

## PROTOCOLO DE VALIDACIÓN DE LOS SISTEMA ELECTRÓNICOS DE PUBLICACIÓN DE INFORMACIÓN FUNDAMENTAL Y DE RECEPCIÓN DE SOLICITUDES DE INFORMACIÓN

### CONSIDERANDOS

**PRIMERO.** Que en la quincuagésima tercera sesión ordinaria del Consejo del Instituto de Transparencia e Información Pública de Jalisco (ITEI), celebrada el día 13 trece de noviembre del año 2012 dos mil doce, fue aprobado el "Protocolo de Validación de los Sistemas Electrónicos de Publicación de Información Fundamental y de Recepción de Solicitudes de Información", el cual tiene como objeto proporcionar reglas, directivas o características de los procedimientos y requerimientos mínimos que los sujetos obligados deberán cubrir para la validación de sus sistemas electrónicos de publicación de información pública fundamental y/o de recepción de solicitudes de información; así como establecer la metodología de trabajo que permita al Instituto emitir dictamen procedente o improcedente sobre la validación de dichos sistemas.

**SEGUNDO.** Que en fecha 08 ocho de agosto del año 2013 dos mil trece, fue publicado en el Periódico Oficial El Estado de Jalisco, el decreto número 24450/LX/13 que expide la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, se reforman y derogan diversas disposiciones del Código Penal, del Código Electoral y de Participación Ciudadana y de la Ley de Responsabilidades de los Servidores Públicos, todos ordenamientos del Estado de Jalisco.

**TERCERO.** En la trigésimo tercera sesión ordinaria del Consejo del Instituto, celebrada el día 28 veintiocho de agosto del año 2013 dos mil trece, fue aprobado el "Acuerdo General que considera vigente la normatividad secundaria existente en lo que no se oponga a la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, hasta en tanto no se expide la nueva", mismo que a la letra dice:

PRIMERO.- Se mantiene la vigencia de la normatividad secundaria consistente en el Reglamento de la Ley de Información Pública del Estado de Jalisco y sus Municipios, el Reglamento Interno del Instituto de Transparencia e Información

Pública del Estado de Jalisco, Reglamento Marco de Información Pública para los Sujetos Obligados, así como los Lineamientos Generales emitidos por el Instituto en lo que no contravenga a las disposiciones de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

SEGUNDO.- La vigencia de la normatividad antes citada se mantendrá hasta la aprobación del Reglamento de la Ley por el Ejecutivo y la expedición de la restante normatividad derivada de la Legislación ahora vigente, acorde con su artículo 35 fracciones VIII, IX, X y XII.

**CUARTO.** Que en alcance a los Considerandos Segundo y Tercero del presente documento, se precisa necesario actualizar los fundamentos del "Protocolo de Validación de los Sistemas Electrónicos de Publicación de Información Fundamental y de Recepción de Solicitudes de Información" de conformidad a la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, a efecto de contar con los elementos que permitan al Instituto atender las solicitudes de validación de los sujetos obligados y emitir dictamen procedente o improcedente sobre la misma.

En razón de lo anterior, la Dirección de Investigación y Evaluación propone al Consejo del Instituto de Transparencia e Información Pública de Jalisco, la aprobación del siguiente:

#### ACUERDO

**ÚNICO.** Se aprueban las modificaciones al Protocolo de Validación de los Sistema Electrónicos de Publicación de Información Fundamental y de Recepción de Solicitudes de Información, para quedar como sigue:

## PROTOCOLO DE VALIDACIÓN DE LOS SISTEMA ELECTRÓNICOS DE PUBLICACIÓN DE INFORMACIÓN FUNDAMENTAL Y DE RECEPCIÓN DE SOLICITUDES DE INFORMACIÓN

### 1. GENERALIDADES

#### 1.1. OBJETO

El presente documento aprobado por el Consejo del Instituto de Transparencia e Información Pública de Jalisco (ITEI), en los términos de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios tiene como objeto proporcionar reglas, directrices y características de los procedimientos y requerimientos mínimos que los sujetos obligados deberán cubrir para la validación de sus sistemas electrónicos de publicación de información pública fundamental y/o de recepción de solicitudes de información; así como establecer la metodología de trabajo que permita al Instituto emitir dictamen procedente o improcedente (con las observaciones correspondientes en su caso), sobre la validación de dichos sistemas.

#### 1.2. FUNDAMENTO Y ALCANCE

La Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, vigente a partir del 09 nueve de agosto del año 2013 dos mil trece, establece en los artículos 35, numeral 1, fracción XV y 41, numeral 1. Fracción VIII como atribución del Instituto y del Consejo del Instituto respectivamente, la de validar los sistemas electrónicos de publicación de información pública fundamental y los sistemas de recepción de solicitudes de información pública de libre acceso, de los sujetos obligados.

En la Sesión Extraordinaria del Consejo del Instituto, de fecha 12 doce de agosto del año 2013 dos mil trece, se aprobó el "Acuerdo General del Consejo del ITEI respecto de la Publicación y Actualización de la Información Fundamental" que a la letra dice:

PRIMERO.- Los Sujetos Obligados deben orientar y facilitar a los particulares el acceso a la información pública fundamental, incluidas las fuentes directas cuando sea posible, señalada por los artículos 8 a 16 de la Ley vigente, según el caso, en tanto se realizan las adecuaciones formales y actualizaciones materiales en el término de un mes contado a partir de la entrada en vigor de la legislación en cita.

SEGUNDO.- A fin de cumplir con lo dispuesto en el numeral 25, fracción VI de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, los Sujetos Obligados podrán publicar permanentemente en otros medios de fácil acceso y comprensión para la población, la información fundamental que les corresponda, en tanto se realizan las adecuaciones formales y actualizaciones materiales a los portales web, y luego proceder a su inmediata actualización que por disposición normativa es cuando menos una vez al mes.



En la trigésimo tercera sesión ordinaria del Consejo del Instituto, celebrada el día 28 veintiocho de agosto del año 2013 dos mil trece, fue aprobado el "Acuerdo General que considera vigente la normatividad secundaria existente en lo que no se oponga a la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, hasta en tanto no se expide la nueva", mismo que a la letra dice:



PRIMERO.- Se mantiene la vigencia de la normatividad secundaria consistente en el Reglamento de la Ley de Información Pública del Estado de Jalisco y sus Municipios, el Reglamento Interno del Instituto de Transparencia e Información Pública del Estado de Jalisco, Reglamento Marco de Información Pública para los Sujetos Obligados, así como los Lineamientos Generales emitidos por el Instituto en lo que no contravenga a las disposiciones de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.



SEGUNDO.- La vigencia de la normatividad antes citada se mantendrá hasta la aprobación del Reglamento de la Ley por el Ejecutivo y la expedición de la restante normatividad derivada de la Legislación ahora vigente, acorde con su artículo 35 fracciones VIII, IX, X y XII.

De conformidad a lo anterior, el Reglamento de la Ley de Información Pública del Estado de Jalisco y sus Municipios, establece en el Capítulo III, Sección Primera, artículos 28 al 35, el procedimiento que deberán observar los sujetos obligados y el Instituto en cuanto a la solicitud de validación y dictamen de la procedencia de la solicitud.

Por último, el Reglamento Interno del Instituto de Transparencia e Información Pública del Estado de Jalisco, establece en el artículo 65 el procedimiento mediante el cual se dictaminará la procedencia de las solicitudes de validación.

El presente protocolo se ejecutará en todos aquellos casos en que los sujetos obligados soliciten la validación de su sistema de publicación de información, y/o del sistema de recepción de solicitudes de información (independientemente si se trata de un sistema de recepción de solicitudes nuevo o se actualiza alguno ya existente).

En lo que refiere a la información pública fundamental que es la materia prima de los Sistemas Electrónicos de Publicación de Información Fundamental, el artículo 3, numeral 2, fracción I de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, establece que "... *Información pública de libre acceso, que es la no considerada como protegida, cuyo acceso al público es permanente, libre, fácil, gratuito y expedito...*". Además, el mismo dispositivo define que: "*Información pública fundamental, que es la información pública de libre acceso que debe publicarse y difundirse de manera universal, permanente, actualizada y, en el caso de la información electrónica, a través de formatos amigables para el ciudadano, por ministerio de ley, sin que se requiera solicitud de parte interesada...*"

Por su parte el artículo 35 del Reglamento de la Ley de Información Pública del Estado de Jalisco y sus Municipios, señala las características que serán evaluadas respecto de la publicación de la información fundamental a través de los sistemas electrónicos de los sujetos obligados, siendo éstas:

*"... I. Publicidad: si se encuentra o no la información publicada, considerando las especificaciones marcadas en los Lineamientos Generales para la Publicación y Actualización de Información Fundamental; II. Vigencia: que la información publicada corresponda a los periodos establecidos en la Ley y en los Lineamientos Generales para la Publicación y Actualización de Información Fundamental; y III. Accesibilidad: que la información sea sencilla de explorar y de fácil localización."*

Además, los Lineamientos Generales para la Publicación y Actualización de la Información Fundamental, establecen en su lineamiento cuarto, los criterios generales que deberán observar todos los sujetos obligados para la publicación de la información fundamental.

Los sistemas electrónicos de publicación de información pública fundamental, independientemente de que cuenten o no con la validación del Instituto, podrán ser sujetos de un recurso de transparencia, de evaluación y/o de investigaciones e inspecciones cuando el Consejo del Instituto así lo determine, conforme a los procedimientos establecidos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios y el Reglamento respectivo.

### 1.3. GLOSARIO

**Criterios:** Los Criterios Generales para la Publicación y Actualización de la Información Fundamental que haya emitido el sujeto obligado;

**Instituto:** Instituto de Transparencia e Información Pública de Jalisco;

**Ley:** La Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios;

**Lineamientos:** Los Lineamientos Generales para la Publicación y Actualización de la Información Fundamental;

**Protocolo:** El Protocolo de Validación de los Sistema Electrónicos de Publicación de Información Fundamental y de Recepción de Solicitudes de Información;

**Reglamento:** El Reglamento de la Ley de Información Pública del Estado de Jalisco y sus Municipios;

**Reglamento Interior:** El Reglamento Interior del Instituto de Transparencia e Información Pública del Estado de Jalisco;

**Sistema Electrónico de Publicación de Información Fundamental:** Los sistemas electrónicos que utilicen los sujetos obligados para hacer pública su información fundamental;

**Sistema Electrónico de Recepción de Solicitudes de Información:** Los sistemas electrónicos que los sujetos obligados dispongan para recibir, tramitar y dar respuesta a las solicitudes de información;

**Solicitud:** Solicitud de información pública;

**Sujeto(s) Obligado(s):** Los previstos en el artículo 24 de la Ley;

**UT:** Unidad de Transparencia de los sujetos obligados o quien haga sus veces;

## 2. SOBRE LAS VALIDACIONES

### 2.1. ¿QUÉ ES VALIDAR?

Es realizar un conjunto de pruebas para conocer y comprobar que los elementos y procesos de los sistemas electrónicos de publicación de información pública fundamental y de los sistemas de recepción de solicitudes de información pública, cumplen las especificaciones de la Ley y las especificaciones técnicas mínimas indispensables para el cumplimiento del fin previsto que establece el Instituto.

### 2.2. ¿POR QUÉ SE LLEVA A CABO LA VALIDACIÓN?

La Ley Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, establece en los artículos 35, numeral 1, fracción XV y 41, numeral 1. Fracción VIII como atribución del Instituto y del Consejo del Instituto respectivamente, la de validar los sistemas electrónicos que utilicen los sujetos obligados para hacer pública su información, principalmente la información pública fundamental; así como los sistemas electrónicos para recibir, tramitar y dar respuesta a las solicitudes de información.

Las validaciones pretenden ser un reconocimiento al trabajo de los sujetos obligados que se esfuercen por facilitar a la sociedad, el acceso a la información que generan.

### 2.3. ¿QUÉ SE VALIDA?

Serán sujetos de validación todos los sistemas electrónicos que utilicen los sujetos obligados para hacer pública su información fundamental, es decir, las páginas de internet u otros medios electrónicos mediante los cuales los sujetos obligados pongan a disposición de cualquier persona por medio de Internet y sin restricción alguna, la información pública fundamental a que están obligados por la Ley, así como los sistemas electrónicos que dispongan los sujetos obligados para recibir, tramitar y dar respuesta a las solicitudes de información.

En el caso del Sistema Infomex Jalisco, que es el sistema electrónico para la tramitación y respuesta de las solicitudes de información que administra el Instituto y pone a disposición de los sujetos obligados, éste también podrá ser sujeto a validación, para dar certeza a los sujetos obligados y usuarios de que el Sistema cumple con todos los estándares que el mismo Instituto establece.

### 2.4. ¿PARA QUÉ SE VALIDA?

El Instituto llevará a cabo la validación de los sistemas electrónicos de publicación de información pública fundamental y de recepción de solicitudes de información, con efectos parecidos a una certificación sobre la observancia de la Ley, calidad, eficiencia, rapidez, sencillez, claridad, accesibilidad, usabilidad, y demás cualidades deseables de los sistemas.

No debe entenderse la validación como requisito indispensable para poder operar dichos sistemas (ya sea para la publicación de información o para dar respuesta a las solicitudes). La validación sólo es una forma de otorgar un reconocimiento al sujeto obligado que se esfuerce por cubrir ciertos estándares de calidad en la forma en cómo publica su información y atiende las solicitudes de transparencia.

La validación del Instituto debe entenderse como una certificación, más que como una autorización para que funcionen dichos sistemas. En ese sentido es preferible que el sujeto obligado opere con un sistema con deficiencias que puedan irse corrigiendo progresivamente, que eliminar su operación por no cumplir con los requerimientos de la validación. El Instituto deberá buscar la forma de proponer mejoras a los sistemas de los sujetos obligados mediante el proceso de validación, más que impedir la utilización de los sistemas que no aprueben la validación.

### 2.5. ¿CUÁNDO Y CÓMO SE LLEVA A CABO LA VALIDACIÓN?

La validación de los sistemas electrónicos de publicación de información pública y de los sistemas de recepción de solicitudes de información, se llevará a cabo previa petición del sujeto obligado.

Corresponde al Consejo del Instituto, bajo el procedimiento que se establece para tal caso en el Reglamento de la Ley, así como los criterios y requerimientos que se establecen en el presente protocolo, aprobar o no la procedencia de la validación y, en tal caso, remitir las observaciones que considere pertinentes sobre los sistemas.

### 3. PROCEDIMIENTO DE SOLICITUD Y DICTAMEN DE LA VALIDACIÓN DE LOS SISTEMAS ELECTRÓNICOS DE PUBLICACIÓN DE INFORMACIÓN Y DE RECEPCIÓN DE SOLICITUDES DE INFORMACIÓN

- I. Los sujetos obligados que cuenten con sistema electrónico de publicación de información fundamental podrán en cualquier momento solicitar al Instituto la validación de sus sistemas.
- II. A efecto de obtener la validación del sistemas de publicación de información fundamental y/o del sistema de recepción de solicitudes de información, el sujeto obligado por conducto de su titular o de la Unidad de Transparencia, hará la petición dirigida al Consejo, por escrito y deberá

contener al menos con los requisitos que señala el artículo 30 del Reglamento:

- a) Nombre del sujeto obligado;
- b) Nombre y cargo del Administrador del Sistema;
- c) Dirección electrónica o localización del sistema electrónico de publicación de información fundamental y/o del sistema de recepción de solicitudes de información
- d) Firma del Titular de la Unidad de Transparencia

III. El procedimiento de solicitud y dictamen de la validación se llevará a cabo bajo los términos establecidos para tal efecto en los artículos 35, numeral 1, fracción XV y 41, numeral 1. Fracción VIII de la Ley, artículos 28 al 35 del Reglamento de la Ley y artículos 44 y 65 del Reglamento Interno.

#### 4. VALIDACIÓN DE LOS SISTEMAS ELECTRÓNICOS DE PUBLICACIÓN DE INFORMACIÓN FUNDAMENTAL

##### 4.1. PRINCIPIOS GENERALES DEL PROCEDIMIENTO DE VALIDACIÓN

La validación de los sistemas electrónicos de publicación de información fundamental, se llevará a cabo bajo los siguientes principios generales:

- Se verificará el cumplimiento de los requerimientos establecidos en el apartado 4.2 del presente protocolo;
- En su caso, se podrá sustentar mediante la impresión de pantallas (o levantamiento de imágenes o fotografías, o cualquier otra prueba que se estime pertinente) el cumplimiento o incumplimiento de estos requerimientos. En los casos de incumplimiento, se fundará y motivará las razones por las que no se considera cumplido el requisito, y se podrán realizar todas las observaciones que se estime pertinente. Estas observaciones serán parte integral del expediente de validación del sistema en cuestión.

#### 4.2. REQUISITOS PARA LA VALIDACIÓN

Las características que tomará en cuenta el Instituto para la validación se distribuyen en tres rubros temáticos:

##### I DE UNIVERSALIDAD



Este rubro integra los requerimientos relativos a los contenidos o de la información que será proporcionada por el sistema electrónico de publicación de información. Cualquier persona conectada a Internet, sin importar el lugar donde se encuentre, ni el sujeto obligado del cual desee consultar información pública fundamental, tiene la posibilidad de hacerlo, puesto que se identifica de manera clara el apartado o sección donde ésta se publica; además, cualquiera que sea el sujeto obligado que se consulte, la información fundamental guarda el orden y el título de las fracciones e incisos que refieren a la información fundamental en la Ley, por lo que la estructura de la información fundamental de libre acceso es común a todos ellos.

Los requerimientos que se considerarán dentro de este rubro serán:

- a. Establecer de forma clara, en la página de inicio el apartado o sección donde se publica la información fundamental, de manera que se permita al usuario identificar fácilmente que en él se encuentra publicada la información fundamental, pudiendo titularse "Transparencia", "Acceso a la Información" o "Información Pública";
- b. Organizar la información atendiendo al orden y el título de las fracciones e incisos que refieren a la información fundamental en la Ley;

En favor de una mejora continua y de retroalimentación hacia los sujetos obligados, el Instituto podrá emitir observaciones y recomendaciones respecto de la publicación de su información fundamental.

## II DE PERMANENCIA Y ACTUALIZACIÓN

Se verificará en este rubro, que el sistema electrónico de publicación de información, posibilite la permanencia y la actualización de la información, así como el acceso libre, fácil, gratuito y expedito a la misma, en los términos siguientes:

- a. **Permanencia:** el Sistema garantiza la permanencia de la información pública fundamental por ciertos periodos de tiempo, permite y tiene la capacidad de soportar el almacenamiento de la información que generan, posean o administren los sujetos obligados.
- b. **Actualización:** El Sistema permite y tiene la capacidad de soportar el almacenamiento de nueva información que generen, posean o administren los sujetos obligados, por lo cual de forma regular se podrá contar con información vigente.
- c. **Acceso libre, fácil, gratuito y expedito:** Se refiere al conjunto de técnicas para categorizar, buscar y acceder a la información que se encuentra en el sistema. El Sujeto Obligado permitirá el acceso a su información utilizando para ello el menor número de recursos (por ejemplo: ingresar al portal web, ingresar al apartado de "Transparencia", "Acceso a la Información" o "Información Pública, se accede a la información pública fundamental); en este sentido, queda prohibido solicitar cualquier tipo de registro o requerir cualquier información para acceder a la información pública fundamental.

Si se cumple la condición de que la información pública sea de acceso libre y fácil se cumplen las condiciones de gratuidad y expeditos, dado que no media solicitud de ningún tipo para que cualquier persona acceda de forma inmediata a la información y esté en condiciones de consultar e incluso imprimirla si así lo desea.

El cumplimiento de los requerimientos de este apartado no exime al Sujeto Obligado de posibles observaciones, recomendaciones y en su caso sanciones con motivo de un recurso de transparencia interpuesto en su contra por la falta de publicación y actualización de alguna información, tampoco se podrá tomar como cumplimiento a los recursos o procedimientos que en un momento dado se encuentre en proceso ante el Instituto.

### III DE ACCESIBILIDAD Y USABILIDAD

La accesibilidad consiste en la capacidad de un sitio web de ser entendido en su totalidad y de ingresar a la información que ahí se encuentra publicada, por todos los usuarios independientemente de las condiciones físicas y/o técnicas en las que se acceda a Internet, e incluso, de las limitaciones propias de las personas como conocimientos o experiencia en el uso de estos sistemas electrónicos.

La accesibilidad debe ser entendida como 'parte de', y al mismo tiempo 'requisito para', la usabilidad.<sup>1</sup>

La usabilidad, es la disciplina que estudia la forma de diseñar sitios web para que los usuarios puedan interactuar con ellos de la forma más fácil, cómoda e intuitiva posible.

Los requerimientos que se considerarán dentro de este rubro serán:

- a. Diseño compatible con diferentes navegadores y resoluciones de pantalla. Debe ser posible el acceso a las páginas del sitio web, utilizando cualquiera de las versiones de los navegadores de uso más generalizado entre los usuarios, como mínimo: Internet Explorer, Chrome, Firefox y Safari.

<sup>1</sup> Qué es la accesibilidad Web: <http://www.nosolousabilidad.com/articulos/accesibilidad.htm> Consultado: 20/05/12

- b. Existencia de versiones alternativas de visualización para los sitios web con presentaciones Flash, que pueden dificultar la carga y legibilidad de los contenidos para aquellos usuarios sin condiciones técnicas en su ordenador para desarrollar ese tipo de aplicaciones.
- c. La información deberá ser presentada preferentemente, en formatos y versiones de uso generalizado, éstos pueden ser: archivos PDF o de Microsoft Office (archivos con extensión .doc. .xls y .ppt).
- d. Posibilidad de imprimir y visualizar correctamente la impresión de los contenidos del sitio.
- e. Establecer, en la medida de lo posible, la menor cantidad de "clicks" para acceder a la información fundamental que busca el usuario;
- f. Establecer un vínculo que permita acceder directamente a los documentos íntegros, cuando otras disposiciones legales obliguen a la publicación de la información y ésta ya se encuentre disponible;
- g. Implementar, preferentemente, criterios de búsqueda avanzada que permitan localizar la información;

Una vez valorados los rubros y requerimientos establecidos en este apartado, la Dirección de Investigación y Evaluación elaborará y dirigirá al Consejo, por conducto del Secretario Ejecutivo el dictamen, señalando el cumplimiento y/o incumplimiento de los requerimientos, así como las observaciones que de esta valoración se deriven.

## 5. VALIDACIÓN DE LOS SISTEMAS ELECTRÓNICOS DE RECEPCIÓN DE SOLICITUDES DE INFORMACIÓN

### 5.1. PRINCIPIOS GENERALES DEL PROCEDIMIENTO DE VALIDACIÓN

El conjunto de políticas que en este apartado se describen, tienen como finalidad servir de guía para evaluar por una parte la observancia de los procedimientos de recepción, tramitación y resolución de las solicitudes de información presentadas

a través de los sistemas electrónicos, que para tal efecto, elaboren los sujetos obligados, a fin de que éstos se substancien bajo los lineamientos que dicta la Ley y el Reglamento; y por otra la calidad, eficiencia, sencillez, usabilidad, seguridad y demás cualidades deseables éstos sistemas. Para ello, el Instituto a través de la Dirección de Investigación y Evaluación:

- Requerirá al sujeto obligado, remitir la documentación técnica del diseño y análisis del sistema para su validación.
- Realizará pruebas al sistema, consistentes en el registro de un usuario nuevo, el ingreso, tramitación y resolución del número de solicitudes de información que se consideren necesarias, a efectos de verificar si se cumple o no con lo establecido en el Capítulo III del Título Quinto de la Ley y en el Capítulo IV, Sección Tercera del Reglamento, sobre el procedimiento de acceso a la información.
- Verificará que los sistemas cuenten con documentación técnica sobre el desarrollo del sistema, así como los manuales para facilitar la operación y uso del mismo.
- En cada uno de los casos, sustentará el cumplimiento o incumplimiento de los requisitos con las pruebas que se estime pertinente. En los casos de incumplimiento se fundará y motivará las razones por las que no se considera cumplido el requisito o proceso y se podrán realizar todas las observaciones que se estimen pertinentes. Estas observaciones serán parte integral del expediente de validación del sistema en cuestión.

## 5.2. POLÍTICAS DE DISEÑO DESEABLES PARA LOS SISTEMAS ELECTRÓNICOS PARA LA RECEPCIÓN DE SOLICITUDES DE INFORMACIÓN

El proceso de solicitud, tramitación y resolución de las solicitudes de información deberá apegarse a lo que se establece en la Ley y el Reglamento, y para asegurar un mínimo de calidad en los sistemas que se desarrollen para recibir, contestar y administrar solicitudes electrónicas de información pública, se dictan las siguientes políticas.

## 5.2.1. DE LOS ELEMENTOS DE DISEÑO GENERALES

5.2.1.1. Los sistemas de recepción de solicitudes de información pública deben ser fieles en su funcionamiento a los procedimientos establecidos en la Ley y el Reglamento.

5.2.1.2. El diseño general de las páginas electrónicas para las solicitudes vía electrónica, debe propiciar el uso de las tecnologías de información, tomando en cuenta que el uso de estos sistemas debe ser adoptado por los usuarios cotidianos y los no usuarios de computadoras.

5.2.1.3. Las páginas desarrolladas con el objetivo de gestionar las solicitudes de información, deben de cubrir en lo posible los aspectos de diseño, como si fuera a ser desarrollada una página electrónica para comercio electrónico o cualquier otro uso comercial.

5.2.1.4. Los colores utilizados: en la actualidad aún se utilizan monitores limitados en colores, por lo que se debe tener en cuenta la selección de colores en el diseño de las páginas; además, por cuestiones de velocidad, algunos navegadores se limitan a mostrar 56 colores.

5.2.1.5. La accesibilidad: la aplicación Web desarrollada debe garantizar que puede ser accedida y usada por todos los usuarios potenciales, independientemente de las limitaciones propias del individuo o de las derivadas del contexto de uso.

5.2.1.6. Asimismo debemos hacer hincapié en la facilidad de uso que debe tener la página; no obstante, no podemos suprimir el proceso de registro de usuarios (nombre de usuario y contraseña).

## 5.2.2. DE LOS ELEMENTOS DE LA PÁGINA DE INICIO

Para que las solicitudes de información sean correctamente recibidas por los sujetos obligados, el sistema electrónico de recepción de solicitudes de información, deberá contener al menos los siguientes nodos o elementos:

5.2.2.1. Una entrada para darse de alta con un nombre de usuario y una contraseña y una entrada para dar acceso a los usuarios registrados donde se requiera:

- a. Usuario
- b. Contraseña

5.2.2.2. Una entrada para elaborar las solicitudes de información, que contenga como elementos mínimos:

5.2.2.2.1. Obligatorios.

- a. De identificación del solicitante:
  - i. Nombre del solicitante y/o autorizados;
  - ii. Domicilio;
  - iii. Correo Electrónico;
- b. De la solicitud de información:
  - i. Nombre del sujeto obligado al que va dirigida;
  - ii. Información solicitada: una descripción que contenga los elementos necesarios para identificarla.
  - iii. Medio de acceso:
    - Consulta directa de documentos;
    - Reproducción de documentos;
    - Elaboración de informes específicos; o
    - Combinación de las anteriores.
  - iv. Forma de Acceso:
    - Consulta en la página electrónica;

- Medio electrónico o magnético;
- Copias simples;
- Correo electrónico;
- Copias certificadas o;
- Consulta directa en las oficinas del sujeto obligado;

#### 5.2.2.2.2. Datos Estadísticos Opcionales:<sup>2</sup>

- i. Sexo;
- ii. Edad;
- iii. Nivel Educativo;
- iv. Ocupación;
- v. Pregunta 1 ¿Solicita información por primera vez? y
- vi. Pregunta 2 ¿Cómo supo que tiene el derecho de acceso a la información pública?

5.2.2.3. Una entrada para dar seguimiento a las solicitudes de información. Debe contener al menos, una pizarra donde se puedan visualizar los datos básicos de cada solicitud:

- a. Folio de la solicitud;
- b. Fecha de solicitud;
- c. Información solicitada;
- d. Respuesta a la solicitud;

5.2.2.4. Una entrada de estadísticas de las solicitudes.<sup>3</sup> Es ideal que este nodo genere estadísticas del tipo siguiente:

<sup>2</sup> El sistema puede contener o no este módulo, la falta del mismo no constituye un incumplimiento de los requisitos para la validación del sistema

<sup>3</sup> El sistema puede contener o no este módulo, la falta del mismo no constituye un incumplimiento de los requisitos para la validación del sistema

- a. Solicitudes hechas agrupadas por tipo de sexo;
- b. Solicitudes hechas agrupadas por rangos de edades;
- c. Solicitudes hechas agrupadas por nivel educativo;
- d. Solicitudes hechas agrupadas por ocupación;
- e. Solicitudes hechas agrupadas por tipo de respuesta a la solicitud.

5.2.2.5. Una entrada para ver un manual de ayuda para el usuario.

5.2.2.6. Una entrada para solicitar ayuda vía electrónica (correo electrónico o ayuda en línea).



### 5.2.3. POLÍTICA DE DISPONIBILIDAD

Los sistemas electrónicos de recepción de solicitudes de información deberán estar disponibles las 24 horas del día, los 7 días a la semana.

Cualquier persona que elabore una solicitud de información podrá consultar el estatus de ésta en cualquier horario, es decir, durante las veinticuatro horas y los siete días de la semana, por lo que no habrá momento en que se le impida al solicitante conocer el estatus de su solicitud.



### 5.2.4. POLÍTICA DE PROCESAMIENTO DE SOLICITUDES

Las solicitudes recibidas fuera del horario de labores (en caso de que el sistema del sujeto obligado lo permita) se procesarán al día hábil siguiente. El comprobante de la solicitud deberá contener la fecha del siguiente día laboral.

Sin obstaculizar el derecho a la información, la solicitud de información que se realice fuera del horario de labores del sujeto obligado, se le tendrá por recibido con fecha u hora siguiente que sea hábil para el sujeto obligado, siendo hasta este momento cuando comienza a contar el término de Ley para el otorgamiento de la respuesta al solicitante.

### 5.2.5. DE LA INFORMACIÓN SOLICITADA

La información que se describa en esta sección será esencial para entender y localizar ágilmente la información solicitada, por lo que será necesario considerar un área lo suficientemente amplia para que el solicitante pueda describir detalladamente su petición, o permitir al usuario adjuntar el archivo que contenga los datos de su solicitud.

### 5.2.6. DE LOS ELEMENTOS DE SEGURIDAD DEL SISTEMA<sup>ii</sup>

#### 5.2.6.1. ACCESO AL SISTEMA DE RECEPCIÓN DE SOLICITUDES DE INFORMACIÓN

Debe contar con un sistema de acceso basado en nombres de usuario y contraseña correspondientes para garantizar que los solicitantes que cuenten con ello, accedan a la información que les corresponde. Se debe considerar que los usuarios que decidan no registrarse tengan derecho a visualizar los elementos públicos, tales como la pizarra de seguimiento a solicitudes, y las estadísticas expuestas anteriormente en las secciones 5.2.2.3 y 5.2.2.4 del presente documento.

#### 5.2.6.2. NÚMERO DE CASO

Se debe contar con un sistema para la generación de un número consecutivo, único e irrepetible (folio) para asignarlo a cada solicitud, de manera que ese número identifique esa solicitud, y sólo ésa.

#### 5.2.6.3. CÓDIGOS DE SEGURIDAD EN EL DOCUMENTO DE ACUSE DE RECIBO

Aunque el objetivo de las políticas de seguridad es mantener las tres características de la información: confidencialidad, integridad y disponibilidad<sup>iii</sup> en un ambiente donde toda la información es pública, estas tres características adquieren una connotación diferente:

- a. La confidencialidad se refiere, en este contexto, a la autenticidad de la información, que como mencionaremos

más adelante, es avalada por un código generado por un sistema criptográfico.

- b. La actualización o mejoras al sistema no deberán repercutir en las solicitudes de información y/o acuses de recibo que el mismo sistema haya generado con anterioridad; estas actualizaciones o mejoras deberán ser efectivas a partir de su implementación. Con ello se pretende evitar la duplicidad de documentos respecto de cualquier solicitud de información o acuse.
- c. La disponibilidad es total para toda la comunidad que esté interesada; deberá ser suficiente proporcionar los datos del número de caso, para conocer la información general del mismo.
- d. La función tradicional de las firmas rubricadas, es garantizar la autoría o acuerdo en el contenido de un documento<sup>iv</sup>. En un ambiente electrónico de intercambio de datos, estas firmas son remplazadas por las firmas numéricas, públicas y privadas, con un esquema explicado en el siguiente párrafo.

Basándose en lo anterior, para validar la autenticidad de las solicitudes ingresadas en las páginas electrónicas de los sujetos obligados, se deben considerar dos puntos obligatorios en los cuales se deben generar firmas electrónicas:

- a. En el momento de generar el acuse de recibo, se debe contar con un sistema criptográfico<sup>v</sup> para generar la firma electrónica del acuse.
- b. .En el mismo sentido, se debe contar con una firma pública para "confiar" en la firma electrónica generada en el paso anterior, y a su vez se debe de contar con una

"función de control "para garantizar que la información contenida en el documento no ha sido modificada desde que fue ingresada la primera vez.<sup>vi</sup>

#### 5.2.6.4. FIRMA ELECTRÓNICA DE RECIBIDO

Para la generación y recepción de la firma de recibido, se debe implementar un sistema electrónico que logre los siguientes objetivos:

- a. Que los usuarios registrados en la página electrónica puedan "firmar" electrónicamente la entrega de la información solicitada, análogamente a como se realiza cuando se entrega de forma personal.
- b. Que los usuarios reciban en su buzón de correo electrónico notificaciones electrónicas, análogamente al proceso de notificar personalmente al solicitante por parte del sujeto obligado, y que el sistema electrónico de la página asegure que efectivamente el solicitante indicado recibió la notificación.

Para lograr lo anterior, se debe contar con un sistema electrónico que realice lo siguiente:

5.2.6.5. Para firmar de recibido en la página electrónica: Debe existir un módulo electrónico que permita que cuando el usuario ingrese al sistema introduciendo su usuario y contraseña, enseguida le notifique que tiene un mensaje, instruyéndole la forma en que se puede acceder a la información, según sea el caso de su elección (véase punto 5.2.2.2). Dentro de estas instrucciones, debe estar contemplado un proceso tal (un hipervínculo), que cuando el usuario haga clic para visualizar la información, el sistema confirme, por medio del usuario, el número de caso y los dos códigos mencionados en el paso 5.6.3.2. del presente protocolo, que la información ha sido recibida por el usuario correcto.

5.2.6.6. Para firmar de recibido mediante el envío de un correo electrónico al buzón del solicitante: debe existir un módulo electrónico que envíe un correo al solicitante comunicándole que su solicitud de información ha sido resuelta favorablemente, instruyéndole la forma en que puede acceder a la información según sea el caso de su elección (véase punto 5.2.2.2); dentro de estas instrucciones, debe estar contemplado un proceso tal (un hipervínculo), que cuando el usuario haga clic para visualizar la información, el sistema confirme, por medio del usuario, el número de caso, y los dos códigos mencionados en el paso 5.6.3.2. del presente protocolo, que la información ha sido recibida por el usuario correcto.

5.2.6.7. Para notificar por medio de correo electrónico: debe existir un módulo electrónico que envíe un correo al solicitante comunicándole que le ha sido enviada una notificación (aclaración de solicitud, notificación de negativa, aclaraciones), instruyéndole la forma en que puede acceder a la información de la notificación según sea el caso; dentro de estas instrucciones, debe estar contemplado un proceso tal (un hipervínculo), que cuando el usuario haga clic para visualizar la información, el sistema confirme, por medio del usuario, el número de caso, y los dos mencionados en el paso 5.6.3.2. del presente protocolo, que la notificación ha sido recibida por el usuario correcto.

### 5.2.7. DE LOS MEDIOS DE ALMACENAMIENTO DE LA INFORMACIÓN

Se deberá contar con algún método de respaldo mínimo, consistente en servidores, discos duros, discos compactos, o cintas de respaldo que garanticen la seguridad y la integridad de los datos referentes a las solicitudes, tanto los datos del solicitante tales como nombre, domicilio, correo electrónico, los datos opcionales (véase punto 5.2.2), como los datos mismos de la información solicitada, de manera que sea posible recuperarla en cualquier momento tanto

por el administrador del sistema, como por la comunidad de usuarios en general a través de la consulta o seguimiento público (véase punto 5.2.2.3).

Los medios de almacenamiento de la información deberán garantizar la seguridad y resguardo de los datos personales derivados del procesamiento de una solicitud de información (nombre, domicilio, correo electrónico, etc.), adoptando las medidas físicas, técnicas y administrativas necesarias para garantizar la integridad, confidencialidad y disponibilidad de los datos personales para evitar su alteración, pérdida, transmisión y acceso no autorizado.

### 5.3. REQUISITOS PARA LA VALIDACIÓN

En los apartados anteriores se establecen los elementos que de manera deseable podrían contener los sistemas electrónicos de tramitación de solicitudes de información, no obstante, para efectos de otorgar la validación los requerimientos que deberán cumplir los sistemas de los sujetos obligados se distribuyen en tres rubros temáticos:

#### I ELEMENTOS DEL SISTEMA

El sistema de validación deberá contener por lo menos los siguientes elementos:

1. Un elemento, ventana o interfaz<sup>4</sup> para dar acceso a los usuarios registrados y/o en su caso permita registrarse como nuevo usuario. Este elemento deberá permitir ingresar con un nombre único de usuario y una contraseña para entrar al sistema y dar seguimiento a las solicitudes de información presentadas por este medio. (Véase punto número 5.2.2.1 y 5.2.6.1)

<sup>4</sup> Se refiere al medio con que el usuario puede comunicarse con una máquina, un equipo o una computadora, y comprende todos los puntos de contacto entre el usuario y el equipo. Incluyen elementos como menús, ventanas, y sonidos que la computadora hace, y en general, todos aquellos canales por los cuales se permite la comunicación entre el ser humano y la computadora.

2. Un elemento, ventana o interfaz para elaborar las solicitudes de información que cumpla con todos los requisitos establecidos en la Ley y el Reglamento (Véase punto número 5.2.2.2)
3. El sistema deberá generar un comprobante de la presentación de la solicitud con un número único e irrepetible (véase punto número 5.2.6.2)
4. Un elemento, ventana o interfaz para seguimiento y consulta del historial de solicitudes de información recién ingresadas y las que se encuentren en trámite (véase punto número 5.2.2.3)
5. El sistema deberá generar las notificaciones y acuses pertinentes para garantizar el derecho al acceso de información del solicitante y el procedimiento que para tales efectos se establece en la Ley de la materia. (véase punto número 5.2.6.4)
6. El sistema deberá establecer los mecanismos que considere necesarios y pertinentes para garantizar la seguridad y protección de la información y los datos del solicitante (véase punto número 5.2.7)
7. Permitir la consulta de las solicitudes de información durante las veinticuatro horas, los siete días de la semana, (independientemente del horario de atención del sujeto obligado) para que no exista ninguna limitante al derecho de acceso a la información pública. (véase punto número 5.2.3 y 5.2.4)
8. El sistema deberá apegarse en el proceso de acceso a la información en los procedimientos que establece la Ley, en el Capítulo III del Título Quinto y en el Capítulo IV, Sección Tercera del Reglamento, sobre el procedimiento de acceso a la información.
9. El sistema deberá contar con métodos de respaldo mínimos, como servidores, discos duros, discos compactos, o cintas de respaldo que garanticen la seguridad, protección e integridad de los datos

relacionados a los usuarios registrados y, asimismo, deberá garantizar el almacenamiento de la información sobre las solicitudes de información que ingresen al sistema (véase punto número 5.2.7).

## II SOBRE EL PROCEDIMIENTO DE ACCESO A INFORMACIÓN

Para el cumplimiento de este apartado, los sistemas deberán observar los procedimientos que se establecen en el Capítulo III del Título Quinto de la Ley y en el Capítulo IV, Sección Tercera del Reglamento, sobre el procedimiento de acceso a la información en la siguiente forma:

1. El interesado entra a la página electrónica donde se encuentra hospedado el sistema electrónico y deberá capturar la información siguiente:

1.1. De acceso :

- i. Usuario
- ii. Contraseña

1.2. Personal

- i. Nombre del solicitante y/o autorizados
- ii. Domicilio para recibir notificaciones; y/o
- iii. Correo Electrónico

1.3. De la solicitud de información

- i. Nombre del Sujeto obligado
- ii. Información Solicitada: una descripción que contenga los elementos necesarios para identificarla.
- iii. Forma de Acceso
- iv. Medio de Acceso

2. El sistema genera un acuse de recibido, el cual deberá contener los datos requeridos en el apartado 1.3, del apartado inmediato anterior y deberá contener un número de folio único e irrepetible, el sistema

deberá garantizar la autenticidad del documento, por las formas que se estimen pertinentes.

3. El sistema deberá permitir al sujeto obligado prevenir al solicitante cuando no cumpla con todos los requisitos para su admisión, para que complete los datos faltantes dentro de los dos días hábiles siguientes al de su presentación.
4. En caso de admitir, prevenir, remitir la solicitud al Instituto con motivo de una incompetencia o no admitir la solicitud de información, el sujeto obligado deberá de notificar al solicitante dentro de los términos establecidos en la Ley y su Reglamento.

- 4.1. En caso de que contenga los elementos necesarios para admitir la solicitud el sujeto obligado deberá admitir la solicitud al día siguiente de su presentación.

- 4.2. En caso que la solicitud sea presentada ante sujeto obligado distinto al que corresponde atender la solicitud, éste deberá remitir la solicitud al Instituto, para que se determine la competencia dentro de los dos días hábiles siguientes a su presentación.

- 4.3. En caso de no contar con los elementos necesarios para admitir y en caso de que no haya respondido el solicitante la prevención, se tendrá por no admitida la solicitud.

5. El Sujeto obligado deberá resolver la solicitud dentro de los 5 días hábiles, o en 2 días hábiles cuando se trate de expedientes médicos o datos de salud del solicitante, la cual deberá estar fundada y motivada, y contener por lo menos lo siguiente:

- 5.1 Nombre del Sujeto obligado;

- 5.2 Número de la Solicitud;

- 5.3 Datos de la Solicitud;
  - 5.4 Motivación y Fundamentación de la Resolución;
  - 5.5 Puntos Resolutivos sobre la procedencia o improcedencia de la solicitud;
  - 5.6 Lugar y fecha en que se suscribe el documento;
  - 5.7 Nombre y cargo de quien resuelve;
  - 5.8 Firma.
- 6 En caso de que la resolución sea procedente o parcialmente procedente se le deberá incluir además de los requisitos marcados en el punto anterior, la forma y medio de entrega de la información atendiendo a lo siguiente:
- 6.1 Información Fundamental Publicada por internet. Se hará referencia en la resolución;
  - 6.2 Consulta directa. En la resolución deberá establecerse los días y horas en que el solicitante podrá realizar la consulta, dicho plazo no excederá los treinta días naturales.
  - 6.3 Reproducción de Documentos. Se debe de establecer en la resolución y en caso de que esta reproducción tenga algún costo, se le deberá de notificar al solicitante y éste tiene un plazo de 10 días naturales para pagar y presentar el comprobante de pago; pasado esto, el sujeto obligado deberá de tener disponible la información solicitada dentro de los 5 días hábiles siguientes a la exhibición del pago de derechos, y también podrá hacer uso de hasta 5 días hábiles adicionales como prórroga; cabe mencionar que el solicitante tiene diez días hábiles para pasar a recoger la información solicitada.

- 6.4 Elaboración de Informes. En esta modalidad el sujeto obligado deberá de tener la información disponible dentro de los 3 días hábiles siguientes a la resolución de la solicitud, y podrá prorrogar el plazo por 3 tres días más.
- 7 En caso de que el sujeto obligado no responda a la solicitud dentro del plazo que para tales efectos establece la Ley, el solicitante podrá acudir ante el Instituto a presentar un recurso de revisión.
- 8 Al recibir la información, el solicitante deberá firmar para avalar la entrega de la información.
- 9 El Sujeto obligado deberá integrar un expediente por cada una de las solicitudes de información recibidas.

### III DE ACCESIBILIDAD Y USABILIDAD

Los referidos en el apartado 4.2, punto III, del presente protocolo.

#### 5.4. DE LA AUDITORÍA A LOS SISTEMAS ELECTRÓNICOS

El Instituto se reserva el derecho de mantener un monitoreo en los sistemas electrónicos de los Sujetos Obligados, a fin de garantizar el acceso electrónico confiable a los usuarios en general. Algunos aspectos que se podrían monitorear, serian:

- a. La accesibilidad de la página<sup>vii</sup>;
- b. Los códigos de seguridad emitidos;
- c. La base de datos de las solicitudes de información y;
- d. Los sistemas de respaldo de las solicitudes de información;
- e. Horario de recepción y de consulta del sistema de solicitudes;
- f. Disponibilidad de presentar solicitud de información;
- g. Resguardo de datos personales en el procesamiento de una solicitud de información (nombre, domicilio o correo electrónico).

## 6. FUENTES CONSULTADAS

Calidad: Metodología para documentar el ISO-9000 versión 2000  
Alberto Alexander Servat  
Pearson, Prentice Hall  
Primera edición, 2005.

Ingeniería de la Web y patrones de diseño,  
Ma. Paloma Díaz, Susana Montero, Ignacio Aedo,  
Primera edición, 2005.

Firma electrónica avanzada, documentos digitales y comprobantes electrónicos,  
tratamiento jurídico y fiscal.  
Pérez Chávez Campero  
Tax editores, primera re impresión 2005

Creación y diseño Web  
Claudia Valdez-Miranda Cros, Enrique Rodríguez Álvarez  
Anaya Multimedia  
Edición 2005

- Calidad y evaluación de los contenidos electrónicos  
[http://www.mariapinto.es/e-coms/eva\\_con\\_elec.htm#e6](http://www.mariapinto.es/e-coms/eva_con_elec.htm#e6)
- Introducción a la *usabilidad*  
[http://www.nosolousabilidad.com/articulos/introduccion\\_usabilidad.htm](http://www.nosolousabilidad.com/articulos/introduccion_usabilidad.htm)
- Qué es la *accesibilidad* Web  
<http://www.nosolousabilidad.com/articulos/accesibilidad.htm>
- Políticas de *accesibilidad*  
[http://www.nosolousabilidad.com/articulos/politicas\\_accesibilidad.htm](http://www.nosolousabilidad.com/articulos/politicas_accesibilidad.htm)

---

<sup>1</sup> El objetivo de la accesibilidad a la Web consiste en garantizar que las aplicaciones Web puedan ser accedidas, usadas por todos los usuarios potenciales, independientemente de las limitaciones propias del individuo o de las derivadas del contexto de uso. Por tanto, incluye el uso de cualquier navegador (actual, antiguo, de propósito especial), de cualquier tipo de computador (de baja o alta capacidad de procesado, baja o alta definición de pantalla, cualquier tamaño de *display*, etc.) de cualquier tipo de conexión (con bajo o alto ancho de banda), y por personas de todo tipo de características físicas, sensoriales o cognitivas.

ii Entre las medidas de carácter técnico se encuentran: Identificación y autenticación de usuarios: mientras que la identificación pretende obtener la identidad del usuario que accede al sistema, la autenticación pretende confirmar que el usuario es quien debe ser. Normalmente la autenticación se realiza, bien por algo que se tiene (v.g. una tarjeta), bien por algo que se sabe (contraseña) o bien por algo que es (características de la persona, como la huella digital).

**Control de accesos:** Una vez confirmada la entrada del usuario en el sistema, el control de accesos pretende asegurar que las acciones realizadas por el usuario están en conformidad con los privilegios del mismo.

**Control del flujo de información:** Complementa al control de accesos, evitando ciertos actos de los usuarios sobre los datos a los que tiene derecho a acceder. Por ejemplo, puede evitar la copia de un fichero de acceso restringido a uno sin restricciones de acceso.

**Confidencialidad:** Pretende evitar el acceso a la información por parte de usuarios no autorizados

**Integridad:** Pretende evitar la modificación de la información por parte de los usuarios no autorizados.

**No repudio:** Evita que un sujeto reniegue de la realización de una acción que previamente sí había efectuado.

**Motorización:** Ofrecen confiabilidad, mediante la certificación de la asociación entre individuos y claves públicas de cifrado.

**Auditoría:** Registran todas las acciones realizadas en el sistema por parte de los usuarios.

**Principios de diseño.** Como se comentó anteriormente, el concepto de seguridad total es inalcanzable. Sencillamente, no existe un sistema cien por ciento seguro, por lo que el esfuerzo se centra en lograr sistemas confiables, en el sentido de garantizar los requisitos de seguridad de la organización y de generar confianza en los usuarios. La experiencia en el desarrollo de mecanismos de seguridad, en concreto relacionados con el control de acceso, ha dado lugar a los siguientes criterios de diseño:

**Abstracción de datos:** Los mecanismos de protección deben definirse usando elementos del nivel de abstracción adecuado, evitando alejarse del dominio de aplicación. Así, al especificar permisos sobre una cuenta bancaria es preferible hablar de "ingresar" y "retirar" antes que de "leer" y "escribir" en un fichero de datos que almacene los movimientos.

**Privilegios mínimos:** Deberán asignarse a los usuarios los mínimos privilegios necesarios para acometer sus tareas y ninguno más.

**Separación de privilegios:** Las tareas críticas del sistema deben diseñarse de forma que sean realizadas por más de una persona, dificultando la posibilidad de uso fraudulento del sistema.

**Separación de administración y acceso:** La administración de política de acceso debe estar separada del acceso a la información del sistema. Además que el administrador pueda dar un permiso no le habilita para ejercer ese permiso.

**Autorizaciones positivas y negativas:** Para añadir flexibilidad, deberán asumirse autorizaciones tanto positivas, que permiten el acceso, como negativas que deniegan el acceso.

**Delegación de privilegios:** Debe ser posible delegar tareas administrativas a los usuarios, cuando éstas no sean críticas para el funcionamiento del sistema o si así lo determina la política de seguridad.

**Transacciones bien formadas:** Las operaciones que manipulan objetos son conocidas, su comportamiento es predecible y carecerán de errores, por lo que tras su aplicación el estado del sistema permanecerá consistente.

- Además sólo puede accederse al mismo a través de dichas operaciones.
- Autenticación

- Participación mínima
- Diseño abierto
- Exigencias de permisos
- Intermediación completa.
- Mecanismos económicos
- Sencillez de uso y aceptabilidad.

**Ingeniería de la Web y patrones de diseño,**  
Ma. Paloma Díaz, Susana Montero, Ignacio Aedo,  
Pearson Prentice Hall  
Págs. 201,206  
Págs. 209,210

iii **Confidencialidad:** garantiza que la información es revelada sólo a los usuarios autorizados, en tiempo y forma precisa.

**Integridad:** asegura que la modificación de la información es realizada por los usuarios habilitados, en el tiempo y forma precisa.

**Disponibilidad:** permite que la información este accesible, en tiempo y forma adecuada, a aquellos usuarios autorizados.

**Ingeniería de la Web y patrones de diseño,**  
Ma. Paloma Díaz, Susana Montero, Ignacio Aedo,  
Pearson Prentice Hall  
Pág. 204

iv **The signature is authentic.** - The signature convinces the document's recipient that the signer deliberately signed the document.

**The signature is unforgettable.** - The signature is proof that the signer, and no one else, deliberately signed the document.

**The signature is not reusable.** - The signature is part of the document; an unscrupulous person cannot move the signature to a different document.

**The signed document is unalterable.** - After the document is signed, it cannot be altered.

**The signature cannot be repudiated.** - The signature and the document are physical things. The signer cannot later claim that she or he didn't sign it.

#### Applied Cryptography

Bruce Schneider

Editorial Wiley

Pag. 35.

v Un sistema criptográfico puede ser entendido como un medio para garantizar las propiedades de confidencialidad, integridad y disponibilidad de los recursos de un sistema.

En criptografía existen deferentes documentos digitales que se usan para garantizar las propiedades de confidencialidad e integridad, estos documentos son la integración de los dos tipos de criptografía: la simétrica y la asimétrica. Al hacer esta integración se compensan las desventajas de los tipos de cifrado y se utilizan las

mejores características de cada uno, combinando rapidez del cifrado simétrico con la facilidad de la administración de llaves del cifrado asimétrico.

#### Certificados digitales:

Un certificado digital básicamente es un documento digital expedido por una autoridad de confianza que contiene los datos que identifican al dueño del certificado, su llave pública, fecha de expedición, fecha de caducidad, los datos de la autoridad de confianza y finalmente todo esto está firmado por la misma autoridad.

Los certificados sirven para establecer lazos de confianza entre sistemas o personas, ya que si se confía en la autoridad de confianza entonces se puede confiar en la llave pública del dueño del certificado. Tratando así de resolver el problema de relacionar las identidades con las llaves públicas.

#### Introducción a la Criptografía

Granados Paredes Gibrán

Revista Digital Universitaria

10 de julio 2006 • Volumen 7 Número 7 • ISSN: 1067-6079

[http://www.revista.unam.mx/vol.7/num7/art55/jul\\_art55.pdf](http://www.revista.unam.mx/vol.7/num7/art55/jul_art55.pdf)

<sup>vi</sup> Las claves complementarias utilizadas para las firmas numéricas se denominan "clave privada", que de ordinario conocen más personas y se utiliza para que el tercero que actúa confiando en el certificado, pueda verificar la firma numérica. El usuario de una clave privada debe mantenerla en secreto. Hay que señalar que el usuario individual no necesita conocer la clave privada. Esa clave privada probablemente se mantendrá en una tarjeta inteligente, o se podrá acceder a ella mediante un número de identificación personal o mediante un dispositivo de identificación biométrica, por ejemplo, mediante el reconocimiento de una huella digital. Si es necesario que muchas personas verifiquen firmas numéricas del firmante, la clave pública debe estar a disposición o en poder de todas ellas, por ejemplo, publicándola en una base de datos de acceso electrónico o en cualquier otro directorio público de fácil acceso. Si bien, las claves del par están matemáticamente relacionadas entre sí, el diseño y la ejecución en forma segura de un criptosistema asimétrico hace virtualmente imposible que las personas que conocen la clave pública puedan deducir de ella la clave privada.

Los algoritmos más comunes para la codificación mediante el empleo de claves públicas y privadas se basan en una característica importante de los grandes números primos: una vez que se multiplica entre sí para obtener un nuevo número, constituye una tarea larga y difícil determinar cuáles fueron los dos números primos que crearon ese nuevo número mayor. De esa forma, aunque muchas personas pueden conocer la clave pública de un firmante determinado y utilizarla para verificar las firmas de este, no podrá descubrir la clave privada firmante y utilizarla para falsificar firmas numéricas.

#### La función control

Además de la creación de pares de claves, se utiliza otro proceso generalmente conocido con el nombre de "función control", tanto para crear como para verificar una forma numérica. La función control es un proceso matemático basado en un algoritmo que crea una representación numérica o forma comprimida del mensaje a menudo conocida con el nombre de "comprendió del mensaje" o "huella digital" del mensaje, en forma de un "valor control" o "resultado de control" de una longitud estándar que suele ser. Mucho menor que la del mensaje, pero que no obstante, es esencialmente única en respecto al mismo. Todo cambio en el mensaje produce invariablemente un resultado control diferente cuando se utiliza la misma función control. En el caso de una función control segura, a veces determinada "función control unidireccional", es virtualmente imposible deducir el mensaje original, aun cuando se conozca su valor de control. Por tanto, las funciones control hacen posible que el programa de creación de firmas numéricas funcione con cantidades más pequeñas y predecibles del datos, proporcionándole una consistente correlación testimonial con respecto al contenido

original del mensaje, y dando garantías efectivas de que el mensaje no ha sido modificado desde que se firmó en forma numérica.

**Firma electrónica avanzada, documentos digitales y comprobantes electrónicos, tratamiento jurídico y fiscal.**

Pérez Chávez Campero.

Tax editores, primera re impresión 2005

Pág. 20.

**vii Accesibilidad como medida de calidad**

La calidad de las aplicaciones Web debe tenerse en cuenta de manera similar al resto de las aplicaciones software. La norma ISO 9126 define seis cualidades que debe tener cualquier producto software para que sea de calidad: habilidad, fiabilidad, eficiencia, usabilidad, facilidad de mantenimiento y portabilidad.

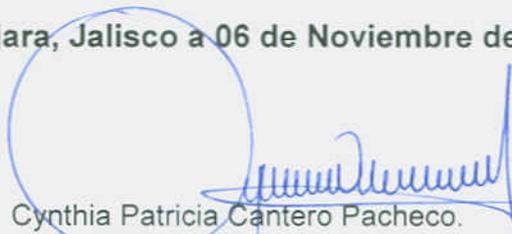
Ingeniería de la Web y patrones de diseño,

Ma. Paloma Díaz, Susana Montero, Ignacio Aedo,

Pearson Prentice Hall

Pág. 300

**Guadalajara, Jalisco a 06 de Noviembre de 2013**

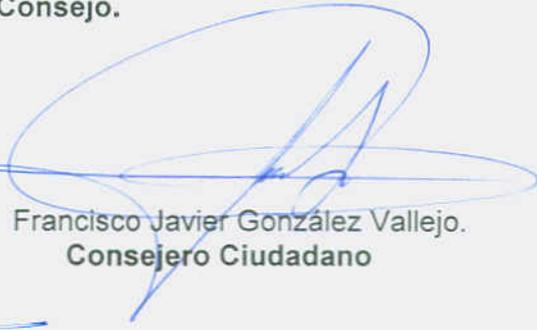


Cynthia Patricia Cantero Pacheco.

**Presidenta del Consejo.**



Pedro Vicente Viveros Reyes.  
**Consejero Ciudadano**



Francisco Javier González Vallejo.  
**Consejero Ciudadano**



Miguel Ángel Hernández Velázquez  
**Secretario Ejecutivo del Instituto de Transparencia  
e Información Pública de Jalisco.**

CPCP/FJGV/PVVR/MAHV/AHG