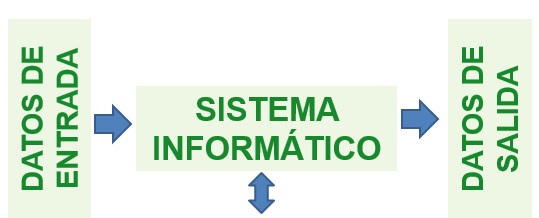
**TEMA 1. INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA**

# Sistema Informático



Conjunto de elementos técnicos, humanos y organizativos, debidamente relacionados a fin de alcanzar un objetivo concreto empleando la informática como herramienta para procesar DATOS.

### Elementos

* **Técnicos**: Software (SO, App), Hardware, Telecomunicaciones, etc
* **Humanos**: Administradores, Operadores, Usuarios, etc
* **Organizativos**: Planes, Políticas, Normas, Procedimientos, etc.

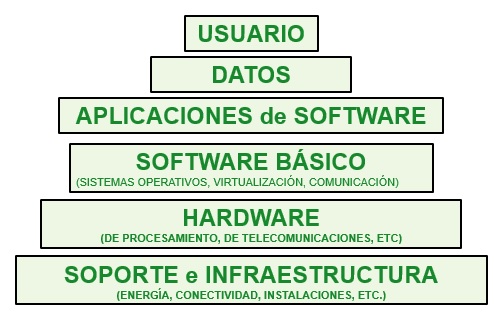
### Propiedades de un sistema informático

* Tiene funciones específicas que cumplir: SERVICIOS.
* Tiene capacidades limitadas: Acceso, Proceso, ...
* Tiene recursos limitados.
* Depende e interactúa con otros Sistemas no informáticos: humanos, mecánicos, eléctricos, etc.
* Existe una posibilidad “finita” de fallo.
* No infalible. !FALLARÁ!
* Tiene posibilidad “real” de tener errores embebidos y hacer lo que no debe. (SW).
* Requiere actualización ante cambios del ambiente

### Clasificación de un sistema informático

* **En tiempo real:** Gestionan procesos a la par que estos ocurren, los tiempos de respuesta son decisivos.
* **Distribuidos:** Los componentes del Sistema poseen ubicaciones diferentes, debiendo interactuar entre si para poder funcionar.
* **De Control:** La finalidad del sistema es Controlar “algo”, ya sea un dispositivo de HW o una salida de SW.
* **Doméstico / Industrial:** Según el área de aplicación y nivel de complejidad.
* **Etc**. Muchas clasificaciones según el análisis.

### Estructuras (Capas) de un sistema informático



### Componentes de los sistemas informáticos

* Hardware: Elementos de la electrónica y las telecomunicaciones que sustentan la captura, procesamiento, almacenamiento o transmisión de información de modo electrónico empleados en computadoras o sus periféricos.
* Software: Conjunto secuencial de instrucciones (ordenes) que posibilitan el manejo de información empleando computadoras.
* La información (Datos): Forma en que se representa una variable real para ser manipulada por una computadora.
* Orgware: Elementos de organización, reglas y normas que permiten funcionar organizadamente el SI.
* El hombre: Elemento integrante o no de un SI que justifica la razón de existencia de este, su creación y funcionamiento.

### Modelación de los sistemas informáticos

Forma gráfica de representar la ubicación, interrelación y papel de los componentes dentro de un sistema informático.

La representación se recomienda hacer por capas, similar al modelo OSI.

#### PROCESO de modelado:

* Identificar cada componente.
* Identificar la interrelación entre los componentes
* Representar componentes e interrelaciones.
* Identificar Entradas al Sistema
* Identificar Salidas del Sistema
* Identificar Reglas de comportamiento del Sistema.

### Componentes de los sistemas informáticos

#### La información (Los datos)

* Recurso intangible
* Único de cada entidad
* Perecedero en el tiempo
* Cada día más valor
* Es la razón de ser de los SI
* Recurso más valioso de un SI (después del hombre)
* Reproducible sigue siendo igual
* Etc.,...

##### Clasificación

* Se clasifica para gradar su tratamiento, acceso, importancia, prioridad, impacto, etc.
* Se clasifica según su uso.
* Se clasifica según su valor.
* Se clasifica según el SI que la manipulará

Puede ser: Priorizada, sensible, clasificada, limitada, crítica, etc.

**Relación entre Componentes y Propiedades de los Sistemas Informáticos.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **RECURSOS->**  **Propiedades** | **Hardware** | **Software** | **Orgware** | **RRHH** | **DATOS** |
| **Integridad** | Evaluar Roturas y  Fallos | Validaciones | Certificaciones  Auditorías | Comprobación  Códigos de ética | Almacenamiento seguro  Repositorios |
| **Disponibilidad** | Sistemas duplicados  Energía | En los sistemas | Control administrativo y técnico | Duplicar por rol | Acceso a más de un sitio  Inspecciones |
| **Confiabilidad** | Experimentación | Pruebas  Certificaciones | Comprobaciones  Certificaciones | Selección  Capacitación | Fuentes  Validación |
| **Accesibilidad** | Físico  Lógico | Acceso  Conectividad | Capacitación  Publicación | Motivación  Compromiso | Control de acceso  trazas |

### La SEGURIDAD en los sistemas informáticos

La Seguridad en los sistemas informáticos comprenderá el conjunto de medidas dirigidas a prevenir, enfrentar o mitigar incidentes que pongan en riesgo la integridad, disponibilidad, confiabilidad o accesibilidad de los componentes y/o del sistema.

* **Enfocada a la integridad:** Los componentes del SI mantendrán su estado y comportamiento según fueron concebidos.
* **Enfocada a la disponibilidad:** Los servicios y resultados de operación de un SI se mantendrán funcionales siempre que se les requiera.
* **Enfocada a la confiabilidad:** Los componentes y el SI se comportarán según fueron concebidos y no harán otra cosa distinta.
* **Enfocada a la Accesibilidad**: Los recursos de un SI estarán utilizables por los autorizados a hacerlo y sólo por ellos.

### El costo de la Seguridad y de la NO Seguridad en los SI

|  |  |
| --- | --- |
| Seguridad | No seguridad |
| Tiempo | Más recursos |
| Recursos | Más riesgos |
| Actualización | Deterioro del sistema informático |
| Menores Riesgos | Deterioro de la entidad |
| Más reconocimiento | Violación legal |
|  | No control |

### Fallos en los sistemas informáticos

Fiabilidad: es una medida del éxito de que el sistema se comporta de acuerdo a una especificación.

Fallo: Cuando el comportamiento del sistema se desvía del especificado, se dice que el sistema tiene un fallo.

#### Tipos de fallos

* **Fallos transitorios.** Un fallo transitorio comienza en un instante de tiempo concreto se mantiene durante algún período y luego desaparece. Ejemplo de este tipo de fallos suelen darse en los componentes hardware debidos a alguna interferencia externa y se mantiene mientras se mantiene la interferencia. Muchos de los fallos de los sistemas de comunicaciones son transitorios.
* **Fallos permanentes.** Son fallos que comienzan en un instante de tiempo y permanece hasta que se repara el sistema.
* **Fallos intermitentes.** Son fallos transitorios que ocurren de vez en cuando. Ejemplo de este tipo de fallos suelen darse en componentes hardware sensibles a la temperatura.

### Clasificación de acuerdo a su comportamiento temporal (fallos de tiempo)

* Fallo descontrolado. El sistema produce errores descontrolados tanto en el dominio de valor como del tiempo, incluido los fallos de improvisación.
* Fallo de retraso. El sistema produce servicios correctos en el dominio de valor, pero sufre errores de retraso en el tiempo.
* Fallo de silencio. El sistema deja de producir servicios debidos a fallos de omisión provocando en el resto del sistema fallos de omisión.
* Fallo de parada. Similar a los fallos de silencio, pero informa a otros sistemas que tiene fallo de silencio.
* Fallo controlado. El sistema falla según una forma especificada.
* Sin fallos. El sistema produce servicios correctos tanto en el dominio del valor como del tiempo.

#### Prevención de fallos

La prevención de fallos se refiere al intento de impedir cualquier posibilidad de fallo antes de que el sistema esté operativo. Para ello es necesario evitar y eliminar los fallos durante la etapa de diseño. Para evitar los fallos se actúa tanto en el hardware como en el software.

Hardware:

* Utilización de los componentes más fiables dentro de las restricciones de coste/prestaciones.
* Utilización de técnicas refinadas para la interconexión y ensamblado de componentes.
* Aislamiento del hardware para evitar interferencias.

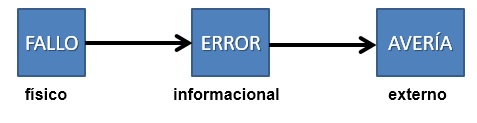
Software:

* Especificaciones de requisitos rigurosas e incluso formales.
* Utilización de probadas metodologías de diseño.
* Utilización de lenguajes que faciliten la abstracción de datos y la modularidad.
* Uso de herramientas de ingeniería de software para ayuda a la manipulación de los componentes software.

### Disponibilidad

Propiedad que garantiza que los usuarios autorizados tengan acceso a la información y activos asociados cuando se requiera. Significa que el sistema se mantenga funcionando y que está en capacidad de recuperarse rápidamente en caso de fallo.

* Fallo: defecto físico ó lógico (de comportamiento) en un componente de un SI. Defecto físico ó lógico (de comportamiento) en un componente de un SI con efecto total o parcial.
* Error: Manifestación o resultado de producirse un fallo. Un error es la consecuencia de un fallo.
* Avería: Manifestación de funcionamiento inadecuado de n SI como consecuencia de producirse un error.
* Con(Fiabilidad): Habilidad de un sistema o componente para desarrollar sus funciones bajo condiciones preestablecidas durante un período de tiempo especificado. [IEEE,90].



|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre** | **Acrónimo** | **Cálculo** | **Definición** |
| Tiempo medio entre fallos | MTBF | Horas / número de errores | Duración media de funcionamiento de la aplicación antes de que produzca errores |
| Tiempo medio de recuperación | MTTR | Horas de reparación / número de errores | Duración media de funcionamiento de la aplicación antes de que produzca errores |

La fórmula de disponibilidad tiene esta forma:

Disponibilidad = (MTBF / (MTBF + MTTR)) X 100

**Ejemplo**: una aplicación concebida para que funcione continuamente. Pongamos un punto de control de 1.000 horas consecutivas, dos errores de una hora durante ese período darían lugar a una disponibilidad de ((1.000/2) / ((1.000/2) + 1)) X 100 = (500 / 501) X 100 = 0,998 X 100 = 99,8 %.

### Redundancia

Empleo de información, tiempo o recursos adicionales por encima a lo estrictamente necesario para el correcto funcionamiento de un sistema [Johnson, 1984, IEEE 4(6)]

De HARDWARE: Multiplicación del hardware:

* Pasiva (enmascaramiento de fallos). Ejemplo TMR.
* Activo o dinámico.
* Híbridos

De Software: Añadir código redundante, de corrección:

* Pruebas de consistencia.
* Pruebas del hardware..
* Programación de N-Versiones.

Informacional: Añadir información adicional a los datos:

* Distancia de Hamming.
* Códigos de paridad.
* Códigos Checksum o CRC.

Temporal: Repetición de operaciones de calculo o control:

* Lógica alternativa
* Operandos desplazados / intercambiados o mixtos.

**Información**

* Es un **conjunto organizado de datos**, que constituye un **mensaje** sobre un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su uso racional es la base del [**conocimiento**](http://definicion.de/conocimiento/).
* la información es un fenómeno que **aporta significado o sentido** a las cosas, ya que mediante códigos y conjuntos de datos, forma los modelos de [**pensamiento**](http://encyclopedia2.thefreedictionary.com/wildcard+mask) **humano**.

**Sistema de Información**

Un sistema de información es un conjunto organizado de elementos, que pueden ser personas, datos, actividades o recursos materiales en general. Estos elementos interactúan entre sí para procesar información y distribuirla de manera adecuada en función de los objetivos de una organización.

El [estudio](http://encyclopedia2.thefreedictionary.com/server) de los [sistemas](http://definicion.de/sistema/) de información surgió como una subdisciplina de las [ciencias](http://definicion.de/ciencia/) de la computación, con el objetivo de racionalizar la administración de la tecnología dentro de las organizaciones. El campo de estudio fue [avanzando](http://es.wikipedia.org/wiki/Internet) hasta pasar a ser parte de los estudios superiores dentro de la administración.

**Identificación y cuantificación de la información en un SI:**

* Datos del Sistema.
* Datos de los usuarios.
* Configuración del Sistema.
* Software (SO, Básico, Aplicación).

**PROCESO DE IDENTIFICACIÓN DE INFORMACIÓN.**

1. Para cada componente del Sistema:

* Identificar tipo de Información que posee.
* Estimar el tamaño de la información. (cuantificar)

2. Clasificar la información: crítica, sensible, etc.

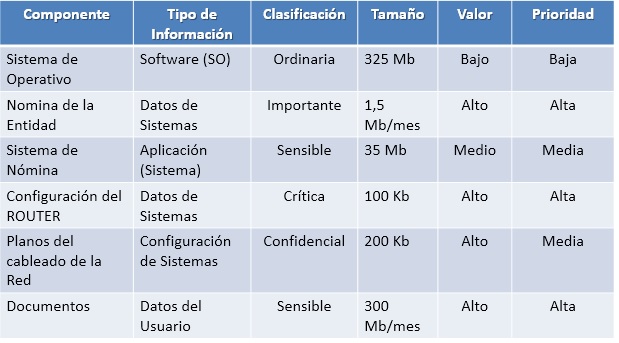
3. Valorar la información: Alto valor estratégico, etc.

4. Graficar todos los componentes de Información.

5. Establecer políticas y prioridades.

**Establecer las categorías y gradaciones a conveniencia.**

**Grafo(Ejemplo)**

****

**Políticas (clasificación) y Prioridades (valor/prioridad):**

**Política**: Forma en que se abordará el tratamiento a esa información desde el punto de vista de la SI.

Ejemplo: Política 1: Todos los componentes que contengan o gestionen información clasificada como Sensible tendrán un duplicado fuera de la entidad con salvas semanales.

**Prioridad**: Secuencia en que se atenderá y gestionará esa información desde el punto de vista de la SI.

Ejemplo: Prioridad 1: Se establecerán mecanismos de control de acceso a toda la información cuya prioridad se ha clasificado como alta.

**Protección de la Información en los S I**

Control sobre el comportamiento de los componentes del SI:

1. Mediante el monitoreo constante. (humano o no).
2. Estableciendo patrones y reglas de comportamiento.
3. Establecer Listas de Control y Acceso (ACL).
4. Manejo ó Gestión de intrusos.

**Mediante herramientas de ORGWARE:**

1. Reglamentos y medidas de seguridad.
2. Códigos de ética o conducta.
3. Libros de Procedimientos.

Permiten: Establecer qué se puede/debe hacer y qué no se puede/debe hacer, según las políticas:

1. Todo está permitido, excepto que se deniegue. (máximo privilegio).
2. Todo está prohibido, excepto que se autorice (mínimo privilegio).

**La Seguridad de la Información en Redes Locales.**

**Protección por Software y Hardware**:

* Proxies
* Firewall
* DMZ
* Segmentación V-LAN
* Virtualización

**Un servidor proxy** es un equipo intermediario situado entre el sistema del usuario e Internet. Puede utilizarse para registrar el uso de Internet y también para bloquear el acceso a una sede Web. El servidor de seguridad del servidor proxy bloquea algunas sedes o páginas Web por diversas razones.

**Servidores proxy:**

**Funcionan como cortafuegos y como filtro de contenidos.**   
Son un mecanismo de seguridad implementado por el ISP o los administradores de la red en un entorno de Intranet para desactivar el acceso o filtrar las solicitudes de contenido para ciertas sedes web consideradas ofensivas o dañinas para la red y los usuarios.

**Mejoran el rendimiento.**   
Guardan en la ante memoria las páginas web a las que acceden los sistemas de la red durante un cierto tiempo. Cuando un sistema solicita la misma página web, el servidor proxy utiliza la información guardada en la memoria caché en lugar de recuperarla del proveedor de contenidos. De esta forma, se accede con más rapidez a las páginas Web.

**Cortafuegos o firewall** es un sistema que previene el uso y el acceso desautorizados a tu ordenador.

Los cortafuegos pueden ser software, hardware, o una combinación de ambos.

**Cortafuegos de hardware**

**Los cortafuegos de hardware** proporcionan una fuerte protección contra la mayoría de las formas de ataque que vienen del mundo exterior y se pueden comprar como producto independiente o en routers de banda ancha.

**Cortafuegos de software**

Es el cortafuegos más utilizado, es un **cortafuego de software**. Protegerá el PC contra intentos de controlar o acceder a tu ordenador desde el exterior, y generalmente proporciona protección adicional contra los troyanos o gusanos de E-mail más comunes.

La desventaja de los cortafuegos de software es que protegen solamente al ordenador en el que están instalados y no protegen una red.

**Tipos de técnicas cortafuegos (según su tecnología):**

**Packet filter:** Chequea cada paquete que entra o sale de la red y lo acepta o rechaza basándose en reglas definidas por el usuario. La filtración del paquete es bastante eficaz y transparente a los usuarios, pero es difícil de configurar. Además, es susceptible al IP spoofing.

**Application gateway:** Aplica mecanismos de seguridad a ciertas aplicaciones, tales como servidores ftp y servidores telnet. Esto es muy eficaz, pero puede producir una disminución de las prestaciones.

**Circuit-level gateway:** Aplica mecanismos de seguridad cuando se establece una conexión TCP o UDP. Una vez que se haya hecho la conexión, los paquetes pueden fluir entre los anfitriones sin más comprobaciones.

**Proxy server:** Intercepta todos los mensajes que entran y salen de la red. El servidor proxy oculta con eficacia las direcciones de red verdaderas.

En la práctica, muchos cortafuegos utilizan dos o más de estas técnicas a la vez.

Un cortafuegos se considera la primera línea de defensa en la protección de la información privada.

**La Seguridad en los SISTEMA S INFORMÁTICOS**

[**Que es una DMZ?**](http://www.solusan.com/que-es-una-dmz.html)

Una **DMZ** (del inglés *Demilitarized zone*) . Una **zona desmilitarizada** (DMZ) o **red perimetral** es una red local que se ubica entre la red interna de una organización y una red externa, generalmente [Internet](http://es.wikipedia.org/wiki/Internet).

El objetivo es que las conexiones **desde** la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones **desde** la DMZ sólo se permitan a la red externa, es decir: los equipos locales ([hosts](http://es.wikipedia.org/wiki/Host)) en la DMZ no pueden conectar con la red interna.

Esto permite que los equipos (hosts) de la DMZ’s puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de [e-mail](http://es.wikipedia.org/wiki/E-mail), [Web](http://es.wikipedia.org/wiki/World_Wide_Web) y [DNS](http://es.wikipedia.org/wiki/Domain_Name_System).

**Auditorías informáticas:**

La auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas. También permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes.

**Auditorías Informáticas:**

* Preventivas o de seguimiento.
* Forenses.

**Fases en la realización de las auditorias informáticas**

Fase 0 Causas de la realización del ciclo Segundad.

Fase1: Estrategia y logística del ciclo.

Fase2: Ponderación de sectores del ciclo.

Fase3: Operativa del Ciclo.

Fase4: Cálculos y resultados del ciclo.

Fase: Confección del informe del ciclo.

**Aspectos a tener en cuenta en una Auditoria Informática.**

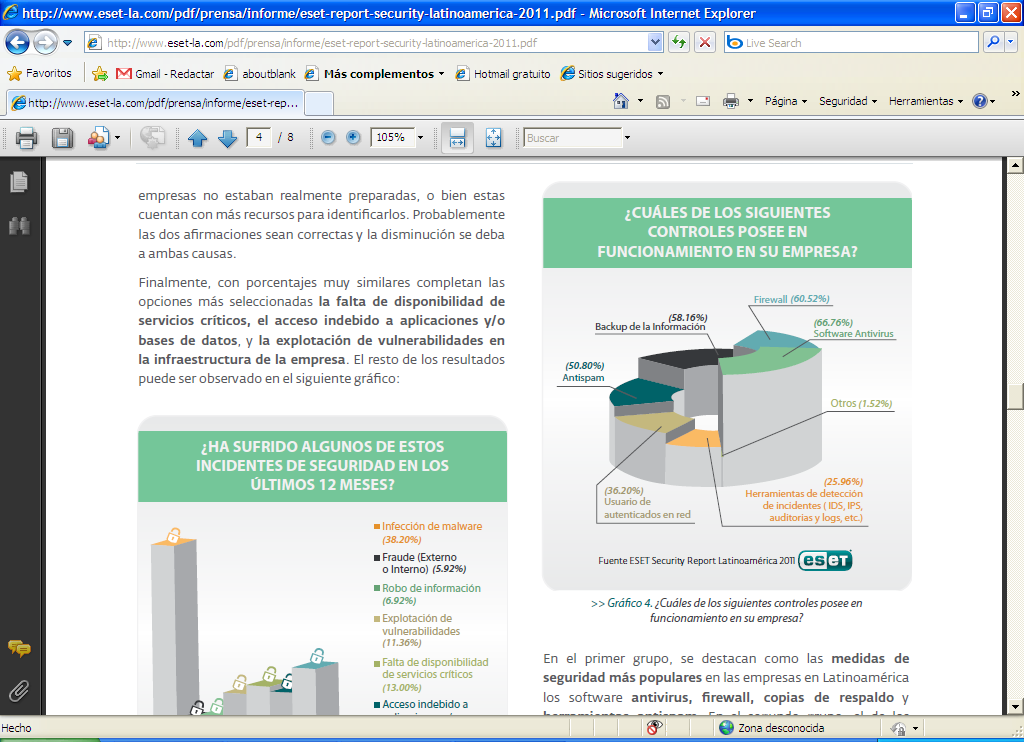
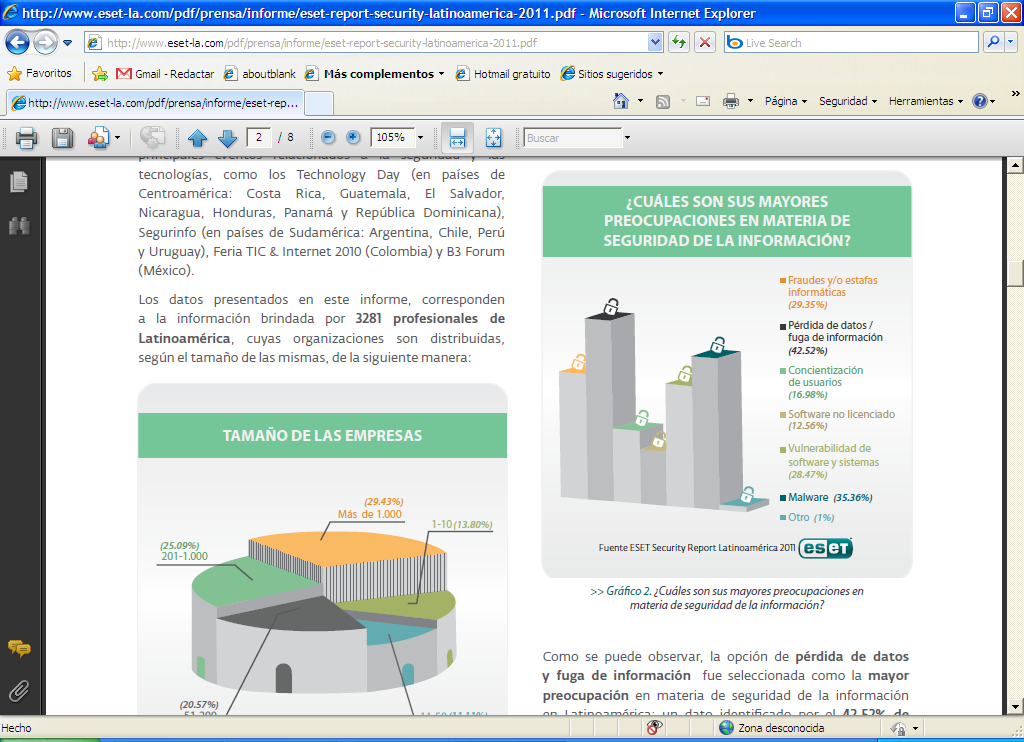
* Alcance y objetivos de la Auditoria.
* Estudio inicial del entorno auditable.
* Determinación de los recursos necesarios para realizar la auditoria.
* Elaboración del Plan y de los programas de trabajo.
* Actividades propiamente dichas de la auditoria de acuerdo al tipo (Informática, de Desarrollo, Sist de Redes, Forenses)
* Confección y redacción del Informe Final.

**Auditorías Informáticas. Herramientas:**

1. Dependen del Objetivo que persigan.
2. Dependen del Alcance con que se conciban.
3. Depende de su relación con la ocurrencia de incidentes.
4. Depende de quién las realiza.

Depende de la estructura física, lógica y tecnológica del Sistema objeto de Auditoría

**Tema 3: La legalidad y la seguridad informática**

****

**Implicaciones actuales de la Seguridad Informática**

1. Económicas
2. Políticas
3. Culturales
4. Tecnológicas
5. Sociales



**La seguridad informática en Cuba:**

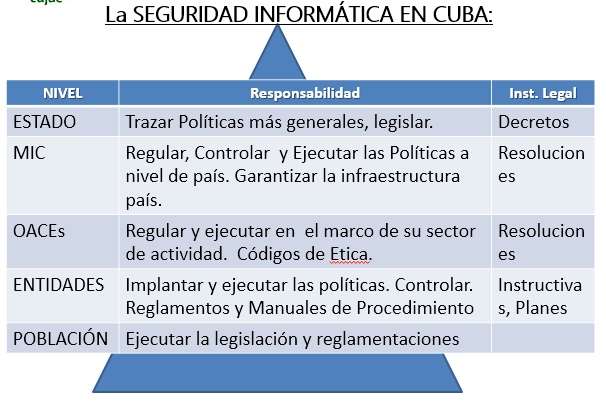
**Roles en la seguridad informática:**

**REGULADOR:** Establece y aprueba políticas generales y específicas, norma, organiza, designa.

**CONTROLADOR:** Supervisa que se cumpla lo normado y legislado.Reporta y sanciona.

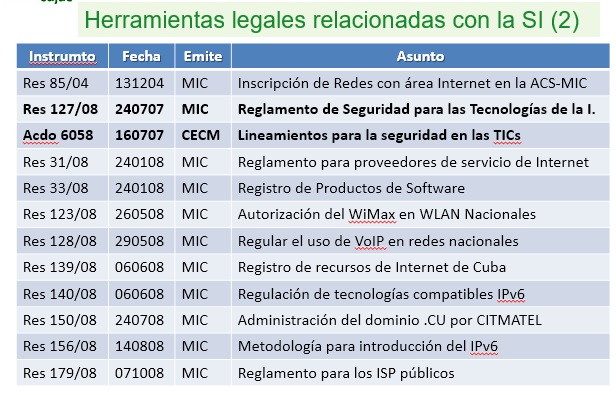
**EJECUTOR:** Realiza las acciones para cumplir lo regulado

**USUARIO:** Utiliza los SI para desarrollar sus actividades









**Herramientas legales relacionadas con la SI (3)**

* **Sobre 06/96 del MININT**.

Define el MININT como responsable de dirigir, controlar y aplicar la política de Seguridad Informática en el país.

Pone en vigor el Reglamento sobre Seguridad Informática, este posee:

Título 1: Objetivos y Alcance.

Título 2: Medidas Administrativas.

Título 3: Seguridad de Operaciones.

Título 4: Prestación de servicios de Seguridad Informática.

Título 5. Salida al exterior de las tecnolog. Y soportes.

Título 6. Enfrentamiento a violaciones de la SI.

* **Sobre DL199/99 del Csjo Estado**

Sobre la información clasificada y sus regulaciones

* **Sobre 127/07 del MIC.**

Pone en vigor el Reglamento de Seguridad para las Tecnolog. Inform.

Faculta a la OSRI para tomar cualquier medida para cumplirlo.

CONTENIDO:

Capítulo 1. Generalidades.

Capítulo 2. El Sistema de seguridad Informática.

Capítulo 3. Empleo conveniente y seguro de las TI.

Capítulo 4. Gestión de incidentes de Seguridad Informática.

Capítulo 5. Prestación de servicios de SI a terceros.

Capítulo 6. Inspección a las Tecnologías de la Información.

Capítulo 7. Incumplimientos.

Diccionario de términos y definiciones.

* **Sobre Acuerdo 6058 del CECM**

Lineamientos para la seguridad en las tecnologías de la información**.**

**Código de ética o de conducta**

* NO son Ley.
* Carácter ramal o de una profesión.
* Consenso de una mayoría del sector o profesión.
* Están entre la moral y la ley.
* Poseen reconocimiento social.
* Regulan el comportamiento.

**¿Qué es una política de seguridad informática?**

Enunciado de un comportamiento esperado de los componentes de un Sistema Informático enfocados a garantizar la Seguridad del Sistema.

**Costos de la Seguridad Informática**

COSTO = VALOR (EN $ o EN ACTIVOS)

**Dos enfoques:**

1. El COSTO de asumir “cierto nivel” de Seguridad Informática.
2. El Costo de “no asumir los costos” de Seguridad Informática.

* Estimar el valor de la información ha sido siempre difícil, y más difícil aún hacer estos costos justificables,
* Establecer el valor de los datos es algo totalmente relativo,
* Las medidas de seguridad no influyen en la productividad del sistema por lo que las organizaciones son reticentes a dedicar recursos a esta tarea.
* La evaluación de costos más ampliamente aceptada consiste en cuantificar los daños que cada posible vulnerabilidad puede causar teniendo en cuenta las posibilidades.

El objetivo que se persigue es **lograr que un ataque a los bienes sea más costoso que su valor**, invirtiendo menos de lo que vale. Para esto se define tres costos fundamentales:

**CP**: Valor de los bienes y recursos protegidos.

**CR**: Costo de los medios necesarios para romper las medidas de seguridad establecidas.

**CS**: Costo de las medidas de seguridad.

Para que la **política de seguridad** sea lógica y consistente se debe cumplir que:

**CR > CP**: o sea que un ataque para obtener los bienes debe ser más costoso que el valor de los mismos.

**CP > CS**: o sea que el costo de los bienes protegidos debe ser mayor que el costo de la protección.

Luego, **CR > CP > CS** y lo que se busca es:

"Minimizar el costo de la protección manteniéndolo por debajo del de los bienes protegidos" (2). Si proteger los bienes es más caro de lo que valen (el lápiz dentro de la caja fuerte), entonces resulta más conveniente obtenerlos de nuevo en vez de protegerlo.

"Maximizar el costo de los ataques manteniéndolo por encima del de los bienes protegidos" (3). Si atacar el bien es más caro de lo que valen, al atacante le conviene más obtenerlo de otra forma menos costosa.

**Los Planes de Seguridad Informática**

* Conjunto de medidas preventivas, operativas y de seguimiento orientadas a mantener la seguridad de los elementos integrantes de los sistemas informáticos y la respuesta esperada de este.
* Las medidas tienen fechas de cumplimiento.
* Las medidas tienen un responsable de ejecución.
* Las medidas tienen una efectividad cuantificable.
* Las medidas son auditables.
* Las medidas están alineadas con las políticas, la legislación y las normas de conducta definidas.

**Incidentes de Seguridad Informática**

Cualquier evento - humano, tecnológico o natural - que incide sobre los elementos de un Sistema Informático de modo que comprometa, o pueda comprometer, su comportamiento concebido.

**Ejemplos:**

* El acceso a un recurso no autorizado.
* El comportamiento anómalo de un componente.
* La salida/entrada de información por vías no autorizadas.
* La perdida de capacidad de respuesta del SI.
* Un nuevo virus.

**Tratamiento**

* Preverlos.
* Registrarlos.

**(Logs, Trazas, Registros, etc.)**

* Identificarlos y clasificarlos.

**(Frecuencia, Impacto)**

* Atenderlos (respuesta, replanteo).
* Aprender de ellos.

**(El Sistema, la Organización, el País)**

**1ra. Ley de Murphy sobre Contingencias:**

“*Todo lo que pueda fallar.... !Fallará*”.

Y lo hará:

*a. En el momento más inoportuno.*

*b. Con las peores consecuencias.*

*c. Del modo menos previsto*.

**Contingencia:**

Evento no deseado, identificado como RIESGO, que se ha convertido en realidad y que compromete la capacidad deseada de respuesta del sistema.

**FASES O ETAPAS:**

* Análisis y valoración de riesgos.
* Jerarquización de las aplicaciones y servicios.
* Establecimientos de requerimientos de recuperación. (tiempos, calidad, servicios, etc.)
* Ejecución.
* Pruebas y validación.
* Documentación.
* Difusión y mantenimiento.

**Reporte de Contingencias y Respuestas: CuCERT**

CUCERT: Entidad del MIC responsabilizada con la prevención y respuesta ante contingencias informáticas.

**PRINCIPALES FUNCIONES**

* Asesorar, capacitar y auditar las medidas y Planes de Contingencias.
* Reportar en línea un incidente.
* Asesorar contribuir a la recuperación ante un desastre de SI.
* Registra los incidentes de SI y proponer políticas nacionales para su enfrentamiento.