Aplicación de mecanismos de seguridad activa (Seguridad informática)

Identificación digital. Firma electrónica y certificado digital

La firma electrónica es un conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico y cuyas funciones básicas son:

- Identificar al firmante de manera inequívoca
- Asegurar la integridad del documento firmado. Asegura que el documento firmado es exactamente el mismo que el original y que no ha sufrido alteración o manipulación
- Asegurar el no repudio del documento firmado. Los datos que utiliza el firmante para realizar la firma son únicos y exclusivos y, por tanto, posteriormente, no puede decir que no ha firmado el documento

Para firmar un documento es necesario disponer de un certificado digital o de un DNI electrónico.

El certificado electrónico o el DNI electrónico contiene unas claves criptográficas que son los elementos necesarios para firmar. Los certificados electrónicos tienen el objetivo de identificar inequívocamente a su poseedor y son emitidos por Proveedores de Servicios de Certificación.

Seguridad en los protocolos para comunicaciones inalámbricas

La configuración por defecto del router no siempre es la más

apropiada.

El router debe incorporar al menos el protocolo WPA entre sus medidas de seguridad. Si es anterior a esta opción de seguridad debemos sustituirlo.

El sistema más avanzado de todos los que hay ahora mismo es WPA2, se utiliza el cifrado de tipo AES para securizar la comunicación inalámbrica.

Utilización de cortafuegos en un sistema o servidor

Cuando un programa de nuestro ordenador necesita acceder a Internet, establece una conexión en la que enviará o recibirá la información que le sea necesaria, desde nuestro ordenador hacia Internet o desde Internet hacia nuestro PC, dando lugar a conexiones entrantes o salientes.

El cortafuegos, más conocido como firewall, es una herramienta que permite gestionar qué programas pueden establecerlas y qué programas no, y qué tipo de conexiones serán permitidas.

Listas de control de acceso

Una lista de control de acceso es una lista de permisos asociados con un recurso del sistema. Una ACL especifica qué usuarios o procesos del sistema tienen acceso a los objetos, así como qué operaciones están permitidas en determinados objetos.

Política de contraseñas

Las contraseñas que se utilizan para validarse contra cualquier sistema tienen que ser robustas, por ejemplo estar formada por al menos 8 caracteres: mayúsculas, minúsculas, números, caracteres especiales.

Recomendaciones básicas para elegir contraseñas:

- **Debemos asegurarnos que la contraseña tenga** una:
  - longitud mínima de ocho caracteres,
  - que combine mayúsculas,
  - minúsculas,
  - números y
  - símbolos.
- **No debemos utilizar como claves:**
  - palabras sencillas en cualquier idioma,
  - nombres propios,
  - lugares,
  - combinaciones excesivamente cortas,
  - fechas de nacimiento,
  - etc.
- **Tampoco debemos usar claves formadas únicamente a partir de la concatenación de varios elementos**. Por ejemplo: «Juan1985» (nombre + fecha de nacimiento).

Recuperación de datos

La recuperación de datos es el conjunto de técnicas y procedimientos utilizados para acceder y extraer la información almacenada en medios de almacenamiento digital que por daño o avería no pueden ser accesibles de manera usual.

Software malicioso. Clasificación. Herramientas de protección y desinfección

Un virus es un software que tiene por objetivo alterar el funcionamiento de cualquier tipo de dispositivo informático, sin el permiso o el conocimiento del usuario principalmente para lograr fines maliciosos sobre el dispositivo.

Las herramientas que sirven para detectar y eliminar virus son

los antivirus. Con el transcurso del tiempo, los antivirus han evolucionado hacia programas más avanzados que además de buscar y detectar virus informáticos consiguen bloquearlos, desinfectar archivos y prevenir una infección de los mismos.