1.

1. Introducción.

En los últimos tiempos el fenómeno Internet está provocando cambios tanto tecnológicos como culturales que están afectando a todos lo ámbitos de la sociedad, con una fuerte repercusión en el área de servicios.

Por lo tanto, la plataforma de servicios de Internet de la Seguridad Social pretende ser la base sobre la que montar todos los servicios que la Seguridad Social ponga a disposición del ciudadano, con el suficiente nivel de seguridad, tanto a nivel de acceso como a nivel de comunicaciones.

Debe permitir los siguientes servicios:

A usuarios externos (ciudadanos) :

- Servicios típicos de Internet (HTTP, FTP, etc.).
- Acceso a las bases de datos de la Seguridad Social, desarrollado apoyándose en servidores HTTP.
- Posibilidad de intercambio de información con la Seguridad Social (carga/descarga de ficheros).

A usuarios internos:

- Conexión con Internet.
- Correo electrónico SMTP.

Estos servicios han de ser prestados satisfaciendo las siguientes propiedades:

- Identificación o autenticación de los usuarios y servidores.
- Integridad de la información transmitida.
- No repudio del destinatario ni del origen.
- Confidencialidad de la información

2. Sistema de direccionamiento.

La Seguridad Social dispone de una red IP, con un sistema de direccionamiento propio, sobre el que descansa toda la infraestructura de comunicaciones.

Este sistema de direccionamiento, como es lógico es compatible con Internet, utilizando direcciones privadas (no válidas). Es decir, una dirección de la red de la Seguridad Social no se corresponde con ninguna dirección de Internet.

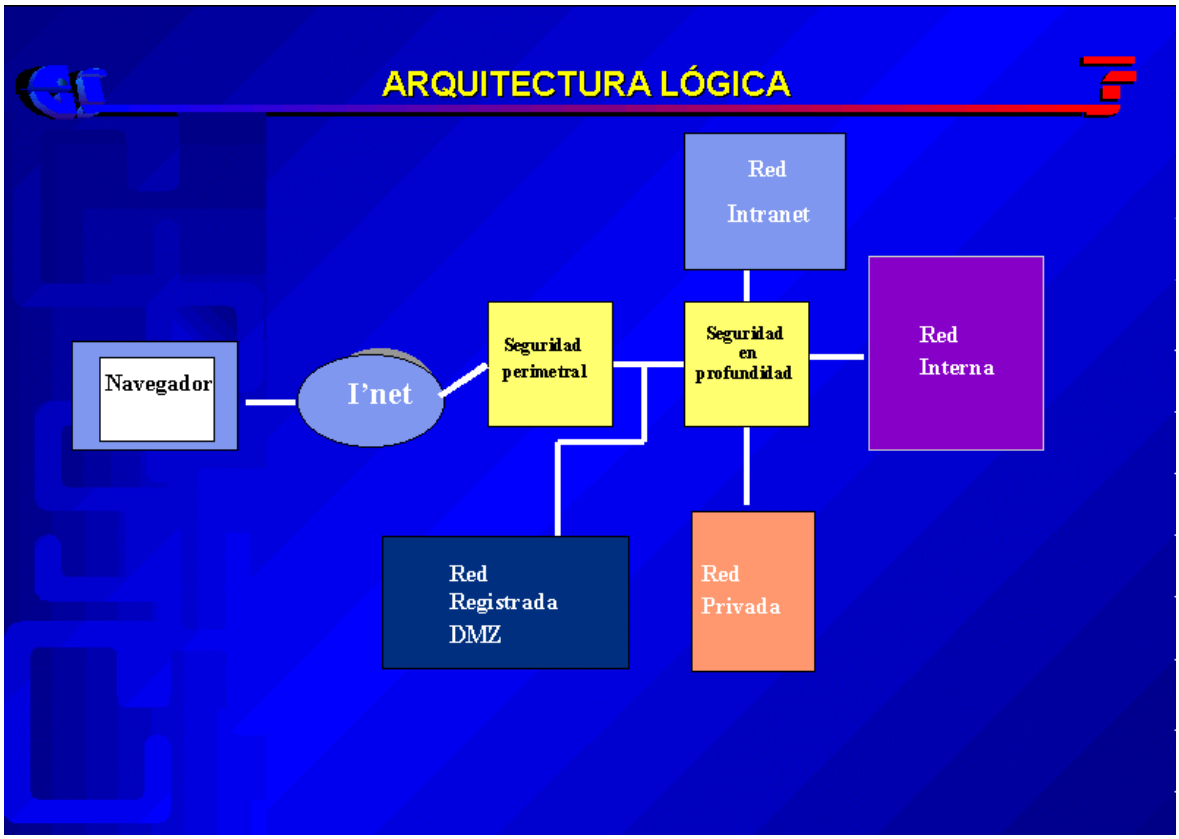
La Seguridad Social dispone de un rango de direcciones de Internet (clase C), suministrado por el proveedor de servicios de acceso, que se asignan a las máquinas, reconocidas en Internet.

Por lo tanto, existe una división lógica entre el entorno de la Seguridad Social y el mundo exterior proporcionada por el sistema de direccionamiento y regulado por el proxy.

Estos dos entornos son conocidos como red privada y red registrada. Cualquier servidor en la red privada, tendrá una dirección no conocida en Internet (dirección privada), mientras que los situados en la red registrada serán conocidos en Internet (dirección pública).

3. Arquitectura lógica de la plataforma.

En el esquema se puede ver que se han establecido cuatro redes diferenciadas:



- **Red Registrada o DMZ**. En esta red se encuentran todos los servidores de Internet que reciben las conexiones desde Internet. En esta red los servidores no contendrán ningún tipo de información confidencial. Aquí residirán los servidores web públicos, el servicio de DNS, el servicio de directorio público y el servidor de correo SMTP.

- **Red Interna.** En ella se sitúan los servidores de Aplicaciones, que establecen las conexiones con las bases de datos situadas en la Intranet.

- **Red Privada.** En esta se sitúan el servidor de directorio no público o maestro y el servidor de certificación.

- **Red Intranet.** Constituida por toda la red IP de la Seguridad Social. En ella se ubican los servidores que poseen los datos de carácter confidencial y crítico.

La existencia de estas redes nos permite tener un control de las conexiones que se establecen entre las distintas redes.

4. Seguridad en las Comunicaciones.

La necesidad de tener seguridad en las comunicaciones surge para:

- Controlar los accesos hacia/desde mi Organización. Al conectar la red de la Seguridad Social a Internet está expuesta a ser accedida desde ordenadores de la Internet.

- Al intercambiar datos confidenciales y acceder a aplicaciones críticas mediante una red pública, debemos asegurar que sólo accedan los que poseen permiso para ello. Para eso se necesita identificar con seguridad al usuario y que las comunicaciones sean seguras (cifradas).

La seguridad se puede establecer a varios niveles, el uso de la seguridad en uno o varios niveles nos permitirá alcanzar un grado mayor o menor de seguridad. En la plataforma se utilizan los siguientes niveles:

- Sistemas de Control de Acceso en red.
- Sistemas Antivirus.
- Sistemas de Cifrado.
- Sistemas de Identificación/Autenticación.
- Sistemas de Autorizaciones/Control de Acceso a aplicaciones.
- Disponibilidad de los servicios.
- Herramientas de auditoría y monitorización.

4.1. Sistemas de Control de Acceso en red.

En la plataforma de servicios de Internet de la Seguridad social se han utilizado los cortafuegos como sistemas de control de acceso en red y control de conexiones.

Un cortafuego o firewall es un dispositivo que controla las comunicaciones entre las distintas redes internas/externas; permitiendo o denegando el tráfico de acuerdo con las políticas de seguridad configuradas.

Por política de seguridad se entiende el conjunto de reglas que determinan desde dónde se puede iniciar conexiones, hacia qué destinos y para qué tipos de aplicaciones o servicios.

El firewall inspecciona todos los intentos de conexión de acuerdo a si se ajustan o no a la política de seguridad.

En la plataforma de Internet de la Seguridad Social se han empleado varios niveles de firewall, consiguiendo lo que se conoce como **Seguridad Perimetral** y **Seguridad en Profundidad**.

- la Seguridad Perimetral consiste en controlar todos los puntos de conexión entre la red Externa (Internet) y la red de la organización, mediante la utilización de un firewall. Con esto se consigue que no entren en la red de la organización todas las conexiones que se dirijan hacia un servidor que no sea público.

- La Seguridad en Profundidad consiste en controlar en cada servidor todas las comunicaciones que se dirigen hacia él. Esta medida sirve para conseguir que un servidor sólo admita conexiones dirigidas a los servicios que se quieran hacer públicos. Sirve para proteger tanto las conexiones externas como las internas.

Se han utilizado varios niveles de firewalls de diferente fabricante y tecnología, que nos permiten alcanzar un mayor grado de seguridad en el control del tráfico tanto de origen interno como externo, como protección de las zonas de la red interna.

4.2. Sistemas Antivirus.

Es importante disponer de un sistema antivirus para inspeccionar y tratar el contenido del tráfico de todo el correo entrante desde Internet . Antes de que un correo sea remitido al usuario final, se pasa por un servidor intermedio que inspecciona si los ficheros que incluye el e-mail contienen virus.

Existen dos posibilidades:

A) El correo no contiene virus. En este caso, el correo se remite al destinatario.

B) El correo contienen virus. En este caso, se detiene dicho correo, y se realizan las siguientes acciones:

Almacenado del correo en el servidor antivirus para su posterior examen (si procede)
Envío de mensaje de aviso al destinatario
Envío de mensaje de aviso al emisor
Envío de mensaje de aviso al postmaster de correo

1.1. Sistemas de cifrado.

La palabra **criptografía** deriva de **"cripto"** (oculto) y **"grafos"** (escritura) y su objetivo es garantizar la privacidad y autenticidad del mensaje y del emisor.

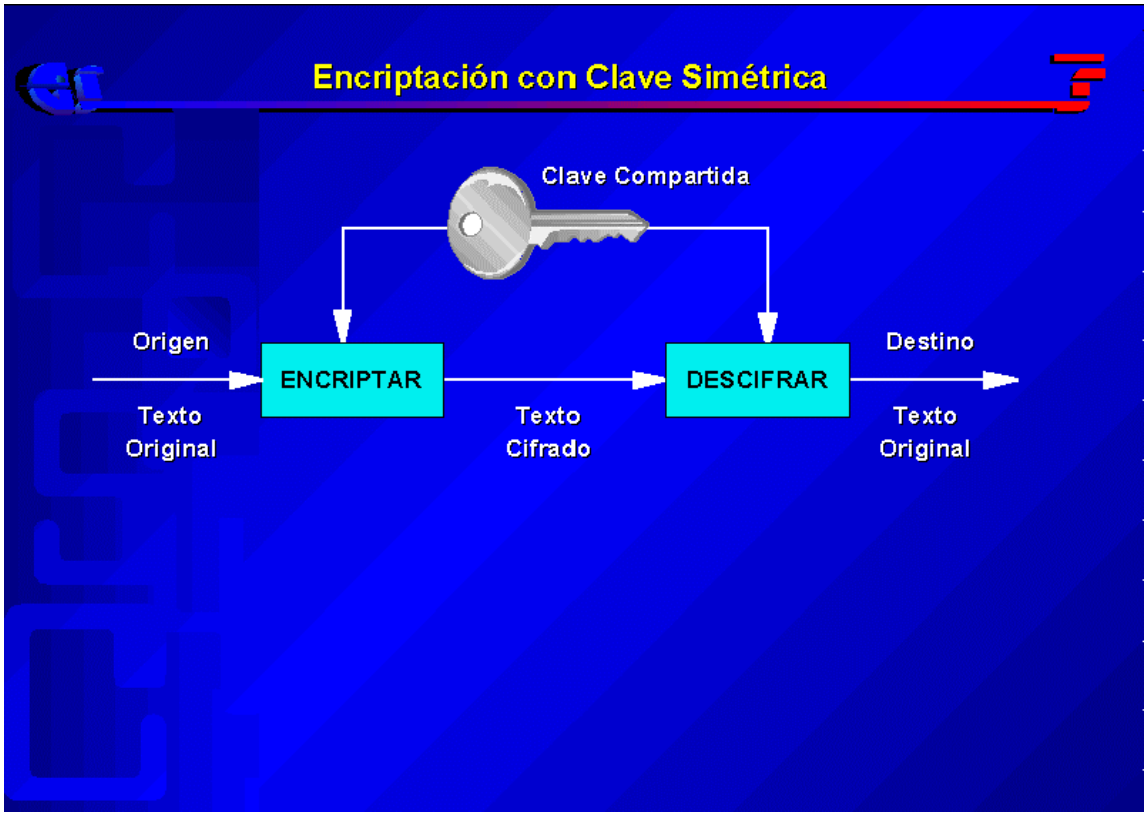
La técnica de cifrado se basa en un algoritmo de cifrado y una clave, de tal forma que se requieren ambos para generar, a partir del texto claro, el texto cifrado. Para descifrar se requiere un algoritmo de descifrado y una clave de descifrado.

La seguridad de las técnicas criptográficas nos se basan en la ocultación del algoritmo de cifrado/descifrado, que es público, sino en la ocultación de la clave de cifrado/descifrado.

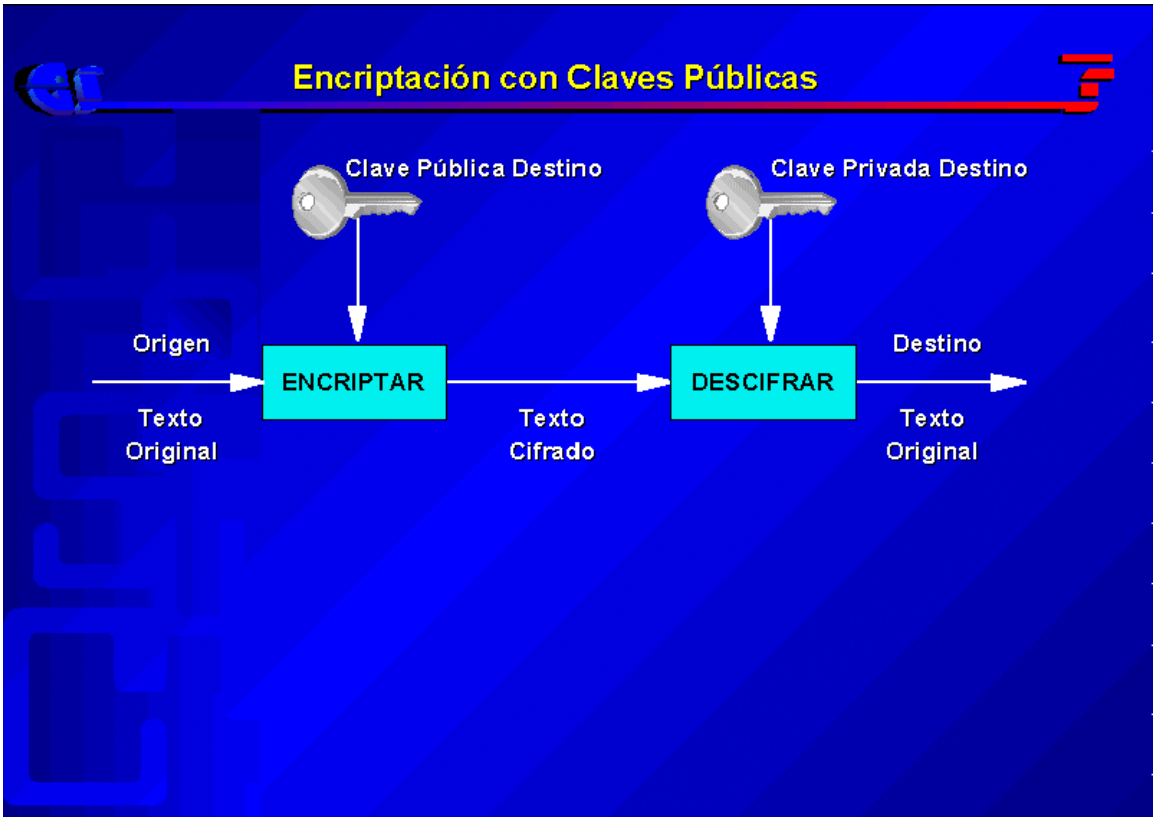
Se distinguen básicamente dos tipos de cifrados:

- Algoritmos de clave privada o simétricos (DES, IDEA). Se caracteriza por un único algoritmo de cifrado/descifrado, aunque en la ejecución de ambas operaciones pueden existir pequeñas variaciones, y una única clave para cifrar y descifrar. Esto implica que la clave tiene que permanecer oculta y ser compartida por el emisor y el receptor. Lo que significa que se debe distribuir en secreto y se necesita una clave para cada par de interlocutores.

Algoritmos de clave pública o asimétricos (RSA, Diffie-Hellman). Se caracterizan por la existencia de dos claves independientes para cifrar y descifrar. Esta independencia permite al receptor hacer pública la clave de cifrado, de tal forma que cualquier entidad que desee enviarle un mensaje pueda cifrarlo y enviarlo. La clave de descifrado permanece secreta. A los mecanismos de clave pública se les puede englobar bajo las



siglas de PKI (Infraestructura de clave pública).



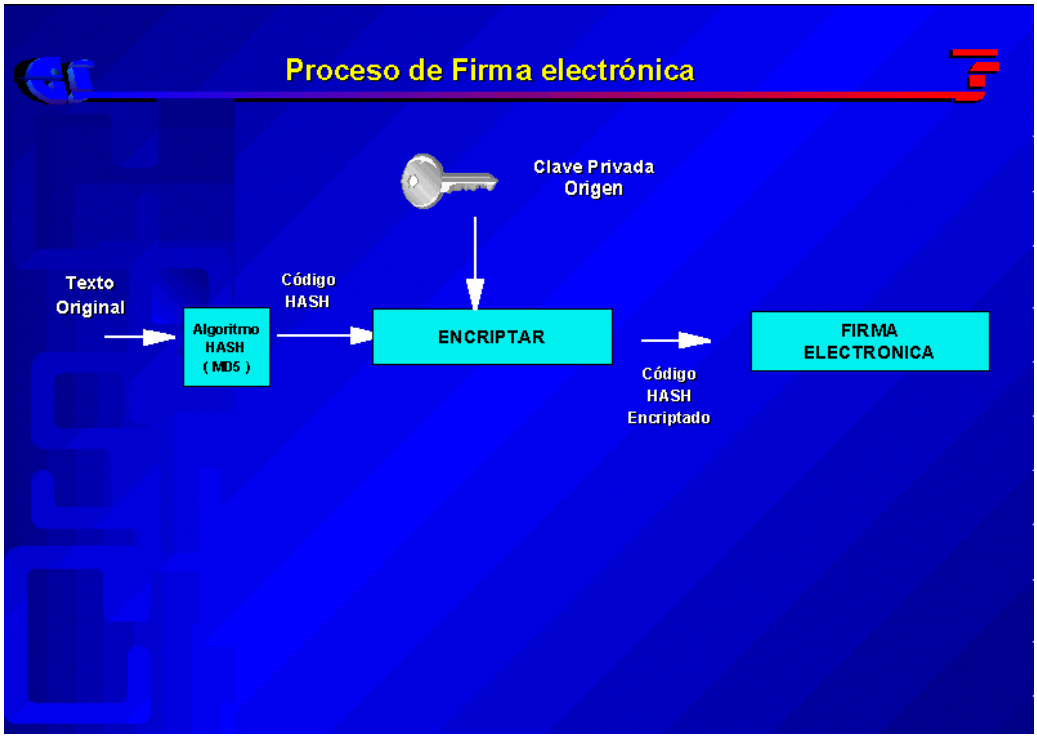
Función hash unidireccional. Una función que acepta un mensaje de entrada y genera un mensaje de salida, es una función hash unidireccional si cumple las siguientes características:

⇒La longitud de los mensajes de salida es fija e independiente de la longitud de los de entrada.

⇒Es fácil obtener el mensaje de salida a partir de la entrada, pero difícil conseguir la entrada a partir de la salida.

⇒Dada una entrada, es muy difícil conseguir otra tal que produzca el mismo mensaje de salida que la primera.

Estas características hacen a estas funciones valiosas para generar una especie de huella dactilar de un mensaje. Dado un mensaje se obtiene su hash, que identifica de forma unívoca al original. Si se conserva el hash de un mensaje se puede, sin almacenar el mensaje original, determinar si un nuevo mensaje presentado coincide con el original sin más que calcular el hash del nuevo mensaje y comprobarlo con el hash almacenado. Esta función hace muy útil este tipo de función para la firma digital.



En el proceso de firma, para evitar el coste computacional del cifrado y descifrado con clave pública de documentos grandes, se realiza lo siguiente:

Se genera un hash del documento a firmar

Se firma, cifrando con la clave privada el hash del documento. Esto es equivalente a firmar el documento.

Se envía el documento y su hash firmado al receptor.

El receptor para verificar la firma, genera el hash del documento. Descifra el hash firmado recibido y lo compara con el que ha producido él mismo. Si son iguales la firma es auténtica.

La firma digital se define como el conjunto de datos que se añaden a una unidad de datos para protegerlos contra la falsificación, permitiendo al receptor probar la fuente.

Permite asegurar:

La identidad del autor de la información.

Integridad (inalterabilidad) del contenido del documento luego haber sido firmado.

Un certificado como concepto es la clave pública del poseedor del certificado, más una información añadida (datos de identidad), todo ello firmado por la clave privada de la Autoridad de

Certificación. Esta Autoridad de certificación es la entidad que avala mediante su firma, que el poseedor del certificado es quien dice ser.

En la plataforma los sistemas de cifrado han sido utilizados tanto a nivel de aplicación como de comunicaciones.

Los mecanismos de cifrado empleados están basados en la utilización de la tecnología de certificación digital mediante criptografía de clave pública PKI. Cuando los usuarios acceden a aplicaciones críticas el canal de comunicación entre el usuario y el servidor está cifrado mediante criptografía fuerte de 128 bits.

Esta tecnología también está disponible para que las aplicaciones hagan uso de ellas, de manera que se ha desarrollado una aplicación de transferencia de ficheros que los envía cifrados y firmados. De esta manera, existe un doble nivel de cifrado; por un lado los ficheros que se transfieren están cifrados y por otro el propio canal es cifrado.

1.2. Sistemas de Identificación/Autenticación.

El sistema de identificación está basado en la utilización de criptografía de clave pública y por tanto del uso de certificados digitales X509v3.

Para la obtención de un certificado es necesario un proceso de registro en el que la Autoridad de Registro verifica los datos del usuario y certifica que es quien dice ser.

Una vez registrado se genera la emisión de un certificado digital X509v3 por la Autoridad de Certificación. Consiste en un sistema de doble par de claves (firma y cifrado). Este tipo de certificado garantiza el no-repudio, puesto que el par de claves de firma se generan en el puesto del usuario.

1.3. Sistemas de Autorizaciones/Control de Acceso a Aplicaciones.

El Sistema de autorizaciones permite establecer qué permisos posee cada usuario que accede a la organización, y controlar que sólo se accede a aquellas aplicaciones e información para las que está autorizado.

El sistema de autorizaciones empleado en la plataforma se basa en dos conceptos:

⇒Recursos
⇒Perfiles

Recurso es toda aplicación (URL) sobre la que se quiere el acceso sólo a determinados usuarios.

Perfil es un conjunto de recursos relacionados, que se quieren permitir o denegar simultáneamente.

El usuario se identifica al sistema mediante un certificado digital, a continuación se pasa la identidad del usuario al servicio de autorización. Este está compuesto de los siguientes elementos:

Servidor de Acceso. Servidor Web encargado de mostrar la página inicial de acceso al sistema, obtener la identificación del usuario y devolver una página con un menú personalizado para el usuario en particular.

Runtime de protección de servidores Web. Es el software encargado de pedir la autorización al servidor de registro para permitir o denegar el acceso a recursos accesibles a través de un servidor web.

Servidor de Registro. Mantiene la información actualizada en su base de datos sobre qué recursos puede acceder el usuario.

1.4. Disponibilidad de los Servicios.

Todos las máquinas utilizadas en la plataforma poseen sistemas de doble alimentación, sistemas de arrays de disco y posibilidad de cambio en caliente de discos averiados.

Existe, además, servicios en alta disponibilidad y balanceo de carga.

El mecanismo empleado para conseguir balanceo de carga y alta disponibilidad está basado en la utilización de equipos conmutadores de nivel 4 que realizan las siguientes funciones:

Reparten las peticiones de los usuarios entre los distintos servidores existentes (de manera transparente al usuario). Las peticiones pertenecientes a una misma sesión son enviadas al mismo servidor final.

Comprueban que los servidores se encuentran activos. En cuanto uno de los servidores no responde, las peticiones se reparten entre el resto de los servidores disponibles.

Los servicios que actualmente se encuentran en alta disponibilidad y balanceo de carga son:

Cortafuegos externos.
Servidores Web.
Sevidores Proxy.

Y en alta disponibilidad se encuentra el servidor de directorio.

1.5. Herramientas de auditoría y monitorización.

Este tipo de herramientas nos permiten tener un control sobre todos los paquetes que entran por el interfaz de red de la máquina: IP (TCP/UDP) e ICMP, o analizando paquetes a nivel de aplicación (telnet, ftp, smtp, login, shell, etc.). Algunas de estas herramientas pueden tener el incoveniente de tener un doble uso, es decir nos permiten protegernos ante posibles ataques, pero también podrían ser utilizadas para intentar comprometer los sistemas. Por eso es importante que el uso de las mismas esté restringido.

Entre estas herramientas tenemos:

TCP-WRAPPERS. Software de dominio público cuya función principal es proteger a los sistemas de conexiones no deseadas a determinados servicios de red, permitiendo a su vez ejecutar determinados comandos ante determinadas acciones de forma automática.

SATAN (Security Administrator Tool for Analyzing Networks). Software de dominio público que chequea máquinas conectadas en red y genera informes sobre el tipo de máquina, servicios que da cada máquina y avisa de algunos fallos de seguridad. Utiliza un interfaz WWW y crea una base de datos de todas las máquinas chequeadas. También tiene el incoveniente de que puede ser usada como ataque al sistema y descubrir la topología de la red de la organización.

COPS (Computer Oracle and Password System). Conjunto de programas que chequean ciertos aspectos del sistema operativo UNIX relacionados con la seguridad. También genera un informe.

Ninguna de las herramientas anteriores u otras del mercado deben reemplazar la monitorización realizada personalmente por el administrador del sistema, pero sí ayuda a realizar esta tarea.

2. Servicios.

En el presente apartado, se indican los principales detalles funcionales de operación de cada uno de los servicios.

SERVICIO WWW

Se encarga de suministrar páginas de información a los clientes, en su mayoría externos, que se conectan al servidor mediante un browser WWW. Asimismo, posee otra serie de características adicionales, como pueden ser:

Logging de las conexiones realizadas
Posibilidad de definir múltiples Sites WWW en un único servidor
Manejo de certificados de servidor (para proporcionar soporte de HTTPS, protocolo HTTP seguro).
Estadísticas, utilidades de administración y varios

SERVICIO DE TRANSFERENCIA DE FICHEROS (SERVICIO FTP)

Propósito del Servicio: Su funcionalidad básica es la de permitir a los usuarios enviar y recibir ficheros de información desde una máquina dada, denominada servidor FTP.

Se soporta el servicio FTP sujeto a las siguientes restricciones:

Solo usuarios muy específicos y desde un número de máquinas determinado tiene acceso a los servidores FTP existentes en la plataforma con acceso a la parte privada de dicho servidor.

Se soporta el servicio público de transferencia de forma pública, restringido a una parte del servidor y con los controles de seguridad correspondientes.

SERVICIO DE ACCESO A INTERNET (SERVICIO PROXY)

Propósito del servicio: Se define a este servidor como punto de salida para todos los usuarios internos que estén autorizados para utilizar servicios WWW de Internet, externos a la

organización. Proporciona funciones de autenticación y validación, caché de las páginas accedidas.

SERVICIO DE RESOLUCIÓN DE NOMBRES (SERVICIO DNS)

Propósito de este servicio: Este servicio permite a los clientes averiguar la dirección IP de una máquina, a partir de su nombre. Se interroga al servidor DNS con el nombre y éste devuelve la dirección IP de dicha máquina. Al proceso de realizar la consulta al servidor DNS se le denomina consulta DNS (en inglés query DNS).

Asimismo, se permite realizar la pregunta inversa: Dada una dirección IP, el servidor DNS responde con el nombre de dicha máquina. A este tipo de consulta se le denomina consulta inversa DNS (inverse query DNS).

Se tienen los siguientes servidores:

Uno maestro, situado en la DMZ.
Uno esclavo, situado en la red privada.

SERVICIO DIRECTORIO (LDAP)

Propósito del servicio: Dada la organización de los usuarios de la GISS, organizada según una estructura jerárquica, se le permite a los clientes realizar consultas sobre dicha información, asimismo, se permiten otras funcionalidades extras:

Replicación de la información entre dos servidores
Ocultación de parte de la estructura jerárquica

SERVICIO DE CORREO (SMTP)

Se tiene una pasarela de correo situada en la DMZ. La función de esta pasarela es la conversión y conectividad entre el correo electrónico propio de Internet y el sistema de correo electrónico corporativo interno (Lotus NOTES).

SERVICIO SINCRONIZACIÓN DE TIEMPO

Se soporta un servidor de Sincronización de Tiempo, de acuerdo al standard NTP, situado en la red Privada. Dicho servidor

proporciona una referencia de tiempo exacta para sincronizar todas las máquinas a él conectadas.

SERVICIO TIME STAMP

Este servicio sirve para suministrar una firma con la fecha y hora de estampación a un determinado documento. Sería el equivalente informático de un matasellos de un registro de entrada. Los clientes podrán solicitar a este servicio que se les firme con la fecha actual documentos a él suministrados.

SERVICIOS PKI (CERTIFICADOS, CA)

Con este servicio se proporciona el soporte de conexiones seguras por parte de los servidores de Internet. En concreto, las cuatro características básicas que se le pueden exigir a una comunicación segura:

Autenticidad. EL usuario que emite la información se identifica al sistema

Confidencialidad. En la conversación entre emisor no se pueden interponer elementos que intercepten la información

No repudio. El usuario emisor no puede negar que no ha sido él el que se ha comunicado con el sistema receptor

Integridad. La información viaja con unos tests que verifican que ésta no ha sido alterada en el camino entre el emisor y el receptor.

Una PKI tiene como objetivos básicos la expedición y gestión de certificados. Esta se compone de cuatro elementos:

1. **La Autoridad de Certificación (CA).** Se encarga de crear (firmar) los certificados.
2. **La Autoridad de Registro (RA).** La CA puede delegar ciertas tareas administrativas en otra(s) entidade(s) confiable(s). Así la RA puede realizar las siguientes funciones:

Verificar identidad del sujeto.

Verificar que el usuario suministra todos los datos que se solicita.

Una vez verificados los datos envía una petición de certificado a la CA, que es la única entidad con responsabilidad para crear certificados. Pueden existir

varias Autoridades de Registro distribuidas físicamente para facilitar la provisión de servicios a las entidades finales.

3. **La entidad Final.** Entidades que solicitan los certificados y que hacen uso de ellos. Se engloba tanto usuarios físicos (personas) y máquinas.

4. **El repositorio directorio.** Es el lugar público donde la CA publica los certificados.

Se proporciona un sistema capaz de realizar las siguientes tareas:

Emitir certificados para un usuario final
Emitir certificados para una máquina servidora
Permitir aceptar certificados de otra CA (autoridad de certificación)
Revocar (dar de baja) un certificado
Comprobar si un determinado usuario tiene permisos para acceder a un recurso
WWW específico
Interactuar con otros sistemas PKI de otras entidades para cruzarse información de gestión.