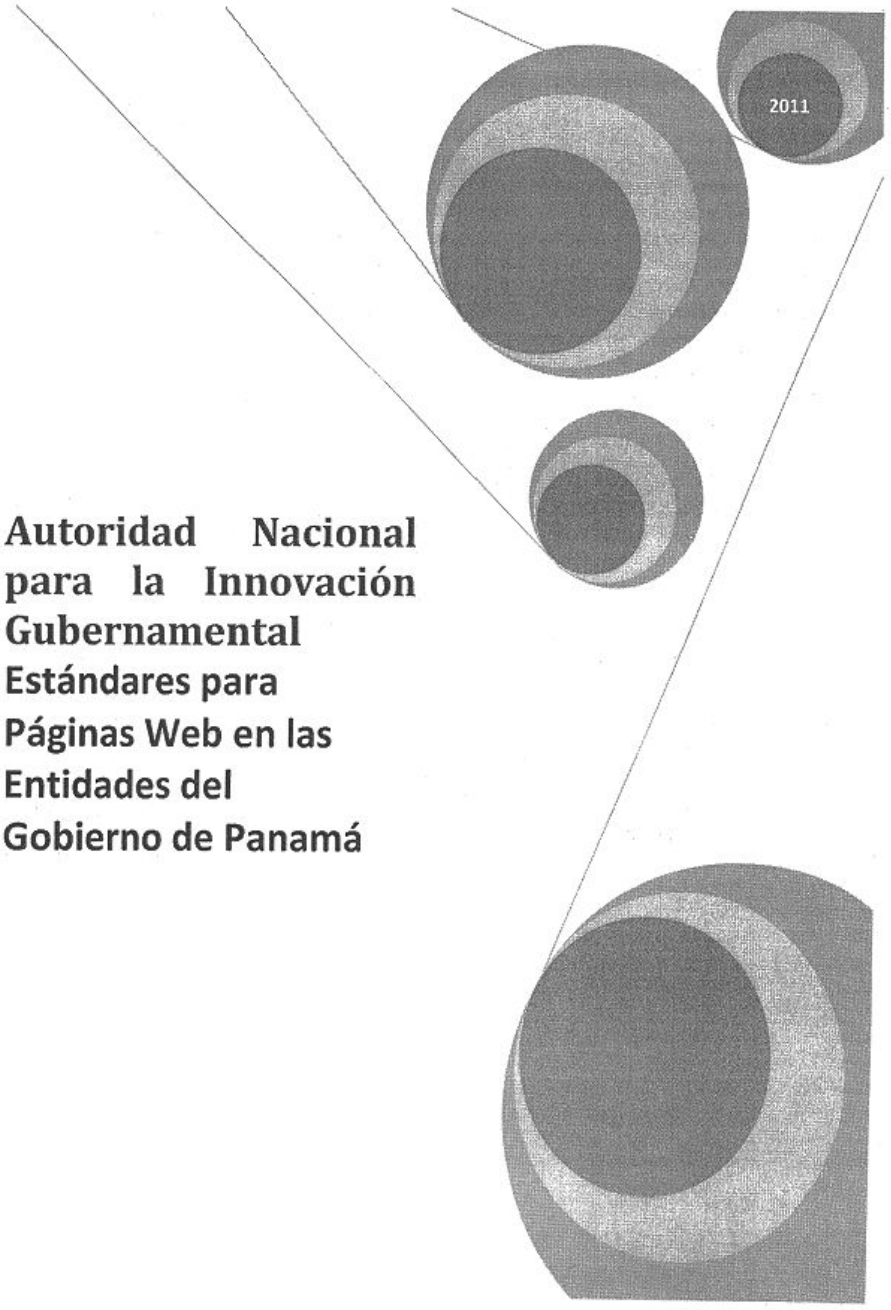


Autoridad Nacional para la Innovación Gubernamental

Estándares para Páginas Web en las Entidades del Gobierno de Panamá

República de Panamá

Autoridad Nacional para la Innovación Gubernamental

Autoridad Nacional para
la Innovación Gubernamental

"Estándares para Páginas Web en las Entidades del Gobierno de Panamá"

Febrero de 2011

Autoridad Nacional para la Innovación Gubernamental

Administración General

Ing. Eduardo Jaén
Administrador General

TABLA DE CONTENIDO

Autoridad Nacional para la Innovación Gubernamental	
TÍTULO: **Estándares para Páginas Web en las Entidades del Gobierno de Panamá.**	**Fecha de Vigencia:** **Fecha de Revisión:**
AUTORIZADO: Ing. EDUARDO JAÉN ADMINISTRADOR GENERAL	

A. Ámbito de Aplicación

La aplicación de los estándares descritos en el presente documento se originará en la Dirección, Unidad u Oficina de Informática o Cómputo de todas las entidades del Estado.

B. Base Legal[1]

Ley Nº 65 de 30 de Octubre de 2009, que crea la Autoridad Nacional para la Innovación Gubernamental

---

[1] "Copyright © 2010 World Wide Web Consortium, (Massachusetts Institute of Technology, European Research Consortium for Informatics and Mathematics, Keio University). All Rights Reserved. http://www.w3.org/Consortium/Legal/2002/copyright-documents-20021231".
"Copyright © 2010 Gobierno de Chile. All Rights Reserved. Licencia Creative Commons. **Guía para el Desarrollo de sitios Web – 1.0 y 2.0 del Gobierno de Chile.** http://www.guiaweb.gob.cl/

Decreto Ejecutivo Nº 205 de 9 de marzo de 2010, "Por La Cual Se Reglamenta La Ley No. 65 De 30 De Octubre De 2009, Que Crea La Autoridad Nacional Para La Innovación Gubernamental".

El contenido del presente documento corresponde a lineamientos de la W3C. Si el lector está interesado en consultar o ampliar las recomendaciones aquí contenidas, puede consultar las siguientes páginas web:

- http://www.w3.org/standards/webdesign/.
- http://www.w3.org/standards/webdesign/accessibility
- http://www.discapnet.es/web_accesible/wcag10/WAI-WEBCONTENT-19990505_es.html
- http://creativecommons.org/licenses/by-nc-sa/2.0/cl/
- http://www.w3.org/Consortium/Legal/IPR-FAQ-20000620#translate
- http://www.w3.org/Consortium/Legal/copyright-documents.html
- Guía para el Desarrollo de sitios Web – 1.0 y 2.0 del Gobierno de Chile. http://www.guiaweb.gob.cl/

C. Objetivo

1. Fructificar el potencial de la web, como medio de comunicación y divulgación de información, a fin de que sea una herramienta que impulse el desarrollo del Gobierno Electrónico en Panamá.

2. Ofrecer en los Sitios Web del Estado información funcional que pueda ser accedida por los ciudadanos, logrando así una amplia interoperabilidad de contenido, mediante la aplicación y cumplimiento de estándares internacionales y mejores prácticas de la industria.

D. Derecho de Autor

1. El texto y el material del presente documento (Estándares y Procedimiento para páginas web del Estado) son propiedad de la Autoridad Nacional para la Innovación Gubernamental.

E. Estándares para el contenido de las páginas web

E.1 Acerca de la Audiencia

1. Las entidades del Estado realizarán estudios, para determinar los usuarios hacia los cuales se orientará la información de la página web.

2. El administrador del Sitio Web desarrollará un permanente monitoreo de la actividad del Sitio Web, para conocer el comportamiento de los usuarios que lo visitan, a fin de introducir acciones que permitan adoptar las medidas preventivas y correctivas oportunas y enfrentar los problemas que genere su operación.

   A continuación se presentan algunas herramientas, sencillas y libres, para realizar revisiones a páginas WEB:

   - ***Site Explorer:*** permite inspeccionar determinados aspectos de una dirección URL. La característica de "Inlinks" muestra detalles acerca de las páginas web que tienen enlaces a la dirección URL específica que está explorando. Site Explorer le da algunas ideas de cómo la popularidad de un sitio web se basa en cuantas páginas web tienen enlaces hacia ella.

   - ***Compete***: herramienta analítica que le permite comparar las estadísticas de tráfico y las tendencias de hasta tres sitios web. Le da una estimación de cuántos visitantes únicos y páginas impresas obtiene un sitio Web, y la rapidez con que un sitio Web está creciendo en popularidad (llamado Velocidad de Crecimiento)

   - ***Quantcast*** sirve para medir el tráfico de los sitios, permite a los editores "Cuantificar" sus sitios web. Un proceso en el que se coloca una secuencia de comandos en sus páginas web, para que ellos puedan medir directamente las estadísticas de tráfico.

   - ***Alexa***: realiza un seguimiento de estadísticas de tráfico de sitios web y proporciona un rango numérico basado en los datos que recogen. Puede encontrar la cantidad de páginas visitadas de un sitio web (el % de los usuarios de Internet que han visitado el sitio web).

   - ***FeedBurner***: determina la popularidad de un sitio web dándole seguimiento a sus tendencias de envío de RSS. Si un sitio web utiliza

FeedBurner el proveedor líder de servicios RSS, puede utilizar *Feed Compare* para ver las tendencias de suscripción en el sitio web y comparar el crecimiento o disminución de suscriptores hasta para 4 fuentes al mismo tiempo.

- ***Popuri.us*** puede ayudar a determinar cuán popular es una dirección URL, basándose en los servicios web y las estadísticas, de herramientas como Alexa, Technorati, Delicious bookmark, número de suscriptores y más. Esta es una herramienta de una sola página que le da una descripción general de cuán popular es un sitio Web, incluso le da la opción de colocar un control en su sitio para mostrar su popularidad.

- ***Socialmeter:*** explora lo popular que es una página web en los principales sitios web sociales tales como Digg, Stumbleupon y Delicious. Le da una "puntuación de socialmeter" que es actualmente sólo una suma de los resultados encontrados (útil para comparar la popularidad de diferentes sitios web).

- ***TweetVolume:*** forma de monitorear la popularidad de un sitio web, viendo si las personas están hablando de él en Twitter, permite buscar palabras claves y frases (es decir, el nombre de un sitio web, URL, el nombre del autor, etc.) para ver cuántos tweets han mencionado los términos de búsqueda.

- ***Quarkbase:*** presenta un sinnúmero de información acerca de un sitio web, tiene la página "Social Popularity" que muestra información acerca de la popularidad de un sitio web, entre sitios de medios de comunicación social como Digg, Stumbleupon y Delicious.

- ***BlogPulse Profiles:*** que proporciona un ranking de blogs, con qué frecuencia es citado en otros blogs, y otras informaciones, como cuántos posts son publicados cada mes y que blogs son similares a él.

- ***Technorati:*** es el principal motor de búsqueda de blogs, permite ver el ranking de un blog particular, para medir su popularidad, determina el ranking de un blog, por el número de *reacciones* (enlaces que vayan al blog).

- ***Statbrain.com:*** indica cuántos visitantes recibe un sitio web por día.

- ***Cubestat:*** proporciona información acerca de las visitas diarias de un sitio web, calcula un valor monetario del sitio web (en dólares estadounidenses). El sitio web más caro, es el sitio más popular.

- ***dnScoop***: calcula el valor de un sitio web, basado en factores tales como vínculos que llevan al dominio, la popularidad del dominio, el page rank, tráfico y más.

- ***WebsiteOutlook:*** permite determinar la popularidad de un sitio web, según su valor estimado, visitas diarias e ingresos.

E.2 Estructura de la Información

La clave del éxito de las páginas web radica en la forma y tipo de información que se presenta en el sitio, para los visitantes.

Una página web es una ilustración que vemos por partes, por esta razón debemos cuidar cómo mostrar cada una de ellas.

Los estudios sobre la percepción, ayudan a entender cómo miramos y vemos las imágenes.

Investigadores han descubierto que nuestros ojos escanean las imágenes no en forma de barrido si no haciendo saltos y pausas breves que, de ninguna manera, son casuales.

Conociendo lo anterior, podemos observar ciertas particularidades.

1. Los ojos tienen una tendencia a explorar cuatro puntos de una forma sucesiva. Estos puntos se encuentran en las intersecciones de unas líneas que dividen la imagen en nueve partes: tres de largo por tres de ancho. (Anexo 1)

2. Los ojos tienden a permanecer en el cuadrante superior izquierdo de la imagen.

3. Los ojos se mueven siguiendo el sentido de las agujas del reloj. (Anexo 1)

4. Los ojos tienen tendencia a fijarse en los seres humanos; luego, en los objetos que se mueven (como las nubes y los coches), y finalmente en los objetos inmóviles. [2]

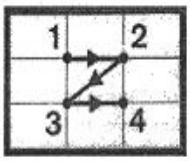


Ilustración 1 – Movimiento de los ojos

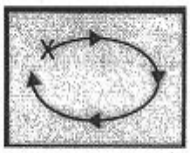


Ilustración 2 – Agujas del reloj

(Anexo No. 1)

E.2.1 Percepción de una Página web

1. Las páginas web son percibidas como una ilustración, definidos por el alto y ancho de nuestra pantalla. Se pueden identificar 2 tipos de página web: Páginas de Inicio y Páginas de Contenido.

2. Las Páginas de Inicio son importantes para la primera impresión, son orientadas como guía rápida, para la navegación dentro del sitio.

3. Las Páginas de Contenido son tan importantes como la página inicial, ya que aquí, es donde la página funciona. Los resultados que buscan los usuarios se dan en estas páginas.

4. Debemos tener especial atención a 3 secciones que podemos definir en una Página de Inicio:

    1. Parte Superior
    2. Parte Media
    3. Parte Inferior

---

[2] DUPONT, Luc:, 1001 Trucos Publicitarios. México: Lectorum, 2004.261p. ISBN 970-732-083-4

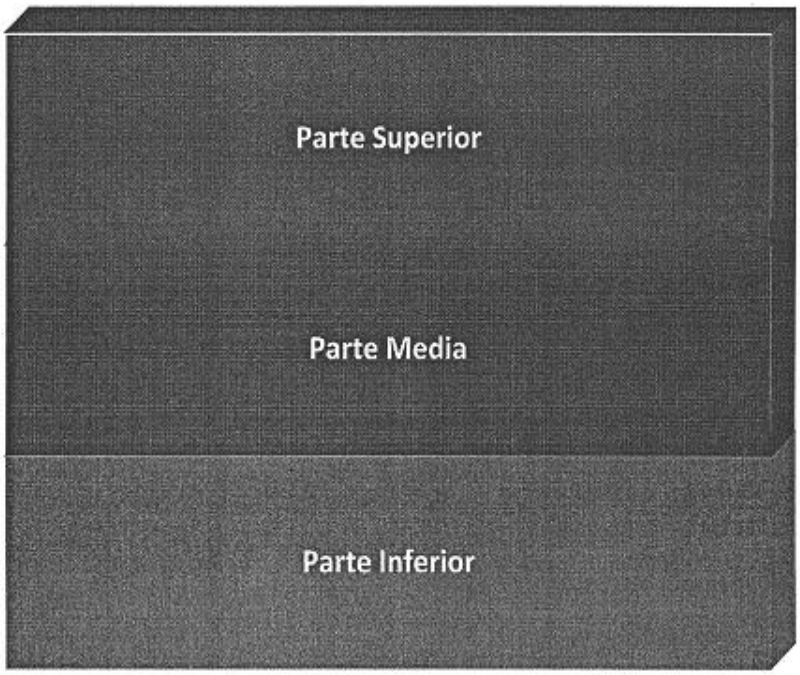


Ilustración 3 – Percepción de Páginas Web

Parte Superior

Es la sección que el 100% de los visitantes verá por primera vez y que en términos de SEO (Search Engine Optimization), se considera como un área importante para el aprovechamiento de anuncios web.

En esta sección se colocará el logo del Gobierno Nacional, el logo de la Entidad, el menú estandarizado y cierta información atractiva al usuario, acompañado de una fotografía, y un titular corto (slogan) .

La parte superior de una página web comprende los primeros 300px u 500px (de alto) aproximadamente.

Ilustración 4 – Percepción de Páginas Web

Parte Media

Depende de la longitud de la página web. Se colocan accesos a información importante para el usuario y de uso común en páginas que brindan información o asistencia pública.

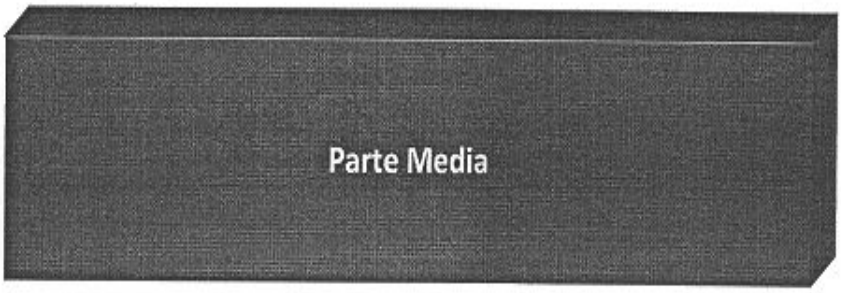


Ilustración 5 – Percepción de Páginas Web

Parte Inferior

Destinada a brindar información guía al usuario. Usualmente se coloca información de contacto, mapas de sitio, y enlaces a herramientas de uso interno. También se utiliza para colocar certificaciones y afiliaciones referentes a la entidad o al sitio web en sí.

Ilustración 6 – Percepción de Páginas Web

E.2.2 Estructura y Maquetado

Forma en que la información y el contenido de un sitio web son categorizados y estructurados.

1. Las páginas web tendrán un aspecto simple, conciso y fácil de Navegar.

2. Brindarán acceso a los contenidos de primer nivel y ofrecerán información acerca de la Entidad, destacando los trámites, novedades y noticias principales de la misma.

3. Para asegurar una similitud entre los diferentes diseños de las páginas Web gubernamentales, la estructura de la información (maquetado) de las páginas cumplirá con el esquema descrito a continuación (Figura 7: Maquetado).

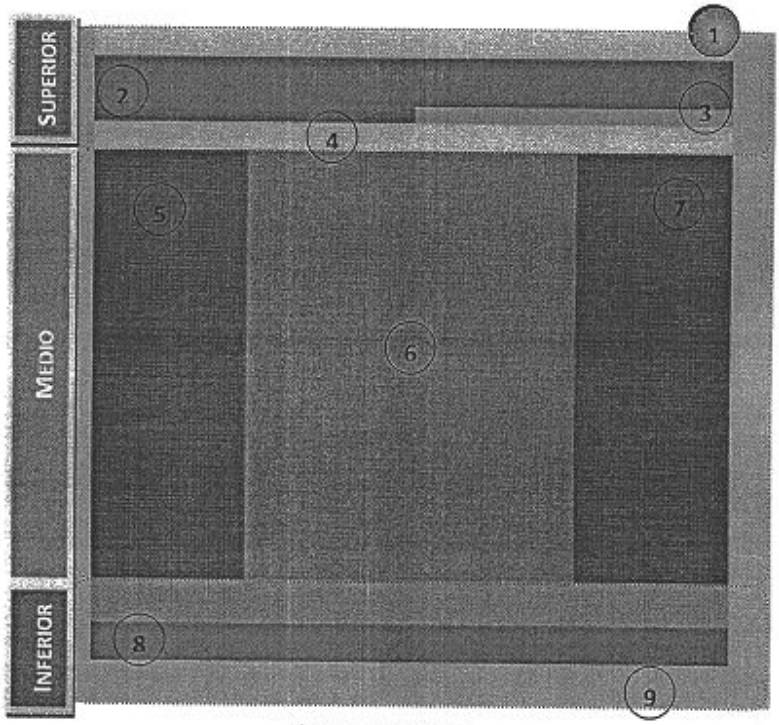


Figura 7: Maquetado

SECCIÓN SUPERIOR

SUPERIOR

1. Barra de opciones nivel superior
2. Barra de logos (*dintel / banner*)
3. Barra de opciones de accesibilidad
4. Barra de opciones / Menú Principal Horizontal Superior

SECCIÓN MEDIA

MEDIO

5. Barra de opciones de Navegación Principal
6. Sección de contenido principal
7. Barra de opciones secundarios (*opcional*)

SECCIÓN INFERIOR

8. Barra inferior de opciones
9. Barra de logos en tonos grises

4. Los portales no deberán incluir procesos que no estén listos a nivel operativo en la organización.

5. Evitar que en las páginas web se den pop-up, se exceptúan aquellas que por el tipo de programación deban utilizarlos.

6. **Las opciones de Inicio, Mapa de Sitio y Buscador**, se colocarán en la parte superior izquierda, antes del logo de Gobierno Nacional, en texto de **11px**, acompañadas cada una de un icono representativo a la acción (**16px por 16px**, aproximadamente) (Figura 8: Organización del Contenido – Sección Superior, punto A).

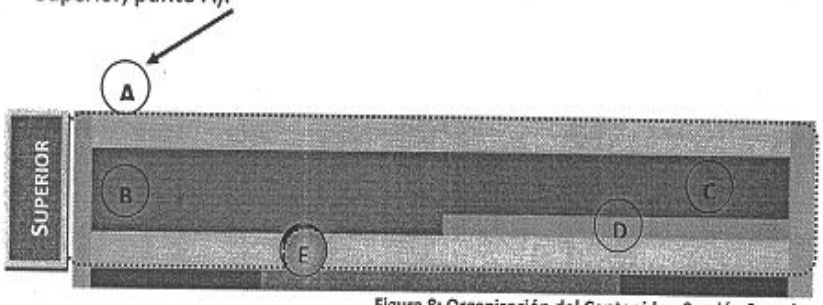


Figura 8: Organización del Contenido - Sección Superior

7. El mapa de sitio o árbol de contenido mostrará de manera práctica cuántas secciones tendrá el sitio en desarrollo y cuántos niveles habrá dentro de cada uno.

8. La sección dispuesta para colocar los logos del Gobierno Nacional, la Entidad y el menú de accesibilidad (Figura 9: Organización del Contenido – Sección Superior, punto B/C/D), no superará los **110px** de alto.

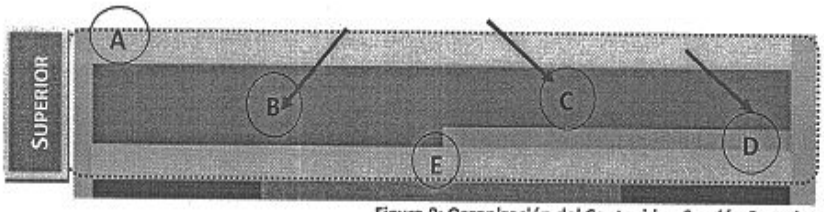


Figura 9: Organización del Contenido - Sección Superior

9. Todas las páginas web de las entidades del Estado, llevarán en la parte superior izquierda, el logo del Gobierno Nacional, (Figura 10: Organización del Contenido – Sección Superior, punto B) proporcionado por la Presidencia de la República, a través de la Autoridad Nacional para la Innovación Gubernamental. El logo tendrá un tamaño no mayor de **245px** de ancho, aproximadamente (sin que el logo se distorsione) y enlazará a la página web de la Presidencia. Nada deberá cubrir el logo del Gobierno Nacional.

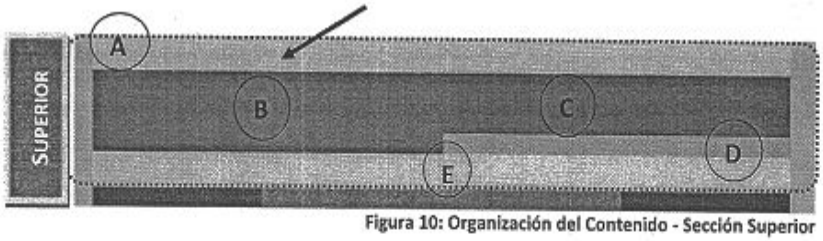


Figura 10: Organización del Contenido - Sección Superior

10. Como fondo de la Sección Superior, (Figura 11: Organización del Contenido – Sección Superior,) se podrá colocar fotos, diseños, dibujos, lo que la entidad crea conveniente, siempre y cuando los logos del Gobierno Nacional y de la Entidad queden legibles.

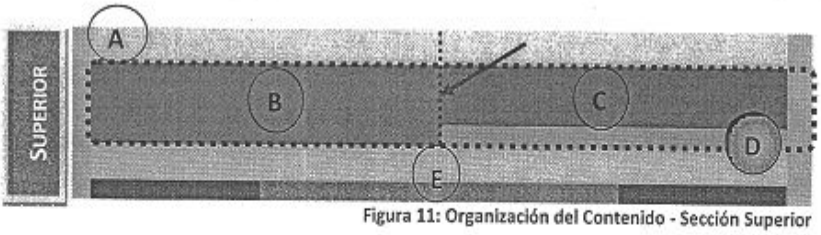


Figura 11: Organización del Contenido - Sección Superior

11. La entidad podrá omitir el uso del logo Gobierno Nacional, previa autorización escrita de la Autoridad Nacional para la Innovación Gubernamental.

12. El logo de la entidad se colocará en la parte superior derecha (Figura 12: Organización del Contenido – Sección Superior, punto C). El logo tendrá un tamaño no mayor al **40%** del ancho del cuerpo de la página. Nada deberá cubrir el logo de la Entidad.

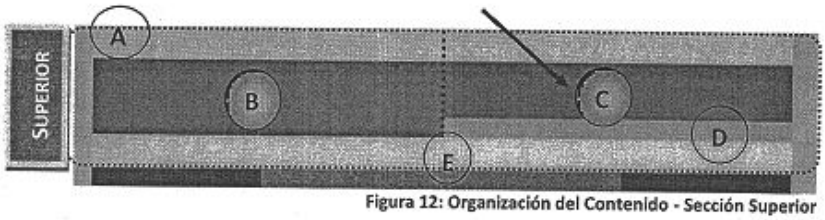


Figura 12: Organización del Contenido - Sección Superior

13. En la parte superior derecha, sobre la barra de menú horizontal (Figura 13: Organización del Contenido – Sección Superior, punto D), se colocarán las opciones de accesibilidad, cambio de contraste, cambio de tamaño de letra y los íconos de español – inglés, en una sección de **25px** de alto, en texto de **11px**, para darle a los usuarios con discapacidades visuales la accesibilidad al sitio web.

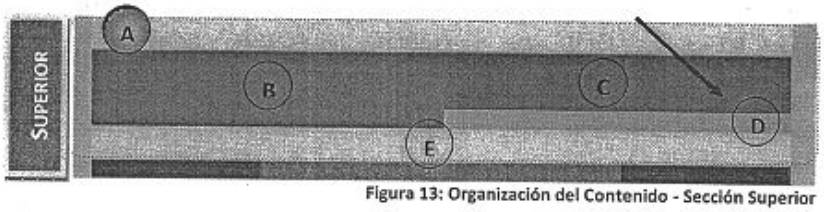


Figura 13: Organización del Contenido - Sección Superior

14. La barra de menú horizontal superior (Figura 14: Organización del Contenido – Sección Superior, **punto E**) estará compuesta de las siguientes opciones: ***¿Quiénes somos?***, ***Contáctenos*** y el logo con el enlace al ***311***, todos en texto no menor a **12px**, ni mayor a **14px**. Esta barra estará sujeta al 100% del ancho del cuerpo de la página y **35px** de alto.

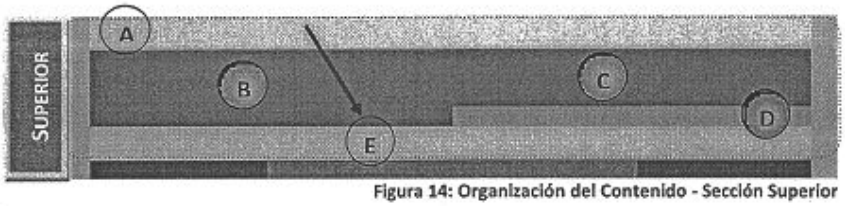


Figura 14: Organización del Contenido - Sección Superior

15. La barra de menú lateral izquierda (Figura 15: Organización del Contenido – Sección Media, **punto A)** estará compuesta de las siguientes opciones: ***Sobre la Entidad, Trámites, Información Financiera, Recursos Humanos, Memorias, Transparencia, Contáctenos*** y enlace al ***311*** todos en texto no mayor a los **13px.**

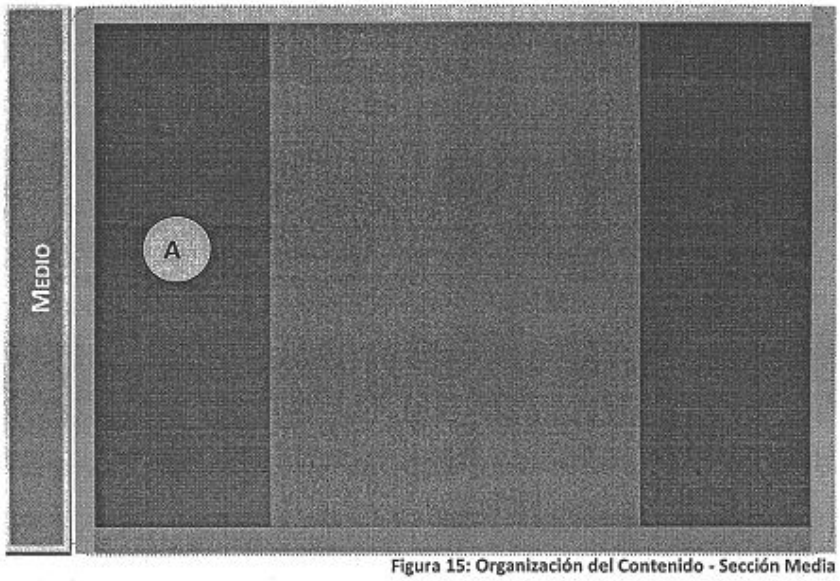


Figura 15: Organización del Contenido - Sección Media

16. Las entidades podrán colocar en su página web (Figura 16: Organización del Contenido –Sección Media, punto B), encuestas a ciudadanos con sus respectivos resultados o cualquier información relevante de la entidad.

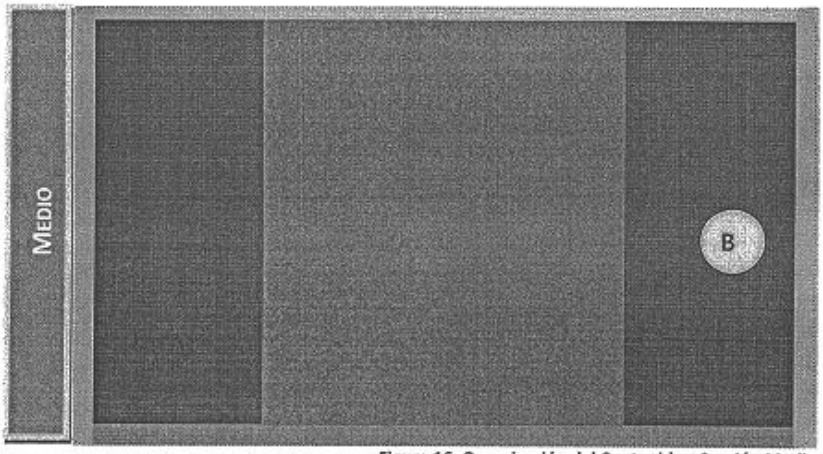


Figura 16: Organización del Contenido - Sección Media

17. Las entidades podrán colocar en su página web (Figura 17: Organización del Contenido –Sección Media, punto C), cualquier información que la entidad crea conveniente publicar).

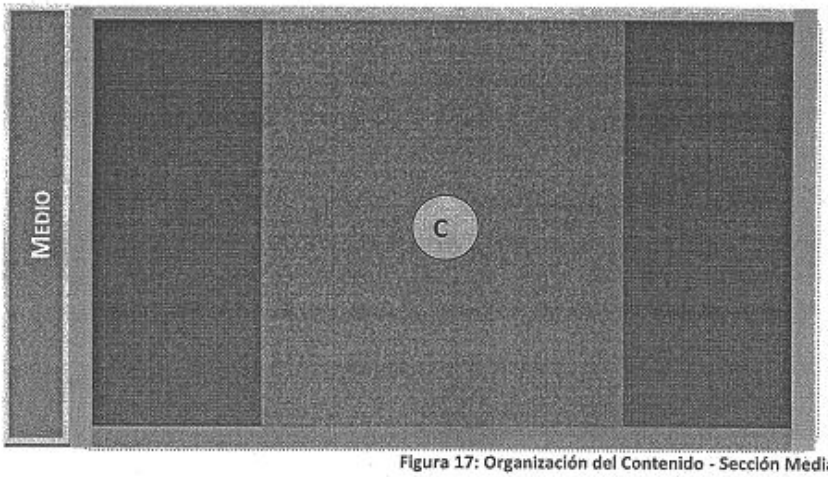


Figura 17: Organización del Contenido - Sección Media

18. El ítem **"Sobre la Entidad"**[3] de la barra de menú lateral izquierda, contendrá a manera de árbol de opciones (Figura 15: Menú Principal – Organización del Contenido – Sección Media, punto A, Sobre la Entidad) la siguiente información: **Historia, Visión, Misión, Políticas o Valores, Organigrama, Régimen Jurídico, Junta Directiva, Ministros/Directores/Administradores, Equipo de Trabajo.** (Esta información puede variar de acuerdo a la Entidad).

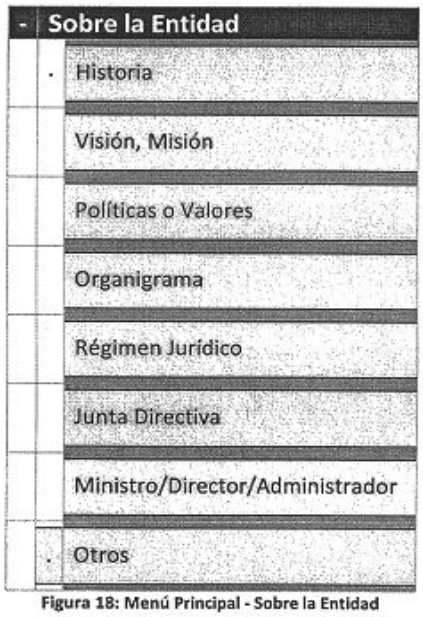


Figura 18: Menú Principal - Sobre la Entidad

- **Historia:** breve redacción del origen y desarrollo de la entidad.
- **Visión:** motivo propósito, fin o razón de ser de la entidad.
- **Misión:** camino al cual se dirige la entidad a largo plazo.

---

[3] Ley 6 de 22 de enero de 2002, "Que Dicta Normas Para La Transparencia En La Gestión Pública, Establece La acción de Hábeas Data Y Dicta Otras Disposiciones.
Carta Iberoamericana de Gobierno Electrónico. Adoptada por la XVII Cumbre Iberoamericana de Jefes de Estado y de Gobierno Santiago de Chile, 10 de noviembre de 2007. (Resolución No. 18 de la declaración de Santiago).

- **Políticas:** Normas o reglas generales que se convierten en pautas de comportamiento no negociables y de obligatorio cumplimiento, cuyo propósito es reducir la incertidumbre y canalizar todos los esfuerzos hacia la realización del objeto de la entidad.
- **Valores:** reglas o pautas mediante el cual una entidad exhorta a sus colaboradores a tener comportamientos consistentes con el sentido de existencia del mismo (orden, seguridad y desarrollo).
- **Organigrama:** representación gráfica de la estructura, jerarquía e interrelación de las áreas que componen a la entidad.
- **Régimen Jurídico** normas jurídicas que establecen la forma de organización y áreas de competencia de la Administración Pública.
- **Junta Directiva:** funciones generales de la junta directiva. Integrantes (fotos) con sus hojas de vida resumida (opcional).
- **Ministro, Director o Administrador General:** mensaje de la autoridad nominadora, con hoja de vida resumida (foto opcional).
- **Equipo de Trabajo:** listado con el nombre de todos los directores y subdirectores que forman parte de la organización.
- **Otros:** cualquier otra información relevante que la entidad considere oportuno publicar.

19. El ítem **"Trámites"** de la barra de menú lateral izquierda, contendrá como mínimo, a manera de árbol de opciones (Figura 15: Menú Principal – Organización del Contenido – Sección Media, punto A, Trámites) la siguiente información: **Trámites en línea, Trámites en sitio.**

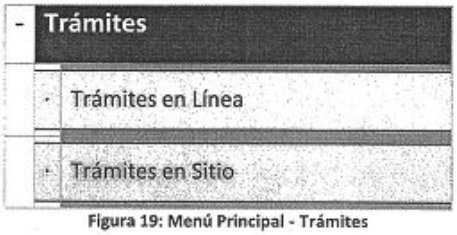


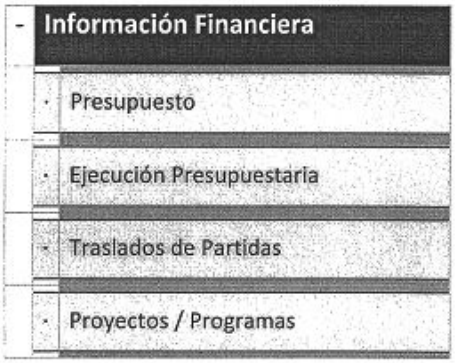
Figura 19: Menú Principal - Trámites

- **Trámites en Línea:** colocar todos los trámites, consulta, etc., que puedan realizar las personas vía Internet, con sus respectivas guías del usuario. En

esta sección se puede colocar el enlace de Panamá Compra, Panamá Tramita u otros.

- **Trámites en Sitio:** colocar todos los trámites o servicios que brinda la entidad en sitio. La información deberá detallar el nombre del servicio o trámite, lugar donde se brinda, personas responsables del proceso, teléfono, correo electrónico, formularios con instructivo, que se utilizan en los diferentes procesos, tiempo mínimo y máximo aproximado que toma el trámite, etc. Esta información podrá presentarse en cuadros, gráficas o en la modalidad que la entidad lo considere presentar. [4]

20. El ítem de **"Información Financiera"** de la barra de menú lateral izquierda contendrá, a manera de árbol de opciones (Figura 15: Menú Principal – Organización del Contenido – Sección Media, punto A, Información Financiera) las siguientes opciones: **Presupuesto, Ejecución Presupuestaria, Traslados de Partidas, Proyectos y Programas que Desarrolla la Entidad, Nivel de Ejecución, Oficina Responsable o Persona Responsable de Proyectos, Rendición de Cuentas, Informe de Viajes al extranjero, y otros.**[5] (Esta información puede variar de acuerdo a la Entidad).



[4] Ley 6 de 22 de enero de 2002, "Que Dicta Normas Para La Transparencia En La Gestión Pública, Establece La acción de Hábeas Data Y Dicta Otras Disposiciones.
Carta Iberoamericana de Gobierno Electrónico. Adoptada por la XVII Cumbre Iberoamericana de Jefes de Estado y de Gobierno Santiago de Chile, 10 de noviembre de 2007. (Resolución No. 18 de la declaración de Santiago).

[5] Ibídem.

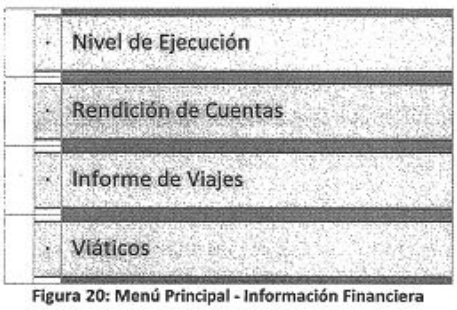


Figura 20: Menú Principal - Información Financiera

- **Presupuesto:** cálculo anual anticipado de los ingresos y gastos de la entidad durante un período. Plan de acción dirigido a cumplir metas, expresada en valores y términos financieros que, deben cumplirse en determinado tiempo y bajo ciertas condiciones.
- **Ejecución Presupuestaria:** indicador que señala el nivel porcentual en la utilización de los recursos humanos, materiales y financieros asignados en el presupuesto con el propósito de obtener los bienes y servicios en la cantidad, calidad y oportunidad previstos en el mismo.
- **Traslado de Partidas:** transferencia de recursos en las Partidas del Presupuesto, con saldo disponible de fondos sin utilizar, a otras que se han quedado con fondos insuficientes o que no tengan asignación presupuestaria.[6]
- **Proyectos / Programa:** listado de los proyectos programados, ya sea a largo mediano o corto plazo, con su nivel de ejecución, persona o entidad responsable del mismo.
- **Nivel de Ejecución:** porcentaje de ejecución de los proyectos / programas
- **Rendición de Cuentas:** informe proactivo a través del cual los agentes públicos informan y justifican sus planes, acciones y resultados.
- **Informe de Viajes:** Informe detallado de los viajes al exterior del país, realizados por el personal de la entidad.
- **Viáticos:** Informe detallado de los viáticos, utilizados por el personal de la entidad.

---

[6] Ley 63 de 2009 Que Dicta el Presupuesto General del Estado para la Vigencia Fiscal de 2010.

21. El ítem de **"Recursos Humanos"** de la barra de menú lateral izquierda contendrá, a manera de árbol de opciones (Figura 15: Menú Principal – Organización del Contenido – Sección Media, punto A, Recursos Humanos) las siguientes opciones: **Planilla** (o el link del portal de la Defensoría del Pueblo), **Vacantes, Contratación de Funcionarios, Gastos de Representación, y cualquier otra información relacionada con el recurso humano de la Entidad.** (Esta información puede variar de acuerdo a la Entidad).

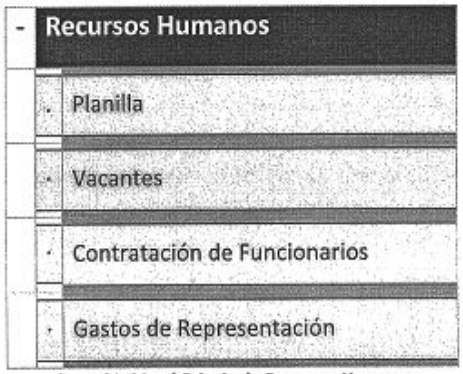


Figura 21: Menú Principal - Recursos Humanos

- **Planilla:** listado del personal de la Entidad con su respectivo salario, gasto de representación y otros.
- **Vacantes:** listado de las vacantes disponibles en la Entidad con sus requisitos mínimos.
- **Contratación de Funcionarios:** listado de los funcionarios que hayan contratado en un periodo determinado por la Entidad.
- **Gastos de Representación:** listado de los gastos de representación que tienen los funcionarios de la Entidad, según el cargo.

22. El ítem de **"Transparencia"** de la barra de menú lateral izquierda contendrá, a manera de árbol de opciones (Figura 15: Menú Principal – Organización del Contenido – Sección Media, punto A, Transparencia) las siguientes opciones: **Actos Públicos** (link con el portal de Panamá Compra), **Estadísticas, Procedimientos, Formularios, Plan Estratégico, Solicitud de Información Presentadas, Solicitudes Resueltas y Negadas, Actos Administrativos**

Sometidos a Participación Ciudadana. (Esta información puede variar de acuerdo a la Entidad).

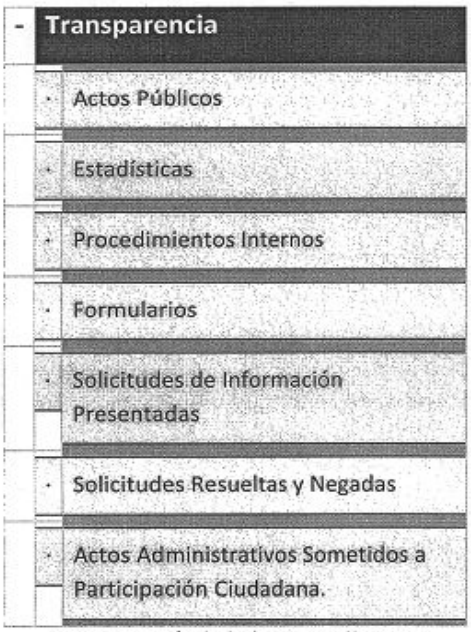


Figura 22: Menú Principal - Recursos Humanos

- **Actos Públicos:** listado de los actos públicos realizados por la entidad o el link del portal de Panamá Compra.
- **Estadísticas:** estadísticas relevantes que realice la Entidad.
- **Procedimientos:** listado de los procedimientos documentados por la entidad.
- **Formularios:** listado de formularios que utiliza la entidad.
- **Solicitudes de Información Presentadas:** estadísticas de la información solicitada a la entidad por los ciudadanos.
- **Solicitudes Resueltas o Negadas:** cuadro sobre las solicitudes resueltas y negadas por la Entidad a los ciudadanos.
- **Actos Administrativos Sometidos a Participación Ciudadana.**

23. Todas las entidades colocarán en su página web la hora oficial de la misma, sincronizados al reloj atómico del CENAMED AID, con su respectivo enlace (link).

Nota: Toda la información establecida en la Ley 6 de 22 de enero de 2002 "Que Dicta Normas Para La Transparencia En La Gestión Pública, Establece La Acción de Hábeas Data Y Dicta Otras Disposiciones.", será se estricto cumplimiento para el presente estándar, la información institucional adicional, quedará a criterio de cada entidad.

E.3 Accesibilidad e Interoperabilidad

E.3.1 Interoperabilidad del contenido

1. Las páginas web se desarrollarán de manera tal que garanticen la disponibilidad y accesibilidad de la información, así como la privacidad a los derechos de los titulares de datos personales (Políticas de Privacidad), asegurando la interoperabilidad de los contenidos, así como los servicios ofrecidos por las entidades del Estado.

2. Los sitios web deben ser accesibles desde diferentes navegadores (browser[7] o programa para ver sitios web), teniendo al menos uno de ellos como uso gratuito y disponible desde el propio sitio web.

- http://www.opera.com/download/
- http://avant-browser.uptodown.com/
- http://www.microsoft.com/spain/windows/internet-explorer/
- http://netscape-esp.uptodown.com/
- http://www.apple.com/es/safari/download/
- http://finebrowser.softonic.com/

[7] http://browsers.evolt.org/ ó http://www.w3.org/Amaya/User/BinDist.html

Figura 23 - Browser

E.3.2 Plugins

1. Las entidades del Estado que empleen archivos, que requieran de programas especiales o plugins, deberán colocar dichos programas a disposición de los usuarios, ofreciendo el enlace (link) a donde puedan descargar los mismos.

Figura 24 - Plugins

E.3.3 Velocidad de descarga

1. Las páginas web no superarán los 100kb como peso ideal o no superar el umbral de 4 segundos de despliegue (en condiciones de bajos recursos tecnológicos).

   a. **Nota:** El rendimiento de una conexión a Internet nunca es del 100%. Deberán tomar en cuenta que en estos tipos de conexiones (Módem analógico, RDSI, ADSL) utilizan diversos protocolos (PPP, TCP/IP) que ocupan ancho de banda (entre un 2% y un 20% del total, según el tipo de conexión y protocolo utilizado), con lo que se reduce el ancho de banda útil para la descarga de datos. El resultado que se muestra en las pruebas de velocidad de conexión existentes (por ejemplo en

http://testacceso.es.tdatacenter.com/) corresponde al ancho de banda útil, esto es, equivale a la velocidad de transferencia de información, y no a la velocidad de acceso.

b. Adicionalmente, existen otros factores que no pueden ser medidos y que contribuyen a reducir la velocidad de la conexión, como son la congestión en la red, interferencias electromagnéticas, etc., que también afectan al resultado final.[8]

2. Evitar el uso de imágenes muy pesadas como fondos o «backgrounds» de las páginas web, ya que agrega un peso excesivo a los sitios, afectando el tiempo de descarga y acceso a la información.

E.4 Codificación de los Sitios Web

1. Las páginas Web deberán cumplir con las normas establecidas en los estándares mundiales en términos de uso de código y accesibilidad como Estándares Mundiales de Calidad de Desarrollo WEB WAI, XHTML, Maquetado con CSS o XML.

2. El código de despliegue del sitio web será HTML (proporciona la estructura de la página WEB) o XML (para transmisión de datos). y cumplir con los estándares HTML 4.01 o XHTML (Extensible Hyper Text Markup Language).[9]

3. Los documentos web estarán compuestos de tres partes que son:
   a. **Declaración del tipo de documento estándar a usar**: corresponde a las primeras líneas que debe tener toda página web, en ella se indica el tipo de documento de que se trata y el estándar que regirá su contenido. Los elementos que son relevantes son los siguientes:
      i. Tipo de documento (`doctype`)
      ii. Referencia del documento (`dtd`)

---

[8] Copyright © 2010 Gobierno de Chile. All Rights Reserved. Creative Commons Compatible License. Guía para el Desarrollo de Páginas Web 2.0 – Chile.

[9] Copyright © 2010 World Wide Web Consortium, (Massachusetts Institute of Technology, European Research Consortium for Informatics and Mathematics, Keio University). All Rights Reserved. http://www.w3.org/Consortium/Legal/2002/copyright-documents-20021231.

iii. Etiqueta (`<html>`)

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="es">
```

b. **Encabezado de la página**: reservadas para crear el encabezado, que se despliega entre las etiquetas **<head>** y **</head>**. Dentro de ellas se ubican los elementos mediante los cuales, se describe el contenido de la página web, a estos elementos se les llama "meta datos". Hay cuatro tipos, que son:

i. Título (**<title>**)
ii. Metadato (**<meta>**)
iii. Enlaces externos (**<link href="styles/main.css" rel="stylesheet" type="text/css" />**)
iv. Scripts (**<script type="text/javascript" src="scripts/uifunctions.js">**)

```
<HEAD>
<meta name="tipo_contenido" content="text/html;" http-
equiv="content-type" charset="utf-8">
</HEAD>
```

c. **Cuerpo de la Página**: zona de contenido propiamente tal la que se despliega entre las etiquetas **<body>** y **</body>**

```
<body>
...
</body>
```

4. Las páginas web serán diagramadas utilizando hojas de cascada de estilo (CSS), separando el contenido, la estructura y la presentación de los primeros. Permite adaptar la presentación a diferentes tipos de dispositivos, como pantallas grandes, pantallas pequeñas o impresoras.

5. El conjunto de caracteres del sitio web será UTF-8 (Unicode Transformation Format -8).

6. El sitio web debe degradarse "aceptablemente" es decir, que sus contenidos se puedan entender adecuadamente, sin la presentación gráfica habitual. Existen varias herramientas que facilitan la revisión de este elemento, un ejemplo de ellas es FireFox[10]:

   a. **Firebug:** software que ocupa la parte inferior de la pantalla y va mostrando el código fuente a medida que se desplaza el cursor sobre el sitio web que se revisa; ofrece mucha información acerca de su código fuente.
   b. **CSS Viewer:** comando que permite ver el estilo utilizado en la página que se revisa, a medida que se desplaza el mouse sobre la página web.
   d. **Web Developer:** barra de herramientas con gran cantidad de opciones para revisar el sitio web.
   e. **Mozilla Accessibility Extension:** barra de herramientas con todas las opciones necesarias para revisar la accesibilidad del sitio web.

Figura 25: Con presentación gráfica habitual

[10] https://addons.mozilla.org

Figura 26 Sin presentación gráfica

Figura 27: Barra de Web Developer de FireFox

E.5 Pautas de Accesibilidad (WCAG)

La W3C ha desarrollado la **Pautas de Accesibilidad al Contenido en la Web (WCAG)**, cuya función principal es guiar el diseño de páginas Web hacia un esquema accesible, reduciendo de esta forma barreras a la información. WCAG consiste en 14 pautas, que proporcionan soluciones de diseño y que utilizan como ejemplo situaciones comunes en las que el diseño de una página, puede producir problemas de acceso a la información. Las Pautas contienen además una serie de puntos de verificación que ayudan a detectar posibles errores.

Cada punto de verificación está asignado a uno de los tres niveles de prioridad establecidos por las pautas.

Prioridad 1: son aquellos puntos que un desarrollador Web tiene que cumplir ya que, de otra manera, ciertos grupos de usuarios **no podrían acceder** a la información del sitio Web.

Prioridad 2: son aquellos puntos que un desarrollador Web debería cumplir ya que, si no fuese así, sería **muy difícil acceder** a la información para ciertos grupos de usuarios.

Prioridad 3: son aquellos puntos que un desarrollador Web debería cumplir ya que, de otra forma, algunos usuarios experimentarían **ciertas dificultades para acceder** a la información.

En función a estos puntos de verificación se establecen los niveles de conformidad:

Nivel de Conformidad "A": todos los puntos de verificación de prioridad 1 se satisfacen.
Nivel de Conformidad "Doble A": todos los puntos de verificación de prioridad 1 y 2 se satisfacen.
Nivel de Conformidad "Triple A": todos los puntos de verificación de prioridad 1,2 y 3 se satisfacen.

Figura 28: – Niveles de Prioridad y Conformidad

Pauta 1: Proporcione alternativas equivalentes para el contenido visual y auditivo.

1.1 Proporcione un texto equivalente para todo elemento no textual (Por ejemplo, a través de "alt", "longdesc" o en el contenido del elemento). *Esto incluye:* imágenes, representaciones gráficas del texto, mapas de imagen, animaciones (Por ejemplo, GIFs animados), "applets" y objetos programados, "ascii art", marcos, scripts, imágenes usadas como viñetas en las listas, espaciadores, botones gráficos, sonidos (ejecutados con o sin interacción del usuario), archivos exclusivamente auditivos, banda sonora del vídeo.

[Prioridad 1]
Por ejemplo, en HTML:

Utilice "alt" para los elementos IMG, INPUT y APPLET o proporcione texto equivalente en el contenido de los elementos OBJECT Y APPLET.
Para contenidos complejos (Por ejemplo, las gráficas) en los que el texto del atributo "alt" no es suficiente, proporcione una descripción adicional usando, por ejemplo "longdesc" con IMG o FRAME, un enlace dentro de un elemento OBJECT o un enlace descriptivo en el documento.
Para mapas de imagen, use el atributo "alt" con AREA o el elemento MAP con elementos A (y otro texto) como contenido.

Consultar también punto de verificación 9.1 y punto de verificación 13.10.
Técnicas para el punto de verificación 1.1

1.2 Proporcione vínculos redundantes en formato texto para cada zona activa de un mapa de imagen del servidor.

[Prioridad 1]
Consultar también punto de verificación 1.5 y punto de verificación 9.1.
Técnicas para el punto de verificación 1.2

1.3 Proporcione una descripción auditiva de la información importante de la pista visual de una presentación multimedia.

[Prioridad 1]
Sincronice la *descripción auditiva* con la banda sonora como en el punto de verificación 8.4.
Técnicas para el punto de verificación 1.3
Consultar también punto de verificación 8.1 para información sobre textos equivalentes para el contenido visual.

1.4 Para toda presentación multimedia tempo dependiente (Por ejemplo, una película o animación) sincronice alternativas equivalentes (Por ejemplo, subtítulos o descripciones de la banda visual) con la presentación.

[Prioridad 1]
Técnicas para el punto de verificación 1.4

1.5 Proporcione vínculos de texto redundantes para cada zona activa del mapa de imagen de cliente.

[Prioridad 3]
Consultar también punto de verificación 1.2 y punto de verificación 9.1.
Técnicas para el punto de verificación 1.5

Pauta 2: No se base sólo en el color asegúrese de que los textos y gráficos son comprensibles cuando se vean sin color.

2.1 Asegúrese de que toda la información transmitida a través de los colores también esté disponible sin color, por ejemplo mediante el contexto o por marcadores.

[Prioridad 1]
Técnicas para el punto de verificación 2.1

2.2 Asegúrese de que las combinaciones de los colores de fondo y primer plano tengan suficiente contraste para que sean percibidas por personas con deficiencias de percepción de color o en pantallas en blanco y negro.

[Prioridad 2 para las imágenes. Prioridad 3 para texto].
Técnicas para el punto de verificación 2.2

Pauta 3: Utilice marcadores y hojas de estilo y hágalo apropiadamente.

3.1 Cuando exista un marcador apropiado, use marcadores en vez de imágenes para transmitir la información.

[Prioridad 2]
Por ejemplo, utilice MathML para marcar ecuaciones matemáticas y *hojas de estilo* para el formato de texto y el control de la maquetación. Igualmente, evite la utilización de imágenes para representar textos. Utilice en su lugar texto y hojas de estilo.

Consultar también pauta 6 y pauta 11. Técnicas para el punto de verificación 3.1

3.2 Cree documentos que estén validados por las gramáticas formales publicadas.

[Prioridad 2]
Por ejemplo, incluya una declaración del tipo de documento, al comienzo del mismo, que haga referencia a una DTD publicada (Por ejemplo, la DTD HTML 4.0 estricto). Técnicas para el punto de verificación 3.2.

3.3 Utilice hojas de estilo para controlar la maquetación y la presentación.

[Prioridad 2]
Por ejemplo, utilice la propiedad 'font' de CSS en lugar del elemento HTML FONT para controlar el estilo de las fuentes. Técnicas para el punto de verificación 3.3.

3.4 Utilice unidades relativas en lugar de absolutas al especificar los valores en los atributos de los marcadores de lenguaje y en los valores de las propiedades de las hojas de estilo.

[Prioridad 2]
Por ejemplo, en CSS, utilice 'em' o medidas porcentuales, en vez de 'pt' (puntos) o 'cm' (centímetros), que son unidades absolutas. Si se usan unidades absolutas, valide que el contenido presentado es utilizable. (Consultar la sección de validación). Técnicas para el punto de verificación 3.4.

3.5 Utilice elementos de encabezado para transmitir la estructura lógica y utilícelos de acuerdo con la especificación.

[Prioridad 2]
Por ejemplo, en HTML, utilice H2 para indicar una subsección de H1. No utilice encabezados para hacer efectos de fuente. Técnicas para el punto de verificación 3.5.

3.6 Marque correctamente las listas y los ítems de las listas.

[Prioridad 2]

Por ejemplo, en HTML, anide los elementos de listas OL, UL y DL adecuadamente. Técnicas para el punto de verificación 3.6.

3.7 Marque las citas. No utilice el marcador de citas para efectos de formato tales como sangrías.

[Prioridad 2]
Por ejemplo en HTML, utilice los elementos Q y BLOCKQUOTE para marcar citas cortas y largas, respectivamente. Técnicas para el punto de verificación 3.7.

Pauta 4: Identifique el idioma usado. Use marcadores que faciliten la pronunciación o interpretación de texto abreviado o extranjero.

4.1 Identifique claramente los cambios en el idioma del texto del documento y en cualquier *texto equivalente* (Por ejemplo, leyendas).

[Prioridad 1]
Por ejemplo en HTML, utilice el atributo "lang". En XML, utilice "xml:lang". Técnicas para el punto de verificación 4.1.

4.2 Especifique la expansión de cada abreviatura o acrónimo cuando aparezcan por primera vez en el documento.

[Prioridad 3]
Por ejemplo, en HTML, use el atributo "title" de los elementos "ABBR" y "ACRONYM". Proporcionar la expansión en el cuerpo principal del documento también ayuda a la usabilidad del documento. Técnicas para el punto de verificación 4.2.

4.3 Identifique el idioma principal de un documento.

[Prioridad 3]
Por ejemplo, en HTML, coloque el atributo "lang" en el elemento HTML. En XML, utilice "xml:lang". Los operadores de servidores podrían configurar sus servidores para aprovechar los mecanismos de transferencia del contenido del protocolo HTTP ([RFC2068], sección 14.13), de forma que los clientes puedan

recibir automáticamente los documentos en el idioma seleccionado. Técnicas para el punto de verificación 4.3.

Pauta 5: Cree tablas que se transformen correctamente.

5.1 En las tablas de datos, identifique los encabezamientos de fila y columna.

[Prioridad 1]
Por ejemplo, en HTML, use TD para identificar las celdas de datos y TH para los encabezamientos. Técnicas para el punto de verificación 5.1.

5.2 Para las tablas de datos que tienen dos o más niveles lógicos de encabezamientos de fila o columna, utilice marcadores para asociar las celdas de encabezamiento y las celdas de datos.

[Prioridad 1]
Por ejemplo, en HTML, utilice THEAD, TFOOT, y TBODY, para agrupar las filas, COL y COLGROUP para agrupar las columnas y los atributos "axis", "scope" y "headers" para describir relaciones más complejas entre los datos. Técnicas para el punto de verificación 5.2.

5.3 No utilice tablas para maquetar, a menos que la tabla tenga sentido cuando se alinee. Por otro lado, si la tabla no tiene sentido, proporcione una alternativa equivalente (la cual debe ser una *versión alineada*).

[Prioridad 2]

5.4 Si se utiliza una tabla para maquetar, no utilice marcadores estructurales para realizar un efecto visual de formato.

[Prioridad 2]
Por ejemplo, en HTML no utilice elemento TH para hacer que el contenido de una celda (que no sea de encabezamiento de tabla) se visualice centrado y en negrita. Técnicas para el punto de verificación 5.4.

5.5 Proporcione resúmenes de las tablas.

[Prioridad 3]
Por ejemplo, en HTML, use el atributo "summary" en el elemento TABLE. Técnicas para el punto de verificación 5.5.

5.6 Proporcione abreviaturas para las etiquetas de encabezamiento.

[Prioridad 3]
Por ejemplo, en HTML, use el atributo "abbr" en el elemento TH. Técnicas para el punto de verificación 5.6. Consultar también punto de verificación 10.3.

Pauta 6: Asegúrese de que las páginas que incorporan nuevas tecnologías se transformen correctamente.

6.1 Organice el documento de forma que pueda ser leído sin hoja de estilo. Por ejemplo, cuando un documento HTML es interpretado sin asociarlo a una hoja de estilo, tiene que ser posible leerlo.

[Prioridad 1]
Cuando el contenido está organizado lógicamente, es interpretado de forma que la organización continúa siendo clara incluso cuando se desconecten o no se soporten las hojas de estilo. Técnicas para el punto de verificación 6.1.

6.2 Asegúrese de que los equivalentes de un contenido dinámico son actualizados cuando cambia el contenido dinámico.

[Prioridad 1]
Técnicas para el punto de verificación 6.2.

6.3 Asegúrese de que las páginas sigan siendo utilizables cuando se desconecten o no se soporten los scripts, applets u otros objetos programados. Si esto no es posible, proporcione información equivalente en una página alternativa accesible.

[Prioridad 1]

Por ejemplo, asegúrese de que los enlaces que lanzan scripts funcionan cuando éstos se desconecten o no se soporten (Por ejemplo, no utilizar un "javascript" como objetivo de un enlace). Si no es posible hacer la página utilizable sin scripts, proporcione un texto equivalente con el elemento NOSCRIPT o utilice un script del servidor en lugar de un script de cliente o proporcione una página alternativa accesible como para el punto de verificación 11.4. Consultar también la pauta 1. Técnicas para el punto de verificación 6.3.

6.4 Para los scripts y applets, asegúrese de que los manejadores de evento sean independientes del dispositivo de entrada.

[Prioridad 2]
Consultar la definición de independencia del dispositivo. Técnicas para el punto de verificación 6.4.

6.5 Asegúrese de que los contenidos dinámicos son accesibles o proporcione una página o presentación alternativa.

[Prioridad 2]
Por ejemplo en HTML, utilice NOFRAMES al final de cada 'frameset'. Para algunas aplicaciones, los scripts del servidor pueden ser más accesibles que los del cliente. Técnicas para el punto de verificación 6.5. Consultar también punto de verificación 11.4.

Pauta 7: Asegure al usuario el control sobre los cambios de los contenidos tempo-dependientes.

Algunas personas con discapacidades cognitivas o visuales son incapaces de leer textos que se mueven con la suficiente rapidez o en absoluto. El movimiento puede también distraer de tal manera que el resto de la página se vuelve ilegible para las personas con discapacidades cognitivas. Los lectores de pantalla son incapaces de leer textos móviles. Las personas con discapacidades físicas podrían no ser capaces de moverse tan rápida o certeramente como para interactuar con objetos móviles.

Nota: Todos los puntos de verificación que siguen, implican alguna responsabilidad por parte del desarrollador del contenido *hasta que las*

aplicaciones de usuario proporcionen adecuados mecanismos de control de la característica.

7.1 Evite provocar destellos en la pantalla.

[Prioridad 1]
Nota: Los usuarios con epilepsia fotosensitiva pueden tener ataques desencadenados por parpadeos o destellos que oscilen entre los 4 y los 59 destellos por segundo (hertzios), con un nivel máximo a los 20 destellos por segundo, así como con los cambios rápidos de oscuridad a iluminación (como las luces estroboscópicas). Técnicas para el punto de verificación 7.1.

7.2 Evite el parpadeo del contenido (por ejemplo, cambio de presentación en periodos regulares, así como el encendido y apagado).

[Prioridad 2]
Técnicas para el punto de verificación 7.2

7.3 Evite los movimientos en las páginas.

[Prioridad 2]
Cuando una página incluye contenido móvil, proporcione un mecanismo dentro de un script o un applet que permita a los usuarios congelar el movimiento o actualización. El uso de las hojas de estilo con scripts que creen movimiento, permite a los usuarios desconectar u obviar el efecto más fácilmente. Consultar también la pauta 8. Técnicas para el punto de verificación 7.3.

7.4 No cree páginas que se actualicen automáticamente de forma periódica.

[Prioridad 2]
Por ejemplo, en HTML, no cree páginas que se actualicen automáticamente con "HTTP EQUIV=refresh" hasta que las aplicaciones de usuario permitan desconectar esta característica.
Técnicas para el punto de verificación 7.4.

7.5 No utilice marcadores para redirigir las páginas automáticamente. En su lugar, configure el servidor para que ejecute esta posibilidad.

[Prioridad 2]

Técnicas para el punto de referencia 7.5.
Nota. Los elementos BLINK y MARQUEE no están definidos en ninguna especificación W3C HTML, y no deberían ser utilizados. Consultar también la pauta 11.

Pauta 8: Asegure la accesibilidad directa de las interfaces de usuario incrustadas.

Cuando un objeto incrustado tiene su "propia interfaz", ésta (al igual que la interfaz de su navegador) debe ser accesible. Si la interfaz del objeto incrustado no puede hacerse accesible, debe proporcionarse una solución alternativa accesible.

Nota: Para información sobre interfaces accesibles, por favor consulte las Pautas de Accesibilidad a las Aplicaciones de Usuario [WAI-USERAGENT] y las Pautas de Accesibilidad para las Herramientas de Creación [WAI-AUTOOL].

8.1 Haga los elementos de programación, tales como scripts y applets, directamente accesibles o compatibles con las ayudas técnicas

[Prioridad 1 si la funcionalidad es *importante* y no se presenta en otro lugar; de otra manera, Prioridad 2.]
Consultar también la pauta 6. Técnicas para el punto de referencia 8.1.

Pauta 9: Diseñe para la independencia del dispositivo.

El acceso independiente del dispositivo significa que el usuario puede interactuar con la aplicación de usuario o el documento con un dispositivo de entrada (o salida) preferido - ratón, teclado, voz, puntero de cabeza (licornio) u otro. Si, por ejemplo, un control de formulario sólo puede ser activado con un ratón u otro dispositivo de apuntamiento, alguien que use la página sin verla, con entrada de voz, con teclado o quien utilice otro dispositivo de entrada que no sea de apuntamiento, no será capaz de utilizar el formulario.

Nota: Proporcionando textos equivalentes para los mapas de imagen o las imágenes usadas como vínculos, se hace posible a los usuarios interactuar con ellos sin un dispositivo de apuntamiento. Consultar también la pauta 1.

Generalmente, las páginas que permiten la interacción a través del teclado son también accesibles a través de una entrada de voz o una serie de comandos.

9.1 Proporcione mapas de imagen controlados por el cliente en lugar de por el servidor, excepto donde las zonas sensibles no puedan ser definidas con una forma geométrica.

[Prioridad 1]
Consultar también punto de verificación 1.1, punto de verificación 1.2, y punto de verificación 1.5. Técnicas para el punto de verificación 9.1.

9.2 Asegúrese de que cualquier elemento que tiene su propia interfaz pueda manejarse de forma independiente del dispositivo.

[Prioridad 2]
Consultar la definición de independencia del dispositivo.
Consultar también la pauta 8. Técnicas para el punto de verificación 9.2.

9.3 Para los "scripts", especifique manejadores de evento lógicos en vez de manejadores de evento dependientes de dispositivos.

[Prioridad 2]
Técnicas para el punto de verificación 9.3.

9.4 Cree un orden lógico para navegar con el tabulador a través de vínculos, controles de formulario y objetos.

[Prioridad 3]
Por ejemplo, en HTML, especifique el orden de navegación con el tabulador a través del atributo "tabindex" o asegure un diseño de página lógico. Técnicas para el punto de verificación 9.4.

9.5 Proporcione atajos de teclado para los vínculos más importantes (incluidos los de los *mapas de imagen de cliente*), los controles de formulario y los grupos de controles de formulario.

[Prioridad 3]
Por ejemplo, en HTML, especifique los atajos a través del atributo "accesskey".
Técnicas para el punto de verificación 9.5.

Pauta 10: Utilice soluciones provisionales.

Nota: Estos puntos de verificación están clasificados como "provisionales" lo que significa que el Grupo de Trabajo de las Pautas de Contenido en la Web los considera válidos y necesarios para la accesibilidad de la Web *en el momento de la publicación de este documento*. Sin embargo, el Grupo de Trabajo espera que estos puntos de verificación no sean necesarios en un futuro, una vez que las tecnologías de la Web hayan incorporado las características y capacidades esperables.

10.1 No provoque apariciones repentinas de nuevas ventanas y no cambie la ventana actual sin informar al usuario.

[Prioridad 2]
Por ejemplo, en HTML, evite usar un marco cuyo objetivo es una nueva ventana. Técnicas para el punto de verificación 10.1.

10.2 Para todos los controles de formularios con etiquetas asociadas implícitamente, asegúrese de que la etiqueta está colocada adecuadamente.

[Prioridad 2]
La etiqueta debe preceder inmediatamente a su control en la misma línea (se permite más de una etiqueta/control por línea) o estar en la línea que precede al control (con sólo una etiqueta y un control por línea) [NdT]. Consultar también punto de verificación 12.4. Técnicas para el punto de verificación 10.2.

10.3 Proporcione un texto lineal alternativo (en la página actual o en alguna otra) para *todas* las tablas que maquetan texto en paralelo, columnas envoltorio de palabras.

[Prioridad 3]
Nota: Por favor, consulte la definición de *tabla alineada*. Este punto de verificación beneficia a aquellos que tienen *aplicaciones de usuario* (como algunos *lectores de pantalla*) que son incapaces de manejar bloques de texto contiguo; el punto de verificación no debe desanimar a los desarrolladores de

contenidos en el uso de tablas para presentar *información tabular*. Técnicas para el punto de verificación 10.3.

10.4 Incluya caracteres por defecto en los cuadros de edición y áreas de texto.

[Prioridad 3]
Por ejemplo, en HTML, haga esto con TEXTAREA e INPUT. Técnicas para el punto de verificación 10.4.

10.5 Incluya caracteres imprimibles (rodeados de espacios), que no sirvan como vínculo, entre los vínculos contiguos.

[Prioridad 3]
Técnicas para el punto de verificación 10.5.

Pauta 11: Utilice las tecnologías y pautas W3C.

Las actuales pautas recomiendan las tecnologías W3C (Por ejemplo, HTML, CSS, etc.) por varias razones:

Las tecnologías W3C incluyen características accesibles "incorporadas".
Las especificaciones W3C pronto serán revisadas para asegurar que los temas de accesibilidad se toman en consideración en la fase de diseño.
Las especificaciones W3C están desarrolladas en un proceso abierto de laborioso consenso.

Muchos formatos no recomendados por W3C (por ejemplo, PDF, Schockwave, etc.) requieren ser vistos bien con plug-ins o con aplicaciones autónomas. A menudo, estos formatos no pueden ser visualizados o navegados con aplicaciones de usuario estándares (incluyendo ayudas técnicas). Evitar estos formatos y características no estándar (elementos, atributos, propiedades y extensiones patentados), tenderá a hacer más accesibles las páginas a más gente que utiliza una amplia variedad de hardware y software. Cuando deba utilizar tecnologías no accesibles (patentadas o no), debe proporcionar una página equivalente accesible.

Incluso cuando se utilicen tecnologías W3C, deben ser usadas de acuerdo con las pautas de accesibilidad. Cuando utilice nuevas tecnologías, asegúrese de que se transforman correctamente (Consultar también la pauta 6).

Nota: Convertir los documentos (desde PDF, Postscript, RTF, etc.) a lenguajes de marcado W3C (HTML, XML) no siempre crea un documento accesible. Por tanto, valide cada página respecto a la accesibilidad y utilidad después del proceso de conversión (consulte la sección de validación). Si una página no se convierte de forma legible, revise la página hasta que su presentación original se convierta adecuadamente o bien proporcione una versión en HTML o en texto plano.

11.1 Utilice tecnologías W3C cuando estén disponibles y sean apropiadas para la tarea y use las últimas versiones que sean soportadas.

[Prioridad 2]
Consulte la lista de referencias para información sobre dónde encontrar las últimas especificaciones W3C y [WAI-UA-SUPPORT] para información sobre como las aplicaciones de usuario que soportan las tecnologías W3C. Técnicas para el punto de verificación 11.1.

11.2 Evite características desaconsejadas por las tecnologías W3C.

[Prioridad 2]
Por ejemplo, en HTML, no utilice el elemento *desaconsejado* FONT; use en su lugar hojas de estilo (por ejemplo, la propiedad "font" en CSS).
Técnicas para el punto de verificación 11.2.

11.3 Proporcione la información de modo que los usuarios puedan recibir los documentos según sus preferencias (Por ejemplo, idioma, tipo de contenido, etc.)

[Prioridad 3]
Nota: Use la negociación de contenidos donde sea posible. Técnicas para el punto de verificación 11.3.

11.4 Proporcione un vínculo a una página alternativa que use tecnologías W3C, sea accesible, tenga información (o funcionalidad) *equivalente* y sea actualizada tan a menudo como la página (original) inaccesible.

[Prioridad 1]
Técnicas para el punto de verificación 11.4.

Nota: Los desarrolladores de contenido sólo deben enviar a páginas alternativas cuando otras soluciones fallen, porque las páginas alternativas se actualizan con menor frecuencia que las páginas primarias. Una página no actualizada puede ser tan frustrante como una página inaccesible, puesto que en ambos casos, la información de la página original no está disponible. La generación automática de páginas alternativas puede conducir a actualizaciones más frecuentes, pero los desarrolladores de contenidos deben asegurar que las páginas generadas siempre tengan sentido y que los usuarios puedan navegar por el sitio siguiendo los vínculos de las páginas primarias, las páginas alternativas o ambas. Antes de enviar a una página alternativa, reconsidere el diseño de la página original; haciéndola accesible es probable que la mejore, para todos los usuarios.

Pauta 12: Proporcione información de contexto y orientación.

Agrupar los elementos y proporcionar información contextual sobre la relación entre elementos puede ser útil a todos los usuarios. Las relaciones complejas entre las partes de una página pueden resultar difíciles de interpretar a personas con discapacidades cognitivas o visuales.

12.1 Titule cada marco para facilitar su identificación y navegación.

[Prioridad 1]
Por ejemplo, en HTML, utilice el atributo "title" en los elementos FRAME.
Técnicas para el punto de verificación 12.1.

12.2 Describa el propósito de los marcos y como éstos se relacionan entre sí, si no resulta obvio solamente con el título del marco.

[Prioridad 2]
Por ejemplo, en HTML, utilice "longdesc" o un *vínculo a una descripción.*
Técnicas para el punto de verificación 12.2.

12.3 Divida los bloques largos de información en grupos más manejables cuando sea natural y apropiado.

[Prioridad 2]
Por ejemplo, en HTML, utilice OPTGROUP para agrupar los elementos OPTION dentro de un SELECT; agrupe controles de formulario con FIELDSET y LEGEND; utilice listados anidados cuando sea apropiado; utilice encabezamientos para estructurar documentos, etc. Consultar también la pauta 3. Técnicas para el punto de verificación 12.3.

12.4 Asocie explícitamente las etiquetas con sus controles.

[Prioridad 2]
Por ejemplo, en HTML, utilice LABEL y su atributo "for". Técnicas para el punto de verificación 12.4.

Pauta 13: Proporcione mecanismos claros de navegación

Los mecanismos de navegación claros y coherentes son importantes para las personas con discapacidad cognitiva o ceguera y benefician a todos los usuarios.

13.1 Identifique claramente el objetivo de cada vínculo.

[Prioridad 2]
El *texto del vínculo* tiene que tener significado suficiente cuando sea leído fuera de contexto (por sí mismo o como parte de una secuencia de vínculos). También debe ser conciso.
Por ejemplo, en HTML, escriba "información sobre la versión 4.3" en lugar de "pincha aquí". Además de textos de vínculos claros, los desarrolladores de contenidos deben aclarar el objetivo de un vínculo con un título informativo del mismo (por ejemplo, en HTML, el atributo "title").Técnicas para el punto de verificación 13.1.

13.2 Proporcione metadatos para añadir información semántica a las páginas y sitios.

[Prioridad 2]
Por ejemplo, use RDF ([RDF]) para indicar el autor de los documentos, el tipo de contenido, etc.

Nota: Algunas *aplicaciones de usuario* de HTML pueden construir herramientas de navegación a partir de las relaciones entre documentos descritas en el elemento HTML LINK y los atributos "rel" o "rev" (por ejemplo rel="siguiente"; rel="anterior"; rel="índice", etc.). Consultar también el punto de verificación 13.5. Técnicas para el punto de verificación 13.2.

13.3 Proporcione información sobre la maquetación general de un sitio (por ejemplo, mapa del sitio o tabla de contenidos).

[Prioridad 2]
En la descripción de la maquetación del sitio, destaque y explique las características de accesibilidad disponibles.
Técnicas para el punto de verificación 13.3.

13.4 Utilice los mecanismos de navegación de forma coherente.

[Prioridad 2]
Técnicas para el punto de verificación 13.4.

13.5 Proporcione barras de navegación para destacar y dar acceso al mecanismo de navegación.

[Prioridad 3]
Técnicas para el punto de verificación 13.5.

13.6 Agrupe los vínculos relacionados, identifique el grupo (para las aplicaciones de usuario) y proporcione una manera de evitar el grupo.

[Prioridad 3]
Técnica para el punto de verificación 13.6.

13.7 Si proporciona funciones de búsqueda, permita diferentes tipos de búsquedas para diversos niveles de habilidad y preferencias.

[Prioridad 3]
Técnicas para punto de verificación 13.7.

13.8 Localice al principio de los encabezamientos, párrafos, listas, etc, la información que los diferencie.

[Prioridad 3]
Nota: Esto es comúnmente denominado "front-loading" (colocar al frente) y es especialmente útil para los que acceden a la información con dispositivos seriales como un sintetizador de voz. Técnicas para el punto de verificación 13.8.

13.9 Proporcione información sobre las colecciones de documentos (por ejemplo, los documentos que comprendan múltiples páginas).

[Prioridad 3]
Por ejemplo, en HTML, especifique las colecciones de documentos con el elemento LINK y los atributos "rel" y "rev". Otro modo de crear una colección es construyendo un archivo (por ejemplo con zip, tar and gzip, stuffit, etc.) de las páginas múltiples.

Nota: La mejora en la presentación ganada por un procesamiento fuera de línea (offline) puede hacer la navegación mucho menos costosa a las personas con discapacidad que puedan estar navegando lentamente. Técnicas para el punto de verificación 13.9.

Pauta 14: Asegúrese de que los documentos sean claros y simples.

La maquetación coherente de páginas, los gráficos reconocibles y el lenguaje fácilmente comprensible benefician a todos los usuarios. En particular, ayudan a personas con discapacidades cognitivas o con dificultades en la lectura. (Por tanto, asegúrese de que las imágenes tienen textos equivalentes para los ciegos, los de baja visión o para cualquier usuario que no puede o ha elegido no ver los gráficos. Consulte también la pauta 1).

La utilización de un lenguaje claro y simple promueve una comunicación efectiva. El acceso a la información escrita puede ser difícil para personas con discapacidades cognitivas o de aprendizaje. La utilización de un lenguaje claro y simple también beneficia a las personas cuyo primer idioma es diferente al del

autor, incluidos aquellos que se comunican principalmente mediante lengua de signos.

14.1 Utilice el lenguaje apropiado más claro y simple para el contenido de un sitio.

[Prioridad 1]
Técnicas para el punto de verificación 14.1.

14.2 Complemente el texto con presentaciones gráficas o auditivas cuando ello facilite la comprensión de la página.

[Prioridad 3]
Consultar también la pauta 1. Técnicas para el punto de verificación 14.2.

14.3 Cree un estilo de presentación que sea coherente para todas las páginas.

[Prioridad 3]
Técnicas para el punto de verificación 14.3.

E.6 Actualización de la Información

1. El contenido de las páginas Web, se actualizará continuamente.

2. Las entidades serán responsables del contenido de sus páginas web, de la actualización, coherencia y veracidad de la información contenida en ellos.

E.7 Políticas de Privacidad

1. Las entidades del Estado deberán adoptar, mantener y declarar una "Política de Privacidad" en la página web y ésta deberá encontrarse accesible desde su primera página.

2. Las entidades del estado deberán seguir los lineamientos establecidos por la AIG en relación a este tema haciendo enlace a http://disclaimer.innovacion.gob.pa.

E.8 Acerca de los Dominios

1. Todas las páginas web del Estado utilizarán el dominio .gob.pa, registrándose ante la Autoridad Nacional para la Innovación Gubernamental, mediante una solicitud en línea.

2. La entidad que solicita un dominio se compromete a regirse por las normas establecidas en el presente documento.

3. Se entenderá que las entidades que solicitan la inscripción de un dominio tienen un conocimiento básico de los términos de uso frecuente en INTERNET.

4. La Dirección de Informática de la AIG será la responsable de solicitar el registro de dominios .gob.pa ante NIC Panamá, en coordinación con los contactos administrativos del dominio respectivo.

E.9 Cumplimiento de la Norma

1. La AIG validará las páginas web del Estado con el objetivo de detectar posibles enlaces rotos y la presencia de imágenes perdidas en el sitio web.

2. La AIG notificará a la entidad (web master), por correo electrónico, los enlaces rotos y las imágenes perdidas en el sitio web, para que sean corregidos.

3. La AIG validará los estándares de la versión de HTML o XHTML que se haya elegido para el desarrollo de la página WEB.

4. La AIG validará las plantillas de las hojas de cascadas de estilo CSS de cada entidad, a través de herramientas provistas por W3C.

5. La AIG colocará un ícono a las páginas WEB, que cumplan con los puntos de verificación y niveles de prioridad (E.3 Accesibilidad e Interoperabilidad), dados por la W3C, con el objetivo de hacer público que la página, cumple con los estándares establecidos.

Figura 20

6. Las normas y estándares establecidas en el presente documento se podrán modificar con el tiempo, si esto ocurre, los cambios serán remitidos a todas las entidades y publicados en nuestro sitio web www.innovacion.gob.pa.

7. El presente documento será de estricto cumplimiento y monitoreado por la Dirección de Tecnología de Información de la Autoridad Nacional de Innovación Gubernamental.

8. El administrador de la página web de cada entidad, deberá monitorear regularmente la actividad del mismo. Revisará periódicamente el log del servidor de la página, prestando atención a los códigos de error y a los elementos más visitados, documentará lo que ocurra con su audiencia y adoptará las medidas preventivas y correctivas oportunas, para así mejorar la calidad de las prestaciones e información que se brinda.

9. Las páginas web en la transmisión de sus contenidos, puede generar errores que están estandarizados mediante códigos para su mejor comprensión. Los que comienzan con el número 4 presentan errores del lado del cliente y los que empiezan con 5 son errores del lado del servidor. Ejemplo:

Error 401: Acceso no autorizado a una página, no se ingresó la password.
Error 403: Acceso prohibido; normalmente aparece cuando la página que se busca no tiene permiso para ser mostrada.
Error 404: La página no existe y no puede ser mostrada.
Error 500: Error en el servidor debido a un problema de software.
Error 503: El servicio web no está disponible.
Error 504: Tiempo de respuesta excede lo normal y por lo tanto la página no se muestra.

10. Se exceptúa los términos de los estándares y normas, a aquellas entidades o proyectos que por la naturaleza de sus funciones, no lo requiera, previa autorización escrita de la Autoridad Nacional para la Innovación Gubernamental (AIG).

F. Seguridad de la Información y Código Web

1. Todas las páginas WEB del Estado poseen importancia relevante para el ciudadano, según los trámites y servicios que éste brinde en línea, a través de su portal.

2. Siendo las páginas Web del Estado una de las principales líneas de interacción con los usuarios, y las más expuestas a incidentes y ataques externos de cualquier origen, es crucial que las páginas Web estén diseñadas de una manera segura y que no pongan en riesgo la información dentro de ellas.

3. Igualmente, es crucial que no puedan ser modificadas para ofrecer información diferente a la oficialmente aprobada por el Estado. Este tipo de modificación pública tienen un gran impacto en la confianza de los ciudadanos en los servicios del Estado.

4. Nunca se debe guardar datos sensitivos de uso confidencial o secreto en texto abierto en una aplicación web. Esto incluye contraseñas de acceso (tanto de usuarios, administradores, etc.), cuentas bancarias, y números de identificación personal (cédulas, teléfonos, direcciones, etc.). Toda esta información siempre debe guardarse de una manera cifrada con una llave secreta, o como una función irreversible de Hash que pueda usarse para verificación de contraseñas.

Todos los principios de codificación segura descritas en la siguiente sección deben ser seguidos por los programadores de páginas Web del Estado. De lo contrario, las páginas Web estarían vulnerables a ataques y si dicho ataque se ejecuta, será responsabilidad del programador no haber seguido dichas pautas.

5. Una opción alternativa a la codificación segura de las páginas Web, es el uso de dispositivos o programas conocidos como Web Application Firewalls (muralla contrafuegos para aplicaciones web). Estas pueden ser incorporadas como un dispositivo de uso exclusivo para esta tarea, un

programa que se instala en el servidor web, o un módulo o funcionalidad adicional que se activa en los Firewalls o murallas contrafuegos de redes.

6. Se deberá programar como mínimo dos pruebas de vulnerabilidad del sitio web al año. Existen sitios web que ofrecen estos servicios de manera continua, y existen empresas locales y/o extranjeras que también pueden ofrecer este servicio. La prueba de vulnerabilidad debe realizarse por una empresa diferente a la que programó el sitio web y diferente a los proveedores de Firewalls o Web Application Firewalls de la Entidad.

7. En caso de que los sistemas o la página web sean atacadas o vulneradas o modificadas sin autorización, deberá notificar formalmente a la AIG que el sistema ha sufrido una caída, luego de una hora continua de haberse dado el hecho.

8. En el momento de que sea detectado un ataque a la página web, deberá inmediatamente desconectar el equipo afectado de la red (desconectar el cable de red), pero dejar el equipo encendido para realizar el análisis forenses informático.

F.1. Principios de Codificación Segura OWASP

Existen múltiples estándares de codificación segura, que difieren según el lenguaje de programación, el servidor web, la base de datos en uso, y múltiples otros factores. Sin embargo, la razón principal de esta codificación es evitar los riesgos de aplicaciones web. La organización **Open Web Application Security Project** (http://www.owasp.org), una organización sin fines de lucro, publica un listado de los Diez Riesgos Más Importantes en Aplicaciones Web, y las siguientes indicaciones están orientadas a prevenir estos riegos en las aplicaciones Web del Estado (fuente:

A1 – Inyección

Inyección significa.

- ✓ Incluir comandos mal intencionados en los datos de una aplicación los cuales son enviados a un interprete

Los intérpretes.

- ✓ Toman estos datos y los interpretan como comandos validos (SQL, OS Shell, LDAP, XPath, Hibernate, etc.)

La Inyección SQL es aun bastante frecuente.

- ✓ Muchas aplicaciones todavía son susceptibles (no tendría que ser así)
- ✓ Por lo general es muy fácil de evitar

Impacto Típico.

- ✓ Por lo general severo. Todos los contenidos de una base de datos pueden potencialmente ser leídos o modificados.
- ✓ También puede permitir el completo acceso al esquema de la base de datos, o cuentas de usuario, o incluso a nivel del sistema operativo.

Como evitar Fallas de Inyección.

- ✓ Evitar el intérprete completamente.
- ✓ Utilizar una interface que soporte variables parametrizadas (Ej. declaraciones preparadas, o procedimientos almacenados).
  - Las variables parametrizadas permiten al intérprete distinguir entre código y datos.
- ✓ Decodificar y convertir todas las entradas del usuario a su forma más simple antes de enviarlas al intérprete.
- ✓ Siempre efectuar una validación 'positiva' de todas las entradas realizadas por el usuario.
- ✓ Seguir el principio de mínimo privilegio en las conexiones con bases de datos para reducir el impacto de una falla.

A2 Secuencia de Comandos en Sitios Cruzados (XSS) – Cross-Site Scripting

Ocurre cada vez que...

- ✓ Datos no validados de un atacante son enviados al navegador de una víctima.

Los datos no validados pueden...

- ✓ Encontrarse ALMACENADOS en una base de datos.
- ✓ Ser REFLEJADOS desde una entrada web (formulario, campo oculto, URL, etc.).
- ✓ Ser enviados directamente a un cliente JavaScript.

Virtualmente todas las aplicaciones web tienen este problema

- ✓ Intentar esto en un navegador –javascript:alert (document.cookie)

Impacto Típico

- ✓ Robar la sesión del usuario, robar datos sensibles, redireccionar un usuario hacia un sitio de malware o phishing.

- ✓ Mas grave: Instalar un proxy XSS que permite a un atacante observar y dirigir todas las actividades de un usuario en el sitio vulnerable y forzarlo hacia otros sitios.

Como evitar Fallas de XSS

- ✓ Eliminar la Falla
  - No incluir entradas suministradas por el usuario en la página de salida.
- ✓ Defenderse de la Falla
  - Recomendación Principal: Codificar todos los datos de entrada en la página de salida (Utilizar OWASP's ESAPI para dicha tarea): http://www.owasp.org/index.php/ESAPI.
- ✓ Siempre efectuar una validación 'positiva' de todas las entradas realizadas por el usuario
- ✓ Cuando grandes cantidades de HTML son suministradas por el usuario, utilizar OWASP's AntiSamy para sanear dicho HTML
- http://www.owasp.org/index.php/AntiSamy

A3 Perdida de Autenticación y Gestión de Sesiones

HTTP es un protocolo "sin estado".

- ✓ Significa que las credenciales tienen que viajar en cada pedido HTTP.
- ✓ Debería utilizar SSL para todo contenido que requiere autenticación.

Fallas en la gestión de sesiones.

- ✓ SESSION ID es utilizado para mantener el estado ya que HTTP no puede.
- ✓ Para un atacante es igual de útil que poseer el usuario y contraseña.
- ✓ SESSION ID es típicamente expuesto en la red, en el navegador, los logs, etc.

Tener cuidado con las "puertas laterales".

- ✓ Cambio de contraseña, recordar contraseña, olvidar la contraseña, pregunta secreta, desconexión del sitio, cambio de correo electrónico, etc.

Impacto Típico

- ✓ Cuentas de usuario comprometidas o sesiones de usuario secuestradas

Como evitar la Perdida de Autenticación y Gestión de Sesiones

- ✓ Verificar la arquitectura.

- Autenticación debería ser simple, centralizada y estandarizada
- Utilizar el gestor de sesiones estándar provisto por el servidor de aplicaciones – no inventar uno propio.
- Estar seguro que SSL protege tanto las credenciales como las sesiones de usuario todo el tiempo.

✓ Verificar la implementación.
- No utilizar solamente análisis automático.
- Verificar el certificado SSL.
- Examinar todas las funciones relacionadas a autenticación
- Verificar que "cierre de sesión" efectivamente destruya la sesión.
- Utilizar OWASP's WebScarab para testear la implementación.

✓ Para mayor información:
- http://www.owasp.org/index.php/Authentication_Cheat_Sheet.

A4 Referencia Directa Insegura a Objetos

¿Cómo proteger el acceso a los datos?.

Esto forma parte de realizar una "Autorización" apropiada, junto con Restringir el Acceso a URLs (A8)

Un error común.

✓ Listar solamente los objetos 'autorizados' para el usuario actual.

✓ Ocultar las referencias a objetos en campos ocultos y luego no imponer estas restricciones del lado del servidor.

✓ Esto se denomina control de acceso en la capa de presentación, y no funciona efectivamente.

✓ El atacante sencillamente modifica los valores de los parámetros.

Impacto Típico.

✓ Usuarios son capaces de acceder ficheros o datos sin autorización.

Como evitar Referencias Directas Inseguras a Objetos.

✓ Eliminar la referencia directa a objetos.
- Reemplazarla con un valor temporal de mapeo (ej. 1, 2, 3)

✓ Validar la referencia directa al objeto.
- Verificar que el valor del parámetro se encuentra adecuadamente formateado.

- Verificar que el usuario se encuentra autorizado a acceder el objeto determinado.
  - Restricciones en los parámetros funcionan muy bien.
- Verificar que el modo de acceso al objeto solicitado se encuentra autorizado (ej., lectura, escritura, modificación).

A5 Falsificación de Petición en Sitios Cruzados (CSRF)

Falsificación de Petición en Sitios Cruzados

- ✓ Es un ataque donde el navegador de la víctima es engañado para que emita un comando a una aplicación web vulnerable.
- ✓ La vulnerabilidad es causada debido a que los navegadores incluyen automáticamente información de autenticación del usuario (ID de sesión, dirección IP, credenciales de dominio Windows) en cada pedido HTTP.

Imagínese

- ✓ ¿Qué pasaría si un atacante pudiera mover su ratón y lograra que usted haga clic en enlaces de su aplicación bancaria?.

Impacto Típico

- ✓ Iniciar Transacciones (transferencia de fondos, desconectar el usuario, cierre de cuenta, etc.).
- ✓ Acceder datos sensitivos.
- ✓ Cambiar detalles de la cuenta.

Como evitar Fallas de CSRF

- ✓ Agregue un token secreto, no enviado automáticamente, a todos los pedidos HTTP sensitivos
  - Esto hace imposible al atacante falsificar el pedido HTTP (al menos que exista una vulnerabilidad XSS en la aplicación).
  - Los tokens deben ser lo suficientemente fuertes o aleatorios.

- Opciones
  - ✓ Almacenar una token único en la sesión y agregarlo en todos los formularios y enlaces
    - Campo Oculto: <input name="token" value="687965fdfaew87agrde" type="hidden"/>
    - URL de uso único: /accounts/687965fdfaew87agrde
    - Token en el formulario: /accounts?auth=687965fdfaew87agrde ...
  - ✓ Tener cuidado de no exponer el token en el encabezado de referencia
    - Se recomienda el uso de campos ocultos

- ✓ Se puede tener un token único por cada función
  - Use un hash del nombre de una función, id de sesión, y un secreto
  - Se puede solicitar una autenticación secundaria para funciones sensitivas

- No permita que atacantes almacenen ataques en su sitio
  - ✓ Codificar todas las entradas en la salida.
  - ✓ Esto "inactiva" todos los enlaces/pedidos en la mayoría de los intérpretes.

A6 Configuración Defectuosa de Seguridad

Las aplicaciones web dependen de cimientos seguros
- ✓ Desde el sistema operativo hasta el servidor de aplicaciones.
- ✓ No olvidarse de todas las librerías utilizadas.

¿Es su código fuente un secreto?
- ✓ Piense en todos los lugares donde se encuentra su código fuente
- ✓ Una seguridad eficaz no requiere que su código fuente sea secreto

La CS debe ser extendida a todas las partes de la aplicación
- ✓ Por ejemplo, todas las credenciales deberían cambiar en el ambiente de producción

Impacto Típico
- ✓ Instalación de código malicioso debido a un parche faltante en el OS o servidor
- ✓ Falla de XSS debido a un parche faltante en el framework de la aplicación
- ✓ Acceso no autorizado a cuentas por defecto, funcionalidad de la aplicación, etc. debido a una defectuosa configuración del servidor

Como evitar una Configuración Defectuosa de Seguridad
- ✓ Verificar la gestión de configuración de sus sistemas
  - Uso de guías de securización.
  - Automatizar tareas es MUY UTIL aquí
  - Mantener actualizadas todas las plataformas
  - Aplicar parches en todos los componentes
    Esto incluye librerías de software, no solo OS y servidor de aplicaciones
  - Analizar los efectos de estos cambios (en un entorno de prueba)

- ✓ ¿Puede "volcar" la configuración de la aplicación?
  - Desarrolle reportes en sus procesos
  - La regla es simple: Si no se puede verificar, no es seguro
- ✓ Verificar la implementación
  - Un simple escaneo puede encontrar problemas de configuración genéricos y parches faltantes

A7 Almacenamiento Criptográfico Inseguro

Ocurre cuando...

- ✓ No se identifican todos los datos sensitivos.
- ✓ No se identifican todos los lugares donde estos datos son almacenados.
- ✓ Base de datos, ficheros, carpetas, archivos de log, backups, etc.
- ✓ No se protege esta información en todas sus ubicaciones.

Impacto Típico

- ✓ Atacantes acceden o modifican información privada o confidencial Ej., tarjetas de crédito, registros médicos, datos financieros.
- ✓ Atacantes extraen secretos a ser usados en otros ataques.
- ✓ Mala Imagen para la Compañía, clientes insatisfechos, y pérdida de confianza.
- ✓ Gastos para corregir el incidente, tales como análisis forense, enviar cartas de disculpas, reemisión de tarjetas de crédito, etc.
- ✓ El Negocio es demandado o multado.

Como evitar un Almacenamiento Criptográfico Inseguro

- ✓ Verificar la arquitectura
  - Identificar todos los datos sensitivos
  - Identificar todos los lugares donde estos datos son almacenados
  - Utilice encripción para contrarrestar las amenazas, no solo para 'encriptar' datos
- ✓ Proteger la información con mecanismos apropiados
  - Encripción en ficheros, base de datos, etc.
- ✓ Utilizar los mecanismos correctamente
  - Usar únicamente algoritmos públicos reconocidos (como AES, RSA, y SHA-256)
  - No utilizar algoritmos considerados débiles (como MD5 o SHA1)
  - Nunca transmitir claves privadas por canales inseguros

- No almacenar información innecesaria. Ej. código CVV de tarjeta de crédito (req. PCI DSS)

✓ Verificar la implementación
- Un algoritmo estándar es utilizado, y es el algoritmo apropiado para dicha situación
- Todas las llaves, certificados, y contraseñas se encuentran debidamente almacenadas y protegidas
- Los métodos para distribuir las llaves son seguros y efectivos
- Mas difícil: Analizar el código de encripción por posibles fallas

A8 Falla de Restricción de Acceso a URL

¿Cómo proteger el acceso a URLs (páginas)?

✓ Esto forma parte de realizar una "autorización" apropiada junto con prevenir Referencias Directas Inseguras a Objetos (A4)

Un error común

✓ Listar solamente enlaces y opciones de menú autorizados
✓ Esto se denomina control de acceso en la capa de presentación, y no funciona efectivamente
✓ El atacante simplemente modifica la URL para acceder a paginas no autorizadas

Impacto Típico

✓ Atacantes invocan funciones y servicios a los cuales no se encuentran autorizados
✓ Acceso a otras cuentas de usuario y datos
✓ Realizar acciones privilegiadas (admin.)

Como evitar Fallas de Restricción de Acceso a URL.

✓ Por cada URL, un sitio necesita realizar 3 cosas.
- Restringir el acceso solo a usuarios autenticados (en caso que no sea pública).
- Imponer los permisos de usuario o rol (en caso que sea privado).
- Deshabilitar completamente los pedidos a páginas .desautorizadas (ej., ficheros de config., ficheros de log, código fuente, etc.).

✓ Verificar la arquitectura.
- Utilizar un modelo simple y positivo en cada capa.
- Asegurarse que existe un mecanismo en cada capa.

- ✓ Verificar la implementación.
- ✓ No utilizar análisis automático para detectar fallas.
- ✓ Verificar que cada URL en la aplicación se encuentra protegida por:
  - Un filtro externo, como Java EE web.xml o un producto comercial.
  - O controles internos en el código – Usar ESAPI's is Authorized For URL.
- ✓ Verificar que la configuración del servidor deshabilite pedidos a páginas no autorizadas (ejemplo: conf.)
- ✓ Utilizar WebScarab para 'falsificar' pedidos no autorizados

A9 Protección Insuficiente en la Capa de Transporte

Ocurre Cuando:

- ✓ No se identifican todos los datos sensitivos
- ✓ No se identifican todos los lugares donde estos datos son enviados
  - En la web, bases de datos, socios de negocios, comunicaciones internas
- ✓ No se protege esta información en todas sus ubicaciones

Impacto Típico:

- ✓ Atacantes acceden o modifican información privada o confidencial (Ej., tarjetas de crédito, registros médicos, datos financieros).
- ✓ Atacantes extraen secretos a ser usados en otros ataques.
- ✓ Mala Imagen para la Compañía, clientes insatisfechos, y pérdida de confianza.
- ✓ Gastos para corregir el incidente, tales como análisis forense, enviar cartas de disculpas, reemisión de tarjetas de crédito, etc.
- ✓ El Negocio es demandado o multado.

Como evitar Protección Insuficiente en la Capa de Transporte:

- ✓ Proteger con mecanismos apropiados
  - Utilizar TLS en todas las conexiones con datos sensitivos
  - Encriptar mensajes individualmente antes de transmitirlos. Ej., XML-Encryption
  - Firmar digitalmente los mensajes antes de transmitirlos Ej., XML-Signature
- ✓ Utilizar los mecanismos correctamente.
  - Verificar los certificados SSL antes de usarlos.

- Utilizar SSL en cualquier comunicación autenticada o al transmitir información sensible.
- Verificar que la comunicación entre componentes (ej., servidor web y base de datos) también utiliza un canal seguro.

A10 Redirecciones y Destinos No Validados

Las redirecciones en aplicaciones web son muy comunes:

- ✓ Frecuentemente incluyen parámetros suministrados por el usuario en la URL destino.
- ✓ Si no son validados, el atacante puede enviar a la victima a un sitio de su elección.

Los destinos (llamados transferencias en .NET) son comunes:

- ✓ Internamente envían el pedido a una nueva página en la misma aplicación
- ✓ Algunas veces los parámetros definen la pagina de destino
- ✓ Si no son validados, el atacante puede utilizar destinos no validados para 'evitar' controles de autenticación

Impacto Típico:

- ✓ Redireccionar a una víctima hacia un sitio de phishing o malware
- ✓ El pedido del atacante es ejecutado, pasando por alto los controles de Seguridad

Como evitar Redirecciones y Destinos No Validados:

- ✓ Existen varias opciones
  - Intentar evitar el uso de redirecciones y destinos (es difícil, verdad).
  - No utilizar parámetros provistos por usuarios para definir la URL destino
  - Si se deben utilizar dichos parámetros, entonces:
    Validar cada parámetro para asegurarse que es válido y se encuentra autorizado para el usuario actual, o
    Preferido – Utilizar mapeos del lado del servidor para 'traducir' la opción provista al usuario en la verdadera pagina de destino
  - Defensa en profundidad: Para las redirecciones, validar la URL destino luego que es calculada para asegurarse que efectivamente sea un sitio externo autorizado
- ✓ Algunas ideas para proteger los destinos no validados

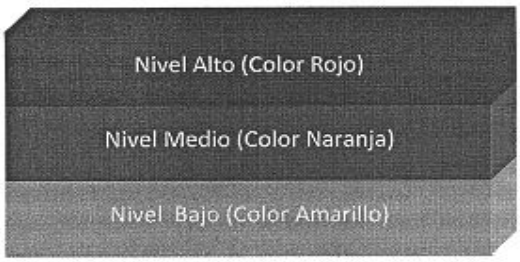
- Idealmente, se invocaría al controlador de acceso para asegurarse que el usuario se encuentra autorizado antes de realizar la transferencia (con ESAPI, es fácil).
- Asegurarse que los usuarios que pueden acceder la página de origen se encuentran TODOS autorizados a acceder la página destino.

G. Disponibilidad de la Información

1. Todas las páginas WEB del Estado poseen importancia relevante para el ciudadano, según los trámites y servicios que éste brinde en línea, a través de su portal.

2. Las páginas web del estado se clasificarán por niveles, según los servicios o trámites en línea que ofrezcan al ciudadano.

Los niveles de clasificación son:



3. Los tres niveles exigirán los mismos requerimientos, la diferencia radica en el tiempo máximo permitido para recuperarse de una caída o falla del sistema.

❖ Nivel Alto:

1. En este nivel se encuentran enmarcadas todas aquellas Entidades que ofrecen el servicio de consultas y trámites de Gobierno a Ciudadano y de Gobierno a Gobierno, sin requerir acto presencial dentro de dicha Entidad.

2. Las Entidades que clasifiquen en este nivel, cumplirán con los siguientes requisitos:

a) Los sistemas WEB tendrán alta disponibilidad y réplica de sus servicios en un sitio remoto, en caso de desastre.
b) Mantener la antigüedad de los Respaldos con un máximo de 24 horas.
c) En caso de caída del sistema, redireccionar el sitio WEB a una página que indique un mensaje de mantenimiento del sistema.
d) El tiempo máximo de caída del Sistema WEB podrá ser de 12 Horas los días sábados y domingos y los días feriados. Los días de lunes a viernes el tiempo máximo de caída del Sistema WEB será de 4 horas.
e) Notificar formalmente a la AIG que el sistema ha sufrido una caída, luego de una hora continua de haberse dado el hecho.
f) Enviar a la AIG sus respaldos los viernes de cada semana.
g) Enviar a la AIG los diagramas de configuración de los sistemas WEB de la Entidad.

❖ **Nivel Medio:**

1. En este nivel se encuentran enmarcadas aquellas Entidades que ofrecen el servicio de consultas y trámites de Gobierno a Gobierno, sin requerir acto presencial dentro de dicha Entidad.

2. Las Entidades que clasifiquen en este nivel, cumplirán con los siguientes requisitos:

a) Los sistemas WEB tendrán alta disponibilidad y réplica de sus servicios en un sitio remoto, en caso de desastre
b) Mantener la antigüedad de los Respaldos con un máximo de 24 horas.
c) En caso de caída del sistema, luego de 15 minutos redireccionar el sitio WEB a una página que indique un mensaje de mantenimiento del sistema.
d) El tiempo máximo de caída del Sistema WEB podrá ser de 24 Horas los días sábados y domingos y los días feriados. Los días de lunes a viernes el tiempo máximo de caída del Sistema WEB será de 8 horas.
e) Notificar formalmente a la AIG que el sistema ha sufrido una caída luego de una hora continua de haberse caído el sistema.
f) Enviar a la AIG sus respaldos los viernes de cada quince días.
g) Enviar a la AIG los diagramas de configuración de los sistemas WEB de la Entidad.

Nivel Bajo:

1. En este nivel se encuentran enmarcadas aquellas Entidades que ofrecen el servicio de consultas, sin requerir acto presencial dentro de dicha Entidad.

2. Todas aquellas entidades que clasifiquen en esta categoría tendrán que cumplir como mínimo con los siguientes requisitos:

   a) Que los sistemas WEB posean alta disponibilidad.
   b) Mantener la antigüedad de los Respaldos con un máximo de 24 horas.
   c) En caso de caída del sistema, luego de 15 minutos redireccionar el sitio WEB a una página que indique un mensaje de mantenimiento del sistema.
   d) El tiempo máximo de caída del Sistema WEB podrá ser de 24 Horas los días sábados y domingos y los días feriados. Los días de lunes a viernes el tiempo máximo de caída del Sistema WEB será de 12 horas.
   e) Notificar formalmente a la AIG que el sistema ha sufrido una caída luego de una hora continua de haberse caído el sistema.
   f) Enviar a la AIG sus respaldos, el último viernes de cada mes.
   g) Enviar a la AIG los diagramas de configuración de los sistemas WEB de la Entidad.

H. Buscadores e Intranet

H.1 Intranet

1. Las entidades del estado utilizarán una red de Área Local o LAN (Intranet), con características, de uso exclusivo de la entidad que la ha instalado. Será una plataforma de colaboración institucional que permita incrementar la productividad y administrar los contenidos a través de interfaz.

2. Utilizará protocolos HTML y el TCP/IP. Protocolos que permiten la interacción en línea de la Intranet, con la Internet.

3. Contendrá niveles de seguridad, según el usuario. Los niveles de seguridad, serán asignados, según la relevancia del cargo dentro de la Entidad.

4. Podrá existir dentro de la intranet niveles compartidos por todos, siempre y cuando los niveles básicos de seguridad, impidan la utilización de la Intranet, por parte de personas foráneas a la Entidad.

5. Los recursos integrados, mejorados por las tecnologías de búsqueda, permitirán responder con rapidez frente a las cambiantes necesidades institucionales.

Tomar decisiones bien informadas e implementar soluciones de forma rápida y segura mejoran y enriquecen la colaboración de todas las entidades, con terceros.

6. Los elementos de la interfaz de usuario (IU), como vínculos, controles de formulario y botones, estarán diseñados para permitir a las personas con discapacidades interactuar con el contenido mediante tecnologías de asistencia, en caso de que la entidad tenga funcionarios con discapacidad.

7. El sistema contendrá protección al acceso no autorizado a la información de la Entidad (firewall), y del daño o rechazo de los recursos y servicios informáticos, así como impedir que los usuarios internos accedan a los servicios de Internet que puedan ser peligrosos, como FTP. Las terminales de las Intranets sólo tendrán permiso para acceder a Internet después de atravesar un firewall.

H.2 Buscadores

1. Las Entidades utilizaran un sistema de búsqueda universal que permita extraer e incorporar información almacenada procedente de fuentes externas e internas el cual incluirá sistemas de archivos, intranets, base de datos, aplicaciones, servicios alojados y sistemas de gestión de contenidos.

2. El buscador será capaz de extraer la información almacenada, dentro de la intranet o internet, en documentos de Microsoft Office (Word DOC, Excel XLS, PowerPoint PPT), PDF o Bases de Datos (Natural, Oracle, DB2, SQL Server, MySQL u otros).

3. El sistema de entrada tendrá una capacidad de indexar todos los documentos del sitio web.

4. El sistema incluirá resultados "cache". Cuando el usuario haga click sobre él verá una versión en HTML del documento sin necesidad de abrirlo.

5. Las páginas de resultados tendrá:
   - ➢ número de resultados obtenidos.
   - ➢ duración de la búsqueda.
   - ➢ título del documento.
   - ➢ dirección de documento.
   - ➢ fecha de modificación.

6. Algunas opciones gratuitas y fáciles de implementar incluyen:
   Google Custom Search: http://www.google.com/cse/
   FreeFind: http://www.freefind.com/

Glosario de Términos

Áreas de Interacción: zonas en las que se ofrece realización de acciones por parte de usuarios del sitio web, a través de las cuales se pueden utilizar los servicios de la entidad que pone en marcha el espacio digital.

Experiencias del usuario: es lo que siente y experimenta el usuario que ingresa a cada página web.

W3C (World Wide Web Consortium): Comunidad Internacional que desarrolla estándares que aseguran el crecimiento a largo plazo de la Web.

CSS (Cascading Style Sheets) Hojas de Estilo en Cascada: mecanismo que describe la manera de mostrar un documento en la pantalla, cómo se va a imprimir, y cómo debe ser pronunciada la información presente en ese documento a través de un dispositivo de lectura. Esta forma de descripción de estilos ofrece a los desarrolladores el control total sobre estilo y formato de los documentos.

Estándares: especificaciones que determinan la manera en que se construye y funciona una tecnología en particular, con el objetivo de regular la realización de sus procesos.

Web Master: profesional encargado de la infraestructura técnica de la página web y de crear puentes entre la tecnología y su uso por parte de especialistas no técnicos.

Colaboradores que implementan la página web: programadores, diseñadores y comunicadores, responsables del diseño e implementación de la herramienta.

Gestores de contenido: Son los profesionales que manejan la información que se incorpora.

Accesibilidad al contenido en una página Web: asegurar que las páginas web de las entidades del estado, sean accesibles (sin barreras de acceso), para todos los usuarios, ya sea discapacitados o con bajos recursos tecnológicos.

Gobierno Electrónico es el uso de las tecnologías de información y comunicaciones que realizan las entidades del estado para mejorar los servicios e información ofrecidos a los ciudadanos, aumentar la eficiencia y

eficacia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación de los ciudadanos.[11]

Plug-ins: programas que extiende las capacidades del navegador de un modo especifico, dado por ejemplo la capacidad de mostrar vídeo, audio, ficheros de un determinado formato (ficheros PDF, presentaciones de ASAP, fichero VRML, etc.).

Usabilidad: es la efectividad, eficiencia y satisfacción con la que un grupo de usuarios específicos puede realizar un conjunto específico de tareas en un ambiente particular[12].

Interoperabilidad (compatibilidad): se refiere a la capacidad con que dispongan los sistemas y servicios informáticos, de comunicar, compartir e intercambiar datos, información y conocimiento de una forma precisa, efectiva y consistente; para de esta forma funcionar e incluso integrarse de manera correcta con otros sistemas, aplicaciones y servicios.[13]

Sistema de navegación: conjunto de elementos presente en cada una de las pantallas, permite a un usuario moverse por las diferentes secciones de una página web y retornar hasta la portada, sin sentir la sensación de haberse perdido en ese camino.

Menú de secciones: es una zona de la interfaz en la que se detallan las secciones o categorías en las que está dividida la información contenida en el sitio web. Normalmente se ubica en la parte superior de cada página o bien en la zona superior derecha o izquierda.

Identificación de secciones: estará en la zona superior de la página, de manera cercana la zona donde se encuentra el logo de la entidad. Puede ser gráfico y por lo mismo tener alguna imagen alusiva a la sección o categoría o bien ser una solución que incorpore sólo texto y color. Debe tener en forma destacada el nombre de la sección o categoría y por lo mismo, debe aparecer en todas las pantallas que pertenezcan a dicha ésta.

---

[11] Copyright © 2010 Gobierno de Chile. All Rights Reserved. Creative Commons Compatible License. Guía para el Desarrollo de Páginas Web 2.0 – Chile.

[12] International Standards Organization – ISO-. http://www.iso.org/iso/iso_catalogue.htm

[13] MARTÍNEZ, José Ángel; y LARA, Pablo (2007). "Interoperabilidad de los contenidos en las plataformas de e-learning: normalización, bibliotecas digitales y gestión del conocimiento". Revista de Universidad y Sociedad del Conocimiento (RUSC). Vol. 3 – N.2.

Menú de rastros: es el menú que indica mediante los nombres de cada sección o categoría del menú, la distancia que separa a la página actual de la portada. Por ejemplo, si el usuario está revisando la página del "Programa A", el menú correspondiente debe indicar Portada > Programas > "Programa A". Este menú debe ir siempre debajo de la Identificación de la sección o categoría y sobre el título

Tag: es una marca con tipo que delimita una región en los lenguajes basados en XML. También puede referirse a un conjunto de juegos informáticos interactivos que se añade a un elemento de los datos para identificarlo.

Interfaz: conjunto de elementos de la pantalla que permite al usuario realizar acciones sobre el sitio web que está visitando.

Anexos

Anexo No. 1

Ejemplos de páginas web gubernamentales a nivel mundial

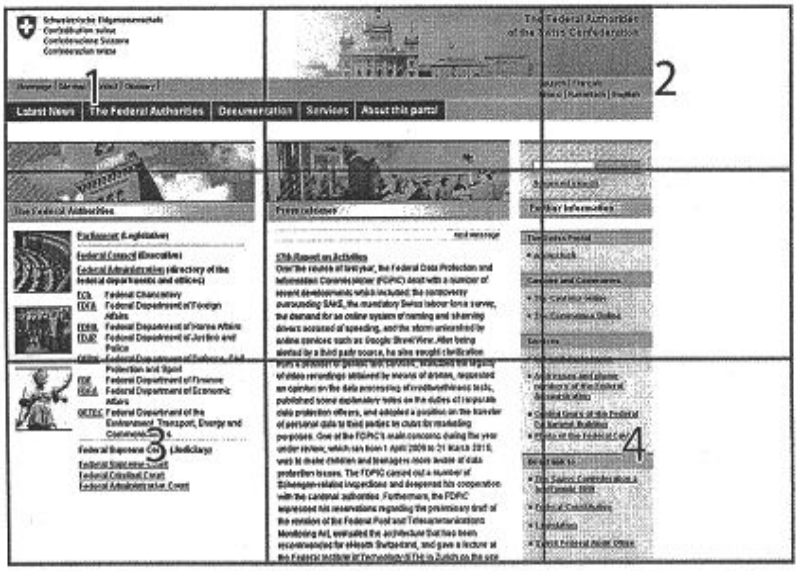


Figura 1 - Suiza: www.admin.ch

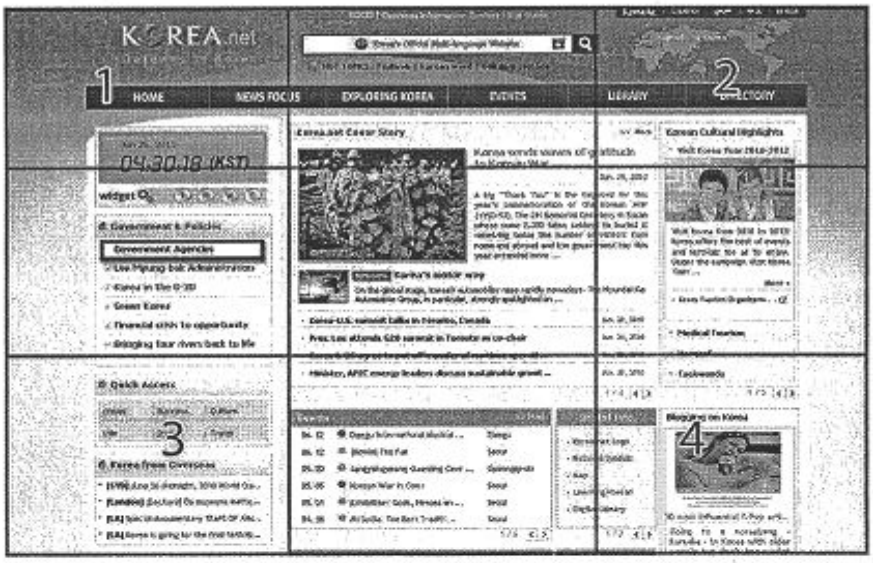


Figura 2 - Corea: www.korea.net

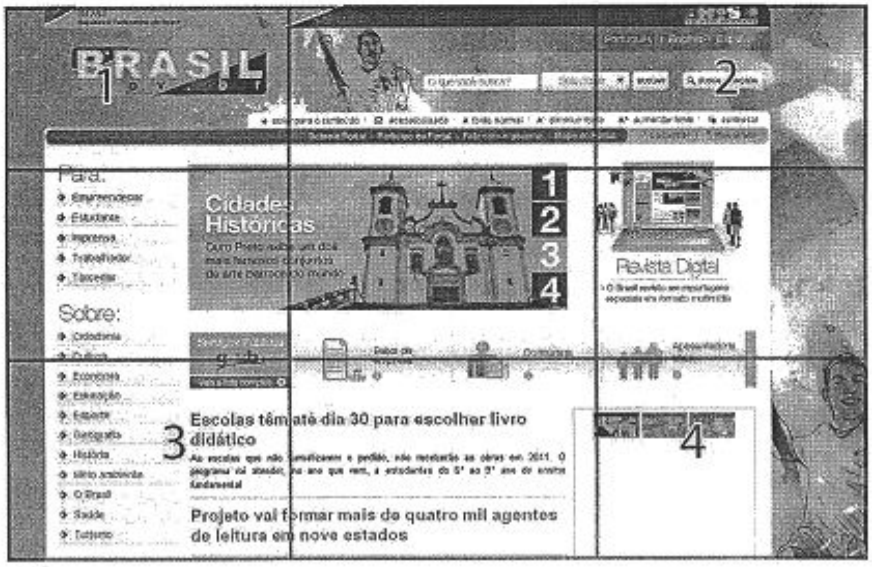


Figura 3 - Brasil: www.brasil.gov.br

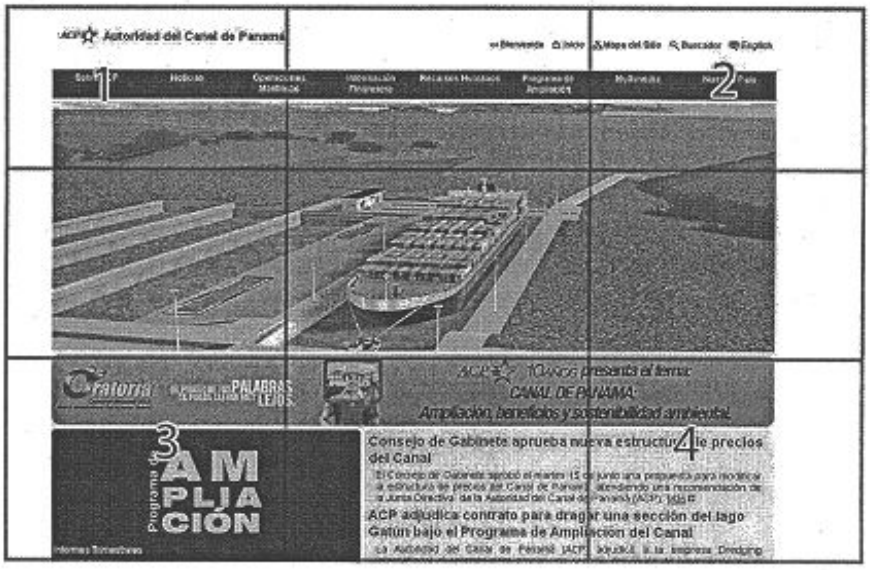


Figura 4 - APC (Panamá): www.pancanal.com

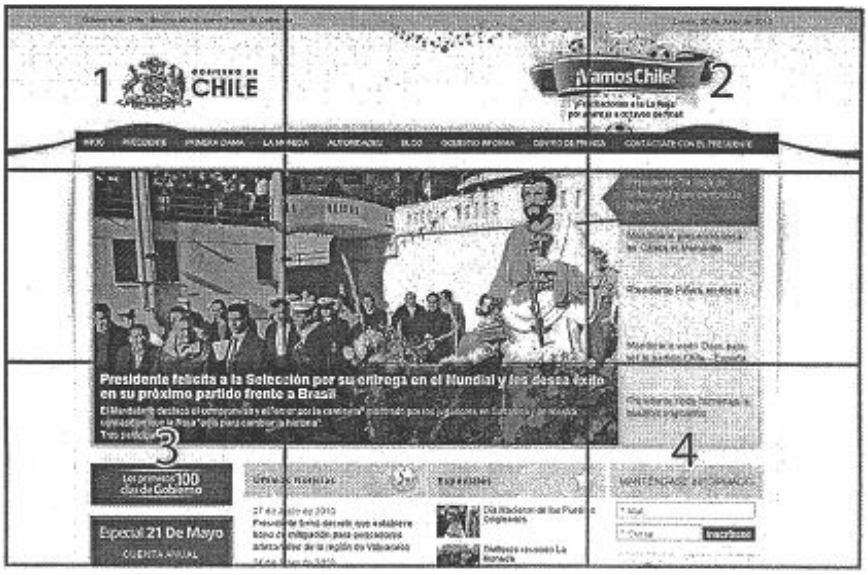


Figura 5 - Chile: www.gobiernodechile.cl


GOBIERNO NACIONAL
¿QUIÉNES SOMOS?
CONTÁCTENOS
Bienvenidos
Noticias mas Recientes [+]
311 CENTRO DE ATENCIÓN CIUDADANA
CONTÁCTENOS

Anexo No. 2

Convenciones de Diseño

1. El ancho de la página debe ser mayor a 900px y menor a 1000px.
2. El menú debe ser horizontal y estar ubicado en los primeros 200px.
3. El Logo debe estar ubicado en el primer cuadrante, superior izquierdo. Y no debe ser más grande que un tercio del ancho de la página.
4. La fotografía que se utilice debe tener un tamaño entre 500px y 700px de ancho y el alto debe estar entre el 56% y el 75% de su tamaño para estar en el rango de relación 16:9 para fotos anchas o 4:3 para fotos un poco más cuadradas.

Los titulares deben procurar tener 7 palabras máximo. De ser necesario usar más palabras se pueden emplear subtítulos.

Aspecto de las imágenes

Hay 5 estándares de imágenes que se han utilizado para fotografías, televisión, cine e impresiones.

Normalmente en la fotografía se emplea la relación 4:3 y 3:2.

Pero nosotros tenemos un rango de visión de aproximadamente 120º con un rango de enfoque de 90º en el plano horizontal. En el plano vertical tenemos aproximadamente 50º de rango de visión.

La razón entre 90 y 50 es de 1.8:1. Y la razón de una imagen en 16:9 es de 1.78:1. Lo que hace que nos resulte más natural apreciar imágenes en esta proporción que en proporciones cuadradas.

La relación de 16:9 es un estándar de TV de alta definición pero la usamos de referencia para imágenes y fotografías dentro de una página web.[14]

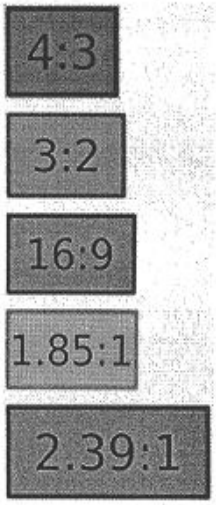
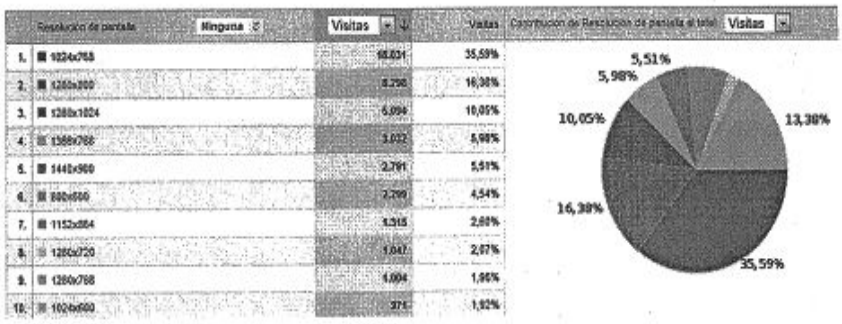


Ilustración 3 - Relaciones de Imagen más comunes.

Resoluciones de Pantalla Más Comunes



	Resolución de pantalla	Ninguna	Visitas	Visitas	Contribución de Resolución de pantalla al total	Visitas
1.	1024x768		48.031	35,59%		
2.	1280x800		8.298	16,38%		
3.	1280x1024		5.094	10,05%		
4.	1366x768		3.032	5,98%		
5.	1440x900		2.791	5,51%		
6.	800x600		2.299	4,54%		
7.	1152x864		1.315	2,60%		
8.	1280x720		1.047	2,07%		
9.	1280x768		1.004	1,98%		
10.	1024x600		975	1,92%		

Ilustración 4 – Resoluciones de Pantalla más comunes a junio 2010.

Esta gráfica se tomó de una muestra de una página web panameña que recibe alrededor de 55mil visitas al mes y comprende una audiencia de 18 a 50+ años de edad. Desde clase baja a clase alta con computadora propia o usando alquiler de computadoras en internet café.

En esta resolución se muestran los primero 600 o 700px de contenido de una página web y es por esta razón que se debe considerar un "área caliente" donde la información más importante va a ser vista de primero.

En esta área deben ir:

- Logotipos
- Anuncios críticos
- Menús
- Noticias importantes
- Anuncios publicitarios más costosos
- Promociones

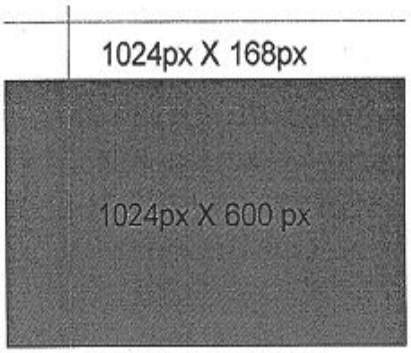


Ilustración 5 - División de Pantalla 1024 x 768

Bibliografía

1. Copyright © 2010 World Wide Web Consortium, (Massachusetts Institute of Technology, European Research Consortium for Informatics and Mathematics, Keio University). All Rights Reserved. http://www.w3.org/Consortium/Legal/2002/copyright-documents-20021231.

2. Copyright © 2010 Gobierno de Chile. All Rights Reserved. Creative Commons Compatible License. Guía para el Desarrollo de sitios Web – 1.0 y 2.0 del Gobierno de Chile. http://www.guiaweb.gob.cl/

3. Copyright © 2010 OWASP Foundation. All Rights Reserved. Creative Commons Compatible License. www.owasp.org/index.php/Top_10_2010.