EL PRESENTE PROTOCOLO DE VALIDACIÓN DE LOS SISTEMAS ELECTRÓNICOS DE PUBLICACIÓN DE INFORMACIÓN FUNDAMENTAL Y DE RECEPCIÓN DE SOLICITUDES DE INFORMACIÓN FUE APROBADO POR UNANIMIDAD EN LA QUINCUAGÉSIMA TERCERA SESIÓN ORDINARIA DEL CONSEJO DEL ITEI, CELEBRADA EL DÍA 13 DE NOVIEMBRE DE 2012.

PROTOCOLO DE VALIDACIÓN DE LOS SISTEMAS ELECTRÓNICOS DE PUBLICACIÓN DE INFORMACIÓN FUNDAMENTAL Y DE RECEPCIÓN DE SOLICITUDES DE INFORMACIÓN

Contenido

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 del Estado de Jalisco, de acuerdo a los términos de la Ley de Información Pública del Estado de Jalisco y sus Municipios y su Reglamento, 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 (con las observaciones correspondientes en su caso), sobre la validación de dichos sistemas.

1.2. FUNDAMENTO Y ALCANCE

La Ley de Información Pública del Estado de Jalisco y sus Municipios, establece en el artículo 9, numeral 1, fracción XIII, como atribución del Instituto, 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. El artículo Cuarto Transitorio, fracción III, establece como obligación de los sujetos obligados elaborar o actualizar y remitir al Instituto para su validación, en su caso, un sistema de recepción de solicitudes y entrega de información pública vía electrónica.

Asimismo, 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).

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 y/o de investigación o auditoría cuando el Consejo del Instituto así lo determine, conforme a los procedimientos establecidos en la Ley de 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 del Estado de Jalisco;

Ley: La Ley de 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: 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 23 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 de Información Pública del Estado de Jalisco y sus Municipios, establece en el artículo 9, numeral 1, fracción XIII, como atribución del Instituto, 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. Asimismo, se establece en el artículo Cuarto Transitorio, fracción III, como obligación de los sujetos obligados elaborar o actualizar y remitir al Instituto para su validación, en su caso, un sistema de recepción de solicitudes y entrega de información pública vía electrónica.

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 será sujeto de 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 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 pública su información, atiende y responde 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. Los sujetos obligados que cuenten con sistema electrónico de recepción de solicitudes de información, podrán solicitar la validación de sus sistema, dentro de los ciento ochenta días naturales siguientes a la entrada en vigor de la Ley de Información, con posibilidad de ampliarse por otros ciento ochenta adicionales, cuando lo autorice el Instituto a petición del sujeto obligado;

III. 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:

   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

IV. El procedimiento de solicitud y dictamen de la validación se llevará a cabo bajo los términos establecidos para tal efecto en los artículos 9, numeral 1,

fracción XIII y Cuarto Transitorio fracción III, 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 sustentará 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 estimen pertinentes. 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 CONTENIDO

Este rubro integra los requerimientos relativos a los contenidos o de la información que será proporcionada por el sistema electrónico de publicación de información.

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;

II. DE COBERTURA

Se verificará en este rubro, que el sistema electrónico de publicación de información, permita la universalidad, la permanencia y la actualización de la información, así como la facilidad en el acceso a la misma y su disposición inmediata.

No se trata de emitir una calificación respecto de la publicación de esta información, sino, solamente, la medición del porcentaje o cobertura de información pública que se pone a disposición de la sociedad, y que es la materia prima de este tipo de sistemas.

Esta valoración, no sustituye en ningún momento la evaluación del nivel de cumplimiento de la publicación de la información fundamental que también realiza el Instituto, y de la que también son sujetos los sistemas electrónicos de publicación de información fundamental.

La valoración de la cobertura de información pública, tampoco exime al sujeto obligado de que se presente en su contra un recurso de transparencia por la falta de publicación de alguna información.

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.[1]

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 o diferentes 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, Crome, Firefox y Safari.
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, el área correspondiente elaborará y dirigirá al Consejo, por conducto del Secretario Ejecutivo

[1] Qué es la *accesibilidad* Web:http://www.nosolousabilidad.com/articulos/accesibilidad.htm Consultado: 20/05/12

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 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. Para ello, el Instituto:

- 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.
- En los casos de incumplimiento, 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 ser apegado 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

El diseño general de las páginas electrónicas para las solicitudes vía electrónica, debe propiciar el uso de las tecnologías actuales, tomando en cuenta que el acceso a este tipo de tecnología debe ser adoptado por los usuarios cotidianos y los no usuarios de computadoras, y no al contrario, ya que se corre el riesgo de ahondar la brecha entre los usuarios y las tecnologías de información; al mismo tiempo, las páginas electrónicas deben ser fieles en su funcionamiento a los procedimientos planteados en la Ley:

5.2.1.1. 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.

5.2.1.2. 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 que se utilizará en las páginas, además que por el tema de velocidad, algunos navegadores se limitan a mostrar 56 colores.

5.2.1.3. 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[i].

5.2.1.4. Asimismo debemos hacer hincapié en la facilidad de uso que debe tener la página; no obstante, no podemos suprimir el proceso de validación 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:
        i. Consulta directa de documentos;
        ii. Reproducción de documentos;
        iii. Elaboración de informes específicos; o
        iv. Una combinación de las anteriores.

iv. Forma de Acceso:
    i. Consulta en la página electrónica;
    ii. Medio electrónico o magnético;
    iii. Copias simples;
    iv. Correo electrónico;
    v. Copias certificadas o;
    vi. Consulta directa en las oficinas del sujeto obligado;

5.2.2.2.2. Datos Estadísticos Opcionales:[2]
    i. Sexo;
    ii. Edad:
    iii. Nivel Educativo;
    iv. Ocupación;
    v. Pregunta 1 ¿Solicita información por primera vez? Y
    vi. Pregunta 2 ¿Como 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 para ver estadísticas de las solicitudes.[3]

Debe de contener al menos las estadísticas siguientes:
    a. Solicitudes hechas agrupadas por tipo de sexo;

[2] El sistema puede contener o no este módulo, la falta del mismo no constituye un incumplimiento de los requisitos para la validación del sistema
[3] El sistema puede contener o no este módulo, la falta del mismo no constituye un incumplimiento de los requisitos para la validación del sistema

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 pedir ayuda vía electrónica (correo electrónico o ayuda en línea).

5.3. POLÍTICAS 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 su estatus de su solicitud.

5.4. POLÍTICAS DE PROCESAMIENTO DE SOLICITUDES

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

Sin obstaculizar el derecho a la información, la solicitud de información que se realice fuera del horario de las 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.

5.5. DE LA INFORMACIÓN SOLICITADA

La información captada 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.

5.6. DE LOS ELEMENTOS DE SEGURIDAD DEL SISTEMA[ii]

5.6.1. 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. Aun así, los usuarios que decidan no registrarse tendrán derecho a visualizar los elementos públicos, tales como la pizarra de seguimiento a solicitudes, y las estadísticas, expedidas anteriormente en las secciones 5.2.2.3. y 5.2.2.4 del presente documento.

5.6.2. 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.

5.6.3. CÓDIGOS DE SEGURIDAD EN EL DOCUMENTO DE ACUSE DE RECIBO

5.6.3.1. Aunque el objetivo de las políticas de seguridad es mantener las tres características de la información: confidencialidad, integridad y disponibilidad[iii], en un ambiente en 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[iv]. 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.

5.6.3.2. 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[v] 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.[vi]

5.6.4. 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:

a. 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 *click* 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.

b. 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 click 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.

c. 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 *click* 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.

5.7. DE LOS MEDIOS DE ALMACENAMIENTO DE LA INFORMACIÓN

Se deberá contar con algún método de respaldo mínimo, consistente en discos duros, discos compactos, o cintas de respaldo que garanticen la seguridad y la integridad de los datos referentes a las solicitudes, tales como nombre, domicilio, correo electrónico, los datos opcionales (véase punto 5.2.2), y los datos mismos de la información solicitada (sujeto obligado, información que se requirió, medio de acceso, etc.), de manera que sea posible recuperarla en cualquier momento futuro, por la comunidad de usuarios en general .

5.8. 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:

8.1.1. La accesibilidad de la página[vii];

8.1.2. Los códigos de seguridad emitidos;

8.1.3. La base de datos de las solicitudes de información y;

8.1.4. Los sistemas de respaldo de las solicitudes de información;

8.1.5. Horario de recepción y de consulta del sistema de solicitudes;

8.1.6. Disponibilidad de presentar solicitud de información;

8.1.7. Resguardo de datos personales en el procesamiento de una solicitud de información (nombre, domicilio o correo electrónico).

5.9. 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[4] 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 5.6.1)
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 5.6.2)

[4] 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.

4. Un elemento, ventana o interfaz para seguimiento y consulta del historial de solicitudes de información recién ingresadas y las que se encuentren en tramite (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 establecen en la Ley de la materia. (véase punto número 5.6.4)
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 5.7)
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 5.3 y 5.4)
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 5.7);

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 (ver anexo 1), 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 :
        1.1.1. Usuario
        1.1.2. Contraseña
    1.2. Personal
        1.2.1. Nombre del solicitante y/o autorizados
        1.2.2. Domicilio,
        1.2.3. Correo Electrónico
    1.3. De la solicitud de información
        1.3.1. Nombre del Sujeto obligado
        1.3.2. Información Solicitada: una descripción que contenga los elementos necesarios para identificarla.
        1.3.3. Forma de Acceso
        1.3.4. 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 de integrar un expediente por cada una de las solicitudes de información recibidas.

III. DE ACCESIBILIDAD Y USABILIDAD

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

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
- Introducción a la *usabilidad*
  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

[i] 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 autentificación de usuarios: mientras que la identificación pretende obtener la identidad del usuario que accede al sistema, la autentificación pretende confirmar que el usuario es quien debe ser.
Normalmente la autentificación 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.
Motorizacion: 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.

Ingeniería de la Web y patrones de diseño,
Ma. Paloma Díaz, Susana Montero, Ignacio Aedo,
Pearson Prentice Hall
Págs. 201,206
Págs. 209,210
Principios de diseño
Como se comento 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
Compartición mínima
Diseño abierto
Exigencias de permisos
Intermediación completa.
Mecanismos económicos
Sencillez de uso y aceptabilidad.

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

[iv] Applied Cryptography
Bruce Schneider
Editorial Wiley
Pag. 35.
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.

v 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
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:

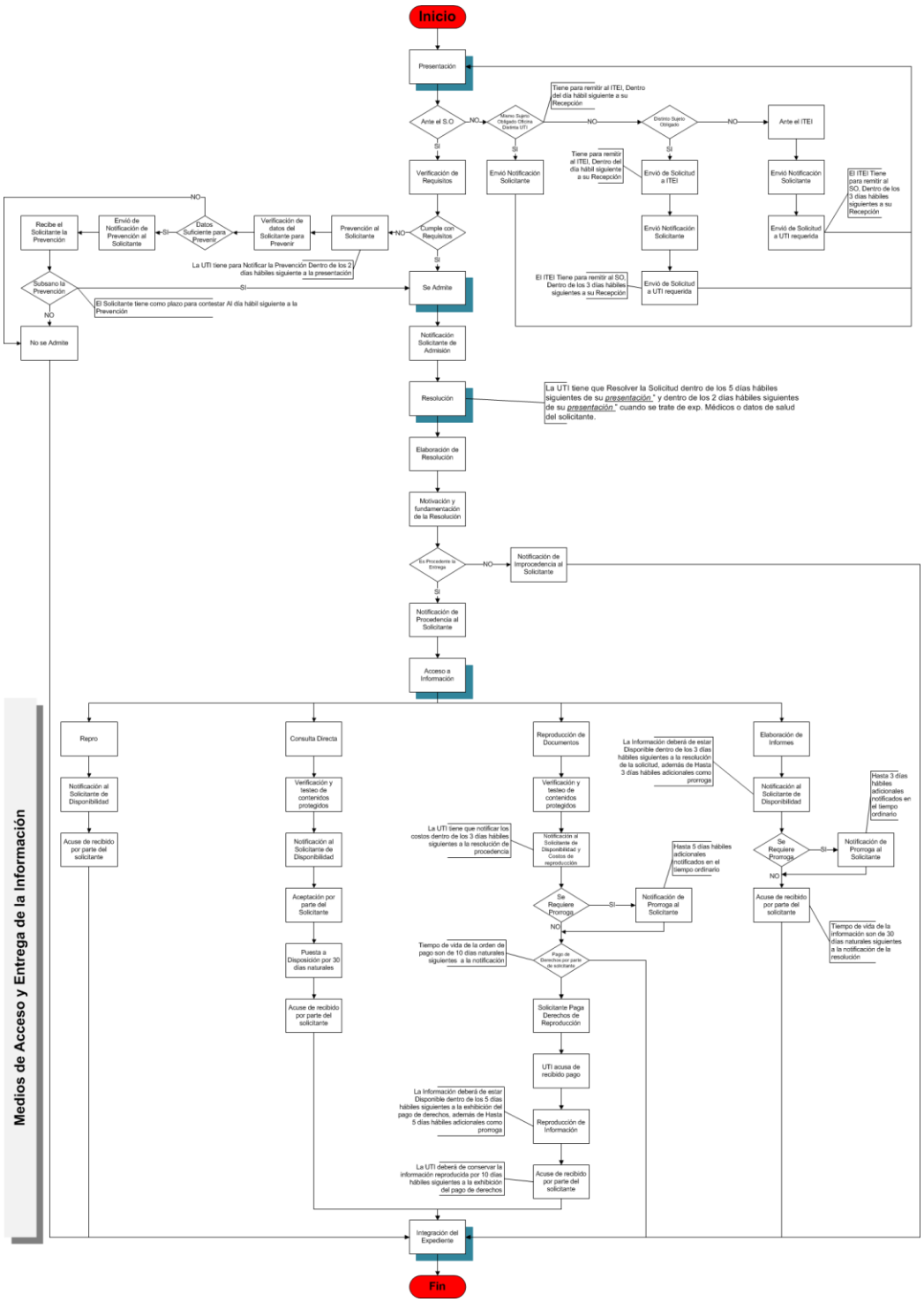
Un certificado digital básicamente es un documento digital expedido por una autoridad de confianza que contiene los datos que identifican al dueño del certificado, su llave pública, fecha de expedición, fecha de caducidad, los datos de la autoridad de confianza y finalmente todo esto está firmado por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

[vi] Firma electrónica avanzada, documentos digitales y comprobantes electrónicos, tratamiento jurídico y fiscal.
Pérez Chávez Campero.
Tax editores, primera re impresión 2005
Pág. 20.
Las claves complementarias utilizadas para las firmas numéricas se denominan “clave privada “, que de ordinario conocen mas 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 publica 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 publico de fácil acceso. Si bien, las claves del par están matemáticamente relacionadas entre si, 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 si para obtener un nuevo número, constituye una tarea larga y difícil determinar cuales fueron los dos números primos que crearon ese nuevo número mayor. De esa forma, aunque muchas personas pueden conocer la clave publica 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 dedicar el mensaje original, aun cuando se conozca su calor de control. Por tanto, las funciones control hacen posible que el programa de creación de firmas numéricas funcione con cantidades mas 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 firmo en forma numérica .

[vii] Ingeniería de la Web y patrones de diseño,
Ma. Paloma Díaz, Susana Montero, Ignacio Aedo,
Pearson Prentice Hall
PAG. 300
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.

Anexo 1


Inicio
Presentación
Ante el S.O
NO
Mismo Sujeto Obligado Diferente Unidad de Transparencia UT
Tiene para remitir al ITEI, Dentro del día hábil siguiente a su Recepción
NO
Diverso Sujeto Obligado
NO
Ante el ITEI
SI
Verificación de Requisitos
Envió Notificación Solicitante
Tiene para remitir al ITEI, Dentro del día hábil siguiente a su Recepción
Envió de Solicitud a ITEI
Envió Notificación Solicitante
El ITEI Tiene para remitir al SO, Dentro de los 3 días hábiles siguientes a su Recepción
Envió Notificación Solicitante
Envió de Solicitud a UTI requerida
El ITEI Tiene para remitir al SO, Dentro de los 3 días hábiles siguientes a su Recepción
Envió de Solicitud a UTI requerida
Cumple con Requisitos
NO
Prevención al Solicitante
Verificación de datos del Solicitante para Prevenir
Datos Suficiente para Prevenir
SI
Envió de Notificación de Prevención al Solicitante
Recibe el Solicitante la Prevención
NO
La UTI tiene para Notificar la Prevención Dentro de los 2 días hábiles siguiente a la presentación
Subsano la Prevención
SI
El Solicitante tiene como plazo para contestar Al día hábil siguiente a la Prevención
NO
No se Admite
SI
Se Admite
Notificación Solicitante de Admisión
Resolución
La UTI tiene que Resolver la Solicitud dentro de los 5 días hábiles siguientes de su presentación." y dentro de los 2 días hábiles siguientes de su presentación." cuando se trate de exp. Médicos o datos de salud del solicitante.
Elaboración de Resolución
Motivación y fundamentación de la Resolución
Es Procedente la Entrega
NO
Notificación de Improcedencia al Solicitante
SI
Notificación de Procedencia al Solicitante
Acceso a Información
Medios de Acceso y Entrega de la Información
Repro
Notificación al Solicitante de Disponibilidad
Acuse de recibido por parte del solicitante
Consulta Directa
Verificación y testeo de contenidos protegidos
Notificación al Solicitante de Disponibilidad
Aceptación por parte del Solicitante
Puesta a Disposición por 30 días naturales
Acuse de recibido por parte del solicitante
Reproducción de Documentos
Verificación y testeo de contenidos protegidos
La UTI tiene que notificar los costos dentro de los 3 días hábiles siguientes a la resolución de procedencia
Notificación al Solicitante de Disponibilidad y Costos de reproducción
Se Requiere Prorroga
SI
Hasta 5 días hábiles adicionales notificados en el tiempo ordinario
Notificación de Prorroga al Solicitante
NO
Tiempo de vida de la orden de pago son de 10 días naturales siguientes a la notificación
Pago de Derechos por parte de solicitante
Solicitante Paga Derechos de Reproducción
UTI acusa de recibido pago
La Información deberá de estar Disponible dentro de los 5 días hábiles siguientes a la exhibición del pago de derechos, además de Hasta 5 días hábiles adicionales como prorroga
Reproducción de Información
La UTI deberá de conservar la información reproducida por 10 días hábiles siguientes a la exhibición del pago de derechos
Acuse de recibido por parte del solicitante
La Información deberá de estar Disponible dentro de los 3 días hábiles siguientes a la resolución de la solicitud, además de Hasta 3 días hábiles adicionales como prorroga
Elaboración de Informes
Notificación al Solicitante de Disponibilidad
Hasta 3 días hábiles adicionales notificados en el tiempo ordinario
Se Requiere Prorroga
SI
Notificación de Prorroga al Solicitante
NO
Acuse de recibido por parte del solicitante
Tiempo de vida de la Información son de 30 días naturales siguientes a la notificación de la resolución
Integración del Expediente
Fin