

7.4 PROTECCIÓN DEL SISTEMA OPERATIVO MEDIANTE PERSONA USUARIA/CONTRASEÑA  
7.4. SISTEMA OPERATIBOA ERABILTZAILEAREN/PASAHITZAREN BIDEZ BABESTE



## IDENTIFICACIÓN DE LA PERSONA USUARIA: MEDIDA BÁSICA DE PROTECCIÓN DE ORDENADORES

### ERABILTZAILEA IDENTIFIKATZEA: ORDENAGAILUAK BABESTEKO OINARRIZKO NEURRIA

*A la hora de implantar medidas de seguridad en el entorno informático de una empresa, no hay que descuidar el elemento más básico: el acceso al ordenador. Se trata de la primera barrera frente a intrusos o personas usuarias sin permisos de entrada, y es el medio para proteger los datos contenidos en el equipo o en la red...*

*Enpresa baten eremu informatikoan segurtasun neurriak ezartzeko, oso kontuan hartu behar da ordenagailurako sarbidea, oinarrizko osagaia baita. Horixe da kanpotarren edo sartzeko baimenik ez duten erabiltzaileen aurrean jartzen den lehenengo oztopoa, eta horixe da, hain zuzen, ekipoan edo sarean dauden datuak babesteko modua...*

... Pedro Eizmendi era consciente de la importancia de dicha medida de seguridad; había trabajado durante cinco años en una compañía de seguros y, en ella, la utilización de los ordenadores y el acceso a determinado tipo de información personal estaba extremadamente vigilado: cada persona trabajadora tenía asignada un nombre como persona usuaria y contraseña que debía introducir para entrar en los PC's; así, en función de los permisos que poseyera, accedía a un nivel u otro de datos. De esta manera, se exigía la identificación de la persona o, en otras palabras, se comprobaba que la persona usuaria y contraseña contaban con los permisos necesarios para entrar al sistema. Con ello se garantizaba:

- La confidencialidad de la información de carácter personal (sólo accedían a ella quienes debían).
- La "correspondencia" entre las funciones del personal y los datos requeridos para su trabajo.
- El acceso no autorizado a tales datos.

No obstante, tras cambiar de trabajo y ser contratado como contable en una clínica, Pedro conoció otro escenario diferente:

... Pedro Eizmendi ohartzen zen segurtasun neurri hori garrantzi handikoa zela; bost urtez jardun zuen aseguru etxe batean, eta bertan, izugarri zaintzen zen ordenagailuen erabilerara eta informazio pertsonalerako sarbidea: langile bakoitzak izen bat eta pasahitz bat zuen erabiltzaile gisa jarduteko, eta haiek idatzi behar zituen, PCetan sartu ahal izateko; hortaz, baimen motaren arabera, datu maila batera edo bestera sartzeko aukera izango zuen. Era horretara, sistemara sartzeko, identifikatzeko eskatzen zitzaion pertsonari, edo beste era batera esanda, erabiltzailearen izenak eta pasahitzak behar ziren sisteman sartzeko; era horretara, baimena zutela egiaztatzen zen. Neurri horien bitartez bermatzen zen:

- Informazio pertsonala ezkutuan gordetzen zela (sartu behar zutenek bakarrik zuten sarbidea).
- Langileen funtzioen eta beren lanerako behar zituzten datuen arteko "korrespondentzia".
- Baimenik gabe datu horietara sarbiderik ez edukitzea.

Dena dela, Pedrok lantegiz aldatu zenean eta klinika batean kontulari gisa jarduteko kontratatu zutenean, beste era bateko egoera ezagutzeko aukera izan zuen:

En dicha clínica, se gestionaba información médica de la clientela (almacenando por tanto datos personales de considerable relevancia); pero, en ninguno de sus seis ordenadores, se requería para "entrar" la introducción de una persona usuaria y contraseña (sólo se encendía y... se tenía acceso a toda la información).

Pedro, sorprendido explicó a Alazne Solana, la directora de la clínica, que aunque el sistema informático de la clínica contase con los mejores sistemas de seguridad física e informática, si por cualquier motivo alguien ajeno a ella se situara delante de uno de sus PC's y lo encendiera, podría acceder fácilmente a información confidencial; quedando en entredicho el trabajo y responsabilidades adquiridas por la clínica (con su clientela y con la normativa vigente en protección de datos de carácter personal). Además, como no existía ninguna diferenciación entre las personas usuarias que empleaban los equipos, sólo existía un único perfil de permisos (cuando no todos/as tenían que acceder a la misma información).

Alazne, la directora de la clínica, una vez hubo comprendido la relevancia del aviso realizado por Pedro Eizmendi, se puso en contacto con su técnica informática habitual; a quien encargó la tarea de creación de perfiles de personas usuarias (tal como le había comentado Pedro, en esta configuración de los ordenadores se recogerían los permisos de las personas usuarias) y establecer como requisito la pantalla de autenticación (identificación: persona usuaria y contraseña) para los distintos accesos a los ordenadores. De este modo, una vez realizada dicha operación:

- El la directora, tras introducir su nombre de usuaria y contraseña, tenía permisos para visualizar cualquier información y ejecutar todas las tareas; ya que era el miembro con perfil más alto.
- El personal médico, previa identificación en el ordenador, tenían permiso para manejar toda la información médica (historiales, tratamientos,...), pero no podían acceder a los datos relativos a la administración y contabilidad de la clínica.
- Y así, sucesivamente...

Asimismo, y como elemento directamente relacionado, la informática también insistió en la importancia de la elección correcta de las contraseñas, ya que de ello podía depender el mantenimiento de la seguridad o privacidad pretendidas: si se requería la entrada de una contraseña, pero ésta era fácilmente reconocible, se perdía el valor de ese paso de identificación.

Por ello, recomendó una serie de criterios elementales aplicables a la correcta elección de las contraseñas:

- Debía elegirse una contraseña fácil de recordar para la persona usuaria, pero difícilmente reconocible para alguien con interés en suplantar su "identidad".
- No era conveniente emplear palabras comunes, ya que existen programas informáticos (poco lícitos) que comprueban este tipo de vocablos a la hora de intentar la penetración en un sistema.
- No debían usarse contraseñas basadas únicamente en números con algún significado (fecha de nacimiento, DNI, etc.).

Klinika hartan, bezeroen mediku informazioa kudeatzen zen (beraz, garrantzi handiko datu pertsonalak gordetzen ziren); baina, bertako ordenagailuetara "sartzeko" (sei ordenagailu zeuden) ez zen erabiltzailearen izena eta pasahitza behar (ordenagailua piztu eta informazio guztia erabil zitezkeen).

Pedrok, harrituta, klinikako zuzendaria zen Alazne Solanari azaldu zion klinikako sistema informatikoak segurtasun sistema onena edukita ere (bai segurtasun fisikoa bai informatikoa), sistema hartatik kanpoko edozein, edozein arrazoirengatik, bertako PC baten aurrean jarriko balitz eta piztuko balu informazio konfidentzialera sartzeko aukera izango lukeela; eta era horretara, zalantzan jarriko zela klinikaren lana eta bere gain hartutako erantzukizuna (bezeroekin eta datu pertsonalen babesaren gaineko araudiarekin). Horrez gainera, tresnak erabiltzen zituztenen artean ez zegoen inolako bereizketarik, baimen profil bakarra zegoen (denek ez zuten informazio mota berera jo behar).

Alazne berehala Pedro Eizmendik emandako oharraren garrantziaz, eta beraiekin lan egiten zuen informatikako teknikariarekin jarri zen harremanetan. Bi gauza agindu zizkion: erabiltzaileen profilak sortzeko (Pedrok esan bezala, ordenagailuen konfigurazio horretan erabiltzaileen baimenak jasoko ziren), eta ordenagailuetan sartzeko baimen pantaila bat zehazteko (identifikazioa: erabiltzailea eta pasahitza). Era horretara, eragiketa hura amaitu ondoren:

- Zuzendariak, bere erabiltzaile izena eta pasahitza sartu ondoren, edozein informazio ikusteko eta zeregin guztiak egiteko baimena zuen; bera baitzen profil altueneko kidea.
- Medikuek, ordenagailuan beren identifikazioa sartu ondoren, informazio medikua erabiltzeko baimena zuten (historiak, tratamenduak...), baina ezin ikus zitzaizketen administrazioarekin eta klinikako kontularitzarekin zerikusia zuten datuak.
- Eta horrela, hurrenez hurren...

Bestalde, informatikako teknikariak azpimarratu zuen garrantzizkoa zela pasahitzak zuzen hautatzea, izan ere, haren mende baitzegoen lortu nahi zen segurtasuna eta pribatutasuna: pasahitz bat sartu behar bazen, baina pasahitz hori oso erraz ezagutzen bazen, identifikaziorako urrats horrek eragin-kortasuna galduko zuen.

Era horretara, oinarrizko hainbat irizpide gomendatu zituen pasahitzak zuzen hautatzeko:

- Erabiltzaileek erraz gogoratuko zuten pasahitza hautatu behar zen, baina haren "nortasuna" ordeztu nahi zuen edonorentzat igartzen zaila izan behar zuen.
- Ez zen komeni hitz arruntak erabiltzea, hainbat programa informatiko baitaude (ez oso legezkoak) era horretako hitzak bilatzen dituztenak sistema batean sartu nahi denean erabiltzeko.
- Nolabaiteko esanahia zuten zenbakiez bakarrik osatutako pasahitzak ere ezin erabil zitezkeen (jaiotza data, NAN, etab.).
- Garrantzizkoa zen pasahitza eta erabiltzailearen izena edo sisteman identifikatuko zuten hitza (esate baterako, izena edo abizena) bat ez etortzea.
- Azkenik, pasahitzak hainbat urrats egin behar zituen "segurua" zela bermatzeko; beraz, komeni da 6 karakterez



- Era importante que no coincidiese con el nombre de la persona usuaria o alguna de las palabras que lo identificasen en el sistema (por ejemplo, su nombre o apellido).
- Finalmente, la contraseña tenía que seguir una serie de pautas que garantizasen su carácter "seguro"; así, era recomendable que estuviera formada por un mínimo 6 caracteres y que combinara números y letras (mezclando mayúsculas y minúsculas). Ahora bien, era conveniente evitar vocales acentuadas y otros signos especiales; ya que podían causar problemas en determinados casos.

osatua izatea, gutxienez, eta zenbakiak eta hizkiak nahastea (letra larriak eta xeheak nahastuz). Baina, azenturik edo bestelako ikur berezirik ez erabiltzea komeni zen; zenbaitetan, arazoak sortzen baitzituzten.



La seguridad de los sistemas informáticos o de la información contenida en los ordenadores de una empresa, debe comenzar por el acceso controlado a éstos en su lugar de origen o en la red a la que pertenezcan. Es decir, la "entrada" en cualquier ordenador tiene que contar siempre con la identificación de la persona a través de una persona usuaria y contraseña otorgados previamente en función de su perfil; de este modo, "arranca" el equipo y accede a los datos o aplicaciones para los que tiene permiso.

En numerosas ocasiones este sencillo paso se obvia o descuida, por lo que conviene recordar los peligros asociados a esta mala práctica

Enpresa bateko sistema informatikoen edo ordenagailuetako informazioaren segurtasunerako lehenengo urratsean, horietarako sarbidea kontrolatu behar da, sorlekuan bertan edo sarean. Hau da, edozein ordenagailutan "sartzeko" identifikatu egin behar da, eta horretarako, profilaren arabera eman zaion erabiltzaile izena eta pasahitza idatzi beharko ditu; era horretara, ordenagailua "abian" jartzen da, eta baimena duen datuetara eta aplikazioetara sartzen da.

Askotan, urrats hori alde batera uzten da edo ez da kontuan hartzen, beraz, urrats hori ez egiteak sortzen dituen arriskuak gogoratzea komeni da.