Guia de Sitios web

Para las Entidades del Distrito Capital

2017

ALCALDÍA MAYOR DE BOGOTÁ D.C.

BOGOTÁ MEJOR PARA TODOS

Guía de sitios Web

Para las entidades del Distrito Capital

◇2017◇

Contenido

Guía de sitios
Web
Para las entidades
del Distrito Capital

◇2017◇

1 Introducción

El Plan de Desarrollo económico, social, ambiental y de obras públicas y plan plurianual de inversiones de Bogotá D.C. para el periodo 2016 – 2020, adoptado a través del Acuerdo Distrital 645 de 2016, establece en su artículo 56 el eje transversal 4 **"GOBIERNO LEGÍTIMO, FORTALECIMIENTO LOCAL Y EFICIENCIA",** el cual busca prever las acciones para restaurar la confianza en las instituciones públicas del Distrito (en adelante entidades distritales) y el buen gobierno de la ciudad, orientando los esfuerzos al servicio a la ciudadanía, y a la consolidación de prácticas habituales de seguimiento y evaluación de alternativas para optimizar procedimientos y costos de la prestación de los servicios.

Uno de los programas incluido en dicho eje transversal es **"Gobierno y Ciudadanía Digital"**, cuyo objeto es *"mejorar la eficiencia administrativa mediante el uso de la tecnología y la información, implementando un modelo de gobierno abierto para la ciudad que consolida una administración pública de calidad, eficaz, eficiente, colaborativa y transparente, que esté orientada a la maximización del valor público, a*

la promoción de la participación incidente, al logro de los objetivos misionales, y el uso intensivo de las TIC" (Artículo 59 del Acuerdo Distrital 645 de 2016).

Por otro lado, a través de la Resolución 378 de 2008, la Comisión Distrital de Sistemas (CDS) emitió la *"Guía para el diseño y desarrollo de sitios Web de las entidades y organismos del Distrito Capital"*, buscando que las entidades y organismos distritales adopten y apliquen lo establecido en dicho documento. Las transformaciones causadas por la actualización de las Tecnologías de la Información y las Comunicaciones, así como las exigencias normativas tendientes a garantizar el acceso a la información pública por parte de la ciudadanía, y a promover su participación en las decisiones de gestión pública, exigen constante revisión y posterior replanteamiento.

De esta forma, la CDS formula la nueva guía de sitios web, considerando el marco legal vigente, los aspectos de arquitectura de la información, usabilidad, accesibilidad y las características de plataforma, herramientas e integración tecnológicas. Dichos aspectos, fueron analizados y están articulados con la estrategia Nacional de **Gobierno en Línea.**[1]

La presente Guía de Sitios Web del Distrito Capital, se constituye en un instructivo que establece sugerencias técnicas, que serán insumo de apoyo eficaz para los equipos y las personas que tienen a cargo la planificación, construcción y modificación de los sitios web del Distrito.

En todo caso, será responsabilidad de cada entidad distrital, asegurar el cumplimiento de la normatividad aplicable y hacer seguimiento a las actualizaciones o cambios normativos sobre los sitios.

1 http://estrategia.gobiernoenlinea.gov.co

2 Normatividad Relevante

Sin perjuicio de normas adicionales que resulten relevantes a cada entidad, las entidades distritales deberán tener en cuenta como mínimo, la siguiente normatividad y sus modificaciones o reglamentaciones:

1. **Ley 1341 de 2009:**

   Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

2. **Ley 962 de 2005:**

   Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.

3. **Ley 1437 de 2011:**

   Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

4 **Ley 1437 de 2011:**

Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

5 **Ley 1581 de 2012:**

Por la cual se dictan disposiciones generales para la protección de datos personales.

6 **Ley 1755 de 2015:**

Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

7 **Ley 1712 de 2014:**

Por medio de la cual se crea la ley de Transparencia y de derecho de Acceso a la Información Pública Nacional y se dictan otra disposiciones.

8 **Acuerdo 380 de 2009:**

Por el cual se modifica el Acuerdo 131 de 2004 sobre Rendición de cuentas de la Alcaldía Mayor de Bogotá.

9 **Decreto 619 de 2007:**

Por el cual se establece la Estrategia de Gobierno Electrónico de los organismos y de las entidades de Bogotá, Distrito Capital y se dictan otras disposiciones.

10 **Ley 1266 de 2008:**

Por la cual se dictan disposiciones generales de hábeas data y se regula el manejo de información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

11 **Decreto 2623 de 2009:**

Por el cual se crea el Sistema Nacional de Servicio al Ciudadano.

12 **Decreto 19 de 2012:**

Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.

13 **Decreto Nacional 1377 de 2013:**

Por el cual se reglamenta parcialmente la Ley 1581 de 2012 de protección de datos personales.

14 **Decreto Nacional 2573 de 2014:**

Por el cual se establecen los lineamientos generales de la estrategia de gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

15 **Decreto Distrital 197 de 2014:**

Por el cual se adopta la Política Pública Distrital de Servicio a la Ciudadanía en la ciudad de Bogotá D.C.

16 **Decreto 1078 de 2015:**

Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

17 **Decreto 103 de 2015:**

Por el cual se reglamenta parcialmente la ley 1712 de 2014 y se dictan otras disposiciones.

18 **Resolución 305 de 2008:**

Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.

19 **Resolución 378 de 2008:**

Por la cual se adopta la Guía para el diseño y desarrollo de sitios Web de las entidades y organismos del Distrito Capital.

20 **Resolución 3564 de 2015:**

Por la cual se reglamentan los artículos 2.1.1.2.1.1, 2.1.1.2.1.11, 2.1.1.2.2.2, y el parágrafo 2 del artículo 2.1.1.3.1.1 del Decreto N° 1081 de 2015 Decreto Reglamentario Único del Sector Presidencia de la República, Directrices generales para la publicación de información pública.

21 **Directiva Distrital No. 5 de 2005:**

Políticas Generales de Tecnologías de Información y Comunicaciones aplicables a las entidades del Distrito Capital.

22 **Conpes 3654 de 2010:**

Política de rendición de cuentas de la rama ejecutiva a los ciudadanos.

23 **Conpes 3785 de 2013:**

Lineamientos para servicio al ciudadano.

24 **Circular 33 de 2008:**

Procedimiento para presentar quejas, reclamos y sugerencias a través del sistema distrital de quejas y soluciones.

25 **Manual Estrategia de Gobierno en Línea**

26 **Manual de Comunicaciones del Distrito Capital.**

27 **Manual de Imagen Distrital 2016.**

3 Planeación del Sitio Web

3.1. Dominio y alojamiento

De acuerdo con las necesidades institucionales y organizacionales de las entidades distritales, la construcción del sitio web es una tarea donde se hace necesario revisar el registro del dominio público

(www.nombreentidaddistrital.gov.co),

el acceso a los servicios de acceso a internet (ISP) habilitados, y direcciones IP validadas en la red institucional.

También, es necesario considerar para la gestión del dominio, las siguientes acciones:

1. Validar los plazos de vencimiento, claves de acceso y definir el funcionario que las administrará. Se sugiere que al efectuar el registro, con el fin de asegurar la continuidad en la operación, se incluyan dos personas de contacto.

2. Identificar y documentar la capacidad y características de los servidores, enrutadores, programas o dispositivos de direccionamiento para el dominio del sitio web.

3. Disponer de los mecanismos tanto de hardware y software de seguridad que propendan por la protección de la conexión contra accesos no permitidos (Firewall y Web Application Firewall, antivirus), conforme a los lineamientos establecidos en políticas de Privacidad y Seguridad de la Información y el Sistema de Gestión de Seguridad de la Información establecidos en la entidad distrital.

4. La Entidad debe gestionar una cuenta de dominio institucional y no personal, que facilite la administración del dominio y entre otras, el proceso de renovación e instalación de certificados digitales.

5. El administrador del sitio web distrital mantendrá contacto con los proveedores de dominio, incluyendo los detalles de la entidad distrital para:

   * Controlar el uso correcto de las direcciones y cuentas del dominio y de hosting (alojamiento).
   * Facilitar la ampliación o migración a otros servidores y gestionar los cambios de dominio (eliminación, transferencia interinstitucional, apertura de páginas y sub-sitios derivados del dominio principal, entre otros).
   * Asegurar que el dominio tenga al menos un servidor secundario de seguridad y que los DNS estén bien configurados. Además que la información de Parent, NS, SOA, CO, Mail y www no presente errores, o éstos no afecten la correcta operación del dominio y su resolución.
   * Definir con el área de sistemas de la entidad, la necesidad de implementar certificados seguros HTTPS para el sitio web.

Asimismo, es importante que cada entidad revise y realice las acciones correspondientes para concentrar, actualizar o eliminar todos aquellos portales desactualizados o huérfanos que sean de su competencia y estructurar un procedimiento para dar de baja las páginas web o portales que no tengan pertinencia a los objetivos y proyectos misionales de la actual administración distrital.

Registro de Dominio

Para entidades del Distrito, el uso o empleo de dominios .gov.co o .edu.co no tiene ningún costo asociado a su adquisición y su tiempo de vigencia es indefinido, aún si la entidad lo deshabilita.

La empresa encargada de la gestión, control y administración de los dominios de primer nivel en Colombia con extensión .co es

http://www.cointernet.com.co.

A través de esta empresa, y dependiendo del tipo de dominio, se deberá presentar toda la información que Cointernet solicite, para la correcta implementación del nuevo nombre de la entidad.

Se recomienda que los trámites a seguir sean validados con la empresa encargada de los dominios (http://www.cointernet.com.co).

3.2. Plataformas y herramientas tecnológicas

En busca de la estandarización de la presencia web de las entidades distritales, la Alta Consejería Distrital de TIC, atendiendo la Ley 1712 de 2014 y basándose en la estrategia de Gobierno en Línea (GEL) liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), encuentra recomendable como estrategia de implementación de proyectos web de entidades distritales, el uso de herramientas CMS *"Content Management System", tal como la Distribución Distrital CMS* ***Govimentum***[2], sin perjuicio de la autonomía de las entidades para determinar las herramientas tecnológicas a usar.[3]

Asimismo, en materia de manejador de base de datos, se recomienda el uso de MySql, MariaDB y PostgreSQL, sin perjuicio de la autonomía de las entidades, para determinar las herramientas tecnológicas a usar.

4 Estándares Web

La organización World Wide Web Consortium (W3C)[4] es la responsable de generar de manera constante las nuevas versiones de los lineamientos y estándares aplicados a sitios web y adicionalmente ofrece diferentes herramientas para realizar la validación del uso de los parámetros que genera dicha organización.

Por lo tanto, recomendamos visitar el sitio web del W3C es:

www.w3.org.

4.1. Estándares a seguir en un sitio web

La presente Guía recomienda seguir los siguientes parámetros para garantizar la calidad en los sitios web:

2 Govimentum está basado en Drupal.

3 Existen CMS que pueden usar las entidades según las necesidades de cada proyecto, tal como ocurre con WordPress u otras, según lo consideren pertinente.

4 https://www.w3.org/

Requisitos de calidad

1 **Disponibilidad:**

El proyecto web debe contar con las medidas técnicas suficientes que permitan mitigar los errores o carga del sistema, eventuales amenazas de seguridad y garantizar la posibilidad de atender picos de alto tráfico.

2 **Integridad conceptual:**

Es conveniente que el proyecto web contenga las mejores prácticas de programación, documentación, codificación y diseño.

3 **Flexibilidad:**

Es aconsejable que el proyecto web pueda adaptarse a ambientes y situaciones variables, y a soportar cambios, es decir, ser fácil de reconfigurar y que se adapte en respuesta a los diferentes requerimientos de sus usuarios.

4 **Interoperabilidad:**

Debe contar con la habilidad funcional de intercambiar información, comúnmente por medio de servicios con desarrollos disponibles en el Distrito, tales como *el Sistema Distrital de Quejas y Soluciones,*[5] entre otros.

5 **Capacidad de mantenimiento:**

Hace referencia a permitir ajustes en sus componentes, servicios, características e interfaces, en la medida en que los mismos, son requeridos.

6 **Capacidad de administración:**

Es conveniente que el proyecto sea de fácil gestión, incluyendo un sistema de monitoreo para efectos de mejoramiento del rendimiento e identificación de errores.

7 **Rendimiento:**

Se recomienda verificar que el proyecto cuente con una apropiada capacidad de respuesta para ejecutar una acción dentro de un intervalo de tiempo dado.

8 **Confiabilidad:**

Es la probabilidad de que el sitio web no falle en ejecutar su función, o una de sus funciones, dentro de un periodo específico de tiempo.

9 **Capacidad de Re-uso:**

Es aconsejable que el proyecto sea desarrollado de manera modular, lo que permitirá usar componentes específicos, por otras aplicaciones, en otros escenarios, con previa autorización.

Esta capacidad de re-uso minimiza la duplicación de componentes, así como el tiempo de implementación, y permite la correcta administración de los recursos públicos.

10 **Escalabilidad:**

El Sitio Web contará con los elementos para funcionar adecuadamente cuando se presentan cambios en la demanda o en la carga del mismo.

11 **Seguridad:**

Debe estar protegido de perder o suministrar información y ante la posibilidad de éxito de un ataque. Es

5 http://www.bogota.gov.co/sdqs

decir, debe proteger sus activos (información) y prever la modificación de información de fuentes no autorizadas.

12 **Capacidad de soporte:**

Debe ofrecer la facilidad para los operadores y desarrolladores, de entender y usar la aplicación, así como poder verificar la capacidad de respuesta ante los errores que se presentan cuando la aplicación falla.

13 **Capacidad de pruebas:**

Hace referencia a la posibilidad de aislar de una forma rápida y efectiva los fallos.

14 **Usabilidad:**

Hace referencia a ofrecer una experiencia adecuada para el usuario, siguiendo los lineamientos fijados por el MinTIC sobre el particular.

15 **Confidencialidad:**

Se deben adoptar medidas tendientes a proteger la información, atendiendo a la normatividad que ampara su carácter confidencial.

16 **Desempeño:**

Es relevante que la solución cuente con un desempeño óptimo para todas las acciones del *Workflow* (ingreso, administración y publicación de contenidos) y no impactar negativamente el hardware sobre el cual está instalado debido a errores en la arquitectura del diseño, por malas prácticas utilizadas en la construcción del *software.*

Es importante tener en cuenta los recursos de *hardware* e infraestructura con que cuenta el sitio web.

4.2. Errores en el sitio web

El protocolo HTTP que utilizan los sitios web para la transmisión de sus contenidos, puede generar algunos errores, para cada error que se muestra en la web hay un código de estado HTTP que es enviado por el servidor web, estos códigos de estado se encuentran en un formato de 3 dígitos y el primer dígito representa la clase del código de estado de la siguiente forma:

- **1XX:** Respuesta Informativa - Solicitud recibida, proceso continuo.
- **2XX:** Respuesta de Éxito - La acción fue recibida con éxito, comprendida y aceptada.
- **3XX:** Redirección - Se deben tomar acciones con el fin de completar la solicitud.
- **4XX:** Error del lado del cliente - La solicitud contiene una sintaxis incorrecta o no puede cumplirse.
- **5XX:** Error del lado del servidor - El servidor no pudo cumplir una posible solicitud válida.

De ellos, los más frecuentes y que deben ser atendidos a través del monitoreo son los siguientes: [7]

- **Error 301:** Movido Temporalmente, y hace referencia al redireccionamiento de dominios más conocido.
- **Error 400:** El servidor interpreta que los datos enviados a través del navegador

6 Sobre el particular se pueden consultar, entre otros, el siguiente link: https://msdn.microsoft.com/es-es/library/aa287675(v=vs.71).aspx

7 https://msdn.microsoft.com/es-es/library/aa287675(v=vs.71).aspx

se encuentran erróneos o mal escritos y que por ello, no respeta el protocolo HTTP. Por tanto, el servidor no entiende y no procesa la solicitud.

- **Error 401:** Acceso no autorizado a una página, no se ingresó el password, se da cuando la autentificación es posible pero ha fallado, o aún no ha sido provisto.
- **Error 403:** Acceso prohibido; se da cuando un usuario desea acceder a una página, pero ésta se encuentra restringida.
- **Error 404:** Recurso no encontrado. La página no existe y no puede ser mostrada. Se presenta cuando el servidor web no encuentra la página o el recurso solicitado.
- **Error 500:** El servidor falló al completar una solicitud aparentemente válida, este error puede ser causado por un problema de software.
- **Error 503:** El servicio web no está disponible, es decir que el servidor no puede responder a la petición realizada por el navegador porque está congestionado o está realizando tareas de mantenimiento.
- **Error 504:** El tiempo de respuesta del servidor excede lo normal, por lo que no responde adecuadamente a la petición del navegador y la página no se muestra.

Guía de sitios Web

Para las entidades del Distrito Capital

◇2017◇

5 Información a publicar a la luz de la normatividad

Es importante recordar a las entidades distritales que se debe cumplir con la Ley 1712 de 2014[8] y las normas que la modifiquen, sustituyan o reglamenten, incluyendo su Decreto Reglamentario 103 de 2015, compilado en el Decreto Nacional 1081 de 2015.

La normatividad aplicable determina la información mínima a publicar, siendo especialmente relevante cumplir con los requisitos de la Ley 1712 de 2014 y aquellos que impone el Ministerio TIC por medio de la Resolución 3564 de 2015[9] *"por la cual se reglamentan los artículos 2.1.1.2.1.1, 2.1.1.2.1.11, 2.1.1.2.2.2, y el parágrafo 2 del artículo 2.1.1.3.1.1 del Decreto N° 1081 de 2015"*(o aquellas que las modifiquen o sustituyan).

Dicha Resolución estableció, entre otros temas, los estándares para la publicación y divulgación de información en su Anexo 01.

8 http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201712%20DEL%2006%20DE%20MARZO%20DE%202014.pdf

9 http://www.mintic.gov.co/portal/604/articles-14476_documento.pdf

Estas regulaciones son de obligatorio cumplimiento para las diferentes entidades públicas del Distrito Capital.

5.1. Diseño del sitio web

En relación al diseño y recomendaciones para dispositivos de escritorio, se recomienda seguir los lineamientos indicados en el Manual de Imagen Institucional vigente[10] así como la Guía de Usabilidad de Gobierno en Línea establecida por el MinTIC contenida en la Resolución 3564 de 2015 o aquella que la modifique o sustituya.

5.2. Funcionalidad en dispositivos móviles

Los lineamientos presentados en este apartado corresponden a sitios web de las entidades distritales que serán visualizados en dispositivos móviles (celulares o tabletas), y no se tratará el diseño para aplicaciones nativas.

Cuando se habla de diseño móvil, se recomienda seguir el concepto de diseño responsivo, este concepto fue mencionado por primera vez por The World Wide Web Consortium[11] en el Mobile Web Best Practices 1.0[12] y se refiere a las recomendaciones con las cuales se puede lograr una mejor experiencia por parte los usuarios de la misma aplicación en diferentes dispositivos; por lo anterior, el diseño responsivo se considera una técnica mediante la cual se busca la correcta visualización de una página web en diferentes dispositivos, independientes de pixeles o densidad, conservando siempre la buena visualización de los contenidos, navegación y experiencia de usuario.

5.3. Velocidad de Carga

Se recomienda que las entidades distritales tengan en cuenta el factor de velocidad de carga para que los usuarios tengan una experiencia adecuada buscando reducir los tiempos de carga de la aplicación web.

10 La guía vigente al momento de la expedición de está guía está disponible en http://tic.bogota.gov.co/transparencia/marco-legal/normatividad/decreto-208-2016

11 https://www.w3.org/

12 https://www.w3.org/TR/mobile-bp/#OneWeb

6 Usabilidad del sitio web

Para facilitar el entendimiento y el cumplimiento de la Usabilidad según como se determina en la Estrategia Nacional de Gobierno en línea, el Ministerio de Tecnologías de la Información y las Comunicaciones, puso a disposición los Lineamientos y metodologías en Usabilidad para Gobierno en Línea.[13]

7 Accesibilidad del sitio web

De acuerdo con la Resolución 3564 de 2015 del MinTIC, se debe cumplir los lineamientos de accesibilidad establecidos a través del Marco de Referencia de Arquitectura Empresarial, disponibles en el portal de la estrategia Gobierno en Línea.

La entidad deberá verificar el cumplimiento de tales obligaciones, teniendo en cuenta que hoy la referida estrategia se remite a la norma técnica colombiana NTC 5854,[14] la cual ratifica que todos los sitios web deben ser accesibles.

13 Adicionalmente, existen herramientas académicas que pueden ser usadas como referencia, entre las cuales se encuentra https://www.nngroup.com/articles/ten-usability-heuristics/

14 http://ntc5854.accesibilidadweb.co

8 Seguridad de la información

Las entidades distritales deberán cumplir con lo previsto en el Decreto 1078 de 2015, que contiene la normatividad nacional en materia de Decreto de Gobierno en Línea (especialmente en el título IX), con el que se busca garantizar al ciudadano la calidad, disponibilidad y seguridad de los trámites con el Estado, junto con el "Manual de Gobierno en Línea".

Las entidades distritales en el marco del Sistema Integrado de Gestión y su subsistema de Gestión de Seguridad de la Información, deben adelantar y considerar acciones que incluyan, entre otras tareas, el análisis de la infraestructura tecnológica, los riesgos sobre seguridad física y del entorno, seguridad informática, el crecimiento de la capacidad de la infraestructura, incluyendo un plan para la recuperación ante desastres.

Asimismo, resulta fundamental que al implementar los esquemas de seguridad de información, se dé cumplimiento a la normatividad que regula la protección de datos personales, tal como ocurre con la Ley Estatutaria 1581 de 2012, mediante la cual se dictan disposiciones generales para la protección de datos personales y la Ley Estatutaria 1266 de 2008, mediante cual se dictan

disposiciones relativas al hábeas data financiero.

Es fundamental que para conformar los esquemas de seguridad de información, se tenga en cuenta la normatividad que resulte aplicable (incluyendo las normas reglamentarias, tal como ocurre, por ejemplo con el Decreto 1377 de 2013, que desarrolla la Ley 1581 de 2012) y las modificaciones que puedan ser introducidas a las mismas. En todo caso, cada entidad deberá definir esquemas de seguridad a la luz de sus necesidades, particularidades y vulnerabilidades.

La seguridad de los Sitios Web involucra diferentes partes de la arquitectura (Sistemas Operativos, Servidores Web, Servidor de Base de Datos, etc.). Por lo tanto, se debe hacer un análisis de riesgos y medidas preventivas y correctivas de protección del Sitio Web. Con fines ilustrativos, a continuación se presentan algunas recomendaciones que son funcionales en cualquier Sistema Gestor de Contenidos, incluyendo:

* WordPress,
* Joomla,
* Drupal,
* Magento,
* vBulletin, etc

Igualmente en servidores de publicación:

* Apache,
* NGINX,
* Servidores Windows IIS entre otros.

Las siguientes sugerencias pueden resultar pertinentes para prevenir algunas vulnerabilidades del estilo de:

* Ataques DDoS,
* Ataques de Fuerza Bruta,
* Prevención de Inyección SQL,
* Ataques URL de tipo semántico,
* Ataques de Cross-Site Scripting,
* Ejecución de Exploits de Vulnerabilidades y demás.

Para ello es importante tener en cuenta las siguientes recomendaciones de tipo general :

1. Actualizar su sitio web tan pronto como un nuevo plugin o la versión de CMS se encuentre disponible.

2. Realizar con regularidad un fortalecimiento (“hardering”) de servidor que incluya manejo de seguridad de contraseñas.

3. Hacer copias de seguridad fiables y seguras del sitio web.

4. Administrar de forma segura los Archivos de Configuración del Servidor.

5. Instalar certificados SSL. Este tipo de certificados ofrecen seguridad para los visitantes, ya que ofrecen confiabilidad para el registro de datos personales.

* SSL busca encriptar la comunicación entre el servidor web y el navegador, este cifrado es importante por una razón específica, impide que alguien pueda ser capaz de interceptar ese tráfico, conocido como un ataque de Hombre en el Medio(MITM).

* ¿Cómo saber si el sitio cuenta con este protocolo? Se puede identificar los sitios que cuentan con este protocolo de seguridad, revisando que el http contenga una s, es decir, https.

6. Certificado digital: Es también conocido como certificado electrónico, informa al usuario que se trata de un sitio confiable, ya que es generado por una entidad de servicios de certificación que asocia los datos suministrados y las identidades.

   * Es una manera de rectificar que el propietario del sitio web es una persona de confianza.

   * ¿Cómo se puede reconocer este certificado? Se puede verificar si el sitio cuenta con este certificado, si la página muestra un candado.

7. Validar los permisos de usuarios sobre los archivos.

A título simplemente enunciativo, se resalta el proyecto OWASP Top 10[15] de la fundación OWASP *(Open Web Application Security Project)*,[16] que presenta las 10 vulnerabilidades web más comunes, así como las recomendaciones para prevenir el aprovechamiento de ellas, garantizando integridad, confidencialidad y disponibilidad de la información.

Las vulnerabilidades listadas fueron extraídas y traducidas del documento OWASP Top 10 - 2017 rc1[17]

Inyección

También se conocen como inyecciones de tipo SQL, OS, XXE y LDAP. Ocurren cuando datos no confiables, son enviados a un intérprete como parte de un comando o una consulta. Un atacante puede engañar al intérprete, alterando el flujo definido de ejecución de los comandos o consultas realizadas, accediendo así a datos sin la autorización apropiada.

Las recomendaciones frente a este riesgo incluyen:

* Validar los datos de entrada a nivel del lado del cliente y del lado del servidor.

* Todos los datos de entrada deben tener los filtros apropiados y deben filtrarse de acuerdo con los tipos de datos definidos. Es decir, si se espera un valor numérico, no deberían permitirse valores como cadenas de caracteres. De ser posible, sería bueno filtrar meta-caracteres tales como, ‘’()?,.\/&#-~^””, eliminandolos de las entradas de datos cuando no sean necesarios.

* Apoyarse en las recomendaciones definidas en los artículos: OWASP SQL Injection Prevention Cheat Sheet, OWASP Query Parameterization Cheat Sheet, OWASP Command Injection Article, OWASP XXE Prevention Cheat Sheet

Pérdida de autenticación y gestión de sesiones

Las funciones de aplicación relacionadas con la autenticación y la gestión de sesiones se implementan a menudo incorrectamente, permitiendo a los atacantes comprometer contraseñas, claves o tokens de sesión, o explotar otros defectos de implementación para asumir la identidad de otros usuarios (temporalmente o permanentemente).

Las recomendaciones frente a este riesgo incluyen:

* Prevenir vulnerabilidades de tipo XSS ya que pueden ser usadas para el robo de sesiones.

* Cumplir con todos los requisitos de autenticación y gestión de sesiones definidos en el Application Security Verification Standard (ASVS) .

* Apoyarse en las recomendaciones definidas en los artículos: OWASP Authentication

15 https://www.owasp.org/index.php/Top_10_2017-Top_10

16 https://www.owasp.org/

17 https://www.owasp.org/index.php/File:OWASP_Top_10_-_2017_Release_Candidate1_English.pdf.

Cheat Sheet, OWASP Forgot Password Cheat Sheet, OWASP Password Storage Cheat Sheet , OWASP Session Management Cheat Sheet

Secuencia de Comandos en sitios cruzados (XSS)

Se presenta cuando una aplicación incluye datos no confiables sin validar o escapar, permitiendo ejecutar código javascript en los navegadores de los usuarios.

Esta vulnerabilidad se puede presentar de manera indirecta (se ejecuta sin ser almacenado el código) o indirecta (cuando el código javascript se almacena en el sitio web).

Las recomendaciones frente a este riesgo incluyen:

- Validar y filtrar los datos de entrada.
- Usar el estándar Content Security Policy para reducir el riesgo de inyección de código en javascript en los navegadores modernos.
- [18] Usar guía de prevención OWASP XSS Prevention Cheat Sheet

Control de acceso roto

Se puede aprovechar esta vulnerabilidad cuando se puede acceder a alguna funcionalidad o información no autorizada, como acceso a otras cuentas de usuario, archivos sensibles, funciones como actualizar datos de otros usuarios, entre otros.

Las recomendaciones frente a este riesgo:

- Deben añadirse validaciones ante los usuarios que intentan ejecutar acciones sobre un componente del sitio web si su rol permite ejecutar cierta acción, sólo de esta manera debería continuar el flujo de ejecución, en caso contrario no debe permitirse el acceso a este recurso.

Configuración errónea de seguridad

Las configuraciones de seguridad deben ser definidas , mantenidas e implementadas. Los servidores, las bases de datos, frameworks, CMS deben tener una configuración segura.

Las recomendaciones frente a este riesgo incluyen:

- Definir un proceso para mantener y actualizar todas las actualizaciones de seguridad de las librerías y aplicaciones necesarias para el sitio web.
- Ejecutar auditorías periódicamente para ayudar a detectar fallos de configuración. Definir y ejecutar un plan de respaldos periódico.
- Definir un plan de recuperación de los respaldos para garantizar la disponibilidad del sitio web.
- No almacenar respaldos ni archivos comprimidos (ejemplo : http://sitioweb.com/backup.zip) en la raíz del sitio que permitan extraer el código fuente o los datos privados.

Exposición de datos sensibles

Se presenta cuando la información sensible en los sitios web no está lo suficientemente protegida. Los datos sensibles deben tener una protección adicional tanto en el cifrado como en el transporte.

18 https://en.wikipedia.org/wiki/Content_Security_Policy.

Recomendaciones:

- No almacenar datos sensibles innecesariamente.
- Usar algoritmos de cifrado fuertes y estándar.
- Deshabilitar la propiedad de autocompletar en los formularios que recolectan datos sensibles.
- Transmitir los datos a través de un canal seguro.
- Apoyarse en las guías: OWASP Cryptographic Storage Cheat Sheet, OWASP Password Storage Cheat Sheet, OWASP Transport Layer Protection Cheat Sheet, OWASP Testing Guide: Chapter on SSL/TLS Testing

Insuficiente Protección ante Ataques

Se presenta por la carencia de la capacidad para detectar, prevenir y responder a ataques manuales o automatizados.
Implica la detección automática, el registro, la respuesta e incluso el bloqueo de intentos de explotación.

- Implementar un sistema de detección de intrusos.
- Implementar un Web Application Firewall (WAF)

Falsificación de petición en sitios cruzados (CSRF)

Obliga al usuario final a ejecutar acciones no deseadas sin que se de cuenta. A través de esta vulnerabilidad, un usuario envía solicitudes a la aplicación con los datos de su sesión.

Recomendaciones:

- Usar tokens de seguridad CSRF en los formularios web.
- Usar la guía de prevención OWASP CSRF Prevention Cheat Sheet.

Uso de componentes con vulnerabilidades conocidas

Sucede cuando las librerías, frameworks o componentes de software que corren como dependencias en el sitio web, tienen vulnerabilidades conocidas y pueden ser aprovechadas.

Recomendaciones:

- Tener un inventario y control de las aplicaciones de terceros que se usan en el sitio web.
- Suscribirse a los boletines de seguridad de las librerías externas instaladas para identificar oportunamente problemas y actualizaciones de seguridad.

APIs desprotegidas

Las aplicaciones modernas a menudo implican aplicaciones cliente ricas y API, como JavaScript en el Navegador y aplicaciones móviles, que se conectan a una API de algún tipo (SOAP / XML, REST / JSON, RPC, GWT, etc.).

Estas API a menudo no están protegidas y contienen numerosas vulnerabilidades.

Recomendaciones:

- Asegurarse que existe un protocolo de comunicación segura entre el cliente y las APIs.
- Validar y filtrar los parámetros que se envían a las APIs.
- Asegurarse de tener un esquema de autenticación robusto donde los usuarios tengan acceso y permiso sólo a los recursos autorizados.
- Definir y usar un estándar de autenticación como OAUTH, SAML u otros.
- Revisar la guía Web Service Security Cheat Sheet.

Adicionalmente se recomienda revisar la guía **OWASP Testing guide v4** para encontrar más recomendaciones de seguridad para aplicaciones web.

Fuentes

Naciones Unidas - Normas Uniformes sobre la Igualdad de Oportunidades Para las Personas con Discapacidad:
http://www.un.org/spanish/disabilities/standardrules.pdf

Unión Europea - Resolución del 6 de febrero de 2003 sobre *"Accesibilidad electrónica"* - Mejorar el Acceso de las Personas con Discapacidad a la Sociedad del Conocimiento.
http://travesia.mcu.es/portalnb/jspui/bitstream/10421/1237/1/ue_resol_6_feb_2003.pdf

Consejo de Derechos Humanos de Naciones Unidas - Resolución A/HRC/L-13 del 29 de junio de 2012, sobre la Promoción, Protección y Disfrute de los Derechos Humanos en Internet.
http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_20_L13.pdf

World Wide Web Consortium (W3C) - Pautas de Accesibilidad de Contenido Web 2.0, 11 de diciembre de 2008 (Siglas en inglés, Web Content Accessibility Guidelines - WCAG).
https://www.w3.org/TR/2008/REC-WCAG20-20081211/

MinTIC - Caja de Herramientas de Gobierno en Línea
http://estrategia.gobiernoenlinea.gov.co/623/w3-article-8056.html

MinTIC - Lineamientos y metodologías en Usabilidad para la Estrategia GEL.
http://estrategia.gobiernoenlinea.gov.co/623/articles-8237_guia_usabilidad.pdf

Presidencia de la República - Lineamientos Generales de la Estrategia de Gobierno en Línea
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60596#14

Constitución Política de Colombia - Artículo 20
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Gobierno de Chile - Guía Digital para la Creación de Sitios Web
http://www.guiadigital.gob.cl/guiaweb_old/guia-v2/archivos/GW2_doc_full.pdf

Gobierno de Canadá - Web Standards for the Government of Canada
http://www.tbs-sct.gc.ca/ws-nw/ROT404.asp?resid=99999&lang=eng

Créditos Institucionales

Este documento fue desarrollado por la Secretaría General de la Alcaldía Mayor de Bogotá D.C., a través de la Oficina de la Alta Consejería Distrital de Tecnologías de la Información y las Comunicaciones y sometida a revisión de la Comisión Distrital de Sistemas.

Guía de sitios Web

Para las entidades del Distrito Capital

2017

ALCALDÍA MAYOR DE BOGOTÁ D.C.

BOGOTÁ MEJOR PARA TODOS