SEGURIDAD EN REDES Y SISTEMAS INFORMÁTICOS

Ada Lovelance

En nuestra vida cotidiana, en nuestra relación diaria con el mundo de la información, no solemos preocuparnos por el tema de la seguridad informática, ya que hemos adquirido una falsa sensación de confianza hacia un mundo que sabemos que existe pero nos es ajeno, o nos lo era…
Si podemos permitirnos este lujo -y aún así surgen problemas ocasionales- es porque hay otros profesionales que dedican su vida a preservar nuestra seguridad.

Bienvenid@ , esperamos que lo disfrutes y sea lo que estabas buscando.

-La Autora-

ÍNDICE GENERAL DEL CURSO

6. Sistemas de detección de intrusiones.
7. Ataques específicos.

UNIDAD 9. SEGURIDAD EN SERVICIOS DE INTERNET.

1. Comercio electrónico y sistemas de pago por Internet.
2. PEM, PGP, S-MIME, SSL.
3. Ataques específicos.
4. Etiquetas inteligentes RFID.
3. Inferencia.
4. Bases de datos multinivel.
5. Ataques específicos: inyección de código SQL.

Contenidos prácticos:

Ejercicios prácticos on-line de cada unidad de contenido del módulo formativo.

Las actividades son de diversa naturaleza: actividades de opción múltiple, de verdadero/falso, de completar…

UNIDAD 1. INTRODUCCIÓN

Índice unidad 1

1. Conceptos básicos de la seguridad de la información

1.1 Introducción

La informatización de la sociedad ha proporcionado claras mejoras pero también nuevos problemas.

Muchas entidades (Bancos, Compañías de Seguros, Administración Pública, etc.) contienen en sus ficheros de datos información personal cuyo acceso o difusión a personas no autorizadas podría perjudicar gravemente a la persona involucrada.

Por ejemplo, cuando nosotros rellenamos un cuestionario de salud para contratar un seguro de vida, ¿qué garantías tengo de que esa información esté protegida y no sea divulgada?.

Por lo tanto, la información contenida dentro de los sistemas informáticos es claramente vital y tiene que ser protegida.

Lo primero que hay que decir, aunque sea evidente, es que este acceso a la información privada es considerado un delito y por lo tanto perseguido por la justicia.

Se pueden diferenciar dos aspectos muy importantes:

- Que la información depositada no se pierda o sea alterada de forma incorrecta y privacidad, que esta información sólo sea accesible cuando sea necesaria o con las autorizaciones pertinentes.

También hay otro tipo de información, que no siendo de carácter personal, si que es claramente vital para una empresa.

Por ejemplo, toda empresa tiene almacenadas en sus sistemas informáticos las patentes de sus productos, nuevas campañas de marketing, planes estratégicos, etc. que si son accedidos por la empresa de la competencia podrían causar un grave perjuicio económico o incluso su ruina.

Y no hablemos ya de los sistemas informáticos que controlan servicios vitales de un país, sistemas de control del tráfico aéreo, generación y distribución de electricidad, sistemas electrónicos de defensa, etc.

Pero antes de adentrarnos más en materia comencemos definiendo:

1.2 ¿Qué es la Seguridad?

Podemos entender como seguridad algo que es libre y exento de todo peligro daño o riesgo, cierto, indubitable y en cierta manera infalible, firme constante y que no está en peligro de faltar o caerse, algo que no es sospechoso.

Según la RAE, Seguridad es definida como cualidad de seguro y seguro queda definido como:

> **Seguro** (Del lat. secūrus).
>
> 1. adj.Libre y exento de todo peligro, daño o riesgo.
>
> 2. adj. Cierto, indubitable y en cierta manera infalible.
>
> 3. adj. Firme, constante y que no está en peligro de faltar o

Pero, ***¿son estas definiciones aplicables a la seguridad informática? ¿Podemos conseguir un sistema libre y exento de todo peligro, daño o riesgo?***

Si nos vamos haciendo esta misma pregunta con cada una de las definiciones dadas por la Rae vamos llegando a la misma respuesta:

No podemos garantizar que nuestro sistema va a estar en todo momento libre o exento de todo riesgo, que valla a ser cierto, indubitable y en cierta manera infalible o que valla a mantenerse Firme y constante.

¿Por qué no podemos garantizarlo?

Porque existen una serie de amenazas constantes clasificadas en:

Amenazas Lógicas, Físicas, y Ambientales que de paliarse de forma completa afectarían a la disponibilidad de nuestro sistema lo que hace que su implementación no sea viable.

De hecho me voy a permitir citar al experto en seguridad Eugene H. Spafford citado también en otros libros sobre la materia:

"EL único sistema que es totalmente seguro es uno que se encuentra apagado y desconectado, metido en una caja fuerte de titanio que está enterrada en cemento, rodeada de gas nervioso y de un grupo de guardias fuertemente armado, ¡Y aún así no apostaría mi vida por ello!"

Todos los posibles conceptos, y terminología que nos os resulte familiar, la vamos a ir aclarando poco a poco, por tanto volvamos a nuestra pregunta inicial.

¿Qué es la seguridad informática?

Pues ya que existen innumerables definiciones para esta materia, nosotros diremos que:

La seguridad informática es una rama dentro de la ingeniería informática que:

Se **encarga del estudio y la puesta en funcionamiento de los diferentes métodos, herramientas y procesos para garantizar la Confidencialidad, Integridad, Disponibilidad, Autenticidad y no repudio** de un sistema informático.

Entendiéndose sistema informático como**:**

"El conjunto de partes interrelacionadas, hardware, software y de recursos humanos que permite almacenar y procesar información." (Wikipedia).

La seguridad no es un conjunto de medidas que se toman por única vez, sino un proceso dinámico en el que todos los actores juegan un rol permanente y debe de abarcar tres áreas de incumbencia:

Personas, Procesos y Tecnología.

Existen varias ramas y profesionales dentro de esta materia o estrechamente relacionados con ella, algunos de ellos son:

Analistas de sistemas: Definen las pautas del sistema, deciden la función y utilidad de ese sistema. Deben crear las políticas adecuadas para el uso del sistema. Elaboran los planes de seguridad de la información, de los equipos y crean los entornos de pruebas

Pentesters: Se encargan de probar o intentar comprometer la seguridad de un sistema o de parte del mismo con el consentimiento de la empresa y a petición de la misma para elaborar un informe detallado de las vulnerabilidades encontradas y como subsanarlas.

Auditan el sistema a petición del cliente. Pueden ser personal propio de la organización y dependiendo de ello hablaremos de diferentes tipos de auditorías, las cuales veremos con más detalle más adelante

Hackers: Son profesionales expertos en una o varias materias relacionadas con la seguridad, en algunos casos son contratados por las empresas o organizaciones para hacer auditorías expertas desde el exterior o para resolver problemas que no entran dentro de las competencias de los profesionales de la empresa. Hay varios tipos de hackers que también veremos con más detalle.

Forenses: Se encargan de la recopilación de pruebas y evidencias una vez el sistema ha sido alterado. Definen como debe tratarse el sistema y su información para poder recopilar evidencias de la intrusión o manipulación del mismo.

Criptólogos y Criptoanalistas: la criptografía es una rama de las matemáticas y actualmente de la informática que se encarga del estudio de métodos, algoritmos y técnicas de cifrado para proteger un mensaje o sistema granizando así su integridad confidencialidad y no repudio

Legalistas: Son los encargados de que la organización cumpla con las normativas vigentes en materia de seguridad, informan a la organización de dichas normativas y de los requisitos necesarios para su cumplimiento

Los principales objetivos de la seguridad informática por tanto son:

- Analizar los riesgos de seguridad adecuadamente para hacer posible la detección de problemas y amenazas minimizando así los riesgos
- Garantizar la adecuada utilización de los recursos, de las aplicaciones, y de los sistemas
- Limitar el impacto de la las perdidas, en el caso de producirse, y conseguir la adecuada recuperación del sistema después de un incidente de seguridad
- Cumplir el marco legal y con los requisitos impuestos a nivel organizativo

Veamos a qué nos referimos en cada uno de los puntos de nuestra definición:

Disponibilidad: Se refiere a la capacidad de que las aplicaciones, los datos y el sistema se encuentre accesible a los usuarios autorizados en todo momento o el tiempo previsto al incluir las suspensiones programadas debidas a actualizaciones o mejoras programadas.

Confidencialidad: La confidencialidad consiste en procurar un acceso confidencial al mensaje, la comunicación, los datos o al sistema en sí.

Quiere decir que sólo tendrán acceso personas o sistemas que hayan sido autorizados para ello y que estos no van a compartir esta información con terceros, haciendo de este modo que los datos resulten ajenos a quien no haya sido autorizado y por tanto confidenciales.

Integridad de la información: Es la característica que hace que un sistema permanezca inalterado a no ser que estas modificaciones sean hechas por personal autorizado y queden registradas y documentadas.

Un sistema integro es aquel que permite comprobar ni el propio sistema ni ninguna de sus partes ha sido manipulada en su forma original, es decir, es un sistema que no ha sido alterado.

Autenticidad: Asegurar la identidad con certeza respeto al origen y procedencia del los datos, la información o el sistema. El objetivo que se pretende es la comprobación de que dichos datos o información provienen realmente de la fuente que dice ser.

No repudio: No repudio quiere decir que ni el emisor ni el receptor de los datos pueden alegar que esa información no proviene de su fuente.

Una vez aclarados todos estos conceptos veamos como se relacionan entre si:

Si no existe la disponibilidad ya que el sistema se encuentra caído o sin servicio, el resto de los factores no son verificables, ya que los usuarios autorizados no tienen acceso así que no es posible procurarles un acceso confidencial ni verificar si los datos trasmitidos son íntegros y ya que no hay datos no hay origen ni destino del cual asegurar su certeza.

¿Se te ocurre algún ataque que afecte a la disponibilidad?

Los ataques los vamos a ver más adelante, pero aún así, puedes haber encontrado en algún momento una página pública a la que no fuese posible acceder.
Esto puede ser debido a una falta de previsión por parte de los administradores ya que están recibiendo más tráfico del esperado, o debido a un ataque que está generando más tráfico del soportado para bloquear el servicio.
Este tipo de ataque se conoce comúnmente como Dos, Deniegal of Service o denegación de servicio.

Lo mismo nos ocurre con el resto de las capas de la seguridad, están íntimamente relacionadas, sin la confidencialidad no podemos garantizar la integridad ya que si la

Lo mismo nos ocurre con el resto de las capas de la seguridad, están íntimamente relacionadas, sin la confidencialidad no podemos garantizar la integridad ya que si la información ha sido divulgada es probable que también haya podido ser modificada o nuestras claves sean conocidas por lo que exista la posibilidad de que un intruso esté actuando con nuestra identidad dentro del sistema.

2. Servicios de la Sociedad de la información, tipos de ataques y métodos de defensa.

¿Qué son los servicios de la sociedad de la información?

Concepto

"Todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario. El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios."

Son servicios de la sociedad de la información, entre otros y siempre que representen una actividad económica, los siguientes:

- La contratación de bienes o servicios por vía electrónica.
- La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.
- La gestión de compras en la red por grupos de personas.
- El envío de comunicaciones comerciales.
- El suministro de información por vía telemática.
- El vídeo bajo demanda, como servicio en que el usuario puede seleccionar a través de la red, tanto el programa deseado como el momento de su suministro y recepción, y, en general, la distribución de contenidos previa petición individual.

No tendrán la consideración de servicios de la sociedad de la información los que no reúnan las características señaladas en el primer párrafo de este apartado y, en particular, los siguientes:

Los servicios prestados por medio de telefonía vocal, fax o télex.

El intercambio de información por medio de correo electrónico u otro medio de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan.

Los servicios de radiodifusión televisiva (incluidos los servicios de cuasi vídeo a la carta), contemplados en el artículo 3.a) de la Ley 25/1994, de 12 de julio, por la que se incorpora al ordenamiento jurídico español la Directiva 89/552/CEE, del Consejo, de 3 de Octubre, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva, o cualquier otra que la sustituya.

Los servicios de radiodifusión sonora, y el teletexto televisivo y otros servicios equivalentes como las guías electrónicas de programas ofrecidas a través de las plataformas televisivas.

Fuente:Wikipedia
http://es.wikipedia.org/wiki/Ley_de_Servicios_de_la_Sociedad_de_Informaci%C3%B3n_de_Espa%C3

información donde el volumen de datos (información) que es procesado, almacenado y transmitido es muy superior al de otra época.

Crece MUCHÍSIMO la importancia de la información.

Los recursos clásicos cómo recursos humanos, materiales y dinero pueden ser alcanzados fácilmente si se dispone de la información correcta en el momento preciso por tanto el conocimiento es poder.

Si la información puede proporcionar beneficios, siempre existirá alguien que ponga todos los medios a su alcance para obtenerla, manteniendo una proporcionalidad entre los medios y el beneficio.

Los nuevos medios para transmitir y utilizar la información han aumentado su inseguridad.

El auge de las redes y de Internet ha sido el factor que ha hecho que la Seguridad Informática cobre importancia.

De donde nace dos nuevos concepto, el de seguridad de los sistemas de información o SSI.

(SSI) = Seguridad de la Información, Seguridad de los Ordenadores, Seguridad de Datos, Protección de la Información.

PSI o protección y seguridad de la información que surge de la idea de que hay que proteger la información para proporcionar acceso a ella.

Las organizaciones se exponen a riesgos por una protección inadecuada de la información (o de los sistemas de tratamiento).

Ejemplos de vulnerabilidad creciente:

- Expansión del uso de ordenadores personales

- Se magnifica el problema de la SSI, debido a la carencia de controles de seguridad básicos.

- Evolución hacia entornos con acceso global y múltiple

El aumento de la conectividad entre organizaciones distintas que plantea retos importantes a la gestión de la seguridad.

Riesgos fundamentales de una incorrecta PSI:

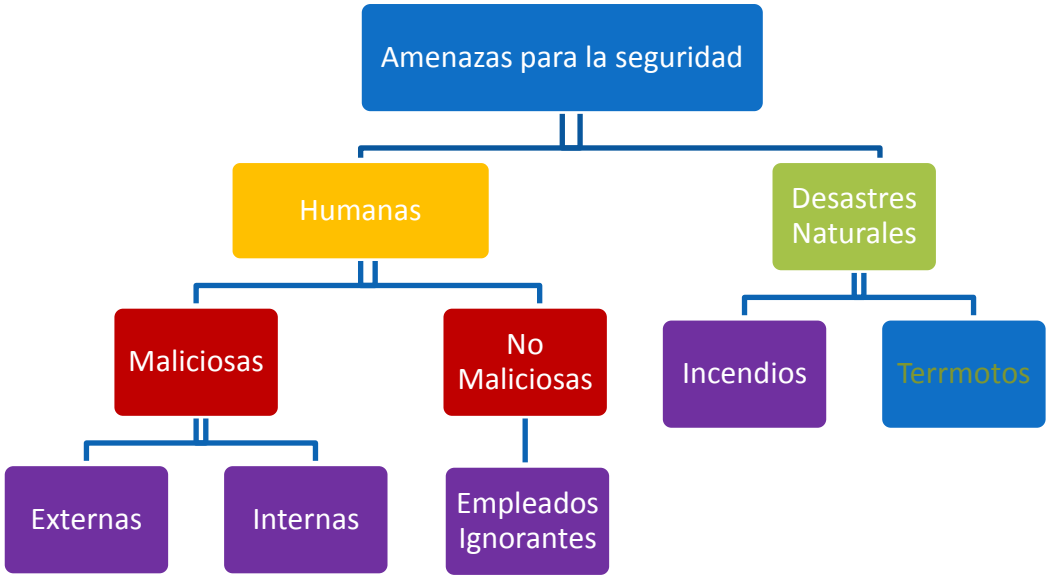
Revelación a personas no autorizadas (confidencialidad).

Inexactitud de los datos (integridad).

Inaccesibilidad de la información cuando se necesita (disponibilidad).

Pero aparte del importante crecimiento de la red hay otra serie de amenazas que debemos conocer y considerar ya que vamos a ver las leyes en la siguiente unidad.

Veamos cómo pueden ser clasificadas en el siguiente cuadro de flujo:



2.1 Amenazas físicas

Pueden ser desastres o catástrofes naturales. Por ejemplo, una inundación por exceso de lluvia, un incendio en el edificio, etc. Ante este tipo de situación poco podemos hacer excepto planificar desde un principio una red redundante tanto en la conexión como en los datos.

Pueden ser provocas por el factor humano:

- La excavadora que corta un tendido de fibra óptica y acaba con la conexión de todos nuestros servidores.
- El vaso de agua que se cae en el lugar menos oportuno...

Pero también puede ser un trabajador descontento que desee llevarse datos de la empresa y saque varios discos duros de algunos equipos.

Por esto nuestras máquinas siempre deben encontrarse en un lugar seguro, protegidas por cámaras de seguridad y otro tipo de medidas que veremos en un capitulo de este mismo curso.

2. 2 Amenazas lógicas

Las amenazas lógicas son aquellas que afectan o comprometen los datos y/o la información del sistema bien sea por un error del software, debido a la falta de actualizaciones oportunas, por una gestión incorrecta de los permisos de seguridad, no haber realizado los backups correspondientes cuando se debía, o por una intrusión ajena.

Por tanto cuando hablamos de seguridad lógica en un sistema hablamos de las barreras y procedimientos que protejan el acceso a los datos e información que contiene.

"Las amenazas pueden ser analizadas en tres momentos: antes del ataque durante y después del mismo. Estos mecanismos conformarán políticas que garantizarán la seguridad de nuestro sistema informático.

a. La Prevención (antes): mecanismos que aumentan la seguridad (o fiabilidad) de un sistema durante su funcionamiento normal. Por ejemplo el cifrado de información para su posterior transmisión.

b. La Detección (durante): mecanismos orientados a revelar violaciones a la seguridad. Generalmente son programas de auditoría.

c. La Recuperación (después): mecanismos que se aplican, cuando la violación del sistema ya se ha detectado, para retornar éste a su funcionamiento normal. Por ejemplo recuperación desde las copias de seguridad (backup) realizadas.

Las preguntas que se hace un técnico en sistemas de información ante un problema de seguridad, normalmente, están relacionadas con medidas defensivas que no solucionan un problema dado, sólo lo transforma o retrasa. La amenaza o riesgo sigue allí y las preguntas que este técnico debería hacerse son:

¿Cuánto tardará la amenaza en superar la "solución" planteada?
¿Cómo se hace para detectarla e identificarla a tiempo?
¿Cómo se hace para neutralizarla?

Ya se trate de actos naturales, errores u omisiones humanas y actos intencionales, cada riesgo debería ser atacado de las siguientes maneras:

1. Minimizando la posibilidad de su ocurrencia.
2. Reduciendo al mínimo el perjuicio producido, si no ha podido evitarse que ocurriera.
3. Diseño de métodos para la más rápida recuperación de los daños experimentados.
4. Corrección de las medidas de seguridad en función de la experiencia recogida.

Luego, el Daño es el resultado de la amenaza; aunque esto es sólo la mitad del axioma. El daño también es el resultado de la no–acción, o acción defectuosa, del protector. El daño puede producirse porque el protector no supo identificar adecuadamente la amenaza y, si lo hizo, se impusieron criterios comerciales por encima de los de seguridad. De allí que se deriven responsabilidades para la amenaza (por supuesto) pero también para la figura del protector.

Luego, el protector será el encargado de detectar cada una de las Vulnerabilidades (debilidades) del sistema que pueden ser explotadas y empleadas, por la amenaza, para comprometerlo.

También será el encargado de aplicar las contra-medidas (técnicas de protección) adecuadas. "
(AUTOR: A.S.S. BORGHELLO, CRISTIAN FABIAN En su tesis de licenciatura).

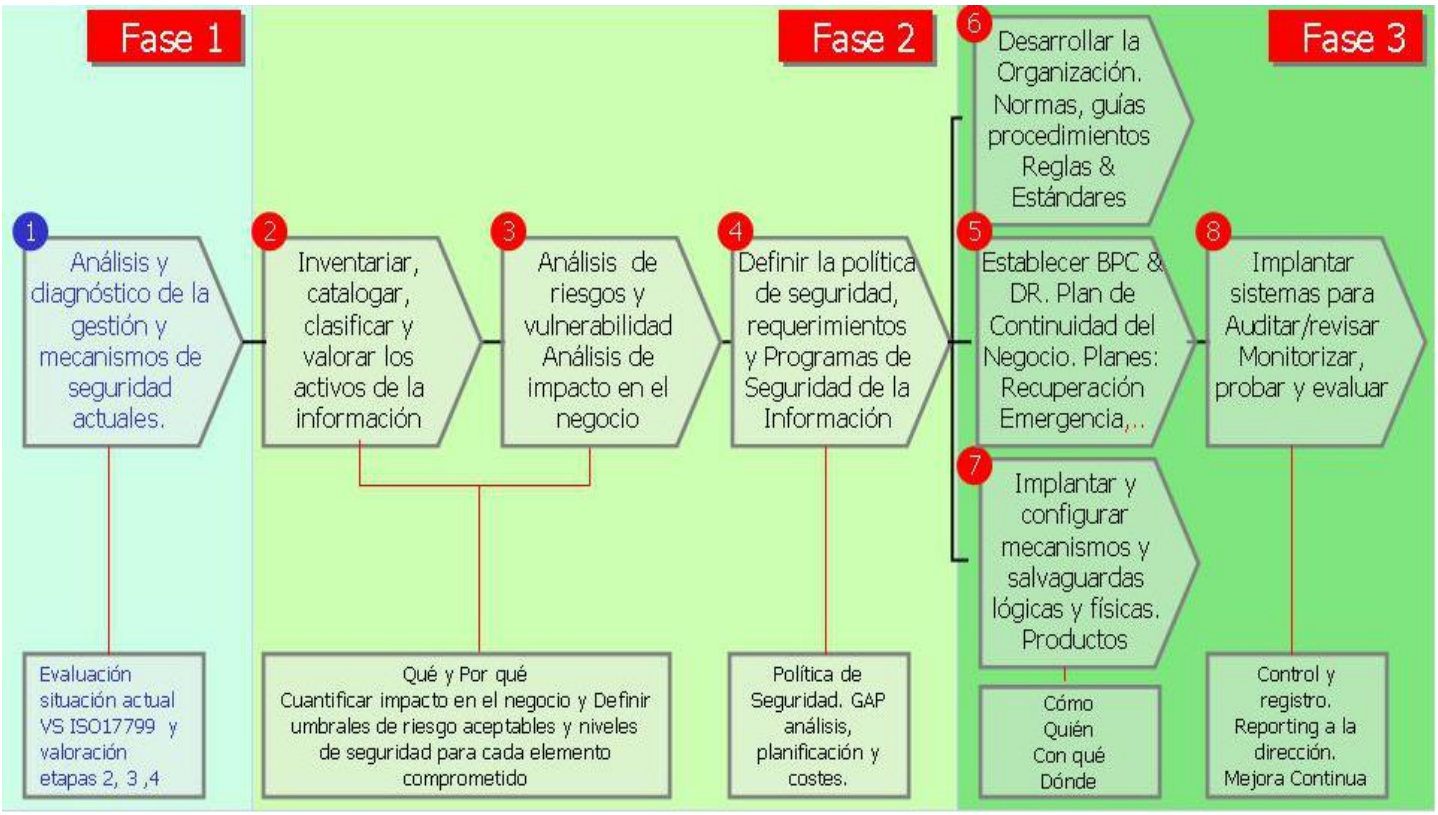
Por supuesto si tenemos una caseta de perro en el jardín no le compramos una alarma antirrobo ni le ponemos puertas blindadas ya que sería un gasto innecesario comparado con el bien a proteger, pero seguramente a la casa donde esté esa caseta si nos parezca adecuado comprar dicha alarma.

En la seguridad informática pasa exactamente lo mismo, las medidas que se tomen deben de ser acordes a la información a proteger.

Pero la seguridad no va a ser la suma de las medidas del sistema, la seguridad del sistema será igual a su parte más débil.

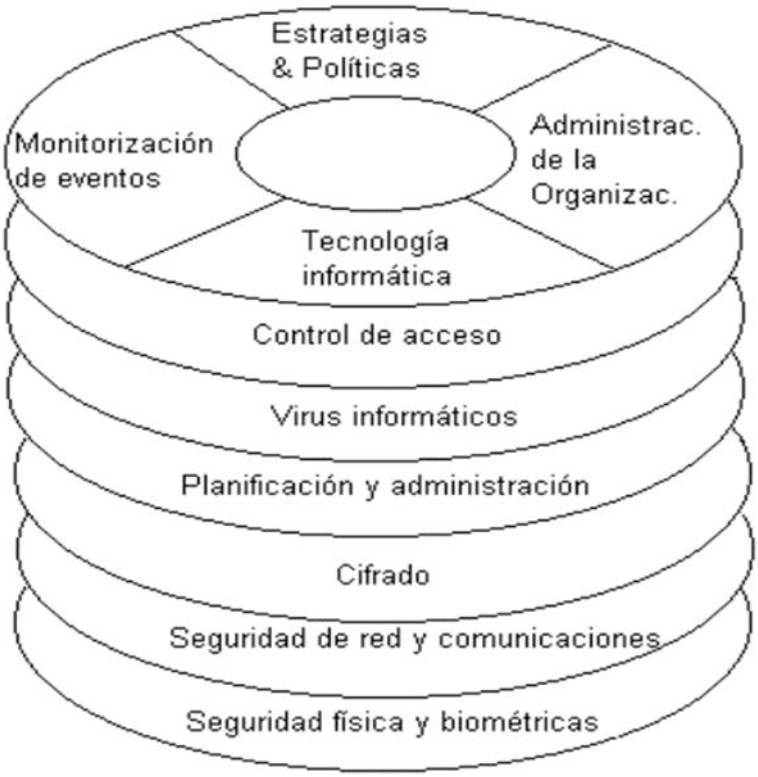
Un administrador de sistemas tiene que administrar cada una de las maquinas, personas, redes, servidores y servicios de sus sistema. Un atacante sólo necesita encontrar un fallo para poder realizar la intrusión.

Veámoslo en las imágenes a continuación:



En primer lugar debemos de analizar la situación en la que nos encontramos siempre teniendo presente el tipo de medidas que se pueden implantar que son las mostradas en la imagen de la derecha.

Una vez estén inventariados y catalogados los activos hemos de analizar los riesgos existentes, estos riesgos pueden llegar a ser tolerables si el valor de nuestros activos es inferior al coste de implantación de las medidas de



seguridad.

Cuando esto haya sido valorado estipularemos las políticas de seguridad adecuadas para nuestra organización

Y con esto finalizamos el primer tema, ahora es momento de pasar a la parte práctica de este tema y cuando la hayas terminado ya puedes continuar con el tema 2.