INSTITUTO DE TRANSPARENCIA E INFORMACIÓN PÚBLICA DE JALISCO

# Políticas de diseño para crear un portal electrónico para la solicitud de información pública.

## Objeto

Crear un conjunto de políticas que regulen el funcionamiento y sirvan de guía para el desarrollo de páginas electrónicas de los Sujetos Obligados que permitan elaborar y dar seguimiento a las solicitudes electrónicas de los ciudadanos, así como visualizar la información solicitada, bajo los lineamientos que dicta la Ley de Transparencia e Información Pública del Estado de Jalisco (LTIPEJ).

## Alcance

Esta política es aplicable a las páginas electrónicas o portales de los Sujetos Obligados en el Estado de Jalisco (SO).

## Antecedentes

## Proceso actual

Actualmente las solicitudes de información son presentadas en las oficinas del Sujeto Obligado (SO), específicamente en la Unidad de Transparencia e Información (UTI). En caso de que en la dependencia no exista una UTI, es la Oficialía de Partes la que procesa las solicitudes de información.

El proceso que se sigue con una solicitud se describe a continuación:

1. El interesado solicita información a través de un escrito libre que debe contener los datos personales mínimos necesarios:
    a) nombre,
    b) dirección ó
    c) correo electrónico y
    d) una descripción de la información solicitada, que contenga los elementos necesarios para identificarla.
    e) Forma en la que desea se entregue la información:
        a. Consulta directa
        b. Consulta por medio electrónico
        c. Copias simples
        d. Copias certificadas
        e. Otro tipo de medio
    f) Información adicional opcional:
        a. Sexo
        b. Edad
        c. Nivel educativo
        d. Ocupación
        e. Pregunta 1. ¿Solicita información por primera vez?
        f. Pregunta 2.¿Cómo supo que tiene el derecho de acceso a la información pública?

Este escrito se presenta ante la UTI del SO.

2. La UTI revisa que la solicitud contenga todos los elementos mencionados en el párrafo anterior para responder la solicitud, en caso contrario, se requiere al solicitante para que complete los datos faltantes.

3. La UTI genera un comprobante fechado y sellado de recepción de la solicitud de información. Aquí comienzan a correr los plazos establecidos en la Ley.

4. La UTI tiene un plazo de 5 días hábiles para contestar la solicitud, negativa o positivamente:

   4.1. Si la respuesta es positiva, el SO debe proporcionar la información solicitada en el soporte material solicitado, siempre y cuando le sea posible, previo pago del soporte material en cuestión.
   4.2. Si la respuesta es negativa, la UTI tiene la obligación de informar al solicitante, dentro del plazo normal o adicional, y al Instituto al día siguiente hábil de la notificación al solicitante, con un informe debidamente justificado y motivado basado en la Ley del porqué de la negativa. El solicitante tiene la opción de solicitar una revisión de su caso si ha quedado inconforme con la respuesta del SO, en cuyo caso tendrá que acudir al ITEI.

5. El SO cuenta con un plazo prorrogable de 5 días hábiles más, período que podrá tomar en caso que requiera más tiempo para dar respuesta a la solicitud, previa notificación personal al solicitante.

6. La información se entregará a la persona que muestre el acuse de recibo de la solicitud de información. En caso de que el solicitante no cuente con el acuse de recibo, debe mostrar una identificación y los datos que permitan localizar la información solicitada.

7. Cabe mencionar que en caso de que la UTI no responda a la solicitud dentro del plazo ordinario o extraordinario que marca la Ley, la respuesta a la solicitud se entenderá resuelta en sentido positivo, previo resguardo de la información confidencial. Para tal efecto el solicitante deberá presentar un recurso de revisión ante el ITEI.

8. Una vez que la información está lista para ser entregada, la UTI tiene la obligación de conservarla hasta por 10 días hábiles, contados a partir del día en que la información debe ponerse a disposición del solicitante.

9. Al recibir la información, el solicitante debe firmar de conformidad para avalar la entrega de la información.

10. Fin del proceso.

El proceso completo en forma de diagrama puede verse en el anexo 1.

INSTITUTO DE TRANSPARENCIA E INFORMACIÓN PÚBLICA DE JALISCO

**Proceso electrónico Propuesto**

La propuesta desarrollada para el proceso electrónico que debe seguir una solicitud de información pública tiene como base tres aspectos:

1. El modelo o proceso actual (que es físico), descrito anteriormente.
2. Las mejores prácticas en procesos similares. Ya que el sistema de solicitudes de información pública y datos personales del Instituto Federal de acceso a la Información Pública (IFAI) en www.sisi.org.mx . ha sido avalado por las instituciones federales gubernamentales nacionales y está reconocido de manera internacional favorablemente, no dudamos en tomarlo como una referencia de las mejores prácticas en el tema.
3. Estándares y procedimientos de intercambio electrónico.

1. El interesado entra a la página electrónica de la dependencia (SO). Debe capturar la información personal:
   1.1. De acceso:
      1.1.1. Usuario
      1.1.2. Contraseña

   1.2. Obligatoria:
      1.2.1. Nombre
      1.2.2. Correo electrónico (de no contar con un correo electrónico, el solicitante podrá consultar el estado de su solicitud en la página de Internet del SO)

   1.3. Y de la información:
      1.3.1. Una descripción detallada de la información solicitada, de tal manera que el SO tenga los elementos necesarios para localizar la información.

2. En caso que el solicitante no cuente con un nombre de usuario y una contraseña, tendrá que solicitar una mediante la página electrónica.

3. Se debe seleccionar un soporte material o electrónico para visualizar o recibir la información solicitada:
   3.1. Consulta en la página electrónica,
   3.2. Consulta directa en las oficinas del SO,
   3.3. Medio electrónico o magnético,
   3.4. Copias simples,
   3.5. Copias certificadas o
   3.6. Correo electrónico.
   En cada caso se debe especificar si tendrá algún costo del soporte solicitado.

4. Información adicional opcional:
   4.1. Sexo
   4.2. Edad
   4.3. Nivel Educativo
   4.4. Ocupación
   4.5. Pregunta 1. ¿Solicita información por primera vez?
   4.6. Pregunta 2. ¿Cómo supo que tiene el derecho de acceso a la información pública?

5. La página electrónica debe generar un comprobante electrónico de recepción de la solicitud de información. Aquí comienzan a correr los plazos establecidos en la Ley. Este comprobante debe contener al menos los siguientes elementos:
   5.1. Fecha y hora de la solicitud
   5.2. Número de folio generado por la página
   5.3. Nombre del solicitante
   5.4. Correo electrónico (en caso de contar con uno)
   5.5. Leyenda 1
   5.6. Descripción de la información solicitada
   5.7. Forma de entrega seleccionada
   5.8. Leyenda 2
   5.9. Código de autenticidad de la información
   5.10. Código de acuse de recibo.
   5.11. Leyenda informativa
   Ver anexo 3.

6. Si el escrito contiene los datos necesarios para iniciar el trámite, se turna a la UTI del SO para responder la solicitud, en caso contrario, se regresa al solicitante por medio del correo electrónico para que complete los datos faltantes o proporcione más datos acerca de la información solicitada.

7. Recibida la solicitud de información por la UTI, se le asignará un número de expediente para su identificación; hecho lo anterior, el trámite de la solicitud continuará por todas sus etapas únicamente con el número de expediente y la información solicitada. Es decir, el trámite continuará omitiendo los datos personales del peticionario, mismos que quedarán en custodia de la UTI.

8. LA UTI tiene un plazo de 5 días hábiles para contestar la solicitud, negativa o positivamente:

   8.1. Si la respuesta es positiva, el SO debe proporcionar la información solicitada en el soporte material solicitado, siempre y cuando le sea posible, previo pago del mismo.
   8.2. Si la respuesta es negativa, la UTI deberá informar simultáneamente al solicitante y al ITEI durante los 5 días hábiles siguientes, (contados a partir del día de la recepción de la solicitud) acompañado de un informe debidamente justificado y motivado (basado en la Ley) del porqué de la negativa. El solicitante tiene la opción de presentar un recurso de revisión de su caso si ha quedado inconforme con la respuesta del SO, en cuyo caso tendrá que acudir al ITEI.

9. El SO cuenta con un plazo adicional de 5 días hábiles más, período que podrá tomar en caso que requiera más tiempo para dar respuesta a la solicitud, previa notificación electrónica al solicitante. Ver sección 4.1 de las Políticas de Diseño.

10. Cabe mencionar que en caso de que la UTI no responda la solicitud dentro del plazo ordinario o extraordinario que marca la Ley de la materia, la respuesta a la solicitud se entenderá en sentido positivo, es decir, el SO deberá poner a disposición del solicitante la información, previo resguardo de la información confidencial, siempre y cuando se presente un recurso de revisión ante el ITEI por parte del solicitante.

11. Una vez que la información está lista para ser entregada, la UTI tiene la obligación de conservarla hasta por 10 días hábiles, contados a partir del día en que la información debe ponerse a disposición del solicitante. La información referente a las solicitudes y de la información solicitada –cuando sea posible- deberá ser almacenada en medios magnéticos (arreglos de discos duros, cintas de respaldo, discos ópticos) que aseguren su integridad, de manera que sea posible recuperarla en cualquier momento futuro.

12. En el momento que la información ha sido entregada y recibida de conformidad, se debe proceder asegurando que el solicitante "firme" de recibido electrónicamente. Ver sección 4.1 de las Políticas de Diseño.

13. Fin del proceso

El proceso completo en forma de diagrama puede verse en el anexo 2.

**Políticas de Diseño**

El proceso anterior se apega a la Ley de Transparencia e Información Pública del Estado de Jalisco, y para asegurar un mínimo de calidad en las páginas que se desarrollen para recibir, contestar y administrar solicitudes electrónicas de información pública, se dictan las siguientes políticas:

1. **De los elementos de diseño generales:**
La popularidad del Internet y su inevitable adopción por parte de los usuarios de computadoras, y de la población en general, han abierto toda clase de oportunidades para dar a conocer información y comercialización de productos, que no dudamos que será la manera de interactuar con muchas entidades de nuestra vida en general, ya sea de manera pública o privada, además que se ha convertido en un excelente medio de expresión mundial. Es por eso que en temas como el de la transparencia y acceso a la información pública no podemos más que tratar de visualizar los retos actuales y futuros que nos planteará en términos de tecnología el tema del acceso electrónico para solicitar información pública.

1.1. El diseño general de las páginas electrónicas para las solicitudes vía electrónica debe de propiciar el uso de las tecnologías actuales (Web), 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 de que las páginas electrónicas deben ser fieles en su funcionamiento a los principios planteados en la LTIPEJ.

1.2. Las páginas desarrolladas con el objeto 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. Entre estos aspectos, están:

1.2.1. Los tiempos de respuesta de la página.
1.2.2. Los colores utilizados.- Todavía en estos tiempos existen personas que cuentan con monitores limitados en colores, por lo que se debe tener en

cuenta la selección de colores que se utilizará en las páginas, además de que para el tema de velocidad, algunos navegadores se limitan a mostrar 56 colores.

1.2.3. Por otro lado, los navegadores más usados, Internet Explorer y Netscape, tienen una paleta de 216 colores comunes y 40 adicionales, así es que es una buena práctica que en las páginas electrónicas desarrolladas se utilicen solamente colores de estas paletas, para lograr que los visitantes a las páginas visualicen los colores como se definieron originalmente.

1.2.4. 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] De esta manera, la Web Content Accesibility (WCAG) ha dictado algunas pautas que aseguran la el acceso para todos los usuarios con la ayuda de la tecnología estándar.

1.2.5. Además de lo anterior debemos hacer hincapié en la facilidad de uso que debe tener la página, aún así, no podemos suprimir el proceso de validación de usuarios (nombre de usuario y contraseña).

**2. De los elementos de la página electrónica principal o inicial.**

Para que las solicitudes de información sean correctamente recibidas por los SO´s, la página electrónica deberá contener al menos los siguientes nodos (elementos):

2.1. Una entrada para dar acceso a los usuarios registrados o en su caso una entrada para darse de alta con un nombre de usuario y una contraseña:
- 2.1.1. Usuario
- 2.1.2. Contraseña

2.2. Una entrada para elaborar las solicitudes de información, que contenga como elementos mínimos:
- 2.2.1. Obligatorios
  - 2.2.1.1. Nombre
  - 2.2.1.2. Una descripción detallada de la información solicitada, de tal manera que el SO tenga los elementos necesarios para localizar la información.
  - 2.2.1.3. Tipos de soporte material o electrónico para visualizar o recibir la información solicitada:
    - 2.2.1.4.1 Consulta en la página electrónica,
    - 2.2.1.4.2 Medio electrónico o magnético,
    - 2.2.1.4.3 Copias simples,
    - 2.2.1.4.4 Correo electrónico,
    - 2.2.1.4.5 Copias certificadas o
    - 2.2.1.4.6 Consulta directa en las oficinas del SO

    En cada caso se debe especificar si tendrá costo.
- 2.2.2. Datos opcionales

2.2.2.1 Correo electrónico
2.2.2.2 Sexo
2.2.2.3 Edad
2.2.2.4 Nivel Educativo
2.2.2.5 Ocupación
2.2.2.6 Pregunta 1: ¿Solicita información por primera vez? Y
2.2.2.7 Pregunta 2: ¿Cómo supo que tiene el derecho de acceso a la información pública?

2.3. Una entrada para dar seguimiento a las solicitudes de información.
2.3.1. Debe contener al menos, una pizarra en donde se pueda visualizar los datos básicos de cada solicitud:
2.3.1.1. Número de caso
2.3.1.2. Fecha de la solicitud
2.3.1.3. Información solicitada
2.3.1.4. Respuesta a la solicitud

2.4. Una entrada para ver estadísticas de las solicitudes
2.4.1. Debe contener al menos las estadísticas siguientes:
2.4.1.1. Solicitudes hechas agrupadas por tipo de sexo
2.4.1.2. Solicitudes hechas agrupadas por rangos de edades
2.4.1.3. Solicitudes hechas agrupadas por nivel educativo
2.4.1.4. Solicitudes hechas agrupadas por ocupación
2.4.1.5. Solicitudes hechas agrupadas por tipo de respuesta a la solicitud (sí y no)

2.5. Una entrada para ver un manual de ayuda para el usuario
2.6. Una entrada para pedir ayuda vía electrónica (correo electrónico)

3. **Políticas de disponibilidad** (24 horas por 7 días a la semana)

4. **Políticas de procesamiento de solicitudes.** (las solicitudes recibidas fuera del horario de labores se procesarán al día hábil siguiente. El comprobante de la solicitud contendrá la fecha del siguiente día laboral.)

Cualquier persona que elabore una solicitud de información podrá remitirla 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 ingresar su solicitud.

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

5. **De la información solicitada:**

5.1. La información captada en esta sección será fundamental para entender y localizar ágilmente la información solicitada, así es que será necesario considerar un área lo suficientemente amplia para que el solicitante pueda describir lo más que pueda su petición.

## 6. De los elementos de seguridad de la página:[ii]

6.1. Acceso a la página electrónica.

Debe contar con un sistema de acceso basado en nombres de usuario y contraseña correspondientes, para garantizar que los solicitantes que cuenten con un nombre de usuario y una contraseña, accedan a la información que les corresponde. Aún 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, explicadas anteriormente en las secciones 2.2 y 2.3 de las políticas de diseño.

6.2. Número de caso.

Se debe contar con un sistema para la generación de un número consecutivo para asignarlo a cada solicitud, de manera que ese número identifique esa solicitud, y sólo esa.

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:[iii] confidencialidad, integridad y disponibilidad, 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 modificación de la información capturada es prácticamente nula, ya que como se acusan de recibido electrónicamente, cualquier modificación es ingresada como si fuera una solicitud diferente.

c. La disponibilidad, como hemos mencionado, es total para toda la comunidad que esté interesada, solamente con proporcionar los datos del número de caso, es suficiente para conocer la información general del mismo.

d. La función tradicional de las firmas rúbricas, es garantizar la autoría o acuerdo en el contenido de un documento[iv]. En un ambiente electrónico de intercambio de datos, estas firmas son reemplazadas por las firmas numéricas, públicas y privadas, con un esquema explicado en el siguiente párrafo.

Basándonos 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 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 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.[v]

La validez de estas firmas está siendo contemplada en las leyes locales, y continuamente se modifica para adecuarse a las necesidades actuales, pero se conserva la esencia del concepto de firma electrónica que tiene la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional.[vi]

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:

6.4.1 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.

6.4.2 Que los usuarios reciban en su buzón de correo electrónico notificaciones electrónicas, -análogamente al proceso de notificar personalmente al solicitante por parte del SO- 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:

**Para firmar de recibido en la página electrónica:**
Debe existir un sistema electrónico que cuando el usurario ingrese a la página introduciendo su usuario y contraseña, enseguida le notifique que tiene un mensaje, instruyéndole la forma en que puede acceder a la información según sea el caso de su elección (ver sección 2 del proceso electrónico); 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 generados en el paso 3 de este proceso, que la información ha sido recibida por el usuario correcto.

**Para firmar de recibido mediante el envío de un correo electrónico al buzón del solicitante:**
Debe existir un sistema 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 (ver sección 2 del proceso electrónico); 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 generados en el paso 3 de este proceso, que la información ha sido recibida por el usuario correcto. Ver anexo 4.

**Para notificar por medio de correo electrónico:**
Debe existir un sistema electrónico que envíe un correo al solicitante comunicándole que le ha sido enviada una notificación (ampliación de plazo,

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 códigos generados en el paso 3 de este proceso, que la notificación ha sido recibida por el usuario correcto.

**7. De los medios de almacenamiento de la información:**

6.1 Los datos referentes a las solicitudes, tales como nombre, domicilio, correo electrónico, los datos opcionales (véase la sección 2 en este mismo documento), y de la información solicitada –cuando sea posible- deberán ser almacenados en algún medio magnético (arreglos de discos duros, cintas de respaldo, discos ópticos) que aseguren su integridad y almacenamiento seguro, de manera que sea posible recuperarla en cualquier momento futuro, por la comunidad de usuarios en general.

6.2 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 mencionados en el párrafo anterior.

**8. De la auditoría de las páginas electrónicas:**

8.1 EL ITEI se reserva el derecho de mantener un monitoreo en las páginas electrónicas de los Sujetos Obligados, a fin de garantizar el acceso electrónico confiable a los usuarios en general. Algunos aspectos que se podrían monitorear, serían:

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 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).

INSTITUTO DE TRANSPARENCIA E INFORMACIÓN PÚBLICA DE JALISCO

## Definiciones

**Sujeto Obligado (SO)**.- Todos los mencionados en el artículo 3 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco.

**Unidad de Transparencia e Información (UTI)**.- La instancia creada al interior de cada una de las entidades que, de acuerdo a la normatividad aplicable, conforman la estructura orgánica de los sujetos obligados y que tiene las atribuciones conferidas por la Ley de Transparencia e Información Pública del Estado de Jalisco.

**Instituto de Transparencia e Información Pública de Jalisco (ITEI).-** Institución encargada de vigilar y promover el cumplimiento de la LTIPEJ, y por tanto, garantizar el derecho de acceso a la información pública.

**Ley de Transparencia e Información Pública del Estado de Jalisco (LTIPEJ).** Marco normativo para garantizar el derecho de acceso a la información pública y el resguardo de los datos personales que se encuentran en manos de los sujetos obligados.

## Bibliografía


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,
Pearson Prentice Hall

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
Caudia Váldes-Miranda Cros, Enrique Rodríguez Álvarez
Anaya Mutimedia
Edición 2005.


---

[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 tipo de 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 con 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 dice 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 se 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 tienen 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 usuarios no autorizados.
**No repudio**: evita que un sujeto reniegue de la realización de una acción que previamente sí había efectuado.
**Notorización**: 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. 205,206
Pags. 209,210
Principios de diseño
Como se comentó anteriormente, el concepto de seguridad total es inalcanzable. Sencillamente, no existe un sistema cien por cien 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 la 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 carecen 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] **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 esté 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 sigature is authentic.-** The signature convinces the document´s recipient that the signer deliberately signed the document.
**The signature is unforgeable.-** 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 e 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 Criptography,
Bruce Schneier
Editorial Wiley
Pag. 35.

[v] 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, puede 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 mas 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 multiplican entre sí para obtener un nuevo numero, 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 pública de un firmante determinado y utilizarla para verificar las firmas de este, no podrán descubrir la clave privada del 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 "compendio del mensaje" o "huella digital" del mensaje, en forma de un "valor control" o "resultado control" de una longitud estándar que suele ser mucho menor que la del mensaje, pero que no obstante, es esencialmente única con 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 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, proporcionando 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.
Perez Chávez Campero.
Tax editores, primera re impresión 2005
Pág. 20.

[vi] Por firma electrónica se entenderán los datos en forma electrónica consignados en un mensaje de datos, a o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar el firmante en relación con el mensaje de datos e indicar que éste último aprueba la información recogida en el mensaje de datos.

**Concepto de mensaje de datos:**

Por mensaje de datos se entenderá la información generada enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el telex o el telefax.
Firma electrónica avanzada, documentos digitales y comprobantes electrónicos, tratamiento jurídico y fiscal.
Perez Chávez Campero.
Tax editores, primera re impresión 2005
Pág. 17.

[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: funcionalidad, 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

2. La UTI revisa que la solicitud contenga todos los elementos mencionados en el párrafo anterior para responder la solicitud, en caso contrario, se requiere al solicitante para que complete los datos faltantes.

3. La UTI genera un comprobante fechado y sellado de recepción de la solicitud de información. Aquí comienzan a correr los plazos establecidos en la Ley.

4. La UTI tiene un plazo de 5 días hábiles para contestar la solicitud, negativa o positivamente:

   4.1. Si la respuesta es positiva, el SO debe proporcionar la información solicitada en el soporte material solicitado, siempre y cuando le sea posible, previo pago del soporte material en cuestión.
   4.2. Si la respuesta es negativa, la UTI tiene la obligación de informar al solicitante, dentro del plazo normal o adicional, y al Instituto al día siguiente hábil de la notificación al solicitante, con un informe debidamente justificado y motivado basado en la Ley del porqué de la negativa. El solicitante tiene la opción de solicitar una revisión de su caso si ha quedado inconforme con la respuesta del SO, en cuyo caso tendrá que acudir al ITEI.

5. El SO cuenta con un plazo prorrogable de 5 días hábiles más, período que podrá tomar en caso que requiera más tiempo para dar respuesta a la solicitud, previa notificación personal al solicitante.

6. La información se entregará a la persona que muestre el acuse de recibo de la solicitud de información. En caso de que el solicitante no cuente con el acuse de recibo, debe mostrar una identificación y los datos que permitan localizar la información solicitada.

7. Cabe mencionar que en caso de que la UTI no responda a la solicitud dentro del plazo ordinario o extraordinario que marca la Ley, la respuesta a la solicitud se entenderá resuelta en sentido positivo, previo resguardo de la información confidencial. Para tal efecto el solicitante deberá presentar un recurso de revisión ante el ITEI.

8. Una vez que la información está lista para ser entregada, la UTI tiene la obligación de conservarla hasta por 10 días hábiles, contados a partir del día en que la información debe ponerse a disposición del solicitante.

9. Al recibir la información, el solicitante debe firmar de conformidad para avalar la entrega de la información.

10. Fin del proceso.

El proceso completo en forma de diagrama puede verse en el anexo 1.