SEGURIDAD LÓGICA

***IDENTIFICACIÓN*:** Momento en que el usuario se da a conocer en la app.

AUTENTICACIÓN: Verificación que hace el sistema sobre la identificación.

MODALIDAD DE ACCESO

Modo de acceso permitido a usuarios sobre los recursos. Pueden ser:

- ***LECTURA***
- ***ESCRITURA***
- ***EJECUCIÓN***
- ***BORRADO***
- ***CREACIÓN***
- ***BUSQUEDA***

CONTROL DE ACCESO INTERNO

PALABRAS CLAVES (PASSWORDS): Se usan para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones.

CIFRADO: Si se cifra información, solo podrá ser descifrada por quienes posean la clave. Provee una potente medida de control de acceso.

LISTAS DE CONTROL DE ACCESO: Es un registro que contiene nombres de usuario con permisos y modalidad de acceso permitidos para un determinado recurso del sistema.

ETIQUETAS DE SEGURIDAD: Consiste en designaciones otorgadas a los recursos (como un archivo por ej) que pueden utilizarse para control de accesos, especificación de medidas de protección, etc. No son modificables.

CONTROL DE ACCESO EXTERNO

DISPOSITIVOS DE CONTROL DE PUERTOS: Autorizan el acceso a un puerto determinado y pueden estar físicamente separados o incluidos en otros dispositivos como, por ejemplo, un modem.

FIREWALLS O PUERTAS DE SEGURIDAD: Es un dispositivo de red que crea una separación entre redes públicas (no confiables) y redes privadas (confiables) mediante el análisis de tráfico de red.

Funcionamiento: lo que no está prohibido, está permitido y viceversa.

CARACTERÍSTICAS:

- *Dispositivos de defensa perimetral que separan redes.*
- *Filtran tráfico según reglas predefinidas.*
- *NO PROTEGEN ATAQUES INTERNOS.*

- *NO PROTEGEN DE ACCESOS AUTORIZADOS.*
- *NO PROTEGEN TOTALIDAD DE ATAQUES DAÑINOS.*

Se clasifican en:

- De tipo software: Componentes lógicos que funcionan en una pc con dos o más NICs.
- Appliances o dispositivos de hardware: (a modo de cajas negras) que fueron diseñados para esta tarea.

DMZ – ZONA DESMILITARIZADA: Es un área de configuración del firewall con reglas específicas orientadas a manejar equipos que deben tener mayor exposición en la infraestructura, como por ejemplo los servidores web, entre otros.

TIPOS DE FIREWALLS:

- ***Packet Filters:*** Este tipo monitorea las direcciones IP de origen y destino de la conexión.
- ***Circuit Level Gateways:*** Es un firewall que opera a nivel de la capa de sesión del modelo OSI o la capa TCP de TCP/IP.
- ***Application Level Gateways:*** Son llamados proxis. Conceptualmente son iguales a los CLG solo que son específicos para cada aplicación/protocolo.
- ***State-Full Multiplayer Inspection:*** Combina los tres tipos previos. Usa protocolos de control de paso de contenidos a través de reglas de validación.

FIREWALLS PERSONALES: Son dispositivos lógicos (software) que se instalan en la propia terminal y permiten aplicar filtros a la información de red correspondiente a cada interfaz y/o aplicación.

IDS – SISTEMA DE DETECCIÓN DE INTRUSIONES: Elemento que detecta, identifica y responde a actividades no autorizadas o anormales.

Intrusión: Conjunto de acciones que intentan comprometer la integridad, confidencialidad o disponibilidad de un recurso.

Se clasifican en:

- **HIDS – Sistema de detección de intrusiones de máquina:** Utilizan los registros de auditoría, del sistema y de aplicaciones.
- **NIDS – Sistema de detección de intrusiones de red:** Utilizan paquetes de red (TCP, UDP, IP...).

IPS – SISTEMA DE PREVENCIÓN DE INTRUSIONES: Es el resultado de combinar un IDS + Firewall en respuesta activa. Estos dispositivos identifican el curso de un ataque y lo bloquean antes de que suceda.

DISPOSITIVOS UTM: Son firewalls de red que manejan diferentes servicios en un mismo equipo, algunos de ellos son:

- Función de un firewall de inspección de paquetes.
- Función de VPN.
- Antispam.
- Antipishing.
- Antispyware
- Filtrado de contenidos.
- Antivirus de perímetro.
- Detección/Prevención de intrusos (IDS/IPS).

TIENEN 2 MODOS DE CONFIGURACIÓN:

MODO PROXY: Usan proxis para procesar y redirigir todo el tráfico interno.

MODO TRANSPARENTE: No redirigen, solo lo procesan y analizan el tiempo real de los paquetes.

NGFW- NEXT GENERATION FIREWALLS: Nueva generación de firewalls se basa en inspección profunda de paquetes + tecnología que evita intrusiones.

WAF – WEB APPLICATION FIREWALL: Dispositivo físico o lógico que analiza el tráfico web (entre servidor web y la WAN), los datos recibidos del usuario y protege de ataques como: SQL Injection, Cross Site Scripting, Remote and Local File Inclusión, Buffer Overflows, Cookie Poisoning, etc. Tiene dos modelos:

POSITIVA: Deniega todas las transacciones, aceptando solo las que considera segura.

NEGATIVA: Acepta todas las transacciones y deniega las consideradas amenazas.