Seguridad Informática

UNIDAD 1
Introducción

Modalidad Virtual

Docente: Ing. Francisco Álvarez Solís, MSc.

UNIDAD 1

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA O CIBERSEGURIDAD

Resumen CIA/Pilares de la Ciberseguridad

- **Confidencialidad**. Es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.
- **Integridad**. Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.
- **Disponibilidad**.
- Es la propiedad que busca mantener activos los servicios a los usuarios autorizados.

Ciberseguridad y Riesgo

Clasificación de la Seguridad Informática

- Seguridad Física
- Seguridad Lógica
- Seguridad Corporativa

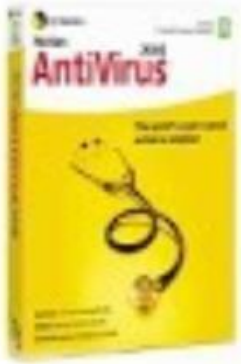
- Seguridad Activa
- Seguridad Pasiva
- De recuperación

Clasificación de la Seguridad Informática

FÍSICA

VS

LÓGICA



ACTIVA

VS

PASIVA

Seguridad Física

Aplicación de barreras físicas y procedimientos de control frente a amenazas físicas al hardware.

Seguridad Lógica

- Aplicación de barreras y procedimientos de control frente a amenazas al software. Está asociada a la autenticación del usuario en las aplicaciones que utiliza la organización.

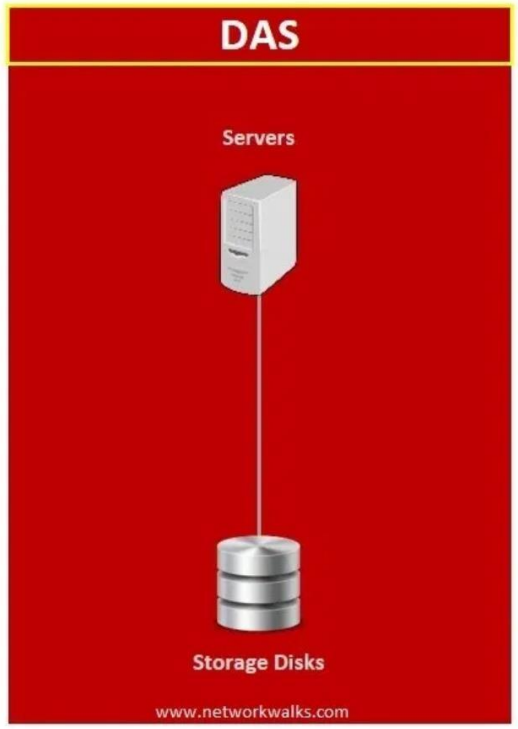
Seguridad Activa

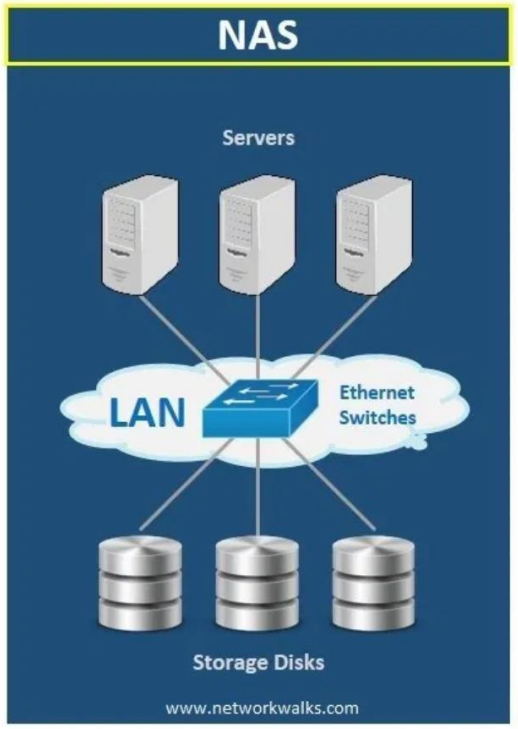
Firewall

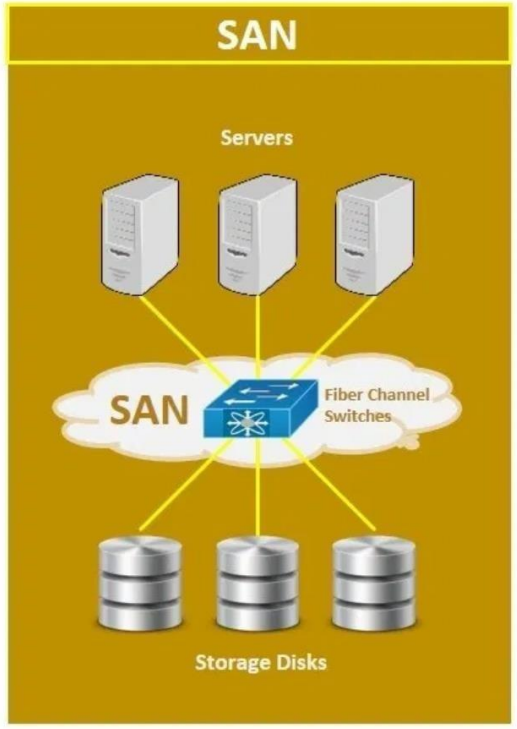
Es un sistema de seguridad para **bloquear accesos no autorizados a un ordenador** mientras sigue permitiendo la comunicación de tu ordenador con otros servicios autorizados. También se utilizan en redes de ordenadores, especialmente en intranets o redes locales. Se trata de una de las primeras medidas de seguridad que empezó a implementarse en los ordenadores tras el nacimiento de Internet.

Seguridad Pasiva

- Sistemas de Almacenamiento y respaldo de la Información







https://networkwalks.com/storage-types-das-nas-san/

Seguridad Física
Seguridad Lógica

Mejores Prácticas Seguridad Física

Tiene como objetivo evitar manipulaciones, extracciones o daños en las instalaciones

Para evitar que personal NO AUTORIZADO acceda a tus Data Center se recomienda tener:

- **Control de accesos:** Validar la entrada mediante tarjetas personales, sistemas biométricos o ambos.
- **Vigilancia 24/7:** Zonas exteriores bien vigiladas por el personal de seguridad.
- **Sistemas de videovigilancia y/o alarmas:** Apoyo con cámaras y alarmas para detectar lo antes posible intrusiones
- **Climatización de los servidores:** para el correcto funcionamiento del Data Center es importante la monitorización periódica de la temperatura y su climatización.
- **Protección contra incendios:** Otra medida de seguridad necesaria en los CPD ante uno de los actores más nocivos para los soportes físicos: el fuego.

Mejores Prácticas Seguridad Lógica

Tiene como objetivo ayudarte a estar protegido de posibles ciberataques.

Para evitar que los cibercriminales puedan acceder a tu Data Center necesitas tu **estrategia de seguridad** enfocada en la **prevención y detección de inicidentes,** por lo que se recomienda tener:

- **Gestión de riesgos.**
- **Segmentación de redes y equipos críticos.**
- **Firewalls físicos y virtuales** en caso de tener infraestructura híbrida o en la nube.
- **IPS** Sistema de Prevención de Intrusos.
- **Adecuación de permisos.**
- **Controles integrales de seguridad.**
- **Gestión de Acceso Privilegiado.**
- **DLP** Solución de Prevención de Pérdida de Datos.
- **DRP** Plan de Recuperación de Desastres.
- **SIEM** Correlacionador de Eventos.
- **Plan de Detección y Respuesta a Incidentes.**

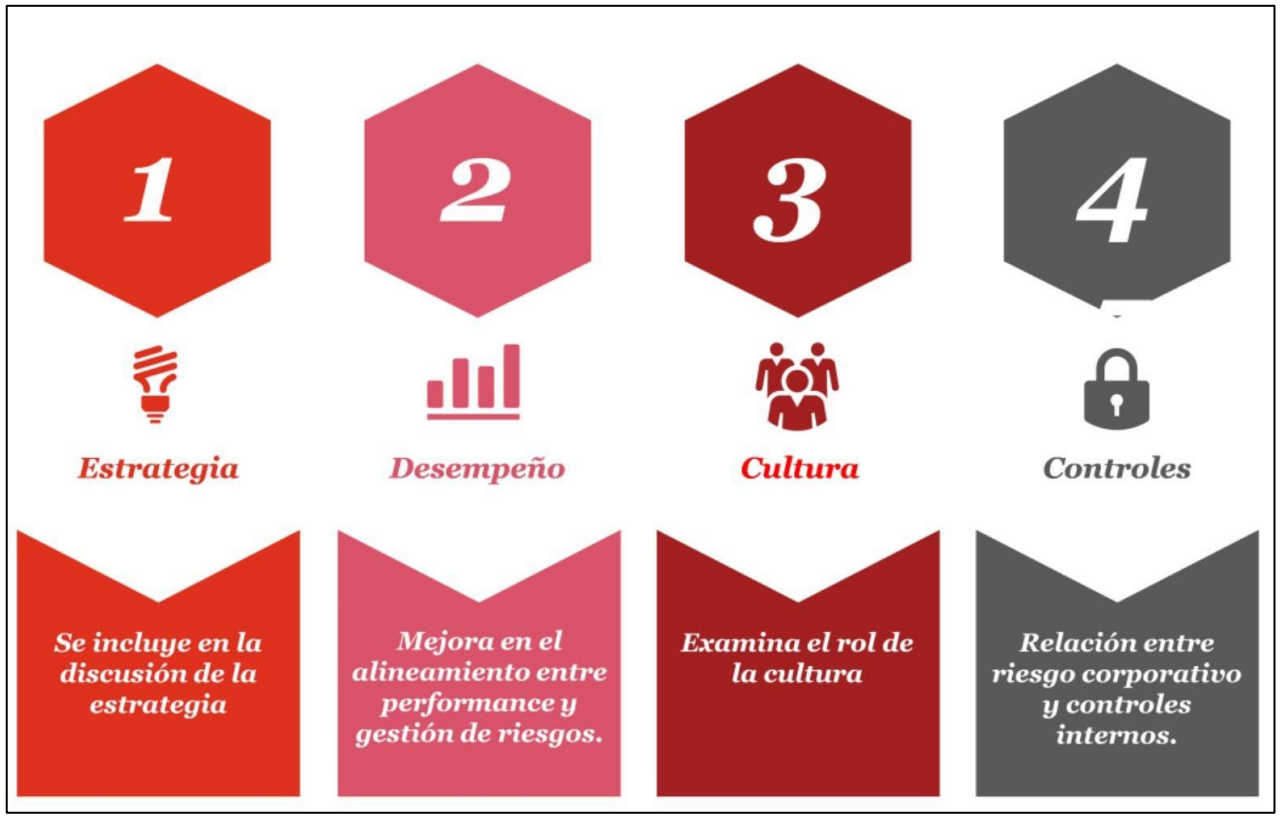
Seguridad Física
Control de Acceso físico

Sistemas de Videovigilancia y Alarmas

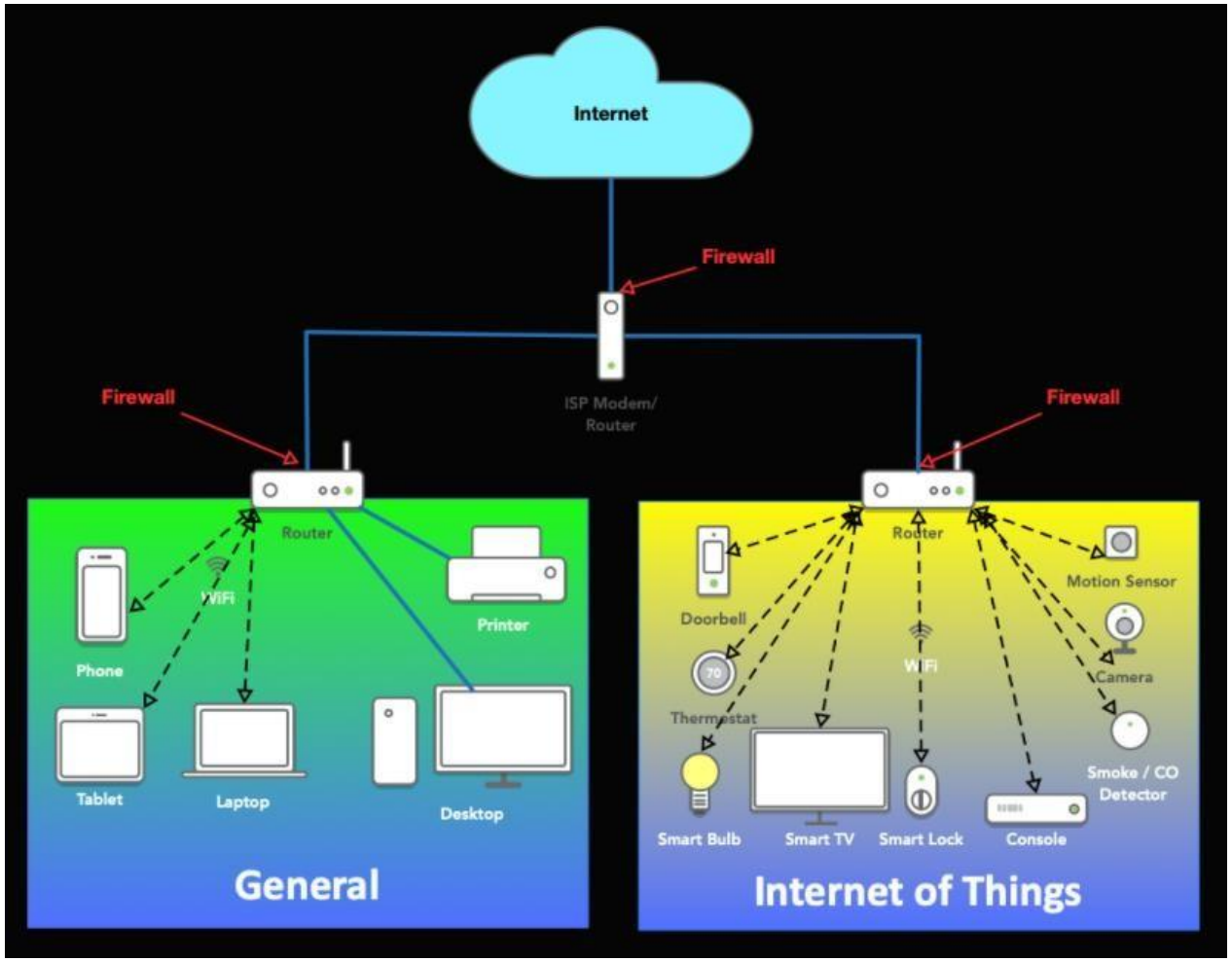
Sistemas de Climatización y Contra Incendios

Seguridad Lógica

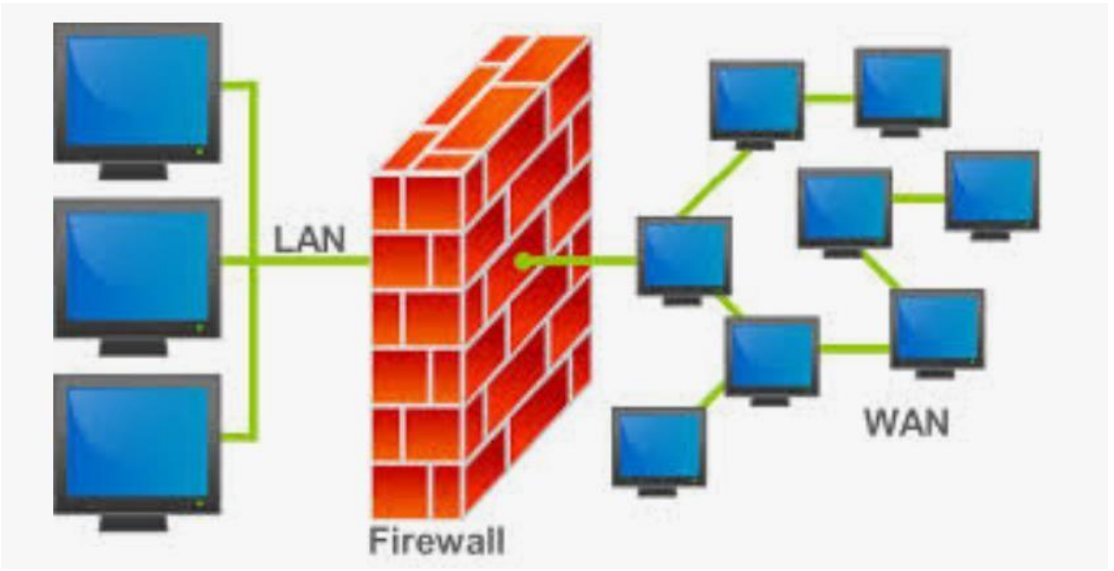
Gestión de Riesgo



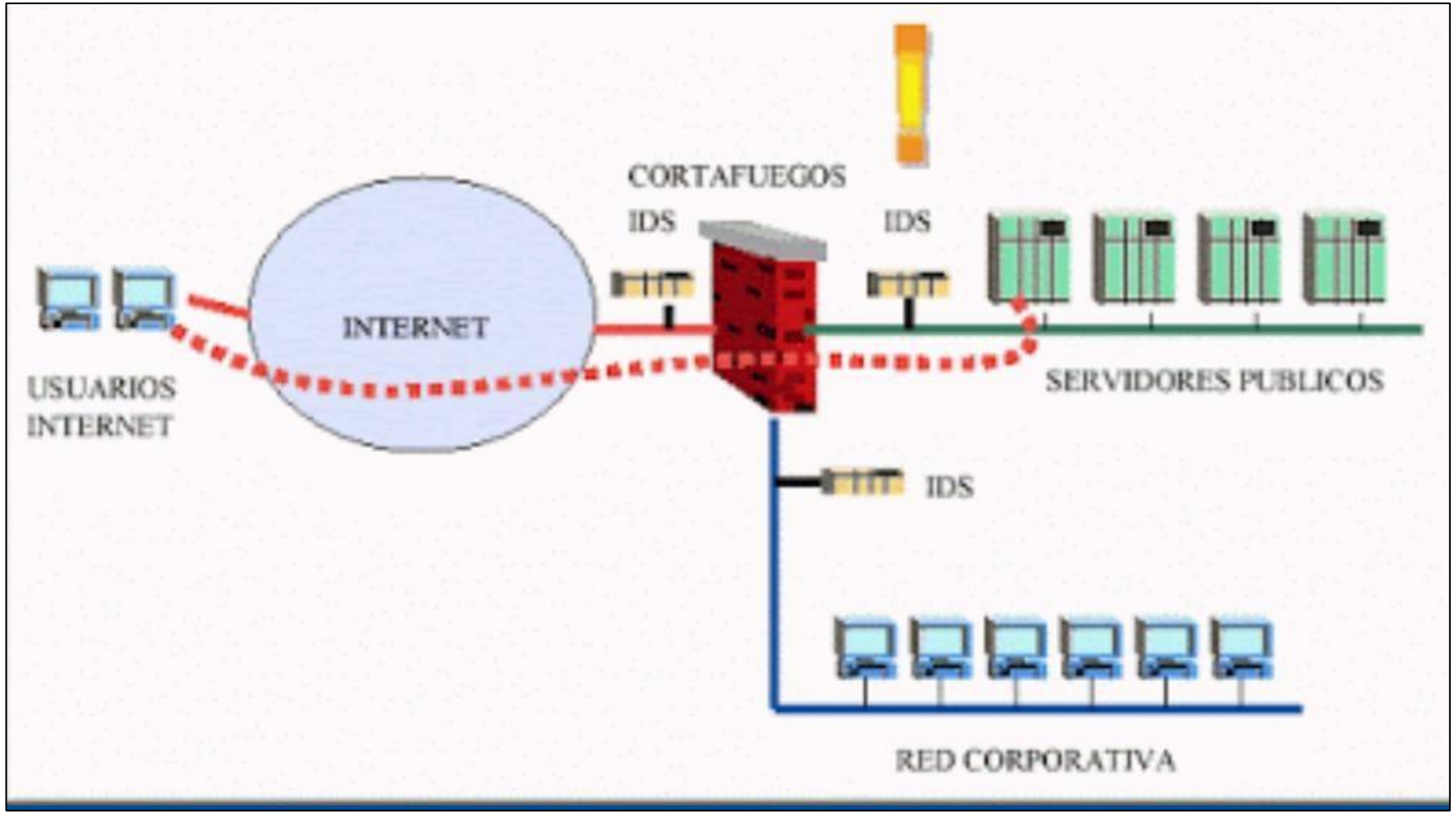
Seguridad Lógica
Segmentación de Redes



Seguridad Lógica
Firewalls

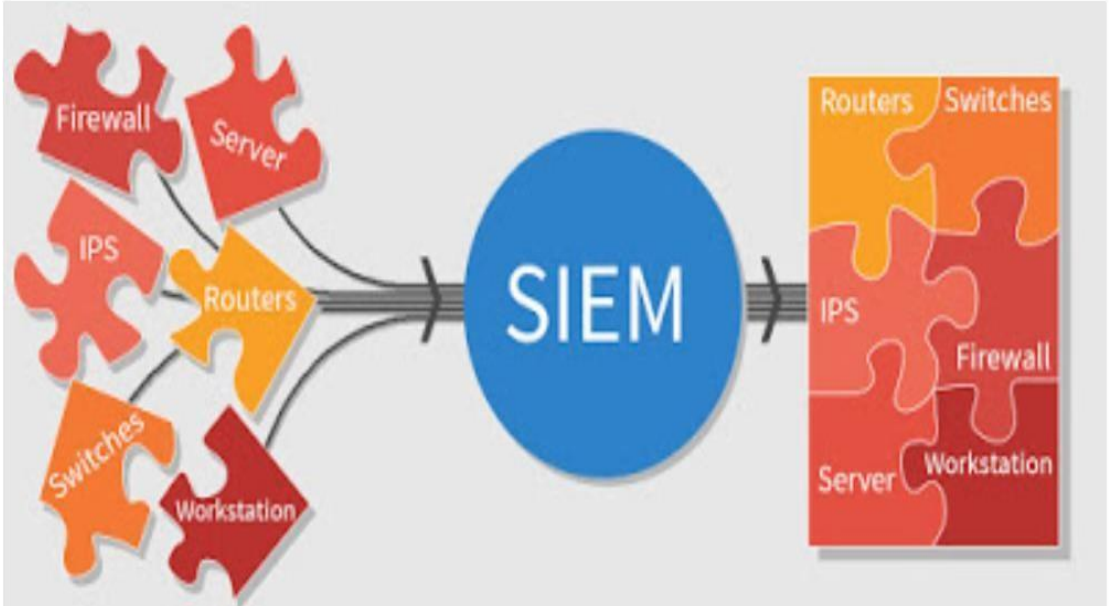


Seguridad Lógica
IDS - Sistema de detección de intrusiones



Seguridad Lógica
SIEM – Security Information and Event Management
Administración de Eventos y Seguridad de la Información

El término SIEM (Security Information and Event Management) fue acuñado en 2005 en la consultora Gartner y viene de la conjunción de dos términos que algunos usan indistintamente y otros procuran separar: SIM (Security Information Management) y SEM (Security Event Management), ambos para referirse al análisis en tiempo real de alertas de seguridad generadas en la red o en aplicaciones.



Seguridad Corporativa

Seguridad político-corporativa: formada por los aspectos de seguridad relativos a política general de la organización, legislación aplicable, normativa, procedimientos y convenciones internas aplicables.