2.Introducción a la seguridad

Las necesidades de seguridad de la información han ido evolucionando al igual que las ciencias de la computación y las tecnologías de la información. De este modo, las herramientas de seguridad empleadas también lo han hecho.

En sus comienzos, la seguridad consistía en el uso de medios físicos, tales como cajas fuertes o armarios con cierre de seguridad. Poco después, aparecieron los medios administrativos, como lo son los contratos de empleados para salvaguardar información confidencial de la empresa.

Con la llegada de la computación, hicieron falta nuevas herramientas de seguridad diseñadas para proteger los datos y evitar la intrusión de los hackers. Estas herramientas se conocen con el nombre de "seguridad informática".

Finalmente, con la aparición de Internet, las redes locales y los sistemas distribuidos, surgió la necesidad de disponer de seguridad durante la transmisión. Las herramientas que satisfacen estas nuevas necesidades se engloban bajo la denominación "seguridad en redes". A continuación se puede observar la evolución en el tiempo tanto de la seguridad como de la informática.

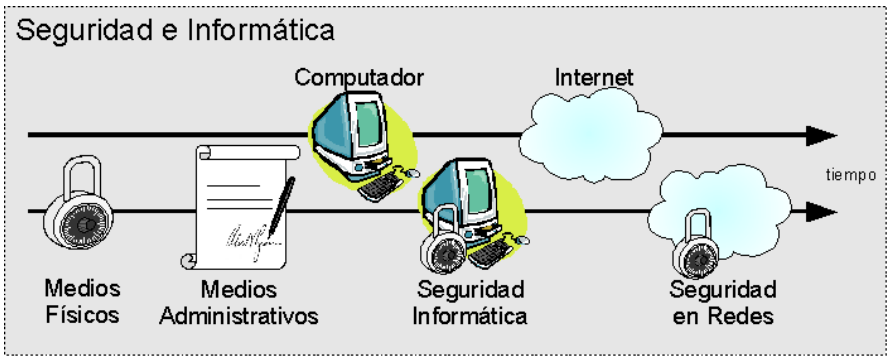

Ilustración 2: Evolución en el tiempo de la seguridad y la informática

Para mayor información puede consultar los recursos bibliográficos utilizados; a los cuales también se puede acceder desde http://jcef.sourceforge.net/doc/resources.pdf.

1 Una arquitectura de seguridad

Para analizar de forma efectiva las necesidades de seguridad de una organización, evaluar y elegir distintos productos y políticas de seguridad, el responsable de la seguridad necesita una forma sistemática de definir los requisitos de seguridad y caracterizar los enfoques para satisfacer dichos requisitos.

Uno de estos posibles enfoques interesantes se centra en los ataques a la seguridad, los mecanismos y los servicios.

Un ataque a la seguridad es cualquier acción que comprometa la seguridad de la información de una organización. Los ataques a la seguridad se detectan, eliminan, previenen y/o se reestablece el sistema de su daño, siendo los encargados de estas funciones los mecanismos de seguridad.

Por el contrario, un servicio de seguridad es un servicio que mejora la seguridad de los sistemas, contrarrestando los ataques a la seguridad, haciendo uso de uno o más mecanismos y políticas de seguridad con el objetivo de proporcionar el servicio.

En resumen, los componentes de una arquitectura de seguridad junto con sus objetivos son:

Componentes	Objetivo
Ataque a la seguridad	Comprometer la seguridad de la información de un sistema
Servicio de seguridad	Contrarrestar los ataques a la seguridad
Mecanismo de seguridad	Ayudar a contrarrestar los ataques a la seguridad

Tabla 2: Componentes de una arquitectura de seguridad y sus objetivos

2 Ataques a la seguridad

Los ataques a la seguridad se pueden clasificar en ataques pasivos y activos. En la siguiente tabla se muestran cada una de ellos junto con sus objetivos primarios y sus soluciones:

Características		**Ataques**	
		Pasivos	**Activos**
Objetivo	**¿Acceden a recursos?**	Sí	Sí
	¿Obtienen información?	Sí	Sí
	¿Alteran el sistema?	No	Sí
	¿Alteran recursos?	No	Sí

Tabla 3: Comparativa entre Ataques Pasivos y Activos (1/2)

Características		Ataques	
		Pasivos	Activos
Solución	¿Se pueden prevenir?	Sí	No
	¿Se pueden detectar?	No	Sí
	¿Se pueden recuperar?	No	Sí

Tabla 4: Comparativa entre Ataques Pasivos y Activos (2/2)

1 Ataques pasivos

De la misma forma, existen varios tipos de ataques pasivos. En la siguiente tabla se muestran cada uno de ellos junto con sus objetivos básicos:

Ataques Pasivos	Objetivos
Obtención de contenidos de mensajes	Copiar información
Análisis del Tráfico	Averiguar la naturaleza de la comunicación
	Desvelar la identidad de los comunicantes

Tabla 5: Ataques Pasivos y sus Objetivos

También es interesante descatar los otros nombres de estos tipos de ataques:

Ataques Pasivos	Alias
Ataques pasivos	Ataques de intercepción
Obtención de contenidos de mensajes	Intercepción de datos
Análisis del Tráfico	Intercepción de entidad

Tabla 6: Otros nombres de los ataques pasivos

En las siguientes ilustraciones se pueden ver cada uno de los diagramas de los ataques pasivos existentes:

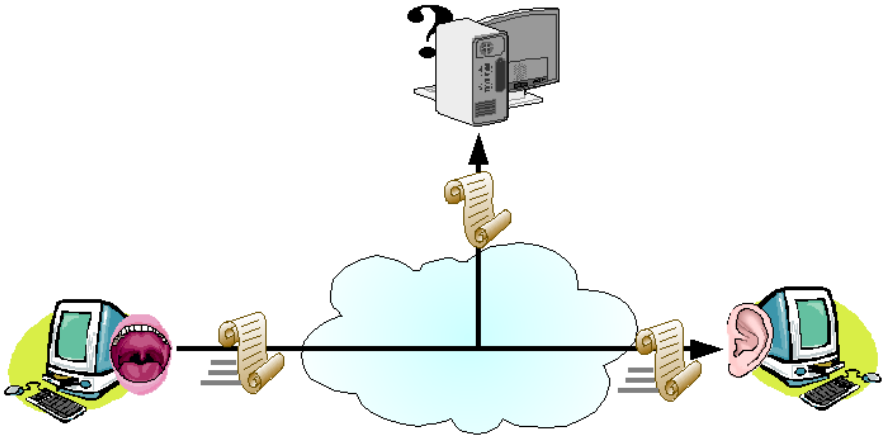

Ilustración 3: Obtención del contenido de mensajes

Un ejemplo de ataque pasivo mediante obtención de contenidos de mensajes podría ser: "Un usuario A envía un archivo a otro usuario B. El archivo contiene información confidencial que debe protegerse, por ejemplo los registros de nóminas. Otro usuario C, que no está autorizado a leer el archivo, observa la transmisión y captura una copia del archivo durante dicha transmisión".

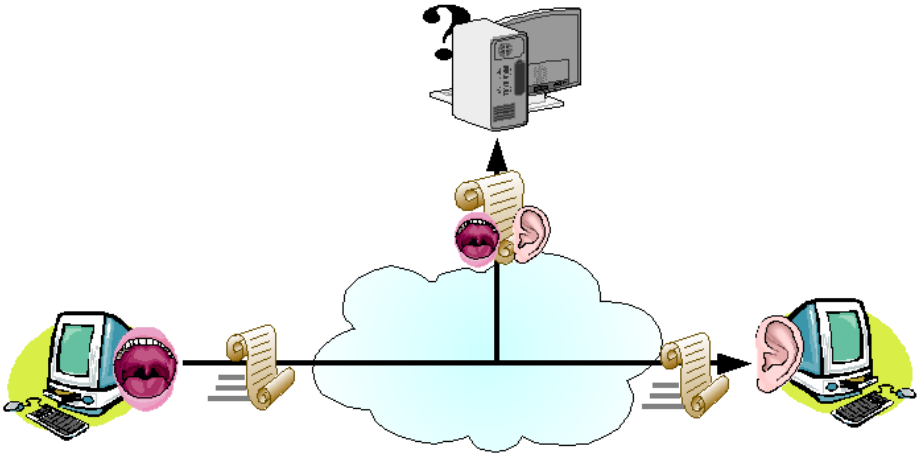

Ilustración 4: Análisis del tráfico

Para el caso de ataques basado en el análisis del tráfico, el ejemplo sería equivalente al anterior, excepto que en lugar de analizar el contenido de los paquetes que se transmiten a través de la red, se observan las cabeceras de cada uno de ellos.

2 Ataques activos

Existen varios tipos de ataques activos, que junto con sus objetivos, se mencionan a continuación:

Ataques Activos	Objetivos
Suplantación de identidad	Fingir ser otra entidad
Repetición	Retransmitir mensajes
Modificación de mensajes	Alterar, retrasar y/o reordenar mensajes
Interrupción del servicio	Dejar fuera de servicio algún recurso del sistema

Tabla 7: Ataques Activos y sus objetivos

Igualmente es interesante destacar los otros nombres de estos tipos de ataques:

Ataques activos	Alias
Suplantación de identidad	Falsificación de identidad
Repetición	Reactuación
Modificación de mensajes	Alteración de mensajes
Interrupción del servicio	Degradación fraudulenta del servicio

Tabla 8: Otros nombres de los ataques activos

A continuación, se pueden observar cada uno de los diagramas para cada uno de los ataques activos existentes:

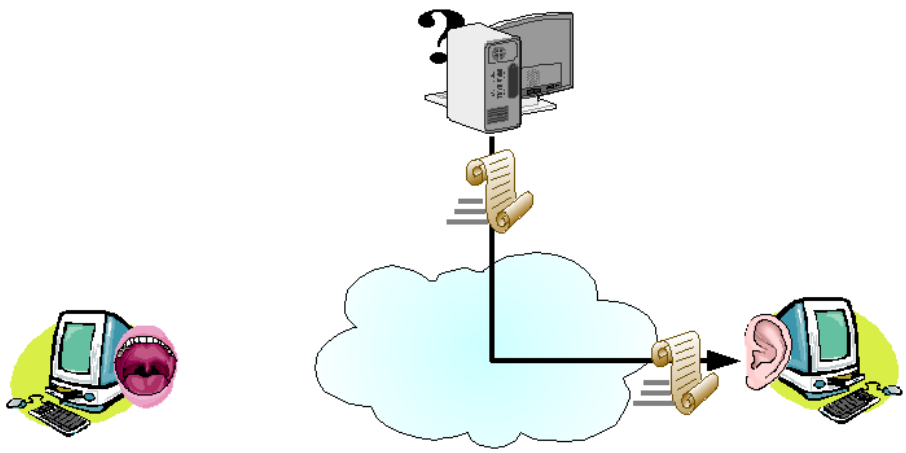

Ilustración 5: Suplantación de identidad

Un ejemplo de ataque por suplantación de identidad podría ser: "Más allá de interceptar un mensaje, un usuario podría construir un mensaje con las entradas deseadas, transmitiéndolo posteriormente a otro usuario como si procediera de la entidad suplantada, como por ejemplo la entidad de un administrador. Por consiguiente, el usuario receptor acepta el mensaje y reacciona ante el mensaje como si del administrador procediera. El mensaje podría ser cualquier tipo de información, como un fichero de los usuarios que están autorizados o no".

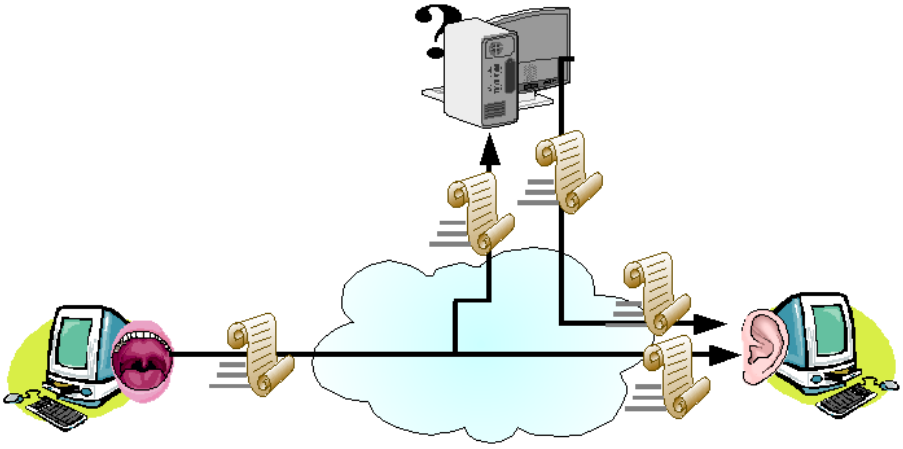

Ilustración 6: Repetición de mensajes

Por otro lado, un ejemplo de una posible consecuencia de un ataque mediante repetición de mensajes sería: "Haber ingresado dinero repetidas veces en una cuenta dada".

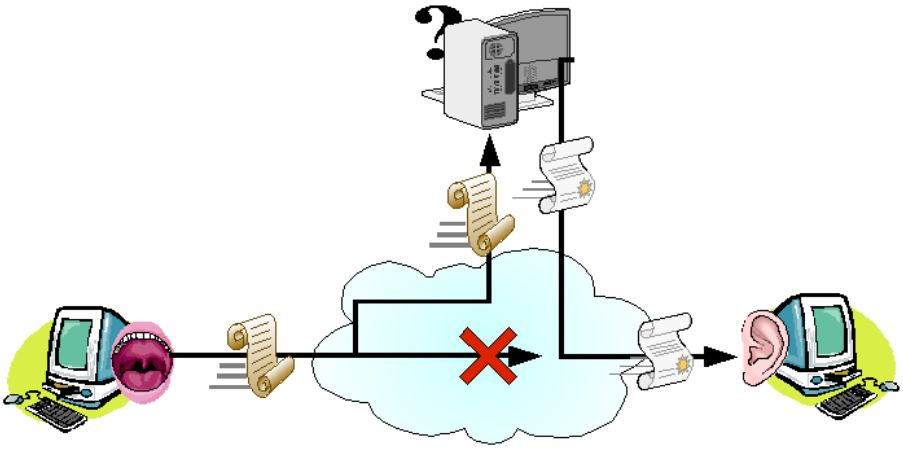

Ilustración 7: Modificación de mensajes

Para el caso de ataques mediante modificación de mensajes, algunos de sus objetivos podrían ser: "alterar un programa para que funcione de forma diferente" o "modificar una orden", por ejemplo, en lugar del mensaje "Ingresa un millón de pesetas en la cuenta A", podría ser modificado para decir "Ingresa un millón de pesetas en la cuenta B".

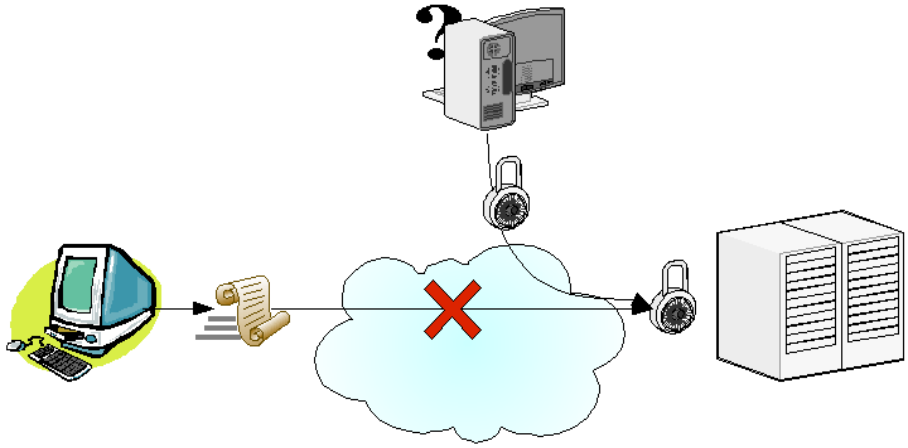

Ilustración 8: Interrupción de servicio

Finalmente, ejemplos de ataques mediante interrupción de servicio son: "Suprimir todos los mensajes dirigidos a una determinada entidad", "Interrumpir el servicio de una red inundándola con mensajes espurios" o "Deshabilitar el sistema de gestión de ficheros".

3 Servicios de seguridad

Un servicio de seguridad es un servicio que mejora la seguridad de los sistemas, contrarrestando los ataques a la seguridad, haciendo uso de uno o más mecanismos y políticas de seguridad con el objetivo de proporcionar el servicio. También pueden definirse como atributos deseables para que un sistema pueda considerarse seguro. Los principales servicios de seguridad, junto con sus objetivos son:

Servicios de Seguridad	**Objetivos**
Autentificación	Garantizar la procedencia de los objetos
Control de Acceso	Prevenir el uso no autorizado de los objetos
Confidencialidad	Proteger los objetos ante entidades no autorizadas
Integridad	Garantizar que no se puedan modificar los objetos sin ser detectado dicho hecho
No repudio	Asegurar que el receptor recibió los objetos
	Asegurar que el emisor envió los objetos
Disponibilidad	Asegurar que los objetos estén disponibles, evitando que entidades no autorizadas afecten a dicha disponibilidad

Tabla 9: Servicios de Seguridad y sus Objetivos

Un símil entre los servicios de seguridad y la vida cotidiana se establece en la siguiente tabla:

Servicios de Seguridad	**Ejemplos de la vida cotidiana**
Autentificación	DNI
Control de acceso	Llaves y cerrojos
Confidencialidad	Tinta invisible
Integridad	Tinta indeleble
No repudio	Firma notarizada

Tabla 10: Los Servicios de Seguridad y la vida cotidiana

Cada uno de los servicios de seguridad está pensado para hacer frente a uno o varios ataques. La siguiente tabla muestra dichas relaciones:

Servicios de Seguridad	**Ataques defendidos**
Autentificación	Suplantación de identidad
Control de Acceso	Suplantación de identidad
Confidencialidad	Obtención del contenido de mensajes
	Análisis del tráfico
Integridad	Repetición
	Modificación de mensajes
No repudio	——
Disponibilidad	Interrupción de servicio

Tabla 11: Ataques defendidos por los Servicios de Seguridad

4 Mecanismos de seguridad

Los mecanismos de seguridad son utilizados por los servicios de seguridad con el objetivo de contrarrestar los ataques a la seguridad. Es decir, para que los servicios de seguridad hagan frente a los ataques, es necesario que utilicen una serie de mecanismos de seguridad:

Servicios de Seguridad	Mecanismos utilizados
Autentificación	Criptografía
Control de Acceso	
Confidencialidad	
Integridad	
No repudio	
Disponibilidad	

Tabla 12: Mecanismos utilizados por los servicios

La criptografía es el mecanismo de seguridad primordial de todo sistema de seguridad, pero no es el único. Se pueden utilizar otros mecanismos tales como: el control de acceso, el intercambio de autentificación, la notarización, el control de enrutamiento, las auditorías de seguridad, la funcionalidad fiable mediante políticas de seguridad, las etiquetas de seguridad, la detección de acciones, los mecanismos de recuperación, etc.

El único mecanismo de seguridad que se tratará será la criptografía, cuyo único objetivo es construir objetos seguros.