



I. POR QUÉ SE USAN LAS CONTRASEÑAS?

Es una de las formas, la más común, en que un usuario puede autenticarse (identificarse) en un ambiente informático (PC, Sistemas Automatizados Informáticos).

II. POR QUÉ SE DEBE AUTENTICAR UN USUARIO?

La razón por la cual debemos identificarnos, es que cada usuario tiene distintos privilegios (permiso) de acceso a recursos (Carpetas compartidas, impresoras, computadoras, sistemas informáticos), que están relacionadas a las responsabilidades de cada cargo.

Ejemplo:

El sistema Nicarao permite consultar(a través del internet) las actuaciones de un asunto, a las partes involucradas en el proceso y los abogados; sin embargo, no permite que modifiquen dichas actuaciones.

Los abogados y partes involucradas, están registradas en el sistema NICARAO y solo tienen permiso de consulta.

III. ¿PUEDO USAR CUALQUIER CONTRASEÑA?

Sí puede utilizar cualquier contraseña ¡incluso en blanco (es decir, cero caracteres)!. ¡PERO CON UNA CONTRASEÑA *INSEGURA* SE EXPONDRÁ A QUE SU ACCESO SEA ROBADO Y OPEREN, EN SU NOMBRE, LOS RECURSOS QUE ESTAN BAJO SU RESPONSABILIDAD!!!

IV. ¿QUÉ CARACTERÍSTICAS TIENE UNA CONTRASEÑA SEGURA?

- Debe tener una longitud mínima de 8 dígitos.
- Utilizar combinación de letras Mayúsculas, Minúsculas y Caracteres especiales (+_*/#)
- Deben ser fáciles de recordar para evitar verse obligado a escribirlas.
- Algunos ejemplos podrían ser:
 - Combinar palabras cortas con números o caracteres de puntuación: Soy2_Yo3.
 - Usar acrónimos, por ejemplo de alguna frase fácil de recordar: En casa De Herrero Cuchillo de palo: EcDHCdp, y hasta añadir algún número para mayor seguridad: EcDHCdp12 .
 - Incluso es mejor si la frase no es conocida: Hasta ahora No He olvidado Mi Contraseña: HaNHoMC.

V. LO QUE NUNCA DEBE HACER CON SUS CONTRASEÑAS:

- Utilizar el nombre de su usuario como contraseña.

Ejemplo. Nombres de usuario: jlopez, Contraseña: jlopez (no lo haga)



- Utilizar sus nombres o apellidos total o parcialmente.
- Utilizar palabras que aparezcan en el diccionario.
- Utilizar números telefónicos como parte de su contraseña.
- Utilizar número de cedula o cualquier otro de identificación personal.
- No utilice su fecha de cumpleaños, las de sus hijos, conyugues u otro familiar.
- Utilizar letras o números consecutivos tal como: 555 o aaa.
- Utilizar la secuencia ascendente o descendente de número o letras. Ejm: 123, abc.
- Compartirla con otro usuario y si lo hace cámbiela inmediatamente. Las contraseñas son secretas y personales.
- Dejarla anotada en un lugar visible cerca de la computadora. De preferencia no las anote, menos aun si alguien está observando.
- Enviarla por correo electrónico, mensaje de texto, llamada telefónica u otro medio físico o electrónico.
- Mencionarla en una conversación.

Nota: Es una norma ética, de buen usuario, no mirar al teclado cuando alguien está digitando su contraseña. No lo haga usted, ni permita que nadie más lo haga.

Recomendación: Siempre que se aleje de su equipo, sin importar el tiempo que vaya a estar lejos, recuerde bloquear el acceso a su equipo. Esto puede hacerlo de dos maneras: 1. usando salva pantalla con contraseña que se activen después de unos 5 minutos de inactividad. 2. Presionando la tecla con símbolo de Windows y la letra L, al mismo tiempo.

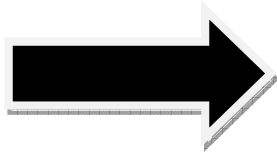
Aunque alguien no conozca su contraseña, podría aprovechar el momento en que ud se aleje y deje su pc o sistema informático, sin protección, para tener modificar registros en el sistema, acceso a los archivos de trabajo, personales, cuenta de correo personal o institucional, incluso su cuenta de banco si dejó su sesión bancaria abierta en su computadora.



VI. QUÉ SUCEDERÍA SI NO SIGUE LAS RECOMENDACIONES?

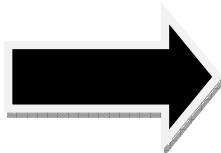
1. CONTAMINACION POR VIRUS

es(o
red



2. ROBO O PERDIDA DE INFORMACION CLASIFICADA.

loras
o el
hasta
las a



3. PERDIDA DE ARCHIVOS DE TRABAJO



Cualquier persona que accese a su pc, teniendo conocimiento de su usuario y contraseña podría borrar o modificar sus archivos, los cuales fueron elaborados después de varios días de trabajo.

De acuerdo a la planificación anual de cada oficina, es de vital importancia entregar en tiempo y forma ciertos archivos de trabajo, desde Sentencias hasta Informes.

La pérdida de esta información no le permitiría cumplir con sus metas, reflejándose en su informe de planificación, e influirá negativamente en su evaluación al desempeño.

4. USURPACION DE IDENTIDAD

Una persona podría leer, buscar, copiar, enviar o recibir información desde se correo electrónico EN SU NOMBRE.

Seguir estas recomendaciones, será de beneficio para usted y la institución.

Si tiene más preguntas sobre cómo aplicar estas medidas de seguridad, por favor comunicarse con la Oficina de Redes, con gusto le atenderemos.

Yolidia Lacayo. Ext. 1206