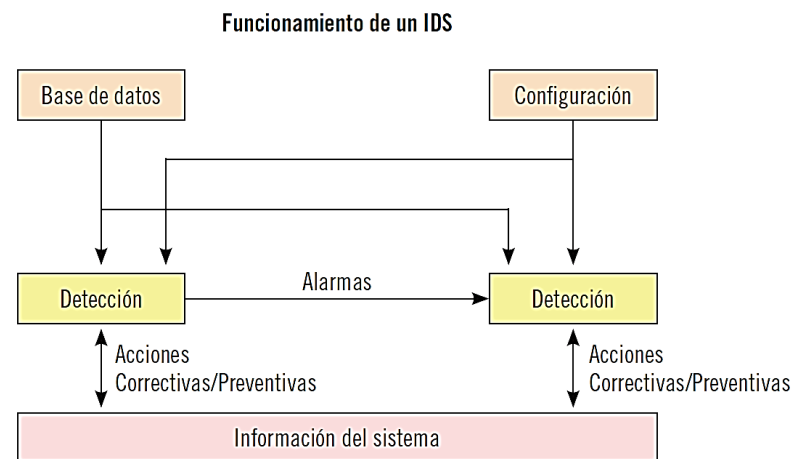




## 4. ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS

**LOS IDS SON UNA ESPECIE DE PROCESO DE AUDITORÍA.**

**SON APLICACIONES QUE MEDIANTE UNA AMPLIA BASE DE DATOS Y UNA SERIE DE CONFIGURACIONES CONSIGUEN PREVENIR Y DETECTAR LOS POSIBLES ATAQUES QUE PUEDEN PRODUCIRSE EN UN SISTEMA. UNA VISIÓN GRÁFICA DEL FUNCIONAMIENTO DE UN IDS PODRÍA SER LA SIGUIENTE:**



## 4. ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS

### VENTAJAS

- **PREVIENEN DE POSIBLES PROBLEMAS PORQUE DISUADEN INDIVIDUOS HOSTILES:** LOS IDS POSIBILITAN EL DESCUBRIMIENTO DE ATACANTES AL SISTEMA, LO QUE RESULTA UN ELEMENTO DISUASORIO ANTE LA POSIBILIDAD DE SER DESCUBIERTOS Y PENALIZADOS.
- **DETECTAN ATAQUES Y OTRAS VULNERACIONES DE LA SEGURIDAD QUE OTROS SISTEMAS DE PROTECCIÓN NO PREVIENEN:** EN NUMEROSAS OCASIONES LOS ATACANTES ACCEDEN SIN AUTORIZACIÓN A LOS EQUIPOS APROVECHANDO SUS VULNERABILIDADES. MEDIANTE LOS IDS SE PUEDEN DETECTAR ESTOS INTENTOS DE ACCESO Y REPORTARLOS DE INMEDIATO AL ADMINISTRADOR, DE MODO QUE PUEDAN APLICARSE MEDIDAS CORRECTIVAS LO ANTES POSIBLE Y MINIMIZAR EL DAÑO.

## 4. ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS

### VENTAJAS

- **DETECTAN PREÁMBULOS DE ATAQUES:** ANTES DE INTENTAR ACCEDER Y ATACAR A UN SISTEMA, LOS ATACANTES SUELEN EXAMINARLO Y HACER PRUEBAS PARA TANTEAR EL ATAQUE. **LOS IDS DETECTAN ESTAS PRUEBAS DE RED Y ACCESOS AL SISTEMA**, LO QUE PERMITE AUMENTAR LA SEGURIDAD CUANDO HAY ESTE TIPO DE DETECCIONES PARA PODER EVITAR FUTUROS ATAQUES.
- **JUSTIFICAN Y DOCUMENTAN EL RIESGO DE LA ORGANIZACIÓN:** EN EL MOMENTO EN EL QUE SE ELABORAN LAS POLÍTICAS DE SEGURIDAD DE LA EMPRESA ES NECESARIO REALIZAR UNA EVALUACIÓN DE LOS RIESGOS JUSTIFICADA CON INDICADORES Y DATOS. **LOS IDS PERMITEN CONOCER ESTOS RIESGOS Y DOCUMENTARLOS**, DE MODO QUE LA POLÍTICA DE SEGURIDAD ESTABLECIDA Y LAS DECISIONES QUE SE TOMEN EN RELACIÓN A ESTA ESTARÁN CORRECTAMENTE JUSTIFICADAS.

## 4. ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS

### VENTAJAS

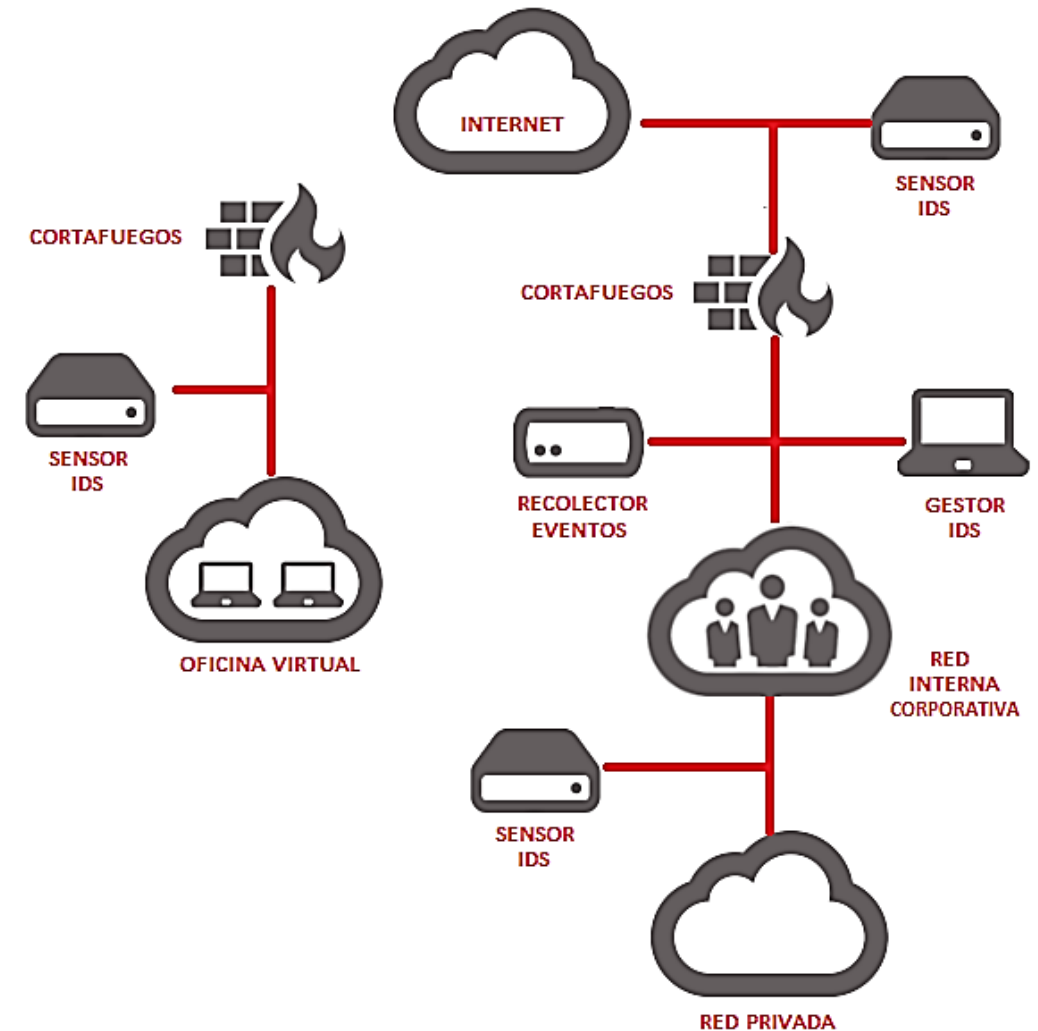
- **APORTAN INFORMACIÓN ÚTIL SOBRE LAS INTRUSIONES Y ATAQUES QUE SE PRODUCEN EN EL EQUIPO:** APARTE DE BLOQUEAR LOS ATAQUES E INTENTOS DE ATAQUE DEL SISTEMA, LOS IDS TAMBIÉN **RECOGEN INFORMACIÓN ÚTIL** DE ESTOS ATAQUES **QUE PUEDE UTILIZARSE COMO PRUEBA DE DELITO** EN EL MOMENTO DE QUERER EMPRENDER ACCIONES LEGALES.

## 4. ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS

### ARQUITECTURA DE LOS IDS

HAY VARIAS ARQUITECTURAS DE IDS Y NO HAY NINGUNA DE ELLAS QUE SE UTILICE DE MODO ESTÁNDAR, LO QUE PROVOCA QUE DISTINTAS TENGAN DIFICULTADES PARA INTEROPERAR ENTRE SÍ.

NO OBSTANTE, HAY CIERTAS PECULIARIDADES COMUNES EN LAS DISTINTAS ARQUITECTURAS DE IDS:



## **4. ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS**

### **ARQUITECTURA DE LOS IDS**

#### **PECULIARIDADES COMUNES:**

- **LA FUENTE DE RECOGIDA DE DATOS.** LAS FUENTES PUEDEN SER LOGS, DISPOSITIVOS DE RED O EL MISMO SISTEMA DE INFORMACIÓN.
- **LAS REGLAS QUE DEFINEN LOS PATRONES Y DIRECTRICES** PARA DETECTAR LAS ANOMALÍAS DE SEGURIDAD DE UN SISTEMA.
- **LOS FILTROS QUE COMPARAN LOS DATOS O LOS LOGS** QUE SE HAN OBTENIDO CON LOS PATRONES DEFINIDOS EN LAS REGLAS.
- **LOS DETECTORES DE LOS EVENTOS ANORMALES** QUE SUCEDEN EN EL TRÁFICO DE LA RED.
- **EL SISTEMA QUE GENERA LOS INFORMES Y LAS ALARMAS** EN CASO DE ENCONTRAR ALGUNA INTRUSIÓN O ATAQUE.

## **4. ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS**

**ARQUITECTURA DE LOS IDS. CIDF (COMMON INTRUSION DETECTION FRAMEWORK)**  
FUE PROMOVIDA POR LA AGENCIA FEDERAL DE ESTADOS UNIDOS DARPA  
(DEFENSE ADVANCED RESEARCH PROJECTS AGENCY) Y, AUNQUE NO  
LOGRÓ ESTABLECERSE COMO UN ESTÁNDAR, DETERMINÓ UN MODELO Y  
UN VOCABULARIO GENERAL PARA TRATAR LAS INTRUSIONES.

ESTA ARQUITECTURA CONTEMPLA CUATRO TIPOS BÁSICOS DE EQUIPOS:

- **EQUIPOS GENERADORES DE EVENTOS O EQUIPOS E**
- **ANALIZADORES DE EVENTOS O EQUIPOS A**
- **BASE DE DATOS DE EVENTOS O EQUIPOS D**
- **EQUIPOS DE RESPUESTA O EQUIPOS R**



## 4. ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS

ARQUITECTURA DE LOS IDS. **CIDF (COMMON INTRUSION DETECTION FRAMEWORK)**

**EQUIPOS GENERADORES DE EVENTOS O EQUIPOS E**

EQUIPOS CUYA FUNCIÓN PRINCIPAL ES LA *DETECCIÓN DE EVENTOS Y LA EMISIÓN DE INFORMES*.

**ANALIZADORES DE EVENTOS O EQUIPOS A**

EQUIPOS QUE RECIBEN LOS INFORMES EMITIDOS Y *SE ENCARGAN DE REALIZAR LOS ANÁLISIS PERTINENTES*.

## 4. ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS

### ARQUITECTURA DE LOS IDS. **CIDF (COMMON INTRUSION DETECTION FRAMEWORK)**

#### BASE DE DATOS DE EVENTOS O EQUIPOS D

COMPONENTES DE BASES DE DATOS QUE *PERMITEN VER EL HISTORIAL DE LOS EVENTOS SUCEDIDOS EN EL SISTEMA.*

#### EQUIPOS DE RESPUESTA O EQUIPOS R

OBTIENEN LOS DATOS DE LOS DEMÁS TIPOS DE EQUIPOS (E, A Y D) Y *RESPONDEN A LOS EVENTOS SUCEDIDOS EN EL SISTEMA.*

## 4. ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS

ARQUITECTURA DE LOS IDS. **CISL (COMMON INTRUSION SPECIFICATION LANGUAGE)** SURGE POR LA NECESIDAD DE UNIR LOS CUATRO TIPOS DE EQUIPOS QUE SE DEFINIERON EN LA ARQUITECTURA CIDEF. EN ESTA ARQUITECTURA DEBEN PODER TRANSMITIRSE LOS SIGUIENTES TIPOS DE INFORMACIÓN:

- INFORMACIÓN DE EVENTOS EN GRUPO
- RESULTADOS DE LOS ANÁLISIS
- PRESCRIPCIONES DE RESPUESTAS

## 4. ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS

### ARQUITECTURA DE LOS IDS. CISL (COMMON INTRUSION SPECIFICATION LANGUAGE) INFORMACIÓN DE EVENTOS EN GRUPO

UNE LOS EQUIPOS C Y A DEFINIDOS EN LA ARQUITECTURA CIDF. *PROPORCIONA INFORMACIÓN SOBRE EL TRÁFICO DE RED DEL SISTEMA Y SOBRE LA AUDITORÍA DE REGISTROS.*

### RESULTADOS DE LOS ANÁLISIS

UNE LOS EQUIPOS A Y D Y *FACILITA INFORMACIÓN COMO LAS CARACTERÍSTICAS DE LAS ANOMALÍAS SUCEDIDAS EN EL SISTEMA Y DE LOS ATAQUES QUE SE HAN DETECTADO.*

### PRESCRIPCIONES DE RESPUESTAS

UNE LOS EQUIPOS A Y R Y *SE ENCARGA DE DETENER CIERTAS ACTIVIDADES Y DE MODIFICAR LOS PARÁMETROS DE SEGURIDAD DE COMPONENTES PARA RESPONDER A POSIBLES ATAQUES.*

## 4. ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS

### ARQUITECTURA DE LOS IDS. **AUSCERT (CERT AUSTRALIANO)**

LA ARQUITECTURA **AUSCERT** ES MUCHO **MÁS SIMPLE** QUE LAS DOS ANTERIORES (**CIDF Y CISL**) Y FACILITA EN UNAS POCAS LÍNEAS UN INFORME EN UNA BASE DE DATOS DE UN INCIDENTE SUCEDIDO EN EL SISTEMA.

LA VENTAJA PRINCIPAL DE ESTA **ARQUITECTURA** ES QUE ES **MUY SENCILLA** PARA CONSTRUIRLA Y ANALIZARLA.

ESO SÍ, EN EL MOMENTO EN EL QUE SE REQUIERA UNA INFORMACIÓN DETALLADA DE LOS EVENTOS E INCIDENCIAS SUCEDIDOS EN EL SISTEMA SE DEBERÁ TENER EN CUENTA QUE **AUSCERT** ES MUY LIMITADA YA QUE SU NIVEL DE DETALLE ES MÍNIMO.

## 4. ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS

ARQUITECTURA DE LOS IDS. **IDWG (INTRUSION DETECTION WORKING GROUP)** PROPONE UN NUEVO FORMATO (**IDEF O INTRUSION DETECTION EXCHANGE FORMAT**) CUYA FUNCIÓN PRINCIPAL ES LA *DEFINICIÓN DE FORMATOS Y PROCEDIMIENTOS DE INTERCAMBIO DE INFORMACIÓN ENTRE LOS DIVERSOS SUBSISTEMAS DEL IDS.*

FACILITA EL INTERCAMBIO DE INFORMACIÓN ACERCA DE LOS INCIDENTES DE SEGURIDAD. SE DISTINGUEN TRES MÓDULOS DISTINTOS:

- **SENSOR**
- **ANALIZADOR**
- **MANAGER**

## 4. ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS

ARQUITECTURA DE LOS IDS. **IDWG (INTRUSION DETECTION WORKING GROUP)** CON ESTOS TRES MÓDULOS DE LA ARQUITECTURA IDWG SE OBTIENEN RESULTADOS COMO LOS SIGUIENTES:

- **LENGUAJE COMÚN** QUE DESCRIBE EL FORMATO DE LOS DATOS.
- **DOCUMENTOS QUE RECOGEN LOS DISTINTOS REQUERIMIENTOS FUNCIONALES** DE ALTO NIVEL QUE PERMITEN LA COMUNICACIÓN ENTRE LOS IDS Y ENTRE LOS IDS Y SUS SISTEMAS DE GESTIÓN DE INCIDENTES.
- **IDENTIFICACIÓN Y DEFINICIÓN DE LOS PROTOCOLOS MÁS APROPIADOS** PARA LA COMUNICACIÓN ENTRE IDS Y PARA EL ESTABLECIMIENTO DEL FORMATO DE LOS DATOS.



## 4. ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS

### ARQUITECTURA DE LOS IDS

Tipo de arquitectura IDS	Características
CIDF (Common Intrusion Detection Framework)	Consta de generador, analizador y base de datos de eventos además de unidades de respuesta ante la aparición de incidentes. Tuvo escasa aceptación en el mercado.
CISL (Common Intrusion Specification Language)	Une los distintos equipos que forman parte de la arquitectura CIDF y facilita información sobre información de eventos en bruto, resultados de los análisis y prescripciones de respuestas.
AusCERT	Arquitectura simple que facilita la información de las incidencias en muy pocas líneas. Es muy limitada si se pretende obtener información detallada de las incidencias.
IDWG (Intrusion Detection Working Group)	Facilita el intercambio de información sobre los incidentes de seguridad y permite definir los protocolos y formatos de intercambio de información entre los IDS.

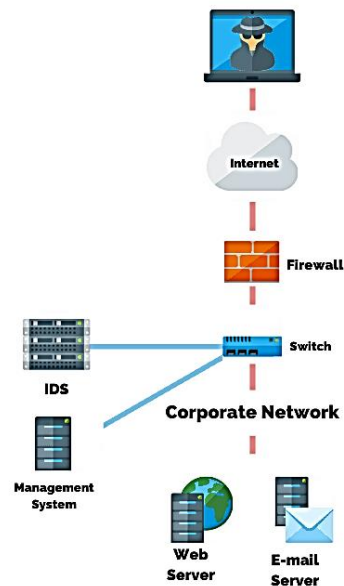
# CONTENIDOS

1. INTRODUCCIÓN
2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN
3. IDENTIFICACIÓN Y CARACTERIZACIÓN DE LOS DATOS DE FUNCIONAMIENTO DEL SISTEMA
4. ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS
5. **RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD**
6. CRITERIOS DE SEGURIDAD PARA EL ESTABLECIMIENTO DE LA UBICACIÓN DE LOS IDS/IPS

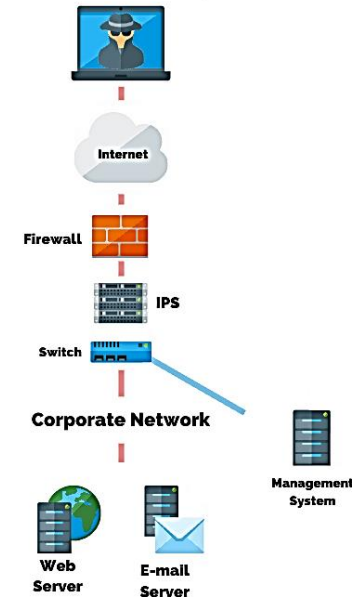
## 5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD

SE VAN A DESCRIBIR LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD DISTINGUIENDO ENTRE LOS **SISTEMAS DE DETECCIÓN DE INTRUSIONES (IDS)** Y LOS **SISTEMAS DE PREVENCIÓN DE INTRUSIONES (IPS)**.

Intrusion Detection System (IDS)



Intrusion Prevention System (IPS)



VS

## **5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD**

### **TIPOS DE IDS**

LOS IDS SE PUEDEN CLASIFICAR ATENDIENDO A SU **UBICACIÓN**:

- **IDS BASADOS EN RED (NIDS)**
- **IDS BASADOS EN HOST (HIDS)**

LOS IDS SE PUEDEN CLASIFICAR ATENDIENDO A SU **FUNCIONALIDAD FUNDAMENTAL**:

- **IDS DE DETECCIÓN DE ABUSOS O FIRMAS.**
- **IDS DE DETECCIÓN DE ANOMALÍAS.**

## 5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD

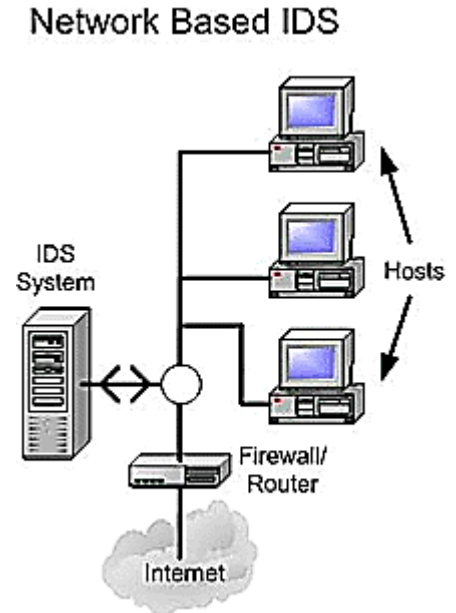
### TIPOS DE IDS. IDS BASADOS EN RED (NIDS)

LA GRAN MAYORÍA DE LOS IDS ESTÁN BASADOS EN RED.

**DETECTAN LOS ATAQUES MEDIANTE LA CAPTURA Y ANÁLISIS DE LOS PAQUETES DE LA RED. SE ENCARGAN DE BUSCAR PATRONES QUE SUPONGAN ALGÚN TIPO DE ATAQUE.**

ANALIZAN EL TRÁFICO EXAMINANDO PAQUETES PARA BUSCAR OPCIONES NO PERMITIDAS Y DISEÑADAS PARA NO SER DETECTADAS POR LOS CORTAFUEGOS.

EMITE ALERTAS CUANDO HAY INTENTOS DE ACCESO O ALGUNA VULNERABILIDAD DEL SISTEMA.



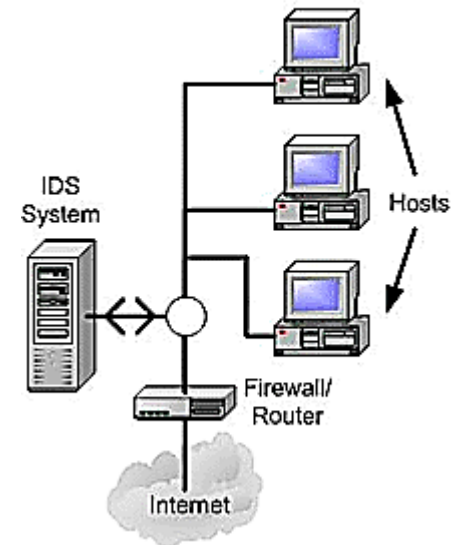
## 5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD

### TIPOS DE IDS. IDS BASADOS EN RED (NIDS)

SU FUNCIONAMIENTO CONSISTE EN:

- **UNOS SENSORES O AGENTES** QUE *SE SITÚAN EN VARIOS PUNTOS DE LA RED PARA MONITORIZAR EL TRÁFICO BUSCANDO TRÁFICO SOSPECHOSO*. LO HABITUAL ES QUE ESTOS SENSORES ANALICEN LOS PAQUETES EN MODO OCULTO PARA NO SER DESCUBIERTOS.
- **UNA CONSOLA** QUE *RECIBE LAS ALARMAS EMITIDAS POR LOS SENSORES Y QUE, ATENDIENDO AL TIPO DE ALARMA, PRODUCIRÁ ALGÚN TIPO DE RESPUESTA*.

Network Based IDS



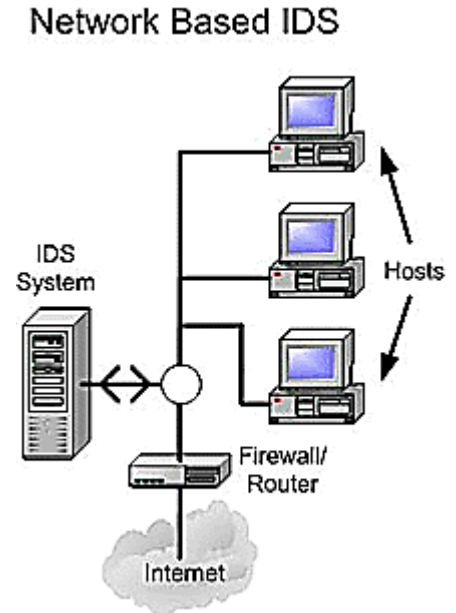


## 5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD

### TIPOS DE IDS. IDS BASADOS EN RED (NIDS)

#### VENTAJAS

- DETECTAN ACCESOS NO DESEADOS EN LA RED.
- NO REQUIEREN LA UTILIZACIÓN DE UN SOFTWARE ADICIONAL EN LOS SERVIDORES PARA PODER FUNCIONAR.
- SON SISTEMAS DE FÁCIL INSTALACIÓN Y ACTUALIZACIÓN.
- TIENEN UN BAJO IMPACTO EN LA RED AL NO INTERVENIR EN SUS OPERACIONES HABITUALES.
- PUEDEN MONITORIZAR REDES DE GRANDES DIMENSIONES SIEMPRE QUE HAYA CAPACIDAD SUFICIENTE PARA ANALIZAR TODO SU TRÁFICO.





## 5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD

### TIPOS DE IDS. **IDS BASADOS EN RED (NIDS)** DESVENTAJAS

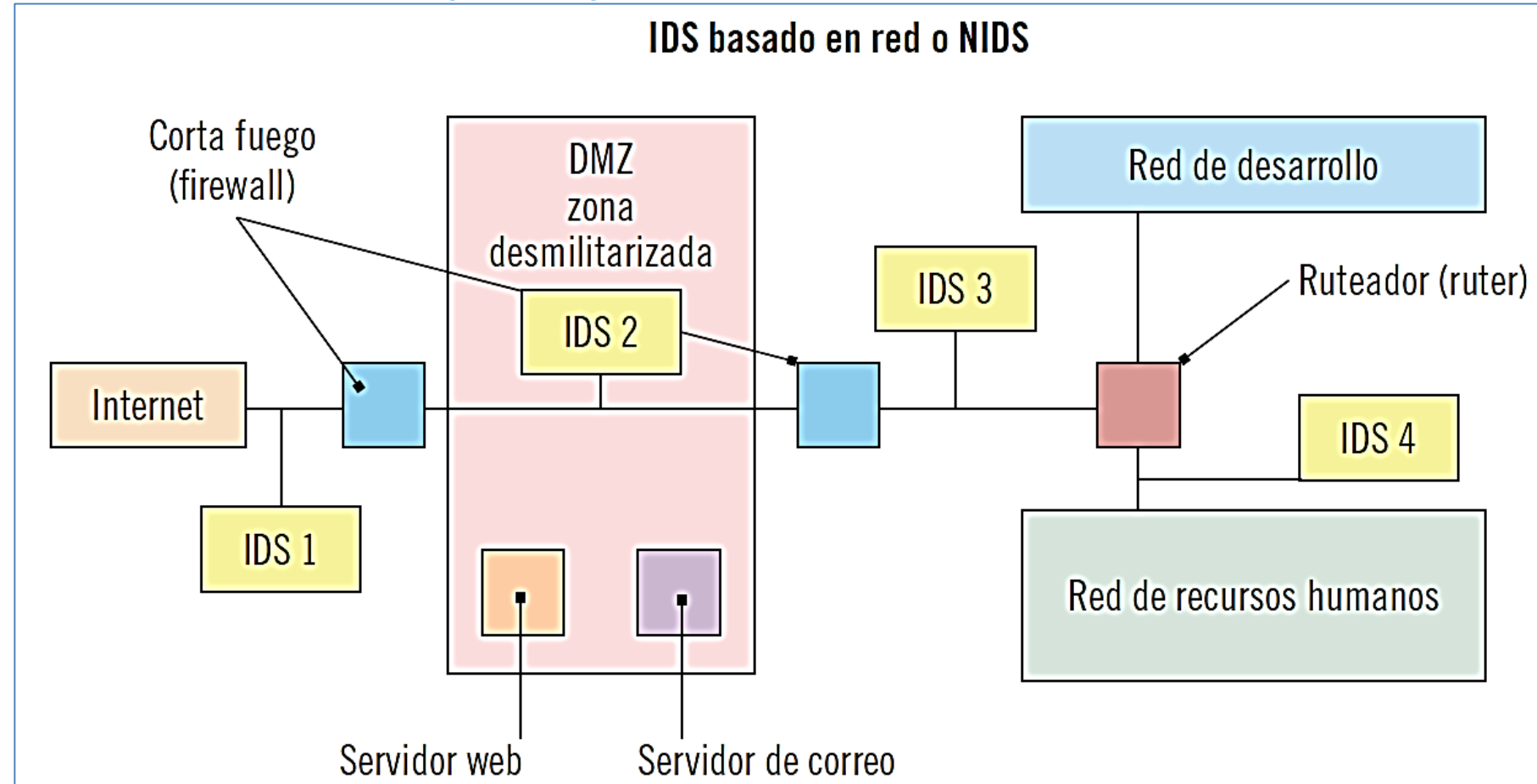
- A PESAR DE PODER MONITORIZAR REDES GRANDES PUEDEN PRESENTAR **DIFICULTADES EN SU PROCESAMIENTO Y FALLAR EN EL RECONOCIMIENTO DE ATAQUES** PRODUCIDOS EN MOMENTOS DE ELEVADO NIVEL DE TRÁFICO DE RED
- TIENEN **DIFICULTADES PARA DETECTAR LOS ATAQUES CON INFORMACIÓN CIFRADA**
- **SE LIMITAN A DETECTAR LOS ATAQUES LANZADOS**, INDEPENDIENTEMENTE DE SI HAN TENIDO ÉXITO O NO, LO QUE IMPLICA QUE ANTE CADA ATAQUE DETECTADO LOS ADMINISTRADORES DEBEN ANALIZARLO UNO A UNO PARA COMPROBAR EL ÉXITO O FRACASO DEL MISMO
- PUEDEN PRESENTAR **PROBLEMAS CUANDO TIENEN QUE DETECTAR ATAQUES QUE VIAJAN EN PAQUETES FRAGMENTADOS**

## 5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD

### TIPOS DE IDS. IDS BASADOS EN RED (NIDS)

#### EJEMPLO DE NIDS

HAY IDS (SENSORES) SITUADOS EN VARIOS PUNTOS DE LA RED QUE SE ENCARGAN DE MONITORIZAR EL TRÁFICO QUE HAY ENTRE ELLOS. DE ESTE MODO SE PUEDEN DETECTAR LAS INCIDENCIAS SUCEDIDAS A LO LARGO DE TODA LA RED DEL SISTEMA Y REACCIONAR ANTE ELLAS.



## 5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD

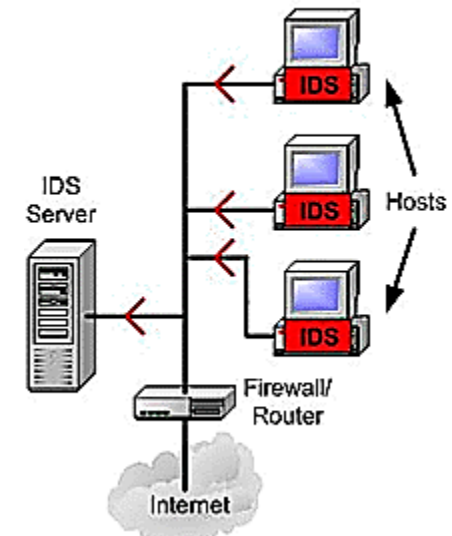
### TIPOS DE IDS. IDS BASADOS EN HOST (HIDS)

UN EQUIPO INFORMÁTICO, ANALIZANDO SU TRÁFICO PARA COMPROBAR SI HA HABIDO ALGÚN TIPO DE ALTERACIÓN DE LOS ARCHIVOS DEL SISTEMA OPERATIVO Y PARA LOCALIZAR ACTIVIDADES SOSPECHOSAS.

FUERON EL PRIMER TIPO DE IDS DESARROLLADO E IMPLEMENTADO.

AL TRABAJAR SOBRE UN EQUIPO Y NO SOBRE EL TRÁFICO DE LA RED OFRECE UNA **GRAN PRECISIÓN** EN EL ANÁLISIS DE LAS ACTIVIDADES, PUDIENDO DETECTAR DE UN MODO EXACTO LOS PROCESOS Y USUARIOS QUE HAN ESTADO INVOLUCRADOS EN UN ATAQUE EN CONCRETO DENTRO DE UN SISTEMA OPERATIVO.

Host Based IDS

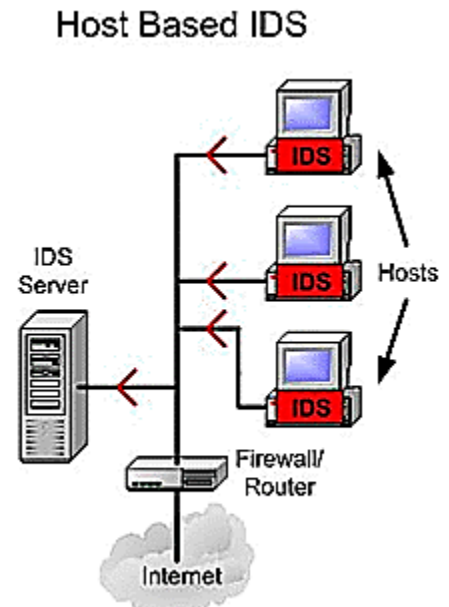


## 5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD

### TIPOS DE IDS. IDS BASADOS EN HOST (HIDS)

INFORMAN DEL RESULTADO DEL ATAQUE EN CUANTO A SU ÉXITO O FRACASO.

TAMBIÉN **MONITORIZAN LOS FICHEROS Y LOS PROCESOS DEL SISTEMA** ATACADO PARA UNA MEJOR DETECCIÓN Y REPUESTA ANTE LOS ATAQUES.



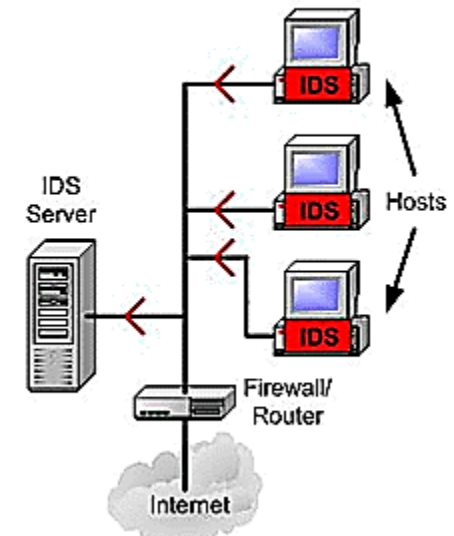
## 5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD

### TIPOS DE IDS. **IDS BASADOS EN HOST (HIDS)**

SUS FUNCIONALIDADES PRINCIPALES SE CONCRETAN EN:

- **ANÁLISIS DEL TRÁFICO SOBRE UN SERVIDOR O SOBRE UN EQUIPO CONCRETO.**
- **DETECCIÓN DE LOS INTENTOS DE ACCESO, TANTO FALLIDOS COMO EXITOSOS.**
- **DETECCIÓN DE LAS MODIFICACIONES REALIZADAS EN ARCHIVOS CRÍTICOS.**

Host Based IDS



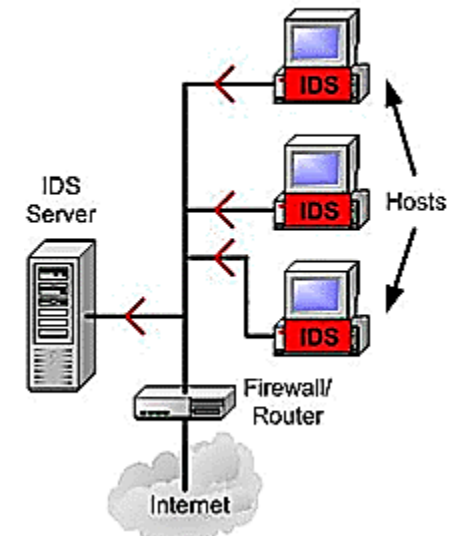
## 5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD

### TIPOS DE IDS. IDS BASADOS EN HOST (HIDS)

#### VENTAJAS

- **DETECTAN ATAQUES QUE NO PUEDEN DESCUBRIR LOS NIDS** AL PODER MONITORIZAR LOS EVENTOS LOCALES DEL EQUIPO O HOST.
- PUEDEN OPERAR Y **DETECTAR ATAQUES ANTE DATOS CIFRADOS** QUE CIRCULAN POR LA RED PORQUE ANALIZAN LOS DATOS EN EL HOST DE ORIGEN ANTES DE SER CIFRADOS O LOS DATOS EN EL HOST DE DESTINO UNA VEZ YA HAN SIDO DESCIFRADOS.
- **FACILITAN INFORMACIÓN SOBRE EL ÉXITO O FRACASO DE LOS INTENTOS DE ATAQUE.**

Host Based IDS

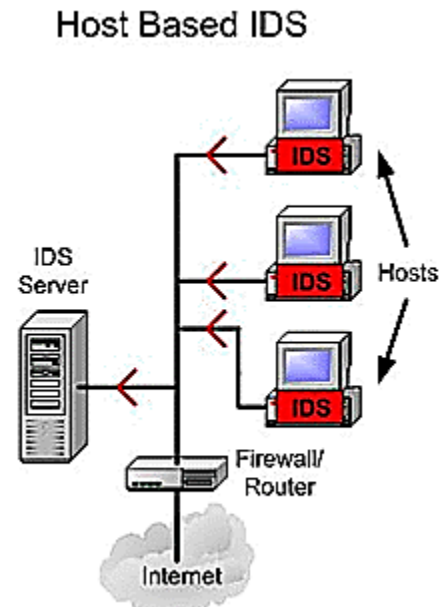




## 5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD

### TIPOS DE IDS. IDS BASADOS EN HOST (HIDS) DESVENTAJAS

- SUPONEN UN **COSTE MAYOR** QUE LOS NIDS YA QUE HAY QUE GESTIONARLOS Y CONFIGURARLOS EN CADA HOST.
- **NO SON ÚTILES** CUANDO SE **PRETENDE DETECTAR ATAQUES A TODA UNA RED**, SOLO ANALIZAN LOS PAQUETES DE RED QUE ENTRAN EN EL HOST EN EL QUE ESTÁN INSTALADO.
- SUPONEN UN **CONSUMO DE RECURSOS DEL HOST AL QUE MONITORIZAN**, LO QUE IMPLICA UNA DISMINUCIÓN DEL RENDIMIENTO DEL SISTEMA.
- LOS HIDS CORREN EL PELIGRO DE **SER DESHABILITADOS POR ALGUNOS DOS**.





## 5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD

### TIPOS DE IDS. **IDS DE DETECCIÓN DE ABUSOS O FIRMAS**

TIENEN COMO FUNCIONALIDAD PRINCIPAL **BUSCAR EVENTOS QUE COINCIDAN CON UN PATRÓN PREDEFINIDO O CON UNA FIRMA QUE DESCRIBA UN ATAQUE CONOCIDO.**

ENTRE LAS **VENTAJAS** DE ESTE TIPO DE IPS DESTACAN:

- **ELEVADO GRADO DE EFECTIVIDAD SIN GENERAR EN EXCESO FALSAS ALARMAS.**
- **RÁPIDO DIAGNÓSTICO DEL USO DE UN ATAQUE DETERMINADO.**

SIN EMBARGO, TAMBIÉN TIENE COMO **DESVENTAJA** LA CONSTANTE NECESIDAD DE **ACTUALIZACIÓN CONTINUA** PARA QUE LA DETECCIÓN DE LOS ABUSOS O FIRMAS SEA EFICAZ.

## 5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD

### TIPOS DE IDS. **IDS DE DETECCIÓN DE ANOMALÍAS**

ESTE TIPO DE IDS, EN LUGAR DE BUSCAR ABUSOS CONFORME A UNOS PATRONES, TIENE COMO FUNCIÓN PRINCIPAL **LA DETECCIÓN DE COMPORTAMIENTOS INUSUALES** QUE SUCEDAN EN UN HOST DE UNA RED. SUS **VENTAJAS** PRINCIPALES SON:

- LA ELEVADA **CAPACIDAD DE DETECTAR ATAQUES** DE LOS QUE **NO HAY UN CONOCIMIENTO DETERMINADO**.
- LA POSIBILIDAD DE **DEFINIR FIRMAS EN LA DETECCIÓN DE ABUSOS** CON LA INFORMACIÓN QUE OBTIENEN.

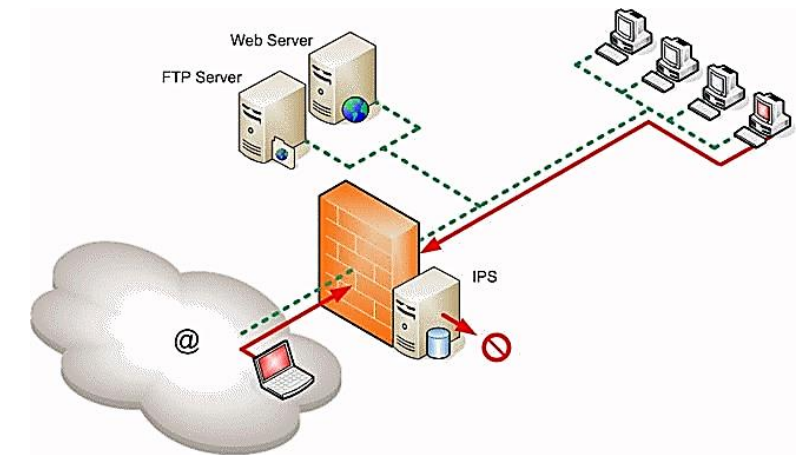
COMO **DESVENTAJAS**, ESTE TIPO DE IPS **GENERA UN ELEVADO NÚMERO DE FALSAS ALARMAS** (AL NO HABER NINGÚN PATRÓN DEFINIDO).

## 5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD

### TIPOS DE IPS

SE DESARROLLARON CON LA FINALIDAD DE MONITORIZAR EL TRÁFICO DE UNA RED EN TIEMPO REAL Y CONSEGUIR PREVENIR LAS INTRUSIONES AL SISTEMA.

SE CONSIDERAN UNA EVOLUCIÓN DE LOS SISTEMAS DE DETECCIÓN DE INTRUSIONES (IDS).

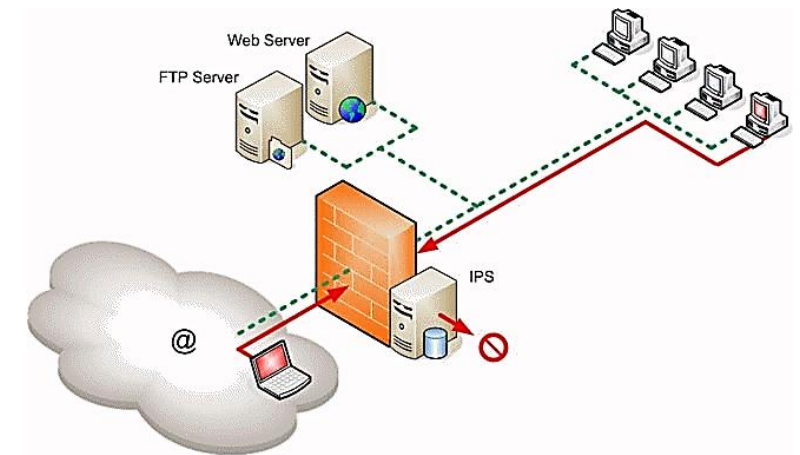


## 5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD

### TIPOS DE IPS

LOS IPS TRATAN DE PREVENIR QUE SE FILTRE CUALQUIER INTRUSIÓN:

EN CUANTO SE PRODUCE LA CAÍDA DE ALGÚN PAQUETE O SE DETECTA QUE ESTÁ DAÑADO O INCOMPLETO, **LA RED BLOQUEA LA TRANSMISIÓN DE ESTE PAQUETE CON EL FIN DE PREVENIR UN POSIBLE ATAQUE.**



## 5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD

### TIPOS DE IPS

LAS **CARACTERÍSTICAS** FUNDAMENTALES QUE TIENEN EN COMÚN LOS DISTINTOS TIPOS DE IPS SON LAS SIGUIENTES:

- TIENEN UNA **CAPACIDAD DE RESPUESTA AUTOMÁTICA** EN CUANTO SE PRODUCE UN INCIDENTE.
- **APLICAN FILTROS NUEVOS** CONFORME SE VAN DETECTANDO ATAQUES EN PROGRESO.
- **REDUCEN LAS FALSAS ALARMAS** DE ATAQUES PRODUCIDOS EN LA RED.
- **BLOQUEAN AUTOMÁTICAMENTE LOS ATAQUES** A LA RED EN TIEMPO REAL.
- **OPTIMIZAN EL RENDIMIENTO DEL TRÁFICO** DE LA RED AL BLOQUEAR DE UN MODO AUTOMÁTICO LOS ATAQUES.

## 5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD

### TIPOS DE IPS VENTAJAS

- OFRECEN UNA **PROTECCIÓN PREVENTIVA** ANTES DE QUE SE PRODUZCA EL ATAQUE.
- OFRECEN UNA **PROTECCIÓN Y DEFENSA COMPLETA** DE VARIOS TIPOS DE ATAQUES COMO: VULNERABILIDADES DEL SISTEMA, TRÁFICO DE RED, CÓDIGOS MALICIOSOS, INTRUSIONES, ETC.
- **OPTIMIZA LA SEGURIDAD Y LA EFICIENCIA** EN LA PREVENCIÓN DE INTRUSIONES Y/O ATAQUES A UNA RED O SISTEMA.
- SON **FÁCILES DE INSTALAR**, CONFIGURAR Y ADMINISTRAR.
- SON **ESCALABLES**, POR LO QUE SE PUEDEN IR ACTUALIZANDO SEGÚN LAS NECESIDADES DE LA ORGANIZACIÓN.
- EN COMPARACIÓN CON UN IDS REQUIEREN DE **MENOS INVERSIÓN** EN RECURSOS PARA ENTRAR EN FUNCIONAMIENTO.

## **5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD**

### **TIPOS DE IPS**

**LOS IPS SE PUEDEN DISTINGUIR EN TRES CATEGORÍAS ATENDIENDO A LA ACCIÓN QUE REALIZAN:**

- **IPS DE FILTRADO DE PAQUETES**
- **IPS DE BLOQUEO DE IP**
- **IPS CON ACCIÓN DE DECEPCIÓN**



## **5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD**

### **TIPOS DE IPS**

#### **IPS DE FILTRADO DE PAQUETES**

TIENEN COMO FUNCIÓN PRINCIPAL DETERMINAR EL TIPO DE TRÁFICO QUE PUEDE ENTRAR Y SALIR DE UN EQUIPO O SERVIDOR.

#### **IPS DE BLOQUEO DE IP**

ESTE TIPO DE IPS TIENE COMO FUNCIONALIDAD PRINCIPAL BLOQUEAR DIRECCIONES IP QUE PUEDAN SER CAUSANTES DE ALGÚN TIPO DE ATAQUE.

#### **IPS CON ACCIÓN DE DECEPCIÓN**

ESTÁN BASADOS EN LA DECEPCIÓN O EN EL ENGAÑO HACIA EL ATACANTE, DE MODO QUE CUANDO SE PRODUCE ALGÚN ATAQUE EL IPS REMITE AL ATACANTE INFORMACIÓN ERRÓNEA DEL HOST.

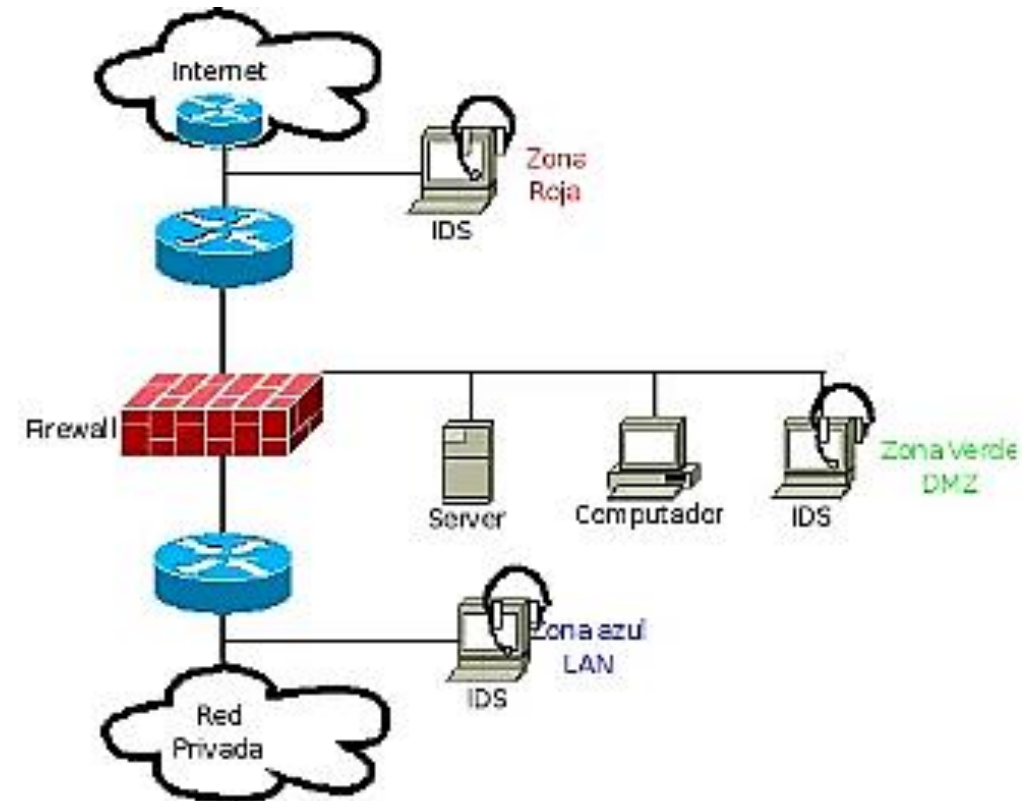
# CONTENIDOS

1. INTRODUCCIÓN
2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN
3. IDENTIFICACIÓN Y CARACTERIZACIÓN DE LOS DATOS DE FUNCIONAMIENTO DEL SISTEMA
4. ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS
5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD
6. CRITERIOS DE SEGURIDAD PARA EL ESTABLECIMIENTO DE LA UBICACIÓN DE LOS IDS/IPS

## 6. CRITERIOS DE SEGURIDAD PARA EL ESTABLECIMIENTO DE LA UBICACIÓN DE LOS IDS/IPS

UNA VEZ DECIDIDO EL TIPO DE IDS/IPS QUE SE QUIERE IMPLANTAR, UNA DE LAS **PREGUNTAS** MÁS IMPORTANTES QUE DEBEN REALIZARSE LAS ORGANIZACIONES ES **DÓNDE LOCALIZARLO**.

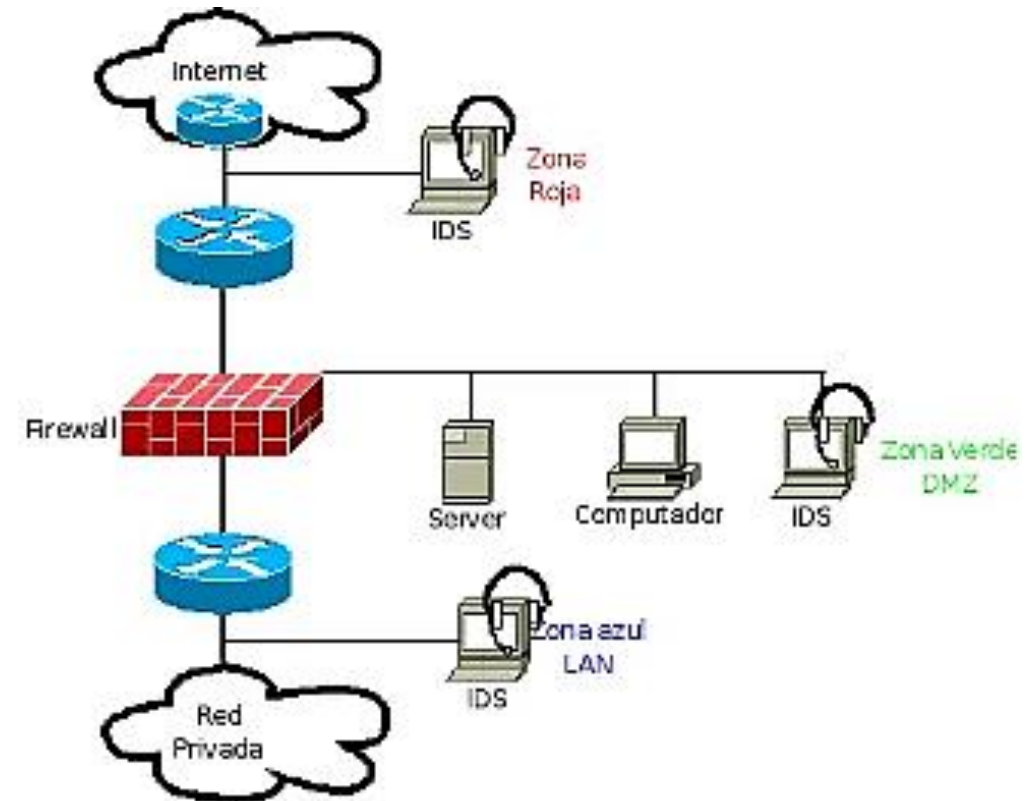
LA **UBICACIÓN** DE LOS SISTEMAS **IDS/IPS** DEPENDERÁN DEL EQUIPO QUE SE VA A UTILIZAR Y DEL SOFTWARE **IDS/IPS** QUE SE VA A IMPLANTAR.



## 6. CRITERIOS DE SEGURIDAD PARA EL ESTABLECIMIENTO DE LA UBICACIÓN DE LOS IDS/IPS

ATENDIENDO A LOS CRITERIOS DE SEGURIDAD PARA EL ESTABLECIMIENTO DE LA UBICACIÓN DE LOS IDS/IPS SE DISTINGUEN **TRES ZONAS** EN LAS QUE SE PUEDE UBICAR UN SISTEMA IDS/IPS:

- **ZONA ROJA**
- **ZONA VERDE**
- **ZONA AZUL**

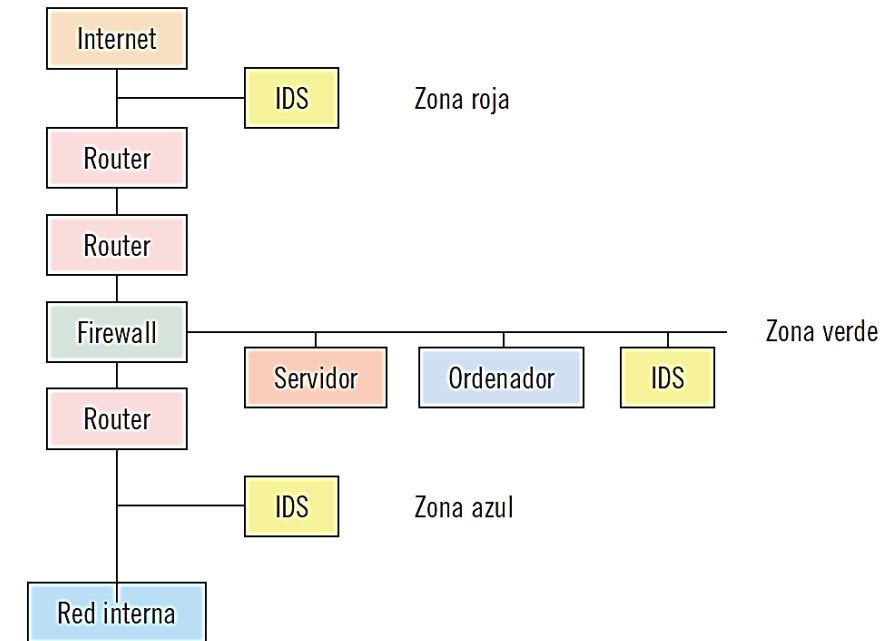


## 6. CRITERIOS DE SEGURIDAD PARA EL ESTABLECIMIENTO DE LA UBICACIÓN DE LOS IDS/IPS

### ZONA ROJA

ES UNA ZONA DE **RIESGO ELEVADO**. EN ESTA ZONA EL SISTEMA **IDS/IPS** DEBE CONFIGURARSE DE MODO QUE TENGA **POCA SENSIBILIDAD**, YA QUE OBSERVARÁ TODO EL TRÁFICO DE LA RED Y HABRÁ UNA ELEVADA POSIBILIDAD DE FALSAS ALARMAS.

Ubicación de los sistemas IDS/IPS

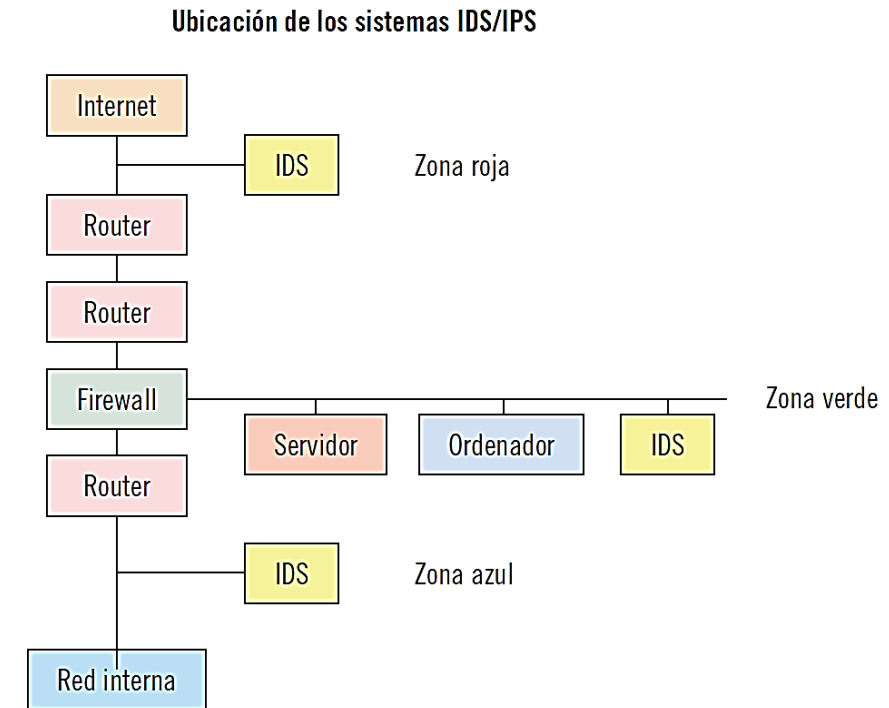


## 6. CRITERIOS DE SEGURIDAD PARA EL ESTABLECIMIENTO DE LA UBICACIÓN DE LOS IDS/IPS

### ZONA VERDE

ESTA ZONA TIENE **MENOS RIESGO** QUE LA ZONA ROJA Y EN ELLA EL **IDS/IPS** DEBE CONFIGURARSE DE MODO QUE TENGA **MAYOR SENSIBILIDAD** QUE EN LA ZONA ROJA PORQUE AQUÍ EL FIREWALL O CORTAFUEGOS REALIZA UN FILTRADO DE ACCESOS PREDEFINIDOS POR LA ORGANIZACIÓN.

EN ESTA ZONA HAY **MENOS FALSAS ALARMAS** QUE EN LA ZONA ROJA.

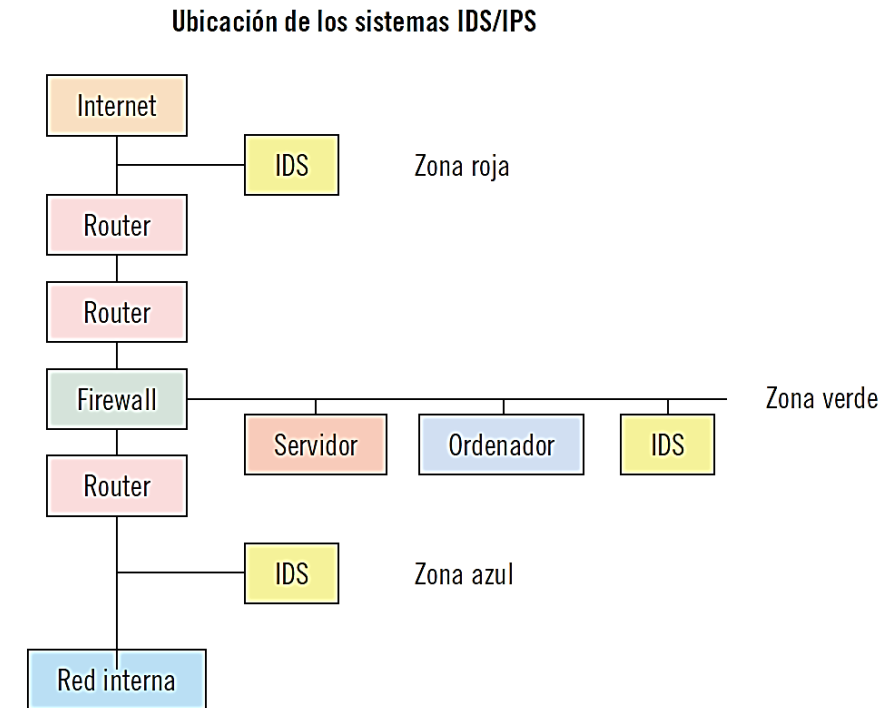


## 6. CRITERIOS DE SEGURIDAD PARA EL ESTABLECIMIENTO DE LA UBICACIÓN DE LOS IDS/IPS

### ZONA AZUL

ES LA ZONA *DE CONFIANZA*. EN ESTA ZONA *CUALQUIER TIPO DE ACCESO ANÓMALO* QUE HAYA EN LA RED HAY QUE CONSIDERARLO COMO ACCESO HOSTIL.

AL HABER UN NÚMERO INFERIOR DE ACCESOS TAMBIÉN **SE REDUCE CONSIDERABLEMENTE EL NÚMERO DE FALSAS ALARMAS**, POR LO QUE ES NECESARIO QUE CUALQUIER FALSA ALARMA DETECTADA POR EL SISTEMA **IDS/IPS** SEA ANALIZADA CON DETENIMIENTO.





# CONTENIDOS

1. INTRODUCCIÓN
2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN
3. IDENTIFICACIÓN Y CARACTERIZACIÓN DE LOS DATOS DE FUNCIONAMIENTO DEL SISTEMA
4. ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS
5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD
6. CRITERIOS DE SEGURIDAD PARA EL ESTABLECIMIENTO DE LA UBICACIÓN DE LOS IDS/IPS

## RESUMEN

UN **INCIDENTE DE SEGURIDAD** ES *CUALQUIER EVENTO QUE PUEDE AFECTAR A LA INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN*. EN OTROS TÉRMINOS, TAMBIÉN SE PUEDE DEFINIR COMO *UN EVENTO NO DESEADO QUE PUEDE COMPROMETER SIGNIFICATIVAMENTE LAS OPERACIONES DE UNA ORGANIZACIÓN Y AMENAZAR SU SEGURIDAD*.

HAY NUMEROSOS TIPOS DE INCIDENTES DE SEGURIDAD:

- ACCESOS NO AUTORIZADOS
- CÓDIGO MALICIOSO
- DENEGACIÓN DE SERVICIO
- INTENTOS DE INFORMACIÓN DE UN SISTEMA
- USO DEFICIENTE DE LOS RECURSOS TECNOLÓGICOS
- ETC.

PARA CADA UNO DE ELLOS LAS ORGANIZACIONES DEBEN TOMAR UNA SERIE DE MEDIDAS QUE LOS CORRIJAN, LOS PREVENGAN O, COMO MÍNIMO, LOS DETECTEN.

## RESUMEN

LA **GESTIÓN DE INCIDENTES** TIENE COMO OBJETIVO LA *ORGANIZACIÓN DE LOS RECURSOS PARA QUE ESTAS MEDIDAS SEAN APLICADAS DE UN MODO EFICIENTE.*

PARA ELLO SE PUEDE UTILIZAR EL *VISOR DE EVENTOS* DE **WINDOWS** O UNA *SERIE DE COMANDOS* EN **LINUX** QUE OFRECEN UNA VISIÓN DE LOS DIFERENTES ARCHIVOS DE REGISTRO DE EVENTOS.

UNA VEZ YA SE CONOCE CÓMO LOCALIZAR LOS EVENTOS QUE OCURREN EN UN SISTEMA, ES BÁSICA LA IMPLANTACIÓN DE **SISTEMAS DE PREVENCIÓN DE INTRUSIONES** O DE **SISTEMAS DE DETECCIÓN DE INTRUSIONES** COMO COMPLEMENTO A LAS DEMÁS MEDIDAS DE SEGURIDAD DE LA ORGANIZACIÓN.

UNA VEZ DECIDIDO EL SISTEMA IDS/IPS A IMPLANTAR, OTRA DE LAS DECISIONES FUNDAMENTALES QUE INFLUIRÁN EN EL SISTEMA DE SEGURIDAD DE UNA ORGANIZACIÓN ES ELEGIR **LA UBICACIÓN** DE ESTOS SISTEMAS. ATENDIENDO A *CRITERIOS DE ASUNCIÓN DE RIESGOS Y GRADO DE CONFIANZA.*

