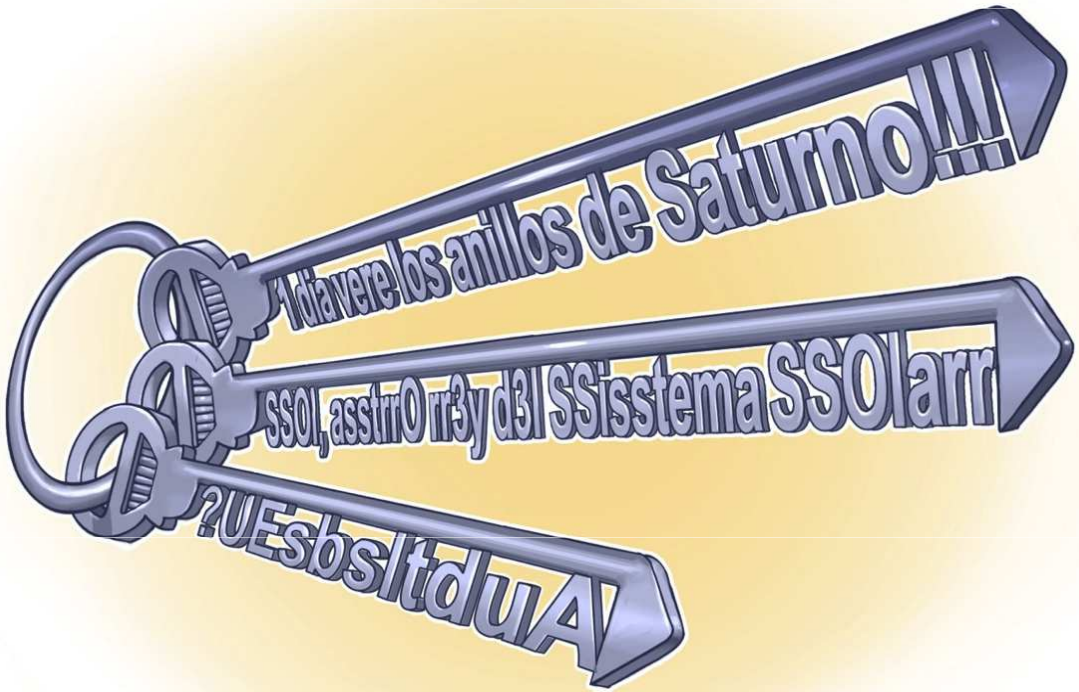
Seguridad de las contraseñas



Univisa S.A.
servclte@univisa.com.ec

Contenido

- Contraseñas
- Principales riesgos
- Cuidados a tener en cuenta
- Fuentes

Contraseñas (1/2)

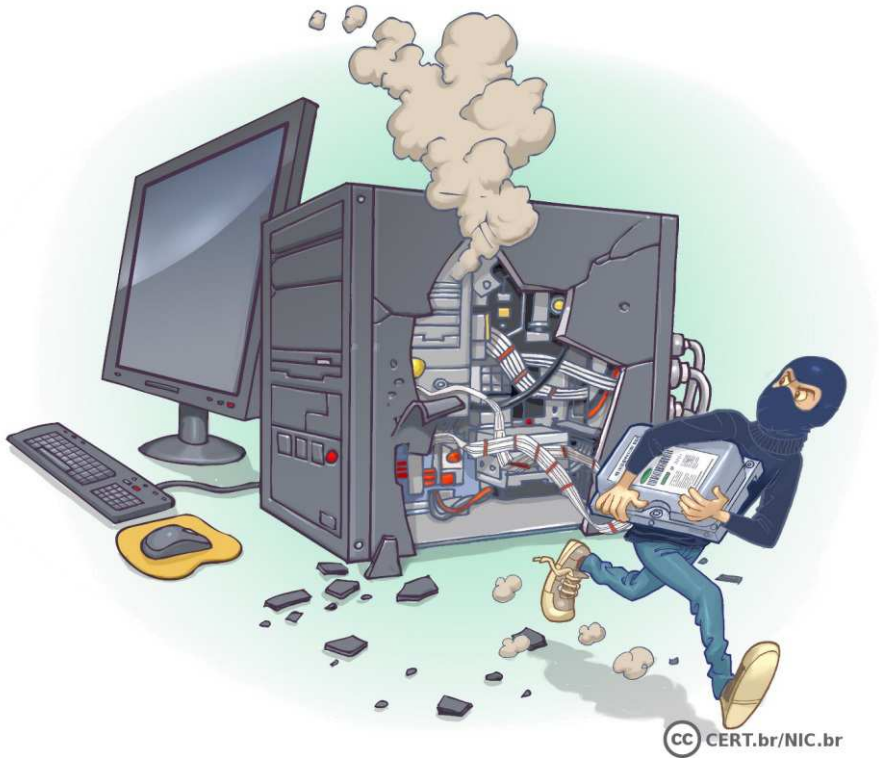
- **Sirven para autenticar un usuario**
  - **aseguran que realmente eres quien dices ser y**
  - **que tienes derecho a acceder al recurso en cuestión**
- **Uno de los principales mecanismos de autenticación utilizados en Internet**
- **Proteger tu contraseña es fundamental para evitar los riesgos que conlleva el uso de Internet:**
  - **la contraseña es el secreto que garantiza tu identidad, es decir, lo que garantiza que eres el dueño de tus cuentas de usuario**

Fuente - http://cartilla.cert.br/

Contraseñas (2/2)

- **Tu contraseña puede ser descubierta:**
  - **cuando la utilizas en:**
    - **computadoras infectadas**
    - **computadoras hackeadas**
    - **sitios falsos (*phishing*)**
  - **intentando adivinarla**
  - **al ser capturada mientras transita por la red**
  - **mediante el acceso al archivo donde está almacenada**
  - **con el uso de técnicas de ingeniería social**
  - **observando el movimiento:**
    - **de tus dedos en el teclado**
    - **de los clics del mouse en un teclado virtual**

Riesgos principales



Riesgos principales (1/4)

- En caso de poseer tu contraseña, un invasor puede:
  - acceder a tu cuenta de correo electrónico y:
    - leer y/o eliminar tus correos
    - robar tu lista de contactos y enviar correos en tu nombre
    - enviar mensajes que contengan:
      - *spam*
      - engaños
      - *phishing*
      - códigos maliciosos
    - solicitar el reenvío de las contraseñas de otras cuentas
      - y así lograr acceder a las mismas
    - cambiar tu contraseña
      - dificultando así que puedas ingresar nuevamente a tu cuenta

Riesgos principales (2/4)

- En caso de poseer tu contraseña, un invasor puede:
  - **acceder a tu computadora y:**
    - **borrar tus archivos**
    - **obtener información confidencial, incluidas otras contraseñas**
    - **instalar códigos y servicios maliciosos**
    - **utilizar tu computadora para:**
      - **realizar ataques contra otras computadoras**
      - **esconder la verdadera identidad de esta persona (el invasor)**

Riesgos principales (3/4)

- En caso de poseer tu contraseña, un invasor puede:
  - **acceder a tu red social y:**
    - **dañar tu imagen**
    - **abusar de la confianza de tus amigos/seguidores**
    - **enviar mensajes en tu nombre, conteniendo:**
      - ***spam***
      - **engaños**
      - ***phishing***
      - **códigos maliciosos**
    - **cambiar la configuración que seleccionaste**
      - **haciendo pública tu información privada**
    - **cambiar tu contraseña**
      - **dificultando así que puedas ingresar nuevamente a tu perfil**

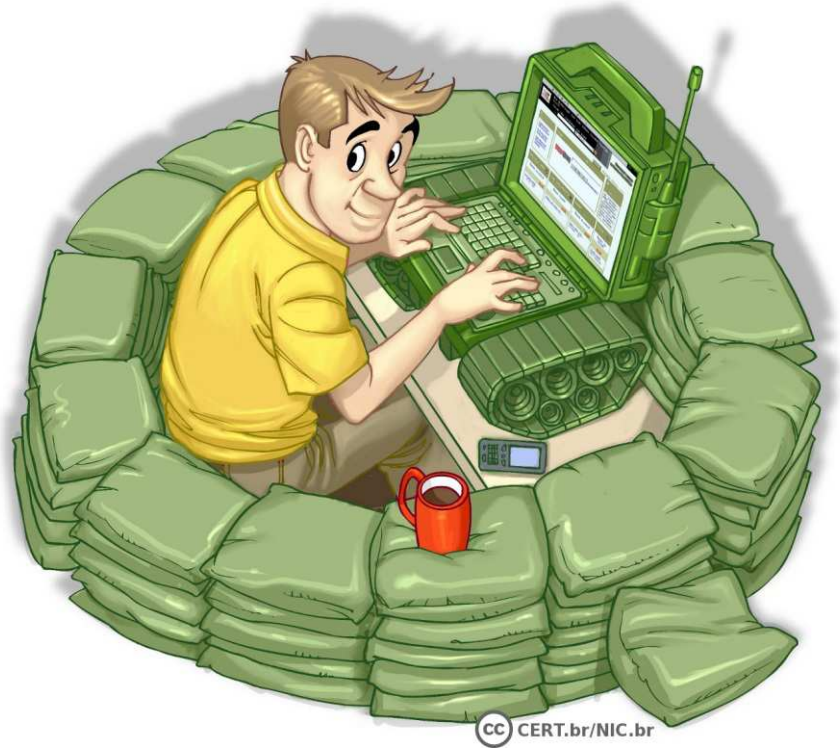
Riesgos principales (4/4)

- En caso de poseer tu contraseña, un invasor puede:
  - **acceder a tu cuenta bancaria y:**
    - **verifica el saldo y el estado de tus cuentas**
  - **acceder a tu sitio de comercio electrónico y:**
    - **modificar la información de registro**
    - **realizar compras en tu nombre**
    - **verificar información sobre tus compras anteriores**
  - **acceder a tu dispositivo móvil y:**
    - **robar tu lista de contactos y tus mensajes**
    - **acceder y/o copiar tus fotos y videos**
    - **bloquear el acceso al dispositivo**
    - **borrar los datos almacenados en el dispositivo**

Diapositiva 9

MVZ1 Miriam von Zuben; 18/10/2012

Cuidados a tener en cuenta



Fuente - http://cartilla.cert.br/

Elección de contraseñas (1/3)

- **Evita usar:**
  - **datos personales**
    - **nombre, apellido**
    - **nombres de usuario**
    - **fechas**
    - **números de documentos, de teléfono o matrículas de vehículos**
  - **datos disponibles en las redes sociales y páginas web**
  - **secuencias de teclado**
    - **“1qaz2wsx”, “QwerTAsdfG”**
  - **palabras que aparezcan en listas conocidas públicamente**
    - **canciones, equipos de fútbol**
    - **personajes de películas**
    - **diccionarios de diferentes idiomas**

Elección de contraseñas (2/3)

- **Usa:**
  - **números aleatorios**
    - **cuanto más aleatorios sean los números, mejor**
      - **principalmente en sistemas que solamente aceptan caracteres numéricos**
  - **muchos caracteres**
    - **cuanto más larga sea tu contraseña, mejor**
  - **diferentes tipos de caracteres**
    - **cuanto más "desordenada" sea tu contraseña, mejor**

Elección de contraseñas (3/3)

- **Consejos prácticos para crear una buena contraseña:**
  - **escoge una frase y selecciona la primera, la segunda o la última letra de cada palabra**

    Frase: “Un Elefante se balanceaba sobre la tela de una Araña”

    Contraseña: “?UEsbsltduA”
  - **escoge una frase larga, fácil de memorizar y con diferentes tipos de caracteres**

    Contraseña: “1 día vere los anillos de Saturno!!!”
  - **inventa tu propio modelo de sustitución**

    Modelo: Duplicar las letras “s” y “r”, reemplazar “o” por “0” y reemplazar “e” por “3”

    Frase: “Sol, astro rey del Sistema Solar”

    Contraseña: “SS0l, asstrr0 rr3y d3l SSisstema SS0larr”

Uso de las contraseñas (1/3)

- **No reveles tus contraseñas**
  - **asegúrate de que nadie esté mirando cuando las digites**
  - **no las dejes anotadas donde otros puedan verlas**
    - **un papel sobre la mesa o pegado a tu monitor**
  - **evita ingresarlas en computadoras y dispositivos móviles de otras personas**
- **No entregues tus contraseñas a otras personas**
  - **cuidado con los correos electrónicos y las llamadas telefónicas solicitando datos personales**
- **Utiliza conexiones seguras si el acceso implica el uso de contraseñas**

Fuente - http://cartilla.cert.br/

Uso de las contraseñas (2/3)

- **Evita:**
  - **guardar tus contraseñas en el navegador**
  - **utilizar opciones como:**
    - **“Recordar cuenta”**
    - **“Seguir conectado”**
  - **usar la misma contraseña para todos los servicios a los que te conectas**
    - **alcanza con que un atacante obtenga una contraseña para que pueda acceder a las demás cuentas donde la utilizas**
- **No utilices las contraseñas de uso profesional para acceder a asuntos personales (y viceversa)**
  - **respeta los contextos**

Fuente - http://cartilla.cert.br/

Uso de las contraseñas (3/3)

- **Crea grupos de contraseñas según el riesgo involucrado:**
  - **crea contraseñas:**
    - **únicas, fuertes, y úsalas en los sitios que involucren recursos valiosos**
    - **únicas, algo más sencillas, y úsalas donde el valor de los recursos protegidos sea menor**
    - **simples y utilízalas para acceder cuando no haya riesgo**
- **Guarda tus contraseñas de forma segura:**
  - **anota tus contraseñas en un papel y guárdalo en un lugar seguro**
  - **grábalas en un archivo encriptado**
  - **utiliza programas de administración de cuentas/contraseñas**

Cambio de las contraseñas:

- **Cambia tus contraseñas:**
  - **inmediatamente, si piensas que tus contraseñas han sido:**
    - **descubiertas o usadas en computadoras hackeadas o infectadas**
  - **rápidamente:**
    - **si pierdes una computadora donde estaban guardadas**
    - **si usas:**
      - **un modelo de formación y crees que alguna contraseña ha sido descubierta**
      - **una misma contraseña en más de un sitio y crees que ha sido descubierta en alguno de ellos**
    - **al adquirir dispositivos accesibles a través de la red**
      - **estos dispositivos pueden estar configurados con una contraseña por defecto**
  - **regularmente:**
    - **en los demás casos**

Fuente - http://cartilla.cert.br/

Recuperación de las contraseñas (1/2)

- **Configura opciones de recuperación para tus contraseñas:**
  - **una dirección de correo electrónico alternativa**
  - **una pregunta de seguridad**
  - **un indicio de contraseña**
  - **un número de teléfono celular**
- **Cuando utilices preguntas de seguridad:**
  - **evita escoger preguntas de seguridad cuyas respuestas se puedan adivinar fácilmente**
  - **intenta crear tus propias preguntas**
    - **preferentemente con respuestas falsas**

Fuente - http://cartilla.cert.br/

Recuperación de las contraseñas (2/2)

- **Cuando utilices indicios de contraseña escógelos de manera que sean:**
  - **lo suficientemente vagos como para que nadie pueda descubrirlos, y**
  - **lo suficientemente claros como para que puedas entenderlos**
- **Cuando solicites el envío de tus contraseñas por correo electrónico:**
  - **trata de cambiarlas lo más rápido posible**
  - **registra una dirección de correo a la cual accedas regularmente**
    - **para no olvidar la contraseña de esta cuenta también**

Fuente - http://cartilla.cert.br/

Phishing y códigos maliciosos

- **Desconfía de los mensajes que recibas:**
  - **aunque hayan sido enviados por un conocido**
    - **estos mensajes pueden haber sido enviados desde una cuenta falsa o hackeada**
- **Evita:**
  - **hacer clic o seguir enlaces recibidos en mensajes electrónicos**
    - **trata de escribir la URL directamente en el navegador**
  - **utilizar un buscador para acceder a servicios que requieran contraseñas, como tu correo electrónico web y tus redes sociales**
- **Ten cuidado al hacer clic en enlaces acortados:**
  - **usa complementos que permitan expandir el enlace antes de hacer clic sobre el mismo**

Fuente - http://cartilla.cert.br/

Privacidad

- **Intenta reducir la cantidad de información que se pueda recolectar sobre tu persona**
  - **alguien podría usar esta información para adivinar tus contraseñas**

- **Ten cuidado con la información que publiques en blogs y redes sociales**
  - **alguien podría usar esta información para intentar:**
    - **confirmar tus datos de registro**
    - **descubrir indicios de contraseñas**
    - **responder preguntas de seguridad**

Computadora (1/2)

- **Mantén tu computadora segura:**
  - **con las versiones más recientes de todos los programas instalados**
  - **instalando todas las actualizaciones, especialmente las de seguridad**
- **Utiliza mecanismos de seguridad y mantenlos actualizados**
  - ***antispam***
  - ***antimalware***
  - ***firewall* personal**

Computadora (2/2)

- **Crea cuentas individuales para todos los usuarios**
  - **asegúrate de que todas las cuentas tengan contraseñas**
- **Configura tu computadora para que solicite una contraseña en la pantalla de inicio**
- **Nunca compartas la contraseña de administrador**
  - **utilízala lo menos posible**
- **Activa la opción de compartir recursos:**
  - **solamente cuando sea necesario, y**
  - **usando contraseñas bien elaboradas**

Dispositivos móviles

- **Registra una contraseña bien elaborada**
  - **de ser posible, configura el dispositivo para que acepte contraseñas complejas (alfanuméricas)**
- **En caso de pérdida o robo:**
  - **cambia las contraseñas que puedan estar guardadas en el dispositivo**

Fuente - http://cartilla.cert.br/

Computadoras de terceros

- **Asegúrate de cerrar tu sesión (*logout*) cuando accedas a sitios que requieran el uso de contraseñas**
- **Siempre que sea posible, intenta usar opciones para navegar en forma anónima**
- **Evita realizar transacciones bancarias y comerciales**
- **Al regresar a tu computadora, trata de cambiar cualquier contraseña que hayas utilizado**

Manténgase informado

Cartilla de Seguridad para Internet

http://cartilla.cert.br/

Fuentes

- **Fascículo Contraseñas**

  http://cartilla.cert.br/fasciculos/

- **Cartilla de Seguridad para Internet**

  http://cartilla.cert.br/

cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

nic.br
Núcleo de Informação e Coordenação do Ponto BR

cgi.br
Comitê Gestor da Internet no Brasil