# Capítulo IV

## Puesta en Marcha del Sitio Web


### Resumen

En este capítulo se revisan los pasos que se deben dar al terminar el desarrollo de un Sitio Web y efectuar su presentación a los usuarios, incluyendo desde criterios técnicos para hacer pruebas sobre el sitio construido, hasta la forma de efectuar la comunicación de sus características, para dar a conocer a la comunidad el trabajo realizado.

# 4 Capítulo IV

# Puesta en Marcha del Sitio Web

## Tabla de Contenidos

# 4 Puesta en Marcha del Sitio Web

## Desarrollo de un Plan de Pruebas

Una vez que el sitio se ha construido, es necesario hacerlo pasar por una serie de pruebas antes de y entrar a la fase de producción. Mediante dichas pruebas, se medirá su reacción integral frente a diversas acciones que realizarán los usuarios desde sus páginas.

Entre otros aspectos será necesario probar el desempeño computacional de la plataforma tecnológica usada; seguridad ante intentos de ataque y exactitud; corrección de su contenido y su despliegue en los diferentes programas visualizadores, entre otros aspectos.

## Errores en la Etapa de Pruebas

Antes de entrar de lleno en el capítulo, se debe hacer una prevención inicial sobre el funcionamiento de los sistemas y sus características, en la etapa que va entre el fin del desarrollo y el comienzo de su uso.

En este sentido, hay que anotar que los errores serán de común ocurrencia y no situaciones aisladas, por lo que hay que utilizar diversas metodologías para llevar un recuento de ellos y hacer un seguimiento ordenado de la forma en que son abordados y corregidos.

Si la metodología de desarrollo ha sido bien aplicada, en esta etapa podrían ocurrir problemas con el funcionamiento de las aplicaciones por diversas condiciones de borde (tipo de programa visualizador usado, enlaces no encontrados, etc.), pero no deberían producirse problemas relacionados con que el sistema ejecute acciones diferentes a las que se hubieran solicitado a través de sus formularios, sistemas de búsqueda u otros.

> Para evitar lo anterior, es muy importante la precisión de las descripciones que se realizan en los Términos de Referencia, a los cuales se hace referencia en el Capítulo 1.

Dado que los errores serán comunes, se debe preparar a los usuarios que harán las pruebas para este tipo de ambiente, explicándoles que las situaciones de error en esta etapa serán lo normal y que gradualmente éstas irán desapareciendo para dar lugar al funcionamiento normal de las aplicaciones probadas. Pero, lo relevante en este caso, será hacerles hincapié en la necesidad de que ellos vayan registrando e informando adecuadamente sus hallazgos, con el fin de contribuir al proceso de corrección de los errores.

## Cómo y Qué Probar

Con el fin de probar las diferentes capacidades de un Sitio Web, es necesario dividir el trabajo en cinco áreas, que son:

- Pruebas de Interfaces y Contenidos
- Pruebas de Funcionalidades y Operación
- Pruebas de Carga
- Pruebas de Seguridad
- Pruebas de Respaldo y Recuperación

Por cada una de ellas hay actividades específicas a realizar, de las cuales se entrega un detalle a continuación.

### > Pruebas de Interfaces y Contenidos

Las actividades de esta etapa consisten en hacer revisiones precisas de la forma en que se despliegan las páginas del sitio y ver si cumplen con los «Términos de Referencia» en estos temas y, además, si cumplen con los estándares mínimos que se hayan definido como meta a ser cumplida (ver Capítulo 3, sobre Usabilidad y Accesibilidad).

Las acciones de prueba sugeridas para realizar en esta etapa son las siguientes:

- Verificación de Contenidos: es una prueba básica para revisar si el Sitio Web desarrollado incluye todos los contenidos que se han especificado en los «Términos de Referencia» o los que se hayan definido en el marco del plan de desarrollo. Se puede hacer en forma manual o automática, de acuerdo a las siguientes orientaciones:

- Sistema Manual: se refiere a hacer una revisión manual de los contenidos del Sitio Web a través de la navegación de sus páginas. Para ello se recomienda primero construir un índice de contenidos y luego verificar la existencia de cada uno de los ítemes que contiene, a través de hacer un recorrido exhaustivo del sitio. Los elementos que deben probarse obligatoriamente son:

  - Verificación de ortografía y redacción
  - Verificación de enlaces principales
  - Verificación de imágenes en páginas
  - Verificación de existencia de Archivos adjuntos
  - Verificación de la Lista de Chequeo de Accesibilidad (ver Capítulo3)

- Sistema Automático: especialmente orientado a la verificación de enlaces rotos, lo cual se puede hacer utilizando sistemas basados en Internet o, bien, software especializado.
- Sistemas Basados en Internet: se recomienda usar el servicio del W3C «Check Link» (http://validator.w3.org/checklink);

- Software: se recomienda bajar y usar desde su computador el software gratuito Xenu (http://home.snafu.de/tilman/xenulink.html). De igual manera, los actuales software de creación de sitios WEB permiten manejar en forma controlada los enlaces internos; un error común de este tipo es que una foto se vea normalmente en el computador de desarrollo, pero no en el Sitio Web, Esto ocurre porque es referida en forma absoluta desde una ubicación en un disco duro local o en red, en lugar de un directorio de imágenes del Sitio Web.

  Nota: se recomienda hacer estas pruebas en ambientes controlados diferentes a los usados para el desarrollo (diferentes redes y computadores), para que los resultados sean confiables.

- Sitio en Construcción: se debe verificar que el Sitio Web no contenga espacios vacíos o que tenga el título de «en construcción». No es adecuado, bajo ningún sentido, usar espacios con dicha leyenda; en tal caso es preferible eliminar esa zona y volver a incluirla cuando exista el contenido correspondiente en el sitio.

- Verificación de Meta Tags: los «meta tags» son marcas en lenguaje html que van en la parte superior de cada página, a través de las cuales se entrega a los sistemas de indexación y búsqueda (como Google, Yahoo! y otros), la información mínima que se debe tener en cuenta para hacer una correcta indexación del contenido que incluye. Los «meta tags» son elementos que obedecen a un estándar definido por el World Wide Web Consortium (http://www.w3c.org) por lo que su uso está regulado. Para verificar que dichas marcas cumplen con los elementos mínimos requeridos por los buscadores, existen herramientas en Internet que permiten hacer tal prueba y ofrecen recomendaciones para mejorar la información ingresada en dicha área. Se recomienda en ese sentido utilizar las aplicación existente en el Sitio Web SearchMechanics.com (http://www.searchmechanics.com/prepare/index.htm) que cuenta con una aplicación en idioma español para hacer dicha comprobación.

- Verificación de Estándares: aunque los sitios web pueden ser construidos a partir de diferentes lenguajes, todos deben cumplir ciertas normas de organización de su código fuente (sintaxis), que permitan su visualización por software equivalente en diferentes plataformas. Dicha sintaxis está estandarizada y puede ser probada a través de herramientas públicas que están disponibles en Internet. Las dos más importantes son:

- Validación de HTML: la realiza el World Wide Web Consortium (http://validator.w3.org) e indica si el código usado en la página es correcto. Como resultado entrega un reporte con los eventuales errores para ayudar a su reparación.

- Validación de CSS: la realiza el World Wide Web Consortium (http://jigsaw.w3.org/css-validator) e indica si la Hoja de Cascada de Estilo (Cascade Style Sheet) cumple con la sintaxis estándar y por lo tanto podrá ser visualizada correctamente en todos los sistemas.

- Verificaciones de Interfaces: mediante esta prueba se revisan aspectos gráficos del Sitio Web, para determinar si su despliegue en las páginas es correcto. Dentro de los elementos más importantes a ser verificados, se incluyen los siguientes:

- Plug-ins necesarios: cuando se utilicen elementos audiovisuales o interactivos que requieran de algún software incrustado para funcionar (plug-ins), se debe ofrecer un enlace para que los usuarios que no lo tengan instalado, puedan bajarlo y hacer el proceso de instalación. En el caso del uso de la tecnología Flash, las últimas actualizaciones del producto permiten que el software pueda ser bajado en forma automática por los programas visualizadores, si se cuenta con la codificación adecuada. Por lo anterior, es necesario hacer la prueba desde un computador que carezca de dicho software, para comprobar que efectivamente hace dicha operación.

- Consistencia de la Diagramación: cada una de las páginas del sitio debe tener elementos consistentes, con el fin de ofrecer al usuario una experiencia similar en cualquier área del Sitio Web; por nombrar sólo tres aspectos, lo anterior implica que los menús deben aparecer siempre en el mismo lugar; que los listados deben estar diseñados de similar manera en todo el sitio y que los colores y formas de uso de las interfaces deben ser similares a lo largo de las páginas.

- Ancho de la Diagramación: si la diagramación del sitio se ha realizado para un ancho determinado (por ejemplo, 800 pixeles de ancho), en esta etapa se debe probar si ello se cumple. Asimismo, se debe probar en una pantalla configurada con una menor dimensión (por ejemplo 640 x 480 pixeles), cuál es el área visible del sitio y cómo afecta eso a la navegación por el mismo. Otra prueba del mismo estilo, se refiere a usar un programa visualizador orientado sólo a texto como Lynx (http://www.delorie.com/web/lynxview.html), para obtener visiones alternativas de la manera en que los usuarios están accediendo a la información que se les ofrece.

  En este aspecto, en caso de existir, es de interés contar con un estudio del «log» del servidor que muestre la forma en que los usuarios están accediendo a las páginas, porque de esa manera se podrá determinar hacia qué configuración de pantalla se debe atender con mayor prioridad. La norma en este aspecto es que sin importar las características técnicas que tenga el computador del usuario que accede al Sitio Web, éste siempre se vea ordenado y legible.

- Diagramación vs. Browsers: aunque la codificación en los lenguajes soportados por los programas visualizadores (browsers) puede apegarse a los estándares, no todos muestran de la misma manera los sitios web. Dado esto, es necesario revisar el sitio en diferentes tipos de programas, especialmente en aquellos que conforman la minoría, al momento de escribir este Manual. Es decir, las pruebas al menos deberían hacerse en Microsoft Internet Explorer (http://www.microsoft.com/explorer), Opera (http://www.opera.com) y Mozilla (http://www.mozilla.org), ya que con ellos se cubrirá un amplio espectro. Lo que se debe

revisar en este caso es el despliegue de todos los elementos que se muestran en la pantalla, para asegurar de que aparecen en las posiciones que se les han asignado en el diseño.

- Diagramación vs. Sistema Operativo: tal como se explicó en el caso anterior, los diferentes sistemas operativos pueden establecer diferencias en la forma en que se muestran los sitios web. Por ello, es importante conocer cuáles son los sistemas operativos utilizados por la audiencia a la que se desea llegar y revisar el despliegue del sitio en ellos. Hay que recordar que, además de Microsoft Windows, los usuarios pueden estar visualizando el sitio desde computadores equipados con Apple Macintosh o diferentes versiones del sistema operativos Unix.

- Imágenes Escaladas: se debe verificar que las imágenes que aparezcan en el sitio no estén siendo mostradas en tamaño reducido artificialmente; es decir, que se tome una imagen de grandes dimensiones y por programación se muestre en un tamaño menor. El efecto de eso es que las páginas con ese tipo de imágenes serán muy pesadas y harán que el acceso a ellas sea lento. Para comprobarlo, se debe solicitar las «Propiedades» de la imagen; en la ventana que se muestra se indica el peso de la imagen, que no debería sobrepasar los 5Kb para las de tamaño pequeño (iconos y thumbnails) y los 25 Kb, para los de tamaño mediano (fotografías en noticias). Es importante considerar que, además de estas verificaciones individuales de peso de imágenes, el límite de peso para una página es de 100Kb, incluyendo todos sus elementos.

- Imágenes Sin Atributo ALT: para cumplir con las normas de accesibilidad es necesario que todas las imágenes que se usen en un Sitio Web, tengan una descripción utilizando el atributo ALT (para texto alterno) del lenguaje HTML. Para comprobarlo, basta situar el mouse sobre una imagen, para que se despliegue una leyenda en texto en una etiqueta amarilla que flota sobre la foto; si eso no ocurre, el atributo no está siendo usado y debe ser corregido e incluido.

### > Pruebas de Funcionalidades y Operación

Las actividades de esta etapa se refieren a hacer chequeos completos respecto de las funcionalidades y aplicaciones que ofrece el sitio, ya sean de aplicaciones simples como formularios hasta más complejas, como consultas y modificaciones de registros en base de datos.

En este sentido, las pruebas se deben hacer sobre diferentes elementos, siendo algunos de los más importantes los siguientes:

- Validación de Formularios: si el Sitio Web tiene formularios para el envío o ingreso de datos, se debe utilizar sistemas de validación del ingreso de datos para asegurar que éstos sean bien ingresados. En este aspecto, algunas de las validaciones más importantes deben ser las siguientes:
- Campos Obligatorios: se debe validar que en los formularios sean ingresados todos aquellos campos que sean necesarios; éstos deben ser marcados de alguna manera (usualmente con

un asterisco) que permita a los usuarios entender la obligatoriedad de ingresar información en ellos; adicionalmente, debe indicarse tal condición en forma explícita

- Validaciones Locales: para reducir la carga de validaciones en el servidor, se recomienda incorporar la mayor cantidad de éstas en el computador del cliente, utilizando en forma estándar el lenguaje Javascript para hacerlas.

- Sintaxis de Ingreso: se debe validar que, en algunos casos, los campos sean ingresados con datos válidos; el mejor ejemplo es el caso del ingreso del número de RUT o Cédula de Identidad, cuyos números tienen un algoritmo conocido para ser validado.

- Suscripción a Servicios: se debe validar que cada vez que se realice la suscripción a un servicio que ofrezca el Sitio Web, se envíe un e-mail al usuario (para lo cual se debe necesariamente solicitar su dirección de correo electrónico) en el que se le informe sobre el resultado de lo realizado. Quien pruebe el sistema debe validar que el sistema esté enviando correctamente los e-mails y que dicho e-mail llegó a la dirección correspondiente; en este caso se recomienda probar con una dirección de recepción externa a la institución desde la cual se prueba.

- Ingreso de Datos: si se cuenta con un sistema que permita el ingreso de información hacia una base de datos, se debe revisar en la tabla de destino que efectivamente se estén enviando los datos de la manera que se ha previsto.

- Reingreso y Corrección de Datos: para mejorar la interacción del Sitio Web, cuando tras el ingreso y envío de los datos de un formulario (después de la validación local del formulario) el usuario presiona el botón «Back» de su programa visualizador para volver atrás y modificar algún campo, se le deben presentar todos los datos que hayan sido ingresados. De esta manera se aprovecha la información ingresada previamente, evitando la frustración del usuario por tener que escribir nuevamente el contenido completo del formulario.

- Elementos de Interfaz: al usar elementos del lenguaje HTML para la creación de las pantallas (input boxes, combo boxes, list boxes, radio y check buttons, etc.), se recomienda no modificar radicalmente sus atributos de despliegue (colores, formas) y comportamientos tradicionales, para lograr que el usuario sepa intuitivamente cómo usarlo y no deba aprender de nuevo su operación.

- Multiplataforma: se debe comprobar que los formularios funcionan en diferentes versiones de programas visualizadores (browsers), de sistemas operativos y de tipos de conexión a Internet (conmutado, banda ancha y dedicado).

- Botones de Interacción: si se cuenta con botones interactivos que permiten imprimir, enviar una página a un amigo, etc. se debe validar que estén realizando correctamente la acción indicada.

- Sistemas de Búsqueda: si se cuenta con ellos, se debe validar que efectivamente permitan encontrar documentos existentes en el sitio; en este sentido se deben ingresar documentos específicos y luego buscarlos de manera de asegurarse que la funcionalidad está operando adecuadamente. Si el sistema de búsqueda tiene una versión de «búsqueda avanzada», se debe asegurar de que las opciones ofrecidas encuentren los documentos de la manera en que se ofrezca. El formulario para hacer la búsqueda debe ser intuitivo, evitándose el lenguaje técnico y específico que impida entender su funcionamiento entre usuarios con menores conocimientos de los temas abordados en la institución.

- Sistemas de Feedback: si se cuenta con sistemas de envío de preguntas o reclamos (al estilo de los indicados para la Oficina de Informaciones, Reclamos y Sugerencias, OIRS), se debe asegurar de que se está completando el ciclo de vida de la consulta. En este sentido se debe validar que el sitio realiza la consulta y que ésta es recibida por el funcionario encargado de atenderla. De otra manera, la funcionalidad podría operar computacionalmente pero no en términos de tramitación.

- Sistemas de Compra: si se cuenta con sistemas de pago en línea, se debe revisar cuidadosamente el flujo de trabajo de la aplicación y asegurarse de que en cada uno de los pasos se está asegurando la calidad y seguridad de la transacción.

- Administración del Error 404: cuando se ingresa una dirección equivocada, el software del servidor web muestra una pantalla de error anunciando el número de código del problema (Error 404). No obstante, dicho software puede ser configurado para que muestre una página diferente, en la que se explique a los usuarios las probables razones del error. Es importante incluir, en dicha página, un enlace al Mapa del Sitio y un Buscador, de tal manera que el usuario tenga más herramientas para resolver la inexistencia del contenido que buscaba. Se recomienda, además, que el Administrador de Sistemas de la institución entregue un reporte semanal basado en los «logs» del servidor, que permita ver qué es lo que más buscan los usuarios y de qué manera el Sitio Web les está respondiendo sus consultas.

### > Pruebas de Carga

La carga de trabajo se refiere a la capacidad máxima que tiene un servidor web (hardware y software), para atender a un conjunto de usuarios de manera simultánea. Por ello, las actividades de esta etapa tienen relación con comprobar, de manera anticipada, el funcionamiento que tendrá el servidor del Sitio Web cuando esté en plena operación.

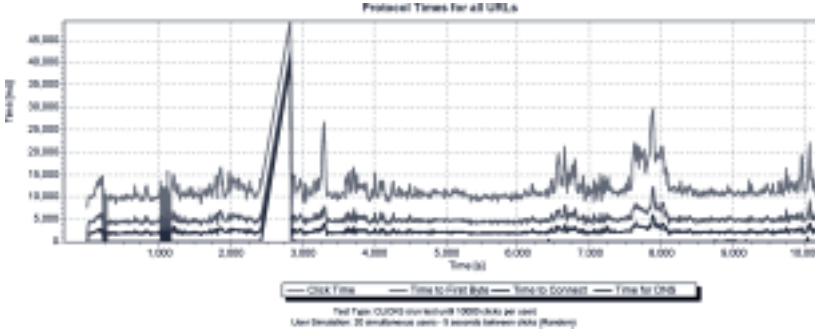
Las pruebas en este caso consisten en simular una carga de trabajo similar y superior a la que tendrá cuando el sitio esté funcionando, con el fin de detectar si el software instalado (programas y aplicaciones) cumple con los requerimientos de muchos usuarios simultáneos y también si el hardware (servidor y el equipamiento computacional de redes y enlace que lo conecta a Internet) es capaz de soportar la cantidad de visitas esperadas.

Es importante considerar que si el servidor está en las dependencias de un tercero que entrega el servicio de alojamiento del Sitio Web (hosting), se le debe solicitar a dicho proveedor un informe en que dé a conocer las características de carga de la solución de hardware y software sobre la cual funciona el Sitio Web de la institución.

Hay diversos software en el mercado que están orientados a este tipo de simulaciones, todos los cuales ofrecen características similares. Entre los datos más relevantes que es posible obtener se cuenta:

- Tiempo de acceso de los usuarios a los datos
- Volumen de datos y ancho de banda utilizado
- Archivos solicitados y tiempos usados en transferencia de datos
- Tiempo de espera de los usuarios tras hacer un clic
- Tiempo de respuesta a clicks de usuarios
- Niveles de error existentes tras clicks de usuarios

Como se puede apreciar del listado anterior, los reportes que se obtienen a través de esta vía se refieren a tiempos de acceso que tienen los usuarios que acceden al Sitio Web y la degradación que ocurre en los servicios cuando aumenta el volumen de visitantes concurrentes.




Un ejemplo de las pruebas que se pueden realizar en este tema se puede ver en este gráfico que muestra los tiempos que demora en atender los requerimientos por las direcciones solicitadas tras un click de usuarios.

Cada una de las líneas representa un valor importante de tener en cuenta:
Click time: demorad el sitio en entregar los datos tras el primer click.
Time to First Byte: tiempo que se demora tras el click, en enviar el primer byte de datos.
Time to Connect: tiempo de demora tras enviar el click, en establecer la conexión entre servidor y cliente.
Time for DNS: tiempo de demora para resolver la dirección solicitada en el click.

Con los resultados obtenidos con pruebas de este tipo se debe hacer una revisión acuciosa de los sistemas, con el fin de hacer las optimizaciones que aparezcan como necesarias. Asimismo, se debe tener en cuenta que será normal la existencia de situaciones excepcionales que harán que los servicios no funcionen adecuadamente.

### > Pruebas de Seguridad

Las actividades que se pueden realizar para hacer las pruebas de seguridad son diversas y se orientan a varios ámbitos, como se describe a continuación. Los temas a tratar son los siguientes:

- Manejo de DNS
- Protección de Estructura Interna del Sitio Web
- Protección contra Robots
- Manejo de Privacidad
- Canales seguros
- Mecanismos de Control de Acceso
- Protección de Programas
- Hosting vs. Sitio Propio
- Roles Mínimos a asegurar

A continuación se entrega información para cada uno de ellos.

#### Manejo de DNS

Un aspecto que se debe cuidar es el de utilizar un nombre de dominio adecuado y relacionado con la identidad y misión de la institución. No obstante, gracias a la forma de operación del Domain Name Service (DNS o Servicio de Nombre de Dominio) es posible asignar más de un nombre de dominio a un mismo Sitio Web. De esta manera es posible incorporar otras denominaciones, bajo el dominio .CL u otro, que permitan generar «alias» adicionales para el sitio y así permitir utilizar las denominaciones más coloquiales con la cual la institución es conocida por los ciudadanos.

No obstante, sin importar cuántos alias tenga un sitio, se recomienda que todos los dominios sean redirigidos para que la primera pantalla, en cualquier caso, corresponda a la portada «oficial» del Sitio Web.

> Recuerde que sobre los nombres de dominio existe una normativa obligatoria definida en el Oficio No. 485, del 10 de noviembre de 2000, en relación con el Decreto Supremo No. 5996, donde se especifica claramente que los sitios del Estado deben registrar su dominio bajo la denominación .GOB.CL y .GOV.CL. Adicionalmente pueden hacerlo bajo el dominio .CL en forma directa.

Dicha operación, en cuanto a procedimientos y alcance, está definida en su totalidad en el sitio http://nic.gob.cl y mayores referencias se pueden encontrar en http://nic.gob.cl/normativa.htm.

### Protección de la Estructura Interna del Sitio Web

Uno de los mecanismos que permite proteger la estructura interna del sitio (especialmente para casos de intentos de ataques externos y/o intentos de violación de confidencialidad), es disminuir la cantidad de información contenida en las URL que se muestran en el programa visualizador. Esto es importante respecto de directorios y nombres de programas, pero especialmente en lo que se refiere a la entrega de parámetros de sesión, datos de usuario u otro mecanismo de transferencia de información entre páginas y/o secciones de código.

Se recomienda que los mecanismos de traspaso de información entre páginas sea a nivel de objetos del servidor, asociados a la sesión, sin que la interacción con el lado cliente deba hacerse responsable de la transferencia de datos y/o información entre sesiones de ejecución del servidor.

De igual forma, se recomienda evitar que el acceso a elementos del servidor web esté asociado a «direccionamientos relativos por sesión» o asociados al UserId o SessionId; esto se debe a que mediante simples pasos se puede conocer «token» de sesión y gracias a eso simular que es el mismo usuario que regresa al sitio. Para evitar el problema se recomienda incorporar protecciones de dirección relativas a la Dirección IP de origen.

Otro método de protección de estructura interna consiste en deshabilitar (excepto para casos excepcionales, como repositorios públicos de archivos) la navegación sobre directorios mediante el servidor web. Esta protección se hace para todos los directorios desde la configuración del software del servidor web. Otra forma de hacerlo consiste en incorporar un archivo por omisión del servidor web en todos los directorios, aun cuando no sea directamente referenciado por otras páginas para que se muestre su contenido cuando un usuario intente revisar el contenido existente en el directorio. En el caso de habilitar la navegación sobre directorios, se debe evitar el acceso a ciertos directorios protegidos.

> Junto con estas protecciones de lectura, se recomienda realizar periódicamente una revisión de los esquemas de permisos otorgados a directorios y archivos. Las permanentes actualizaciones del software de un servidor web, generalmente provocan un problema de control del acceso a nivel de archivos, lo cual requiere procedimientos claros de supervisión.

### Protección Contra «Robots»

No todos los directorios del sitio deben estar disponibles para que los robots de búsqueda (conocidos más popularmente como «arañas» o «spiders» de los buscadores) entren en ellos. Para impedirlo, se debe utilizar el archivo «robots.txt» o las instrucciones específicas en los «meta-tags» de la página de inicio, para impedir su ingreso.

El archivo «robots.txt» es un archivo de texto plano (no de html) ubicado en directorios el servidor web que contiene instrucciones precisas respecto de qué hacer en ellos. Cada vez que un robot visita un sitio, primero revisa si existe ese archivo.

Si no lo encuentra, indexa la página en el sistema buscador que lo haya enviado; si lo encuentra, analiza su contenido buscando la siguiente información:

```
User-agent: *
disallow: /
```

La primera línea «User-agent» indica que es válida para todos los robots que lleguen (porque tiene un asterisco; puede restringirse a un robot, indicando su nombre), mientras que la segunda indica con «disallow» que no está permitido avanzar por los enlaces de la página al uras % hace referencia a la raíz del sitio.

En otro caso, si se quiere evitar el acceso de todos los robots a un directorio determinado (por ejemplo cgi-bin, donde están los archivos más sensibles), se puede indicar esa información de la siguiente manera:

```
User-agent: *
disallow: /cgi-bin/
```

Adicionalmente se puede usar el commando «allow» que permite incluir directorios específicos, gracias a lo cual ciertos contenidos sí son indexados. Por ejemplo:

```
User-agent: *
disallow: /imagenes/
allow: /imagenes/logotipo-institucion.jpg
```

En este caso la segunda línea indica con «disallow» que no está permitido ingresar al directorio de Imágenes, pero que sí se puede indexar un archivo específico, que corresponde al Logotipo institucional.

Otra forma de impedir el acceso de un robot es poniendo marcadores específicos en los «meta-tags» de las páginas. No obstante, este mecanismo no es soportado por todos los robots, por lo que su alcance es más limitado.

La forma precisa de incluir dicho «meta-tag» es la siguiente:

```
<html>
<head>
<meta name=»robots» content=»noindex,nofollow»>
<meta name=»description» content=»Este sitio....»>
<title>...</title>
</head>
<body>
...
```

Las cuatro posibles combinaciones de este «meta-tag» son las siguientes:

- <meta name=«robots» content=«index,follow»>
  - Indica que la página puede ser indexada y sus enlaces seguidos

- <meta name=«robots» content=«index,nofollow»>
  - Indica que la página puede ser indexada, pero sus enlaces no pueden ser seguidos

- <meta name=«robots» content=«noindex,follow»>
  - Indica que la página no puede ser indexada, pero sus enlaces pueden ser seguidos

- <meta name=«robots» content=«noindex,nofollow»>
  - Indica que la página no puede ser indexada ni sus enlaces seguidos

Manejo de Privacidad

Mantener la privacidad de los usuarios debe ser un objetivo permanente del sitio. Para ello se requiere de contar con una Política de Privacidad formal y explícita en el sitio y, además, deben existir mecanismos de seguridad concretos para proteger los datos de sus usuarios.

Más información en :
*http://www.robotstxt.org/wc/robots.html*
*http://www.robotstxt.org/wc/norobots.html*

Entre estos, se debe contar con protecciones físicas y lógicas sobre dicha información.

En el caso de disponer de arquitecturas multicapas reales, se recomienda proteger la información de clientes en servidores físicos distintos de almacenamiento de datos, incluyendo interfaces idealmente separadas de consulta de datos. Además, incorporar mecanismos de encriptación de los datos para información sensible.

Se recomienda que la información, si es almacenada para efectos de que los usuarios la recuperen desde el Sitio Web, sea encriptada con claves administradas por ellos mismos (por ejemplo, su clave de autenticación frente al sitio).

Una decisión de arquitectura que disminuye el riesgo de robo de información de clientes o cuentas de acceso, consiste en evitar que desde la Base de Datos sea posible generar parejas UserId/Clave que permitan autenticarse frente al sitio. La forma de hacerlo es incorporar mecanismos que almacenen un valor de índice de la clave en la Base de Datos, en vez de almacenar la clave propiamente tal. Gracias a esto, cuando un cliente se autentica frente al sitio, la comparación de claves se realiza sobre los valores de índice y se evita conocer directamente esa información.

Es importante destacar además que un buen diseño de los mecanismos de autenticación junto con mecanismos de auditoría, almacenamiento y recuperación posterior, son adecuados para la implementación de la Firma Electrónica Simple, requisito definido como suficiente para múltiples interacciones del Estado, de acuerdo con la Ley 19.799 y su reglamento (analizar recomendaciones asociadas al Uso del Documento y Firma Electrónica al interior del Sector Público).

Finalmente, se recomienda un control particular de todos los procesos de respaldo, recargas, manejo de medios removibles y generación de copias de información, por ser mecanismos internos de fugas o compromiso de confidencialidad de la información.

### Canales Seguros

Es importante incorporar mecanismos de encriptación del canal de comunicaciones (como el protocolo Secure Socket Layer o SSL), para la transferencia de información privada entre los usuarios y el Sitio Web, a través de la red Internet. Hacerlo no requiere de programación adicional a las funcionalidades de interacción, y asegura la protección de toda la información intercambiada entre el servidor y los usuarios.

Desde un punto de vista de desempeño, si bien el inicio («hand shaking») del proceso de establecimiento del canal SSL puede significar un pequeño retardo en la conexión inicial, posteriormente no provoca un aumento significativo del ancho de banda utilizado en la conexión, ni tampoco obliga a un aumento significativo de recursos del servidor.

> Es importante considerar que la seguridad asignada a un Sitio Web debe ser correspondiente con la inversión y la importancia de los datos almacenados, siendo estas capacidades obligatorias para el caso de los sitios transaccionales.

### Mecanismos de Control de Acceso

Otro aspecto que genera mejoras en la protección de la privacidad de los usuarios y de la información contenida en el Sitio Web, es la incorporación de mecanismos modernos de generación de claves y autenticación, como los que se plantean a continuación.

- Firma Electrónica Simple y Avanzada: es un sistema que identifica al usuario cuando realiza trámites a través de Internet o redes cerradas. Existe una ley y el correspondiente reglamento que la regula y empresas que las ofrecen en el mercado (más información en http://www.entidadacreditadora.cl). Ambas firmas constituyen las bases legales para que ciudadanos y empresas puedan identificarse virtualmente y de esa manera enviar comunicación y hacer negocios de manera más segura y confiable. Se trata de un mecanismo de complejidad media, aunque incluye funcionalidades de seguridad y criptografía. No obstante, la incorporación de este mecanismo en forma única dependerá del control absoluto que se tenga de la comunidad de usuarios de la solución. Para comunidades abiertas es preferible establecer dos mecanismos de autenticación: uno fuerte, mediante Firma Electrónica (usando certificados digitales) y otro, mediante autenticación de Usuario y Clave. Por otro lado, la Firma Electrónica

Simple podría ser usada para las comunicaciones oficiales enviadas por la institución a sus usuarios. El uso de la Firma Electrónica debe definirse al momento de determinar la arquitectura de solución del Sitio Web.

- Autenticación con par Usuario y Clave: si se emplea esta solución, debe existir un procedimiento concreto para los casos en que un usuario pierda o no recuerde su clave. Se recomienda ofrecer mecanismos de «regeneración de clave», mediante la entrega de respuestas a preguntas predefinidas por los usuarios, en lugar de hacer el «envío de la clave por e-mail». En el caso de contar con mecanismos de Ayuda, se debe ofrecer apoyo para la regeneración de las claves, sin que el personal de la institución tenga acceso a la información de seguridad del cliente. Se debe evitar el uso de mecanismos de autenticación administrados por terceros, en caso de que puedan comprometer la confidencialidad o la suplantación del usuario.

- Sistemas de Hardware para Autentificación: para sistemas de seguridad que requieren una autenticación absoluta del usuario, es preferible considerar mecanismos de autenticación fuerte. Para ello, se deben incorporar mecanismos que incluyan elementos de hardware que deben estar en posición del usuario, tales como tarjetas u otros similares (security token) que permiten el acceso a las áreas de autenticación. Allí el usuario debe ingresar su identificación de Usuario (security challenge response) y se le genera una clave de sesión que al ser digitada en pantalla, le permite acceder al sistema. Dicha clave cambia frecuentemente para aumentar la seguridad de acceso.

### Protección de Programas

Es fundamental proteger los códigos y programas internos del servidor web, particularmente evitando la transferencia de parámetros o información a través de la dirección de acceso a las páginas (por ejemplo, al usar el método GET para la entrega de parámetros), los cuales son mecanismos frecuentes de «hackeo» o robo de información.

De igual forma, se debe evitar la lectura de ejecutables desde los directorios del servidor, controlando los permisos adecuados de acceso a éstos, con el fin de evitar desensamblaje y/o ingeniería reversa para analizar accesos internos.

En cuanto a los «scripts» ubicados en el lado del cliente, en caso de ser críticos, se recomienda utilizar compactadores de código y eliminar documentación de apoyo que permita su fácil comprensión a partir de la lectura del código.

Es importante que estas medidas sean incluidas junto a las acciones de seguridad informática normales de la institución.

### Hosting Externo vs. Sitio Propio

Sin entrar en profundidad en cuanto al detalle de los elementos a considerar para esta decisión, la principal recomendación es hacer una evaluación objetiva basada en los siguientes aspectos:

- Evaluar las reales capacidades disponibles para la operación permanente del sitio, desde un punto de vista técnico.
- Evaluar los requerimientos de control y seguridad necesarios.
- Evaluar el nivel de soporte efectivo que el personal técnico del servicio puede realizar sobre los servidores.

Con estos parámetros se debe definir la mejor opción, no sólo desde el punto de vista del interés de las áreas técnicas, sino que mediante una evaluación de impacto global de la decisión asociada.

La amplia oferta disponible permite realizar combinaciones de servicios e infraestructura de muy diversos tipos, lo cual facilita configurar una solución óptima en términos del costo-beneficio asociado (por ejemplo, hosting compartido, dedicado, collocation, housing, red administrada, monitoreo de seguridad, administración de seguridad perimetral, control de aplicaciones, fulfillment, etc.).

En caso de que se decida externalizar esta área, es importante contar con altos estándares de parte del proveedor en todo lo referido a tiempo de desempeño («uptime»), respaldos y recuperación, actualizaciones de software, etc.

### Roles Mínimos a Asegurar

Un último aspecto considerado en esta área de recomendaciones, consiste en definir los diversos roles profesionales dentro de la definición y diseño de un Sitio Web para una institución.

Desde un punto de vista exclusivamente técnico, es fundamental considerar al menos los siguientes roles, identificando tanto sus responsabilidades como el personal más competente que pueda cumplirlos.

Si bien más de uno de estos roles funcionales puede ser desarrollado simultáneamente por una persona o área de la organización, es importante que dichas áreas sean cubiertas no sólo durante la puesta en marcha de la solución sino también durante su etapa de producción.

- Arquitecto: encargado de hacer las configuraciones de trabajo de los servidores y aplicaciones.
- Administrador de Aplicaciones: encargado del funcionamiento del software operativo.
- Administrador de Control de Calidad: encargado del cumplimiento de las políticas de calidad.
- Administrador de Seguridad: encargado de hacer generar y hacer cumplir las directivas de seguridad.

- Administrador de Operaciones: encargado de los aspectos operativos relacionados con el hardware.
- Administrador de Contenidos: encargado de las informaciones contenidas en el Sitio Web.
- Administrador de HelpDesk y Soporte: encargado de dar soporte a usuarios sobre las funcionalidades del Sitio Web.
- Administrador de Contingencias: encargado de enfrentar en primera línea los problemas que se generen en la operación.
- Auditor / Contralor: encargado de llevar registro de las operaciones realizadas, con el fin de apoyar la revisión de procedimientos.

Finalmente, aunque los roles del área Informática pueden estar muy claros, es necesario que se entienda que la operación del Sitio Web es una tarea conjunta en la que participan funcionarios de diversas áreas de la institución.

### > Pruebas de Respaldo y Recuperación

Respaldar la información de un Sitio Web se refiere a copiar el contenido completo del sistema (datos, programación, imágenes, etc.) a un medio que sea confiable, que esté en un lugar seguro y que permita la recuperación de manera rápida y eficiente.

En este sentido, hay que preocuparse no sólo de probar la confiabilidad del sistema al momento de respaldar, sino también para la acción de recuperar y volver a instalar lo respaldado.

Más información en *http://www.monografias.com/trabajos14/respaldoinfo/respaldoinfo.shtml*

### > Registro y Control de Pruebas y Errores

Para que una prueba sea válida, debe ser lo más documentada posible, con el fin de que, quien deba efectuar la corrección, pueda replicar el error para analizarlo y luego proceder a tomar medidas correctivas. Para ello se recomienda llevar una planilla de cálculo (que se puede obtener del Sitio Web: de la Guía) en que se vayan anotando por columna los siguientes datos:

- Detección del Error: para ser anotado por quien prueba.
  - Módulo: indica la sección en la que se produce el error.
  - URL: dirección de la página donde ocurrió el error.
  - Acción: Indicar la secuencia de pasos que siguió para que ocurra el error.
  - Lo que hace o dice: es la explicación más detallada posible del error, en particular señalando la secuencia de pasos seguida hasta dar con el error.
  - Lo que debe hacer o decir: se debe indicar lo que se espera que debería ocurrir cuando se hace la acción que se ha descrito.
  - Encontrado por: nombre de quien prueba.
  - Fecha: fecha en la que se hace la anotación.

  - Reproducible: indicar si el error se repite al hacer nuevamente la prueba.
  - Clasificación: permite definir el grado de complejidad del error, al señalar si afecta el funcionamiento del sitio (caso extremo) o sólo su presentación.

- Diagnóstico del Error: para ser anotado por quien corrige.
  - Causa: motivo por el cual se produce el error.
  - Efectos laterales: indicar en qué otros módulos la existencia de este error puede estar causando impacto negativo; muchas veces errores diversos tienen una causa común, por lo que al reparar ésta se arreglan los demás.

- Corrección del Error: para ser anotado por quien corrige.
  - Descripción: acción realizada para hacer la reparación del error.
  - Archivos intervenidos: archivos en los que se hicieron modificaciones o, al menos, el principal de ellos.
  - Corregido por: persona que hizo la corrección.
  - Fecha corrección: fecha en que quedó reparado el error.

- Comprobación de la Corrección: para ser anotado por quien revisa la corrección realizada.
  - Revisor: Nombre de quien revisa si el error fue efectivamente reparado.
  - Fecha: fecha en que se realiza la revisión.
  - Reparado: indicar si está reparado o no. Si no lo está, se debe copiar la línea de error en blanco en una nueva planilla, con el fin de solicitar nuevamente el proceso de corrección.

## Derechos del Usuario

Los usuarios que acceden a un Sitio Web de carácter general, tienen derechos y obligaciones, aunque muchas de ellas existen por un compromiso tácito y basado en la costumbre, más que en la existencia de una ley, reglamento o contrato que se refiera a ellos.

No obstante, en el caso de sitios web de instituciones públicas, la situación es mucho más restrictiva, ya que existe cierta normativa sobre el uso y acceso a la información, que debe ser respetada y atendida.

Por lo anterior, se recomienda que todo Sitio Web de Gobierno ofrezca en todas sus páginas la información necesaria para indicar cuáles son esos derechos y obligaciones. Dentro de ellos, lo más importante que se debe puntualizar se describe en los siguientes títulos.

### > Política de Privacidad

Se trata de incluir, en un solo documento, toda la información relativa a los derechos que tiene una persona frente a la información que le ofrece un Sitio Web de una institución pública. Entre los aspectos más importantes que debe indicar, se cuentan los siguientes:

- Recopilación de datos: debe indicar si el sitio recopila o no datos de los usuarios (en forma manual o automática) y qué es lo que hace con ellos.
- Eliminación de datos: si el sitio recopila datos de usuarios con el fin de guardarlos en una base de datos, se debe informar de los mecanismos existentes para que puedan eliminarse de dicha base.
- Uso de los datos: debe indicar de qué manera se utilizarán los datos los usuarios recopilados a través de las diferentes funcionalidades del Sitio Web, con el fin de que ellos tengan conocimiento de esas operaciones.

### > Política de Uso de Información

En este ámbito se debe indicar quién es el propietario de la información que se está mostrando a través del Sitio Web y qué derechos y deberes tiene el usuario que revisa esos contenidos. Por lo anterior, los temas que deben ser cubiertos a través de esta área, son los siguientes:

- Uso de la Información: dado que el Sitio Web habitualmente será utilizado por diferentes personas e instituciones para acceder a información de primera mano respecto del servicio propietario del sitio, se debe informar que los contenidos del Sitio Web pueden ser utilizados sin restricciones por los usuarios. No obstante, deben tener cuidado de cumplir con las normas señaladas en el punto «Fuente de Información» citado más adelante.

- Derechos de Autor: aunque por definición los contenidos de los servicios del Estado se entienden como públicos y, por ello, no existe restricción para su uso, se debe indicar quién es el dueño de los derechos de autor de la información que se está entregando. Esto es complementario al hecho concreto de que se da permiso para el uso de la información, siguiendo los lineamientos que se exponen en el siguiente subtítulo. En el caso de que se ofrezcan documentos u otros elementos de contenido que tienen derecho de autor propio; se debe indicar claramente quién es el propietario y las restricciones de uso del contenido. Para más información sobre la Ley de Propiedad Intelectual N° 17.336, consultar en http://www.dibam.cl/prop_intel/ley.html

- Sitio Web como Fuente de Información: cuando terceros utilicen información del sitio para divulgación a través de otros medios, se debe solicitar que lo hagan citando la procedencia de la información a través de una frase estándar que se debe incluir en el Sitio Web. De esta manera se podrá asegurar que dicha cita aparezca en los términos que la institución considere adecuados.

### > Otros Temas

Adicionales a lo anterior, hay varios temas que requieren de hacer comunicaciones específicas a los usuarios, con el fin de que ellos conozcan cuáles son las reglas de uso de la información que se puede dar a través del sitio.

Entre los temas más importantes, se cuenta:

- Cobro de los Servicios: aunque no es lo habitual cobrar por los servicios o contenidos de un Sitio Web de una institución pública, en el caso de que se realice se debe declarar qué áreas de contenido son pagadas o restringidas. En dicha situación se deben indicar claramente los precios y las formas de pago.

- Calidad de los Servicios: dado que un Sitio Web puede ser alterado maliciosamente a través de ataques informáticos, se sugiere incluir una advertencia dentro del área de «Uso de la Información» en la que se indique que, debido a problemas de fuerza mayor, la emisión de estos servicios puede verse suspendida, por lo que la institución no asume obligaciones referidas a su mantención cuando enfrente dichos eventos. Este tipo de mensajes ayuda a cuidar la imagen de la institución frente a imprevistos.

### > Ley de Silencio Administrativo

Tras la promulgación de la Ley de Silencio Administrativo durante el año 2003, a través de la cual se instaura el concepto del «silencio positivo», se establecieron las «obligaciones de cumplimiento de los plazos» en los servicios públicos.

Debido a dichas normas, las instituciones públicas tienen ahora la obligación de responder a determinados trámites y peticiones dentro de los tiempos que se hayan indicado para ellos. Esto significa que en los diferentes niveles existen ahora obligaciones concretas respecto del intercambio de información.

Como a través de un Sitio Web se pueden recibir mensajes de los usuarios, se deben tener en cuenta dos obligaciones que impone dicha ley y que puede ser afectadas por la operación web. Estas son:

- El funcionario del organismo al que corresponda resolver, que reciba una solicitud, documento o expediente, deberá hacerlo llegar a la oficina correspondiente a más tardar dentro de las 24 horas siguientes a su recepción.

- Los casos de mero trámite, como los acuse de recibo, deberán despacharse dentro del plazo de 48 horas, contado desde la recepción de la solicitud, documento o expediente.

Como a través del Sitio Web es posible recibir datos enviados por los usuarios que pueden acogerse a las normas de esta ley, es importante verificar que existen los resguardos administrativos necesarios para que siempre se dé cumplimiento a ellas.

Como punto de partida se recomienda iniciar la aplicación de estas normas para la atención de los correos electrónicos que llegan desde el Sitio Web, a través de la sección de Contacto.

## Desarrollo de un Plan de lanzamiento

Para hacer el lanzamiento de un nuevo Sitio Web es obligatorio que el nuevo sitio haya cumplido adecuadamente las pruebas antes descritas, con el fin de que todos los contenidos prometidos estén incorporados y las funcionalidades realicen todo aquello que se describe respecto de ellas.
Si hay contenidos o funcionalidades descritas que no pueden estar disponibles para el momento en que se desea hacer el lanzamiento del Sitio Web, es preferible eliminarlos en ese momento e incorporarlos cuando estén listos, en lugar de dejarlos en el sitio y que den una mala imagen sobre el mismo.

### > Lista de Chequeo Previa

Para llegar al lanzamiento del sitio, se recomienda asegurarse del cumplimiento de las siguientes actividades como mínimo:

- Cumplir Listas de Chequeo: el sitio debe haber cumplido adecuadamente las pruebas indicadas en este capítulo, antes de hacer su lanzamiento.
- Dominio Distintivo: se debe contar con un nombre de dominio que sea reconocible y se asocie a la institución, de tal manera que sea fácil relacionarlo con la actividad o el nombre de la misma. Es importante en este aspecto que se recuerde la obligación de inscribir el Sitio Web dentro del dominio .GOB.CL y GOV.CL
- URL Simple: la dirección de acceso de la primera página del sitio debe ser simple, de tal manera que sea fácil comunicarla. Idealmente no se debe mencionar el nombre del archivo de inicio (que corresponde a su página inicial o portada), si sólo con el nombre del dominio se puede acceder a ella.
- Chequear Disponibilidad: si el dominio es nuevo y recién se está levantando un Sitio Web en él, antes de lanzarlo se debe verificar que el sitio se ve desde diferentes lugares, para asegurar su disponibilidad para diferentes públicos.
- Respaldo Administrativo: muchas veces los sitios generarán necesidades de interacción entre los usuarios de un servicio y los funcionarios del mismo, lo cual podrá estar resuelto a través de comunicaciones generadas por medio del Sitio Web. Si este es el caso, antes del lanzamiento se debe incorporar en el flujo de trabajo.

### > Desarrollo de un Plan de Comunicaciones

Una vez que se han hecho las comprobaciones descritas en el título anterior, se está en condiciones técnicas de lanzar el sitio. Lo que viene a continuación es realizar la presentación e incorporar el Sitio Web a las actividades de difusión de la institución.
Para hacerlo, se debe contemplar que dicho plan debe tener componentes online y offline, tal como se indica a continuación:

- Actividades Online: dado que estamos presentando un medio de comunicación tecnológico, es importante cubrir adecuadamente esta área a través de las siguientes actividades:

Registrar el Sitio en Buscadores: es la actividad mediante la cual el Sitio Web comienza a formar parte de todos los directorios y buscadores de Internet. Si bien hay empresas que ofrecen esta actividad como un servicio, esto puede ser realizado por cualquier encargado del sitio, sin necesidad de tener conocimientos técnicos avanzados. A continuación cuatro lugares «clave» donde inscribir el sitio:

Google - http://www.google.com/intl/es/addurl.html
Yahoo - http://e1.docs.yahoo.com/info/sugerir.html
Dmoz.org - http://www.dmoz.org/World/Espa%f1ol/add.html
Estado.cl - http://www.estado.cl/inscribir.html

Generar Enlaces con Otros Sitios: varios de los algoritmos que usan los sitios de búsqueda y los directorios para incluir un sitio y mostrarlo en los primeros lugares de un directorio, revisan la cantidad de enlaces «desde sitios importantes» que llegan al sitio. Pero ello, el administrador del sitio debe propiciar los enlaces hacia el sitio y conseguir que siempre haya nuevos. Para ver cuántos llegan desde otros sitios web, se puede usar en www.google.com y www.altavista.com la instrucción «link».

Ejemplo - link:http://www.premioweb.cl/ para ver cuántos enlaces referencian el sitio del Premio Web.

Ofrecer Elementos de Fidelización: se refiere a ofrecerle a los usuarios motivos diversos para volver al sitio; puede ser un boletín de noticias en el que se envíen enlaces con contenidos de interés; fondos de pantalla; información útil de áreas relevantes, etc. Cada institución puede buscar dentro de sus contenidos, aquellos que son los más buscados por sus usuarios y ofrecerlos de manera atractiva para garantizar que siempre estén accediendo y regresando al sitio.

- Actividades Offline: se refiere a todas las actividades que se realizan fuera del ambiente Internet, con el fin de consolidar también en este mundo la «marca Internet» de la institución. Incluye las siguientes acciones:

  - Imagen Corporativa: la dirección del Sitio Web de la institución debe incorporarse en la imagen corporativa de la institución para que todo documento de la institución la incluya (desde informes internos, hasta tarjetas de visita). De esta manera, se logrará una unidad muy concreta en términos comunicacionales y se dejará diseminada esa dirección en todos lugares, permitiendo difundirlo y hacerlo conocido entre quienes deseen ponerse en contacto o revisar información provista por la institución.

- Actividades de Prensa: en el lanzamiento del Sitio Web se debe ofrecer un elemento tecnológico atractivo y no sólo confiar en que la aparición del Sitio Web sea la noticia. Por lo anterior, se debe definir cuál de las funcionalidades del sitio podrá ser destacada, para transformarla en la noticia que convoque a los medios.

### > El Sitio como Apoyo de la Institución

Una vez que el Sitio Web está operando normalmente, la tarea a realizar es incorporar el Sitio Web en el plan de comunicaciones, es decir, no sólo utilizar el web para hacer difusión, sino que también comenzar a incorporar la dirección web en cualquier comunicación que se haga y, más aún, hacer que el Sitio Web forme parte de las actividades.

Un ejemplo virtuoso de esto lo han dado muchas instituciones que insertan publicidad en los medios de comunicación para diferentes actividades y normalmente lo hacen en un aviso de pequeño formato, en el caso de prensa escrita, en el que indican que toda la información está disponible en el Sitio Web de la institución.

Esto genera dos efectos: Baja los costos de la publicación del aviso, Permite anunciar de manera simple y efectiva la existencia de un Sitio Web activo y útil.

## Métricas de Evaluación de Desempeño Internas y Externas

Una de las características interesantes que tiene un Sitio Web, es que ofrece información permanente de las actividades que están ocurriendo en su interior, lo que permite tener siempre cifras que ayudan a evaluar la gestión.

No obstante, para entender dichas cifras es necesario primero establecer ciertas definiciones, que tienen que ver con la terminología que se emplea en Internet para describir los fenómenos que se registran. En este sentido, hay tres conceptos importantes:

- Hits: se refiere a cada elemento que pasa desde el servidor del sitio al computador del usuario; una página puede tener muchos hits, ya que se cuenta uno por cada elemento que la compone. En términos reales, esta información no tiene valor.

- Páginas Vistas o Visitadas: se refiere a la cantidad de páginas que han sido solicitadas por los usuarios al Sitio Web; su uso más importante tiene que ver con la capacidad de establecer rankings internos en el sitio, respecto de los contenidos y funcionalidades más vistos y usados.

- Sesiones de Usuario: se refiere al número de personas que ha visitado el Sitio Web, independiente de cuántas páginas hayan visto o solicitado durante su visita; esta métrica es la única que puede entregar información real en torno a la audiencia de un sitio.

## > La Importancia del Archivo «log»

Con las definiciones anteriores ya especificadas, hay que indicar que el servidor web en que está alojado el sitio va generando un archivo de texto donde se registra línea por línea cada operación que realiza un usuario en el Sitio Web.

Los datos que incorpora este archivo pueden ser definidos según las necesidades que exista en el Sitio Web. Entre los más importantes se encuentran la fecha; hora; Número IP de origen; páginas visitadas; páginas desde las cuales llegaron al sitio; palabras que usaron el buscador y países de origen de los visitantes, entre otros.

Este archivo aumenta de tamaño a medida que hay más visitantes, a razón de 1 Mb por cada 10 mil hits; por lo anterior, es muy importante coordinar su extracción y análisis, con el fin de obtener información que ayude a la gestión y a entender mejor la forma en que los usuarios están empleando el sitio.

Para hacer el análisis del «log» del servidor existe una gran cantidad de herramientas. Para acceder a ellas se recomienda visitar http://www.uu.se/Software/Analyzers/Access-analyzers.html

Más información en:
W3C.org:
http://www.w3.org/TR/WD-logfile.html
Apache:
http://httpd.apache.org/docs/mod/mod_log_config.html
Microsoft IIS:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/log_logging.asp

## > Presencia del Sitio en Buscadores

Otra métrica relevante para saber el grado de efectividad que está teniendo el Sitio Web, consiste en revisar periódicamente su presencia a través de los buscadores de Internet más populares.

La recomendación es hacerlo a través de los buscadores más populares, como son Google, Altavista y Yahoo!, puesto que ellos son los que concentran el mayor tráfico y, por lo tanto, que el Sitio Web aparezca en ellos garantizará que los usuarios que estén buscando la institución la podrán encontrar.

Adicional a ellos, se recomienda que el sitio sea indexado en directorios como el DMOZ.org, puesto que se trata de un proyecto realizado a nivel mundial, cuyo contenido es ofrecido gratuitamente y actualmente es ocupado por los directorios más importantes. Por lo tanto, al estar en DMOZ.org se garantizará la aparición en los demás sitios.

Es importante que la búsqueda que se haga del sitio en los buscadores y directorios con el fin de ver cómo está indexado, se haga a través de dos criterios:

- Buscar por el Nombre: cuando se busca por el nombre de la institución, normalmente el Sitio Web debería aparecer en los primeros lugares de la primera página. Si no es así, hay un trabajo fuerte que hacer para mejorar los meta tags.

- Buscar por los Temas: cuando se busca por los temas que maneja la institución, es menos claro que su Sitio Web aparezca en los primeros lugares. Para mejorar ese posicionamiento es necesario refinar los meta tags y la forma de desplegar la información en el sitio, con el fin de ir aumentando la posibilidad de que siga ascendiendo en las listas de los buscadores.

### > Enlaces desde Otros Sitios

Es importante que el Sitio Web de la institución esté enlazado desde otros sitios web reconocidos de la Internet (buscadores, directorios, instituciones reconocidas), para mejorar su posición relativa y aparecer más arriba en las páginas de resultados de los sistemas de búsqueda de Internet.

Para conseguirlo, es muy relevante que como parte del plan de puesta en marcha del sitio, se asegure la existencia de los enlaces, especialmente desde y hacia sitios de la red de Gobierno (especialmente Estado.cl que es un directorio de sitios de Gobierno) y desde y hacia los Sitios Web sectoriales a los que pertenezca la institución.