PROTOCOLO PARA LA CREACIÓN Y BUEN USO DE CONTRASEÑAS DE ACCESO A LOS SISTEMAS DE INFORMACIÓN O SERVICIOS DE TIC´S DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

A. Objetivo.

Generar un documento formal para la creación y buen uso de contraseñas de acceso a los Sistemas de Información o Servicios de TIC´s de la Universidad de las Fuerzas Armadas ESPE; mediante la definición de lineamientos concretos para su gestión.

B. Alcance.

El presente protocolo está dirigido para cumplimiento de estudiantes, docentes, investigadores, militares, administrativos y trabajadores (bajo cualquier modalidad de prestación de servicios) de la Universidad de las Fuerzas Armadas ESPE, Matriz, Sedes, Unidades Académicas Externas y Unidades Académicas Especiales.

C. Protocolo.

Para gestionar correctamente la seguridad de las contraseñas utilizadas para el acceso a los Sistemas de Información de la Universidad de las Fuerzas Armadas ESPE, la Unidad de Seguridad Integrada establece los siguientes lineamientos:

1. Antes de Construir Contraseñas Seguras.

Revisar el siguiente método para la creación de contraseñas seguras:

a. Piense en una frase memorable y que sea fácil de recordar por usted, tal como:
   i. "Mi nueva contraseña segura la voy a utilizar desde ahora."

b. Cambiar la frase a un acrónimo, se debe incluir el signo de puntuación.
   ii. mncslvauda.

c. Añadir complejidad; sustituyendo números y símbolos por letras en él acrónimo descrito. Por ejemplo, cambie el signo de ampersand (&) por la letra "d", arroba (@) por la letra "a" y el símbolo de mayor que (>) por la letra "v":
   iii. mncsl>@u&@.

d. Añadir más complejidad, colocar al menos una letra mayúscula como M.
   iv. Mncsl>@u&@.

e. Añadir más complejidad, colocar al menos un número que reemplace a una letra y que le sea fácil de relacionar; por ejemplo el 2 por la n
   v. M2csl>@u&@

f. Finalmente, no utilice esta contraseña de ejemplo en ninguno de los sistemas de información de la Universidad.

2. Durante la Construcción de Contraseñas Seguras.

Se deberá:

a. ***Crear contraseñas de al menos 5 caracteres y máximo 20 caracteres.***
Mientras la contraseña contenga el mayor número de caracteres será considerada más segura y por consecuencia más complicada de descifrar.

b. ***Incluir letras mayúsculas y minúsculas.***
Algunos sistemas operativos, son sensitivos a las mayúsculas y minúsculas lo cual permitirá asegurar al usuario reforzar la seguridad de la contraseña.

c. ***Mezclar letras y números.***
Agregar números a las contraseñas, especialmente cuando se añaden al medio (no solamente al comienzo o al final), puede fortalecer su contraseña.

d. ***Incluir caracteres especiales.***
La utilización de caracteres especiales tales como $, %, &,> y <, pueden mejorar considerablemente la fortaleza de su contraseña.

e. ***Actualizar periódicamente las contraseñas.***
Se requiere de manera obligatoria que los miembros de la Comunidad Universitaria, cada 3 meses renueven las contraseñas de acceso a los Sistemas de Información; con la finalidad de precautelar el acceso no autorizado a la información.

f. ***Utilizar software especializado para generación de contraseñas.***
En la actualidad existen herramientas informáticas avaladas y que disponen técnicas de cifrado para la construcción de contraseñas (Anexo A. Herramientas para la Generación de Contraseñas).

NO se deberá:

a. ***Utilizar solamente letras o números.***
Nunca considerar contraseña que únicamente contengan letras o sólo números. Ej.: "8675309", "abcdefg", entre otros.

b. ***Utilizar secuencias básicas de teclado.***
Evitar la utilización de contraseñas que sean formadas para la secuencia de teclas. Ej.: "qwerty", "asdfg", o las típicas en numeración: "123456" ó "09876", entre otros.

c. ***Utilizar parcial o totalmente los caracteres de documentos personales.***
Evitar la utilización de números de la cédula de ciudadanía, pasaporte, ruc, placas vehiculares, entre otros.

d. ***Utilizar palabras reconocibles o identificables.***
No deben ser usados nombres propios de familiares o amigos, palabras del diccionario o hasta términos de shows de televisión o novelas; aún si estos son terminados con números. Ej: Daniel1990, Friends, entre otros.

e. ***Utilizar palabras o frases extranjeras.***
Por lo general aplicaciones de descifrado de contraseñas a menudo realizan la verificación contra listas de palabras que abarcan diccionarios de muchos idiomas, razón por la cual no es seguro confiarse en un idioma extranjero para asegurar una contraseña. Ej: cheguevara, bienvenue1, 1dummKopf, entre otros.

f. ***Utilizar terminología técnica o usada por "hackers".***
En caso de disponer de competencias técnicas relacionadas con seguridad informática, es recomendable no utilizar términos similares para construir palabra o frases. Ej: 3$P3 (ESPE), L337 (LEET), p@$$w0rd (password)

g. ***Utilizar información personal.***
Es recomendable mantenerse alejado de la información personal al momento de generar una contraseña. Si un "atacante" dispone de información relacionada de "quién es usted" será más fácil descifrar la contraseña.

A continuación, se muestra la información que debería evitar cuando construya una contraseña:

I. Sus nombres
II. El nombre de sus mascotas
III. El nombre de los miembros de su familia (Principalmente de sus hijos)
IV. Fechas de cumpleaños o aniversario
V. Número telefónico o cédula de ciudadanía

h. ***Invertir palabras reconocibles o identificables.***
En el internet existe una gran variedad de herramientas que permiten verificar contraseñas, por tanto, invertir una mala contraseña, no la hace más segura. Ej: naitsabes (Sebastián), 3P$3 (ESPE), entre otros.

i. ***Escribir su contraseña.***
Nunca guarde su contraseña en un papel y mucho menos la pegue en el monitor utilizando "post-it" o papel adhesivo, es mucho más seguro memorizarla.

j. ***Utilizar la misma contraseña para todos los Sistemas de información o Servicios de TIC´s.***
Es importante que se dispongan contraseñas diferentes para cada aplicación, servicio o sistema de información, con la finalidad de que, si un sistema es comprometido, no todos estarán en riesgo.

3. Después de la Construcción de Contraseñas

a. Actualizar las contraseñas, principalmente en caso de que el usuario acceda por primera vez a los Sistemas de Información o Servicios de TIC´s de la Universidad de las Fuerzas Armadas ESPE.

b. La contraseña, deberá ser secreta e intransferible.

c. Los Sistemas de Información o Servicios de TIC´s de la Universidad de las Fuerzas Armadas ESPE, permitirán hasta por 3 ocasiones el ingreso de contraseñas incorrectas. Una vez superado este número de intentos, las credenciales de acceso del usuario serán bloqueadas.

d. Deberá actualizar cada 3 meses las contraseñas de acceso a los Sistemas de Información o Servicios de TIC´s de la Universidad de las Fuerzas Armadas ESPE.

Elaborado por:	Revisado por:	Revisado por:
Unidad de Seguridad Integrada	**Unidad de Seguridad Integrada**	**Unidad de Tecnologías de la Información y Comunicaciones**
Ing. Mauricio Javier Baldeón Garzón, MGS **Especialista de Unidad de Seguridad Integrada**	Tcrn. (SP) David Alfredo Molina Yizcaino **Director de la Unidad de Seguridad Integrada**	Ing. Rommel David Asitimbay Morales **Director de la Unidad de Tecnologías de la Información y Comunicaciones**

Supervisado por:	Aprobado por:
Vicerrectorado Académico General	**Rectorado**
Tcrn. Víctor Emilio Villavicencio Alvarez, Ph. D **Vicerrector Académico General**	Tcrn. Humberto Aníbal Parra Cárdenas, Ph. D **Rector de la Universidad de las Fuerzas Armadas ESPE**

ANEXO A: HERRAMIENTAS PARA LA GENERACIÓN DE CONTRASEÑAS

MaxPasswords

Instalación:

1) Descargar MaxPasswords para Windows desde el sitio oficial http://www.max2k.com/programs.php?id=3, ó; desde el servidor FTP[1] de la Universidad. (ftp://ftp.espe.edu.ec)
2) Ejecutar el asistente de instalación, solicitará que acepte los términos del "Acuerdo de Licencia", y de no haber ningún inconveniente, clic en "I Agree".
3) El asistente de instalación, solicitará que escoja los componentes de instalación, "Choose Components".
4) Seleccionar el tipo de instalación, normal o personalizada. En la instalación personalizada, el asistente permitirá seleccionar de manera opcional, si desea: crear menú de inicio, crear elemento de escritorio, o crear elemento de inicio rápido. Una vez completado, clic en "next".
5) El siguiente punto, es seleccionar la localización de la instalación "Choose Install Location". Elegir la carpeta donde queremos que se instale el programa, dando clic en "Browse"; caso contrario, el asistente le ubicará el programa por defecto en la unidad C. Una vez completado aquello, clic en "Install" y proceder a instalar el software.
6) Por último, clic en "Close" para completar la instalación.

Uso:

1) Abrir la aplicación con este icono que se denomina "MaxPasswords".
2) Se abrirá una ventana donde destacan en la parte superior, tres pestañas: "General", "Specific, y "Strings". Estas pestañas, las dos primeras se refieren a la forma de generar las contraseñas, por lo que la primera pestaña, indica que la generación será de forma general (recomendado) y la segunda de manera específica. La tercera pestaña es para personalizar las cadenas de codificación.
3) En la generación de contraseñas de forma general, seleccionar los parámetros de seguridad que se pueden incluir a la contraseña, como los son: Lowercase (minúsculas), Uppercase (mayúsculas), Numeric (numérico), Symbols (símbolos), y Extended (Extendido de todos los caracteres). Adicionalmente, brinda la opción de establecer la longitud o número de caracteres de la contraseña, así como el número de contraseñas que se desean generar.
4) En la generación de contraseñas de forma específica, dispone de las mismas opciones que la pestaña de generación general, pero en esta pestaña se permite establecer como la manera y orden que se requieren que se inserten los caracteres de la contraseña. De la misma forma se puede incluir, excluir, repetir caracteres, e incluso insertar un texto estático en la contraseña, al hacer clic en el botón ☑. Todos los opciones y caracteres que se hayan incluido o excluido se verán reflejados a modo de patrón de caracteres en una celda abajo de las opciones que se denomina "Pass mask", que en su traducción vendría a ser la máscara codificada.
5) En la pestaña "Strings", las cadenas de codificación por su traducción, se puede añadir hasta cuatro tipos de cadenas de codificación, en el orden a, b, c, d, donde se puede incluir el abecedario, la numeración, palabras o símbolos, las cuales servirán para las pestañas generales y especifico de generación de contraseñas del software.

[1] FTP: File Transfer Protocol

6) Destacar que, en la parte inferior de la herramienta en las tres pestañas, se encuentra el campo de contraseñas generadas "Generated Passwords", donde se visualiza las contraseñas generadas. La aplicación permite guardar o borrar todas estas contraseñas en un archivo plano (.txt).

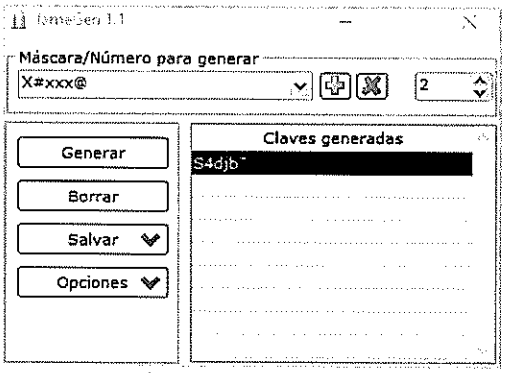
LameGem

Instalación:

1) Descargar LameGem para Windows desde el sitio oficial https://lame-industries.net/gen/ ó; desde el servidor FTP de la Universidad. (ftp://ftp.espe.edu.ec)
2) El asistente de instalación, solicitará que cierre todas las aplicaciones abiertas antes de continuar. Una vez completado aquello, clic en "next".
3) Aceptar el Acuerdo de Licencia, y clic en "next".
4) Posteriormente, el asistente de instalación mostrará la opción para seleccionar el directorio de destino de la herramienta, clic en "Browser", por defecto se instalará en la unidad C. Una vez completado, clic en "next".
5) A continuación, el asistente de instalación mostrará la opción de seleccionar el directorio de destino de los programas de método abreviado "program´s shortcuts", por defecto el asistente de instalación le ubicará en la unidad C, o simplemente seleccione el casillero "Don´t create a Start Menu folder". Una vez completado, clic en "next".
6) El asistente de instalación, solicitará de manera opcional si desea crear un icono de escritorio "Create a desktop icon", y así mismo, si desea crear un icono de inicio rápido "Create a quick launch icon". Una vez completado, clic en "next".
7) Clic en "Install" para iniciar con la instalación de la herramienta.
8) Finalmente, clic en "finish", para dar por finalizado la instalación.

Uso:

1) Abrir la aplicación a través del icono , "generar contraseñas".
2) Se abrirá una ventana, en la parte superior se muestra una serie de patrones para generar la contraseña. En la parte inferior de la ventana se tiene los botones: generar, borrar, salvar, opciones, y las claves generadas.



3) El botón "Generar", sirve para crear las contraseñas, y el botón "Borrar" para eliminarlas.
4) El botón "Salvar", se utiliza para guardar las contraseñas en el computador "Como Texto" ó "Como CSV".
5) El botón "Opciones" tiene una serie de aspectos como los son: opciones del programa, opciones de interfaz, opciones de la generación, opciones de la máscara, y otras propias de la herramienta como lo son minimizar, salir y ayuda de usuario.

6) En "Opciones del Programa", se dispone de una serie de casilleros opcionales del programa como lo son: Comprobar si hay nuevas actualizaciones; Salvar la última máscara usada; Salvar el último número generado; Confirma el borrado; Auto-salvar la(s) clave(s) generada(s); y Borrar el portapapeles al salir.
7) En "Opciones de Interfaz", se tiene una serie de casilleros opcionales de la interfaz de la herramienta, como: Mantener delante; Sonidos; y Estilo XP. Además de estos casilleros tenemos otro de lista desplegable, que tiene que ver con el idioma en que deseamos utilizar el interfaz, donde se puede escoger el idioma español.
8) En "Opciones de Generación", se dispone de dos casilleros, en los que se puede escoger entre "Usar la generación por defecto" (recomendada) y "Usar la generación elegida" que permitirá añadir o eliminar patrones de "mayúsculas", "minúsculas", "número", y "caracteres especiales".
9) Por último, en "Opciones de la Máscara" en caso de requerirlo; se puede seleccionar: mayúsculas, minúsculas, número, caracteres especiales, e incremento de números, lo cual es importante en el casillero desplegable de la ventana principal "Máscara/Número para generar", previo a generar la contraseña.

Roboform

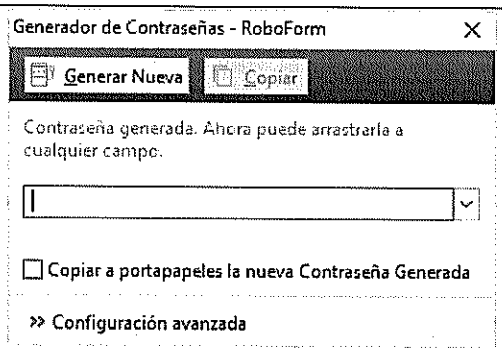
RoboForm

Instalación:

1) Descarga Roboform para Windows desde el sitio oficial https://www.roboform.com/download,ó; desde el servidor FTP de la Universidad. (ftp://ftp.espe.edu.ec)
2) Seleccionar el idioma de preferencia, clic en "Siguiente."
   NOTA: En el botón; "Mostrar opciones avanzadas" elegir qué navegadores desea utilizar con Roboform y personalizar su configuración de Roboform.
3) Roboform solicitará que las aplicaciones se cerrarám para completar el proceso de instalación. Para continuar, clic en "Instalar." Las aplicaciones se cerrarán y la configuración de Roboform se ejecutará automáticamente.
4) El usuario, deberá crear una cuenta gratuita; ingresando la dirección de correo electrónico, contraseña maestra y haciendo clic en "Siguiente". La contraseña maestra asegurará sus inicios de sesión, identidades y notas seguras.
   NOTA: No puede recuperar su contraseña maestra, por lo que es imperativo que recuerde esta información.
5) Seleccionar cualquier navegador adicional que desee utilizar con Roboform, clic en "Siguiente."

Uso:

1) Abrir la aplicación, a través del icono, que se denomina "generar contraseñas".
2) Se abrirá una ventana, donde hay dos campos principales, la -contraseña generada- en la parte superior, y la -configuración avanzada- en la parte inferior.



3) En la sección de -configuración avanzada- aparece los diferentes tipos y número de caracteres que se pude incluir en la contraseña generada, como los son: número de caracteres Número de caracteres 12 ,Mayúsculas ☑ A-Z , minúsculas ☑ a-z , números ☑ 0-9 , y caracteres especiales ☑ !@#$%^&* .
4) Una vez ingresado e incluido todos los caracteres conforme a los campos que se requiera, clic en el botón -generar nueva- Generar Nueva , en consecuencia se habrá generado la contraseña, la herramienta indicará la fortaleza de la misma (débil, medio o bueno).
5) Por último, si ya se copia la contraseña y se establece la misma para uso, no olvidar borrar la lista de contraseñas generadas, a modo de borrar historial.