2.0.1. Manual del Estudiante de Aspectos básicos de Internet y Seguridad cibernética

Aspectos básicos de Internet y *Seguridad Cibernética* es un curso de dos horas de duración que está diseñado para que los estudiantes se familiaricen con los aspectos básicos del navegador web, los motores de búsqueda y las estrategias de búsqueda. También se tomarán en cuenta los asuntos sobre ética y seguridad.

Objetivos de aprendizaje:

- Describir las diferencias entre Internet y Red Mundial
- Describir los navegadores web y cómo se usan
- Identificar los componentes de la pantalla de Internet Explorer
- Identificar las partes básicas de la Red Mundial
- Identificar los componentes de una dirección URL
- Llevar a cabo búsquedas efectivas en Internet
- Entender los resultados de la búsqueda
- Evaluar los sitios web
- Hablar acerca de la seguridad cibernética (seguridad en Internet)

Definiciones

Redes - .....

.....

Internet - .....

.....

Red Mundial

.....

Navegador Web.....

.....

Repase los componentes de Internet Explorer de la parte superior a la parte inferior.

Title Bar (Barra de título):.....

.....

Minimize (Minimizar):.....

.....

Restore (Restablecer):.....

.....

Close (Cerrar):.....

.....

Address Bar (Barra de direcciones):.....

.....

Botones Back (Retroceder) y Forward (Avanzar):.....

.....

Tabs (Pestañas):

.....

Status Bar (Barra de estado):.....

....

Más definiciones

Hyperlink (Hipervínculo).....

.....

Dirección URL

.....

Search Engine (Motor de búsqueda).....

.....

Consejos de búsqueda en Internet

- **Cada palabra es importante.** Generalmente, se usarán todas las palabras que se incluyen en la consulta.
- **Para la búsqueda no son relevantes las letras mayúsculas o la puntuación.** La búsqueda [new york times] es la misma búsqueda que [New York Times].
- **Recuerde que** los motores de búsqueda no son humanos. En lugar de escribir [¿Tengo gripe?], escriba [síntomas de gripe].
- **Seleccione palabras descriptivas.** Mientras más específica sea la palabra, más relevantes serán los resultados. Las palabras que no son muy descriptivas, como ‘documento’, ‘sitio web’, ‘compañía’ o ‘info’, generalmente no son necesarias.

2.0.2 La Búsqueda de tesoros en Internet *se completa con las siguientes preguntas y con la computadora.*

1. ¿Cuándo escribió William Barret Travis la famosa carta del Álamo?

2. ¿Qué dice el Juramento de la bandera del estado de Texas?

3. ¿Quién fue la “Reina de los bandidos de Dallas”?

4. ¿Quién oficializó, en 1955, el símbolo de la mano “hook ‘em horns” de la UT?\

5. ¿Dónde nació Lyle Lovett?

6. ¿Cuál era el nombre de la escuela del condado de Rusk que explotó debido a una fuga de gas, matando a 319 estudiantes y maestros?

7. ¿Cuál es el número aproximado de canciones cuyos títulos incluyen Texas o algún lugar de Texas?

8. ¿Cuál es la concha estatal de Texas?

9. ¿Cuál es el estado que es más pequeño que King Ranch?

10. ¿Qué libro infantil se desarrolló en Camp Green Lake, Texas?

¿Cómo evaluar una página web?

1. **Propósito:** ¿**Por qué** se creó la página? Para:
   - Informar
   - Divertir
   - Anunciar o vender un producto o servicio
   - Influir en las opiniones, creencias, elecciones
   - Proporcionar noticias actuales
   - Entretenimiento personal

2. **Patrocinador/Propietario:** ¿En qué tipo de proveedor de Internet u organización reside esta página?
   - Agencia de gobierno
   - Educación
   - Negocio/Compañía
   - Asociación: Profesional, Comercial, Entretenimiento
   - Agencia noticiosa: televisión, periódico, radio
   - Personal (Individual)

3. **Organización y Contenido:** ¿Está organizada y enfocada la página? ¿Está bien diseñada? ¿Está bien escrito el texto? ¿Son relevantes y apropiados los vínculos? ¿Se evaluaron los vínculos?

4. **Influencia en la postura política o en la opinión sobre el tema** (del autor o patrocinador): La mayoría de páginas web tiene un sesgo inherente que afectará todo lo que aparece en ellas. Es el autor o patrocinador:
   - ¿de izquierda/liberal?
   - ¿de derecha/conservador?
   - ¿intermedio?
   - ¿un grupo o asociación de acción política?
   - ¿un negocio?

5. **Fecha** de la producción**/revisión:** ¿Cuándo se produjo la página web? ¿Cuándo fue su última revisión? ¿Cuán actualizados están los vínculos? ¿Todavía son viables los vínculos?

6. **Utilidad:** ¿Es la página web relevante para su búsqueda?

7. **Autoridad/Autor:** ¿Quién es el responsable de la página? ¿Es el autor un experto en este campo? ¿Qué otra cosa ha escrito o producido? ¿Proporciona el autor una dirección de correo electrónico? ¿Cuán exacta es la información proporcionada? ¿Es evidente un sesgo?

8. **Público:** ¿Para qué tipo de lector está dirigida la página web? ¿Es adecuado el nivel para sus necesidades? La página es para:

    - ¿lectores en general,
    - estudiantes (primaria, secundaria, universidad, posgrado),
    - especialistas o profesionales,
    - investigadores o estudiosos?

9. **Cobertura:** ¿El tema lo cubre la página de forma integral, parcial o es un resumen?

10. **Ilustraciones:** ¿Son claras las imágenes en lo que respecta a su intención, relevancia y aspecto profesional? ¿Añaden o mejoran el contenido las imágenes?

11. **Seguridad** ¿Se emplean los sistemas de seguridad y/o cifrado cuando son necesarios?

2.0.3 La Rúbrica de evaluación de sitios web *se completa con las siguientes preguntas y con la computadora.*

HTTP://WWW.LOC.GOV/EXHIBITS/LEWISANDCLARK/LEWISANDCLARK.HTML

SITIO WEB N.° 1	1	2	3	4	5
Propósito					
Patrocinador/Propietario					
Organización y contenido					
Influencia en la postura política o en la opinión sobre el tema					
Fecha de la producción/revisión					
Utilidad					
Autoridad/Autor					
Público					
Cobertura					
Ilustraciones					
Seguridad					

NOTAS: ....

.....

2.0.3 Rúbricas de evaluación de sitios web (Continuación)

HTTP://WWW.UNMUSEUM.ORG/UNMAIN.HTM

SITIO WEB N.° 2	1	2	3	4	5
Propósito					
Patrocinador/Propietario					
Organización y contenido					
Influencia en la postura política o en la opinión sobre el tema					
Fecha de la producción/revisión					
Utilidad					
Autoridad/Autor					
Público					
Cobertura					
Ilustraciones					
Seguridad					

NOTAS: .....

.....

Terminología de Aspectos básicos de Internet

Acosador cibernético, acosadores cibernéticos, acoso cibernético: el acoso que se produce en línea.

Adware: un código malicioso que muestra la publicidad no solicitada en la computadora.

Blog: un diario personal o profesional almacenado en un sitio web que se actualiza con frecuencia. Los blogs suelen tener un tema y pueden ser públicos o privados.

Compartir archivos: se refiere a la capacidad para almacenar archivos en un lugar central para compartirlos con tan solo una persona, o con el público en general.

Cookie *(cookie de rastreo, cookie, cookie HTTP):* cookies son pequeños archivos de texto almacenados que un navegador web coloca en la computadora de un usuario.

Crimen cibernético: actividad criminal que ataca a las computadoras o que usa información en línea para atacar a las víctimas del mundo real.

Descargar: transferir material desde un servidor o computadora remota a otra computadora.

DIRECCIÓN URL: (Localizador Uniforme de Recursos) hace referencia a la dirección de Internet exclusiva de un archivo o un destino. Para encontrar un determinado sitio o documento debe escribir la dirección URL en la ventana del navegador y el navegador mostrará esa dirección en particular.

Estafa: estafar, hacer trampa, embaucar, engañar a otros.

Filtrado de contenido: permite bloquear el acceso a Internet de determinados tipos de contenido.

Firmas de correo electrónico: este es un bloque de texto agregado al final de los correos electrónicos. A menudo contiene su nombre completo, posiblemente la descripción de su puesto, la ubicación, un número de teléfono, un pensamiento inspirador, etc.

Freeware: este software es propiedad de alguien y está protegido por derechos de autor, pero el propietario decidió entregarlo en forma gratuita.

Malware: significa **mal**icious soft**ware** (software malicioso) y es un término genérico que incluye cualquier tipo de código dañino, “troyanos”, “gusanos”, “spyware”, “adware”, etc., que se infiltra en una computadora

sin el consentimiento del usuario de la misma y que está diseñado para dañar el equipo, recopilar información o corromper la computadora para usarla de forma remota para enviar spam, etc.

Página web: un documento en la web. Cada página web tiene una dirección URL única.

Phishing: cuando las personas intentan hacerse pasar por un negocio con el fin de engañarlo para que proporcione su información personal.

Publicar: significa cargar información en la web.

Redes sociales: se refiere a una categoría de aplicaciones de Internet que ayudan a conectar amigos, socios u otras personas entre sí, a través de una variedad de herramientas.

Robo de identidad: robar la identidad de una persona con el fin de suplantarla.

Sala de chat: un sitio en línea usado para la interacción social, generalmente acerca de un tema o asunto en particular, donde las personas con intereses compartidos pueden "conversar" con otras personas.

Servidor web: computadoras conectadas a Internet que alojan sitios web.

Shareware: shareware es el método publicitario de productos que le permite 'probar antes de comprar'. Este tipo de software se puede descargar en Internet o se puede distribuir en un CD y su uso es gratuito.

Sitio web: grupo de páginas web relacionadas.

Spam: correo electrónico no solicitado que intenta venderle algo. También se le conoce como correo no deseado.

Spyware: software sigiloso que aprovecha su conexión a Internet para recopilar información acerca de usted sin su consentimiento o conocimiento para enviarla de vuelta a quien escribió el programa espía. Como sucede con el adware, a menudo se instala cuando usted descarga programas de "freeware" o "shareware". El spyware puede estar buscando su información bancaria, información personal, etc. Es ilegal y generalizado.

Virus: un programa informático que puede duplicarse y propagarse de una computadora a otra.

11 Consejos para comprar en línea de manera segura

Estos consejos están abreviados por razones de espacio. Lea el texto completo en http://www.pcmag.com/article2/0,2817,2373131,00.asp

1. **Use sitios web conocidos:** empiece en un sitio de confianza en lugar de comprar con un motor de búsqueda.
2. **Busque el candado:** nunca, nunca compre nada en línea con su tarjeta de crédito cuando el sitio no tiene instalada, por lo menos, la codificación SSL (capa de sockets seguros). Sabrá si el sitio tiene SSL porque la dirección URL del sitio comenzará con HTTPS:// (en lugar de sólo HTTP://). Aparecerá el icono de un candado cerrado, normalmente en la barra de estado en la parte inferior de su navegador web, o justo al lado de la dirección URL en la barra de direcciones.
3. **No lo diga todo:** ninguna tienda de compras en línea necesita su número de seguro social o su fecha de cumpleaños para hacer negocios. De ser posible, proporcione la menor cantidad de información.
4. **Verifique los estados de cuenta:** conéctese a Internet y verifique regularmente los estados de cuenta electrónicos de su tarjeta de crédito, tarjeta de débito, y cuentas de depósitos monetarios. Si ve que algo no está bien, llame por teléfono para solucionar la cuestión rápidamente.
5. **Vacunar la PC:** usted necesita protegerse contra el malware con actualizaciones regulares a su programa antivirus.
6. **Use contraseñas seguras:** este tema se soluciona con solo asegurarse de usar contraseñas seguras, sobre todo cuando se trata de banca y compras en línea.
7. **Navegar con un dispositivo móvil:** realmente no debe sentirse nervioso por usar un dispositivo móvil, en lugar de una computadora, para hacer sus compras en línea. La clave está en usar aplicaciones directamente proporcionadas por los minoristas, como Amazon, Target, etc.
8. **Evite las terminales públicas:** esperemos que no sea necesario decirle que es una mala idea usar una computadora pública para hacer compras, pero de todos modos se lo vamos a decir. *Si lo hace, recuerde cerrar la sesión cada vez que utilice una terminal pública,* aunque solo haya sido para ver su correo electrónico.

9. **Wi-Fi privado:** si decide salir de compras con su computadora portátil, necesitará una conexión Wi-Fi. Utilice solamente la conexión inalámbrica si accede a la Web a través de una conexión de red privada virtual (virtual private network, VPN).

10. **No olvide verificar las tarjetas:** todos los años, las tarjetas de regalo son el regalo de navidad más solicitado, y este año no será la excepción. Cuando compre una, adquiérala directamente del emisor de la misma; hay estafadores que subastan tarjetas de regalo sin fondos en sitios como eBay.

11. **Reconozca que hay cosas demasiado buenas para ser ciertas:** en la mayoría de los casos, será el escepticismo el que lo salve de que le roben el número de su tarjeta.

Seguridad de las redes sociales (de AARP)

Los sitios de redes sociales, tales como MySpace, Facebook, Twitter y Windows Live Spaces, son servicios que la gente puede utilizar para conectarse con otras personas y compartir información, como fotos, videos y mensajes personales. A medida que la popularidad de estos sitios de redes sociales crece, también lo hacen los riesgos que se corren al usarlos.

1. **Tenga cuidado cuando haga clic en los vínculos** que usted recibe en los mensajes de los amigos que tiene en los sitios de la redes sociales a las que pertenece. Trate los vínculos en los mensajes de estos sitios como si fueran vínculos en los mensajes de correo electrónico.

2. **Esté consciente de lo que publica acerca de usted.** Una forma común en que los piratas informáticos entran en las cuentas financieras o de otro tipo es haciendo clic en el botón "¿Olvidó su contraseña?" que aparece en la página de inicio de sesión de la cuenta. Para entrar en su cuenta, buscan las respuestas a sus preguntas de seguridad, tales como su fecha de cumpleaños, ciudad natal, año de graduación de la escuela secundaria o segundo nombre de su madre.

3. **No confíe en que un mensaje viene de quien dice que es.** Los hackers pueden entrar en las cuentas y enviar mensajes que parecen ser de sus amigos, pero no lo son. Si usted sospecha que un mensaje es fraudulento, utilice un método alternativo para comunicarse con su amigo para averiguarlo.

4. **Para evitar revelar las direcciones de correo electrónico de sus amigos, no permita que los servicios de las redes sociales analicen su libreta de direcciones de correo electrónico.** Cuando usted se une a una nueva red social, esta podría pedirle que introduzca su dirección de correo electrónico y contraseña para averiguar si sus contactos están conectados a la red. El sitio puede utilizar esta información para enviar mensajes de correo electrónico a todos los que aparecen en su lista de contactos o incluso a todos a los que usted alguna vez les envió un mensaje de correo electrónico con esa dirección de correo electrónico. Los sitios de redes sociales deben explicar que van a hacer esto, pero algunos no lo hacen.

5. **Escriba la dirección de su sitio de redes sociales directamente en su navegador o utilice los marcadores personales.** Si para acceder al sitio hace clic en un vínculo que aparece en un correo electrónico o en otro sitio web, usted podría estar ingresando su nombre de cuenta y contraseña en un sitio falso donde podrían robarle su información personal.

6. **Sea selectivo para aceptar amigos en una red social.** Los ladrones de identidad pueden crear perfiles falsos con el fin de obtener información suya.

7. **Elija su red social con cuidado.** Evalué el sitio que va a utilizar y asegúrese de entender la política de privacidad. Averigüe si el sitio controla el contenido que la gente publica. Como estará proporcionando información personal a este sitio web, es importante usar los mismos criterios que usaría para seleccionar el sitio en donde va a introducir su tarjeta de crédito.

8. **Asuma que todo lo que pone en un sitio de redes sociales es permanente.** Incluso si usted puede eliminar su cuenta, cualquier usuario de Internet puede imprimir fácilmente fotos o texto o guardar imágenes y videos en una computadora.

9. **Tenga cuidado al instalar extras en su sitio.** Muchos sitios de redes sociales le permiten descargar aplicaciones de terceros que le permiten hacer más cosas con la página personal. Para descargar y utilizar de forma segura las aplicaciones de terceros, tome las mismas precauciones de seguridad que usted toma con cualquier otro programa o archivo que se descarga desde la web.

10. **Piense dos veces antes de utilizar los sitios de redes sociales en el trabajo.**

11. **Hable con sus hijos acerca de las redes sociales.**