1. **Concepto de seguridad lógica**

La seguridad lógica es el conjunto de medidas destinadas a la protección de los datos y aplicaciones informáticas, así como a garantizar el acceso a la información únicamente por las personas autorizadas

1. **Políticas de seguridad corporativa**

Normas claras de lo que se puede y no al operar con un sistema informático, estas normas configuran el marco de actuación de todos los usuarios.

Son aplicables a toda la empresa, también existen normas específicas para los distintos sectores

* Instalación, mantenimiento y actualización de los equipos
* Control de acceso a áreas críticas de la empresa y a recursos críticos del sistema
* Utilización de recursos de las redes informáticas
* Mantenimiento de las redes
* Adquisición, instalación y actualización de software
* Privacidad de la información
* Autentificación de usuarios
* Información de errores o de accesos al sistema
* Contraseñas

1. **Medidas o mecanismos establecidos en las políticas de seguridad**

* Autentificación de usuarios
* Listas de control de accesos
* Criptografía
* Certificados digitales
* Firmas digitales
* Cifrado de unidades de disco o sistemas de archivos

1. **Contraseñas**

Son la llave que permite el acceso a aplicaciones y sistemas informáticos. Está formada por símbolos, números, letras, mayúsculas y minúsculas

Hay que ser estrictos a la hora de controlar las contraseñas de acceso al sistema desde todos los puntos de vista

Existen gestores de contraseñas que almacenan nuestras contraseñas de forma segura

Existen diversos sistemas para averiguar una contraseña

* Sniffers: Registran la actividad de un equipo e interceptan las comunicaciones
* Keyloggers: Programas que capturan las pulsaciones de un teclado
* Fuerza bruta: Probar todas las combinaciones
* Por diccionarios: Generan diccionarios con términos relacionados con el usuario y prueban todas esas palabras como contraseñas
* Ingeniería social: Engañar a los usuarios para que proporcionen sus contraseñas a los intrusos

Hay que seguir unas reglas a la hora de establecer nuestra contraseña

* No deben ser o tener palabras usuales ni relacionadas con nuestro entorno
* No deben ser palabras con significado
* Combinación de mayúsculas, minúsculas, números y otros caracteres
* Longitud min de 8 caracteres
* No utilizar la misma en varios sitios
* Cambiar las contraseñas

1. **Sistemas de control de acceso**

* Dependientes: También llamados online, están conectados por red y permiten la supervisión a través de internet
* Autónomos: Se auto gestionan o lo hacen mediante un dispositivo adjunto, con el inconveniente de estar aislados de la red y la ventaja de que se reducen costes de conexión
* Autónomos convertibles: Sistemas autónomos que permiten ser configurados para su conexión a un ordenador que controla sus funciones

1. **Teclados**

Abren puertas tras introducir la contraseña, tienen una limitación en cuanto a número de usuarios

1. **Tarjetas de proximidad**

Permiten la entrada al portador de la tarjeta y permiten conocer la identidad del titular

Hay dos tipos, de banda magnética (sufren mas deterioro) y con código de barras

Son sistemas autónomos, limitación por números de usuarios (miles), borrar cada persona que deja la tarjeta

1. **Llaves electrónicas de contacto**

Pastilla electrónica incluida dentro de una carcasa de acero inoxidable y montada en un soporte de material plástico

1. **Sistemas biométricos**

La biometría es el estudio de métodos que permiten reconocer a seres humanos basándose en factores genéticos o determinados rasgos físicos o conducta

Para que un control biométrico sea fiable debe crearse un torno a características humanas.

Es efectivo, no provoca rechazo ni pone en peligro la salud ni integridad física, tiene que ser robusto y que no se pueda usar de forma fraudulenta

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Voz | Iris Ojo | Retina | Huellas dactilares | Geometría de la mano | Escritura Firma |
| Fiabilidad | alta | alta | alta | alta | Alta | alta |
| Facilidad de uso | alta | media | baja | alta | alta | alta |
| Prevención de ataques | medio | alta | alta | alta | alta | medio |
| Aceptación | media | Media | media | media | alta | Muyalta |
| Interferencias | Ruido, resfriados | Gafas, lentillas | Enfermedadesoculares | Heridas | Roturas de brazo, quemaduras | Firmas simples |

1. **Listas de control de acceso**

Herramienta que permite controlar que usuarios pueden acceder a las distintas aplicaciones, sistemas, recursos, dispositivos.

Ventajas:

* Mejora el rendimiento de la red limitando determinado trafico
* Permitir o denegar el acceso de equipos a ciertas zonas de la red
* No se ejecuten determinados comandos por la red destinados a fines malintencionados

Inconvenientes

* Exhaustividad en el nivel de control complica bastante la administración de la seguridad del sistema

1. **Acceso a aplicaciones por Internet**
   1. Mantener actualizados tanto el sistema operativo como el navegador y un antivirus actualizado
   2. Correcta administración de los nombres de usuario y contraseñas
   3. Desconfiar de webs en las que par regenerar una contraseña olvidada permiten introducir una cuenta de correo
   4. Acceder a las distintas aplicaciones desde un ordenador seguro si los datos son muy sensibles
   5. No facilitar por correo electrónico ni por teléfono las contraseñas ni modificarlas
   6. Nunca acceder a través de enlaces
   7. Cerrar la sesión correctamente
2. **Phishing**

Fraude que suplanta la identidad de personas o entidades de Internet para conseguir la contraseña de usuarios reales.

1. **VeriSign**

Empresa proveedora de servicios de autentificación que actúa como autoridad de certificación a nivel mundial. Emite certificados SSL para la protección de sitios en Internet

1. **HTTPS**

Aparece en la barra de navegación, si la dirección no empieza por https no es segura, además suele aparecer un candado cerrado

1. **John theRipper**

* Sudo apt install John
* John --test ( probar rendimiento)
* Touchpassword.txt (crear archivo y poner dentro **user:AZL.zWwxIh15Q**)
* John password.txt (indicar que John empiece a trabajar FUERZA BRUTA)
* John –show password.txt (mostar contraseña FUERZA BRUTA)
* Touchpasswords.lst (crear diccionario y copiar lo del fichero .txt)
* Catpaswords.lst (ver lo que contiene el archivo)
* John –wordlist=passwords.lst password.txt (ejecutar John con el parámetro --wordlist seguido de la ruta de nuestro archive
* John –show password.txt (mostrar la contraseña)

1. **Instalar ACL**

* Sudo apt-get install acl
* Sudo adduser tarzan (crear usuario)
* Sudo addgroup jungle (crear gruo)
* Usermod –a –G jungle tarzan (meter usuario en grupo)
* Mkdir /home/mydir (crer directorio)
* Chmod 770 /home/mydir (dar permisos al directorio)
* Touch docum1 (dentro de mydir)( crear archivo)
* Chmod o+r+w jungle (dar permisos al grupo)
* Chmod john -r-w (quitarpermisos a john)
* Cd /home/mydir (entramos con el usuario de john y luego ejecutamos el commando)
* Setfacl –m user:tarzan rwx /home/mydir (crear acl para tarzan)

1. **Crear árbol de directorios**

* Mkdir –p SMR/SMR1/SMR101 …
* Tree SMR
* Sudo useradd –g SMR1 SMR101 (Crear grupos y usuarios)
* Sudo passwd SMR101 (ponerle contraseña a los usuarios)
* Setfacl –m g:SMR1: rwx SMR101 (dar permisos al usuario)
* Su SMR101 (cambiar de usuario desde terminal)
* Touch docum1 (crear documento como usuario SMR101)
* Sudo getfacl /home/usuariolinux/SMR/SMR1/SMR101 (ver permisos de SMR101)
* Sudo apt-get install tree (instalar tree)