# UNIVERSIDAD TECNOLÓGICA DE PANAMÁ
## CONSEJO ADMINISTRATIVO

## AUTORIDAD DE CERTIFICACIÓN DE LA DECLARACIÓN DE LA POLÍTICA DE CERTIFICACIÓN

Resumen de los derechos y obligaciones fundamentales contenidos en esta CPS [1].

- Esta CPS y los documentos afines regulan todo lo relativo a la solicitud, emisión, aceptación, y revocación de certificados entre otros muchos aspectos vitales para la vida del certificado y el régimen jurídico que se establece entre la Universidad Tecnológica de Panamá (a partir de ahora CA-UTP), los Usuarios y terceros.

- Tanto la CPS como todos los demás documentos afines son puestos a disposición de futuros Usuarios en la dirección de Internet http://www.utp.ac.pa/certificados para que conozcan las normas y reglas aplicables a nuestro sistema de certificación.

- Es imprescindible la custodia de la frase clave privada que el Usuario debe hacer respecto de su certificado, pues si no se toman las medidas adecuadas carecería de sentido el sistema de seguridad que se pretende implantar. En este sentido, es necesario informar inmediatamente a CA-UTP cuando concurra alguna causa de revocación del certificado establecidas en la CPS y proceder, de esta manera, a su revocación para evitar un uso ilegítimo del certificado por parte de un tercero no autorizado.

- El usuario deberá comunicar a CA-UTP cualquier modificación o variación de los datos que se aportaron para conseguir el certificado, tanto si éstos aparecen en el propio certificado como si no.

- El uso del certificado está limitado, única y exclusivamente, para su utilización en la Universidad Tecnológica de Panamá, para los servicios que ella determine.

- Es obligación del Usuario comprobar en el Repositorio de Certificados publicado por CA-UTP que el certificado en el que pretende confiar es válido y no ha caducado o ha sido revocado. Esto para los casos en que el certificado se utilice para confianza hacia terceros según los servicios que determine la UTP.

- En la CPS y documentos afines se establece la responsabilidad de CA-UTP y los Usuarios, así como la limitación de la misma ante la posible producción de daños y perjuicios.

  Para más información, consulte nuestra página web en la dirección:
  http://www.utp.ac.pa/ca/certificados

  O póngase en contacto con nosotros a través de la siguiente dirección de correo electrónico: autoridad.certificacion@utp.ac.pa

[1] CPS por sus siglas en inglés (Certification Practices Statement)

# 1. INTRODUCCIÓN.

## 1.1 Presentación

El presente documento constituye el Estatuto de Prácticas de Certificación (Certificate Practice Statement) de la Autoridad de Certificación para la Universidad Tecnológica de Panamá, al cual se hará referencia mediante el acrónimo de su denominación en inglés CPS.

El presente CPS, recoge las políticas que la Universidad Tecnológica de Panamá, actuando como Autoridad de Certificación Digital, empleará en la expedición de sus Certificados.

Esta Autoridad Certificadora establece un nivel de seguridad para todos los usuarios que depositarán su confianza en la validez de dicho certificado, como instrumento que da garantías sobre la identidad del titular del mismo. En ese sentido, este documento establece que se han tomado las medidas y procedimientos adecuados para constituir la correspondencia entre dicho certificado y una cierta entidad en particular (individuo, servidor, etc.)

Como punto de referencia y con deseos de promover la transparencia y calidad de los certificados que se emiten, la CA-UTP, como será conocida de ahora en adelante la Autoridad de Certificación de la Universidad Tecnológica de Panamá, ha adoptado criterios internacionalmente reconocidos en la definición, estructura y presentación de estas prácticas de certificación. Específicamente, es consistente con las recomendaciones surgidas en la Internet Engineering Task Force (IETF)[2] expresadas en el documento denominado "Marco estructural para políticas y prácticas de certificación" (RFC2527), aceptadas por organismos internacionales de seguridad informática.

## 1.2 Identificación.

Esta CPS puede localizarse en la siguiente dirección de Internet:

http:/ /www.utp.ac.pa/certificados

## 1.3 Llaves públicas y privadas y certificados digitales.

Los certificados digitales básicamente son documentos electrónicos que establecen que cierto dato denominado "llave pública" le pertenece exclusivamente a una entidad en particular (individuo, servidor, etc.). Además dicha llave pública está ligada de manera única con otro dato, denominado "llave privada", la cual la conoce y mantiene exclusiva y privadamente la entidad dueña del par de llaves. Es decir, dada una llave pública existe una única llave privada correspondiente y viceversa. Además, conociendo sólo la llave pública no es posible derivar y conocer la llave privada asociada.

Por otro lado, estas llaves tienen la particularidad que, mediante el uso de técnicas matemáticas (criptográficas), se puede cifrar[3] información usando para ello cualquiera de las llaves; pero luego sólo se puede recuperar o descifrar la información usando el otro par de llave correspondiente.

---

[2] Comunidad Internacional compuesta por ingenieros, diseñadores, vendedores y expertos que investigan y promueven las distintas tendencias, estándares e investigaciones relacionadas con Internet,

2 Cifrar es el mecanismo por el cual se transforma un texto en otro texto totalmente inteligible. Para ello se utiliza cierta información secreta o "llave", la cual se requerirá posteriormente para descifrar o recuperar el texto a su estado original.

Adicionalmente, dado el mecanismo matemático utilizado para generar el par de llaves, se garantiza que dos entidades distintas no generen el mismo par de llaves, por lo tanto, se asegura que la llave privada es única. Esto permite que por medio de ésta llave privada se establezca un medio seguro para la autentificación de la identidad de las entidades, de una manera electrónica.

Para garantizar que una llave pública le pertenece a cierta entidad, una CA emite un certificado digital en el cual aparecen una serie de datos de la entidad, como el nombre que la identifica, su llave pública, el periodo de validez de dicho certificado, mas otros datos como el correo electrónico, tamaño de la llave, etc. La autenticidad de estos datos es asegurada pues la CA anexa en el mismo certificado su propia "firma digital".

La firma correspondiente luego se puede verificar usando la llave pública de la Autoridad Certificadora, de manera que si alguno de los datos del certificado es alterado en lo más mínimo, la firma se invalida automáticamente.

Para el formato de los certificados digitales, hemos acogido el estándar internacional ampliamente reconocido: denominado "X.509". Este estándar permite que un certificado sea compatible y reconocido con distintas aplicaciones de software en variados ambientes.

## 2. COMUNIDAD DE USUARIOS Y APLICABILIDAD.

### 2.1 Ámbito de CA-UTP

El ámbito de CA-UTP viene determinado por la política general de la Universidad Tecnológica de Panamá. (Institución destinada al servicio público de la educación superior).

CA-UTP certificará exclusivamente a los miembros de la Universidad Tecnológica de Panamá: personal docente, investigador y administrativos, y adicionalmente los equipos que mantenga y requieran algún vínculo con el servidor de firma.

Se puede encontrar más información sobre la Universidad Tecnológica de Panamá en http://www.utp.ac.pa/

### 2.2 Identidad de la CA-UTP

El nombre distintivo de la Autoridad de Certificación de la Universidad Tecnológica de Panamá es:

C= PA, S= Panama, L= Panama, O= UTP, OU= Pannet, CN= Autoridad de Certificación de la Universidad Tecnológica de Panamá

CA-UTP será gestionada por:

**PANNet**
Universidad Tecnológica de Panamá
Edif. Postgrado – Campus Metropolitano Víctor Levi Sasso
Avenida Universidad Tecnológica
PANAMA

Datos de contacto:

**PANNet**
Correo Electrónico: autoridad.certificacion@utp.ac.pa
Teléfono: 507.205.66.43
Fax: 507.223.23.88

### 2.3 El árbol de certificación

El árbol de certificación se compone de los siguientes elementos:

1. **Autoridad de certificación raíz de la Universidad Tecnológica de Panamá**, CA-UTP que se auto certifica y firmará los certificados de los miembros de la comunidad universitaria.

2. **Agencias de registro**, que serán las encargadas de la autenticación e identificación de los usuarios y de completar el protocolo definitivo en este documento para la emisión y revocación de certificados.

3. **Certificados digitales** de identidad personal y de host.

#### 2.3.1 Autoridad de Certificación

La Universidad Tecnológica de Panamá, actúa como Autoridad de Certificación (CA-UTP) relacionando una determinada clave pública con un sujeto o entidad concretos a través de la emisión de un Certificado, de conformidad con los términos de esta CPS.

LA CA-UTP es la encargada de la generación de los certificados de los Usuarios, para su exclusivo uso en el ámbito de esta Universidad.

#### 2.3.2 Autoridad de Registro

Para llevar a cabo la prestación del servicio de Certificación, la CA-UTP se vale de una Autoridad de Registro responsabilidad así mismo de la Universidad Tecnológica de Panamá.

Inicialmente se establece una única Agencia de Registro que se localizará en la dirección de Recursos Humanos de la Universidad Tecnológica de Panamá. Los Agentes de Registro formarán parte del personal de la Universidad.

El intercambio de información para verificar la identidad, y los protocolos de certificación que se seguirán son descritos en este documento, y dependerán del tipo de certificado a emitir.

#### 2.3.3 Usuario o Subscriptor.

Por usuario final de esta infraestructura de seguridad, entendemos el suscriptor de certificados (Certificados de Identidad), que voluntariamente confía y hace uso de los certificados de la CA-UTP y que deberán ajustarse a los procedimientos establecidos para la petición de certificados y revocación, así como cumplir los requisitos que se establezcan en esta política.

En el momento actual los usuarios son, potencialmente, todos los Cargos de la Universidad Tecnológica de Panamá, y aquellos equipos de comunicación que requieran certificados digitales, previamente autorizados por la CA-UTP.

#### 2.3.4 Tipos de Certificados.

Sólo se emitirán Certificados Digitales de Identidad Personal para aquellos beneficiarios que mantengan vínculo contractual con la Universidad. Esto es, personal docente e investigador y personal de administración y servicios.

Los usos autorizados de los Certificados emitidos por la CA-UTP vienen especificados en esta CPS.

Los Certificados para Host (equipos de comunicación) serán emitidos para todos los equipos que mantengan comunicación con el Servidor de Firmas, o para aquéllos servicios que requieran algún tipo de autenticación.

### 2.3.5 Contacto

El centro responsable del registro, mantenimiento e interpretación de esta CPS es la Red Académica y de Investigación Nacional (PANNet).

La dirección de correo electrónico de contacto es: autoridad.certificacion@utp.ac.pa

## 3. SEGURIDAD Y PRIVACIDAD.

Requisitos de seguridad y privacidad impuestos a las claves e identidades de la CA-UTP son:

1. CA-UTP operará en una estación de trabajo dedicada.

2. El intercambio de información, si fuese necesario, entre esta estación de trabajo dedicada y cualquier otra, se realizará a través de medios de comunicación seguros.

3. La clave privada de la CA-UTP estará en todo momento cifrada cuando se almacene en modo permanente.

4. Tanto el hardware como el software de la estación que opera la CA-UTP se mantendrá en todo momento físicamente seguro.

5. El par de claves RSA de la CA-UTP será de al menos 2048 bits.

## 4. POLÍTICA DE CERTIFICACIÓN.

### 4.1 Política de seguridad.

Sólo se emitirán Certificados Digitales de Identidad Personal para aquellos usuarios que mantengan vínculo contractual con la Universidad Tecnológica de Panamá. Esto es, personal docente e investigador, administrativos y servicios. La Autoridad de Certificación raíz de la Universidad Tecnológica de Panamá (CA-UTP) será gestionada por personal propio vinculado de forma permanente con esta institución.

### 4.2 Periodo de validez de los certificados digitales.

El intervalo de validez de los Certificados Digitales de Identidad Personal será como máximo el especificado en la relación contractual del individuo que lo solicita.

En el caso del personal fijo, tanto si es docente, investigador o de administración y equipos de comunicación, el plazo de validez será de cuatro años.

### 4.2.1 Convención de nombres.

CA-UTP se encargará de asegurar la unicidad de los DN (Distinguished Names) de los Certificados Digitales de Identidad Personal.

El DN de los Certificados Digitales de Identidad Personal consta de los siguientes campos, con los siguientes valores:

C = PA
S = Panama
L = Panama
O = UTP
OU = <Facultad, departamento o servicio al que pertenece>
CN = <Nombre completo de la persona>

E = <Correo electrónico de la persona>
Número de serie = <Tipo>-<Número (CIP, pasaporte)

## 5. MANEJO DE CERTIFICADOS.

CA-UTP mantendrá constancia en su base de datos de todos los certificados firmados o revocados por ella, aunque no se guardará la frase clave de ningún certificado, necesaria para acceder a la llave privada del mismo.

El uso para el que están especialmente preparados los certificados emitidos por la CA-UTP son la identificación, autenticación y securización de los usuarios y/o documentos intercambiados entre los distintos usuarios con los servicios que brinde y así disponga la UTP.

Se considerará que se hace un uso indebido de un Certificado cuando éste sea utilizado para realizar operaciones no autorizadas según las Prácticas de Certificación aplicables a cada uno de los Certificados.

## 6. MANEJO DE CRL'S.

Las CRLs (Certificate Revocation List) se firmarán periódicamente, al menos una vez al mes, por CA-UTP. CA-UTP es responsable de establecer una extensión en su certificado que indique la URL donde encontrar la Lista de Certificados Revocados para que de esta manera sea fácilmente accesible por los usuarios.

CA-UTP se compromete a mantener actualizada la CRL, incluyendo todos los certificados revocados desde la última actualización.

## 7. OBLIGACIONES.

### 7.1 Obligaciones de la Universidad Tecnológica de Panamá como autoridad certificadora.

La Universidad Tecnológica de Panamá se obliga, en todo caso, a:

1. Ofrecer y mantener la infraestructura necesaria para los servicios de certificación de la Universidad Tecnológica de Panamá, incluyendo el establecimiento y operatividad del depósito de certificados, así como los controles de seguridad física, de procedimiento y de seguridad técnica descritos en este documento.

2. Aprobar definitivamente o denegar las solicitudes de certificados y, en el primer caso, emitir los certificados de acuerdo con lo establecido en el apartado 10.

3. Poner copias de sus propios certificados y de cualquier información de revocación a disposición de quien desee verificar una firma digital con referencia a dichos certificados.

4. Revocar los certificados de acuerdo a las disposiciones de este documento.

5. Proteger los datos personales de los solicitantes que le suministre la Agencia de Registro, de acuerdo a la normativa vigente de protección de datos y las políticas de esta Universidad al respecto.

**7.2 Obligaciones de las Agencias de Registro.**
La Agencia de Registro debe:

1. Llevar a término la identificación y autenticación de los solicitantes de certificados, de acuerdo con los procedimientos de validación.

2. Llevar a término la identificación y autenticación para la revocación de certificados, de acuerdo con los procedimientos de validación establecidos.

3. Proteger los datos personales de los solicitantes, que no podrá ceder a terceros bajo ningún concepto.

4. Atender las solicitudes, peticiones y requisitos de los solicitantes referidas a los procedimientos propios de la Agencia de Registro y de la entidad de emisión, que no deberá comunicarse con el usuario final en ningún caso.

**4.3 Obligaciones de los suscriptores de Certificados**

Los solicitantes de Certificados de Identidad Personal y, tras la aceptación de los certificados, los suscriptores, deben:

1. Proteger sus frases claves privadas.
2. Guardar el certificado expedido por la CA-UTP que será enviado al correo electrónico institucional, el cual es garantía para el mismo, en cualquier eventualidad.
3. Comunicar inmediatamente a la Universidad, a través de sus Agencias de Registro, el compromiso, pérdida, divulgación, modificación o uso no autorizado.

**8. RESPONSABILIDADES.**

**8.1 Responsabilidad de la Universidad Tecnológica de Panamá.**
La CA-UTP pone a disposición del usuario la tecnología informática requerida para la creación de las llaves pública y privada a través de una frase clave con que se verificarán y firmarán los documentos susceptibles de firma electrónica, garantizando la unicidad de las mismas; certifica la identidad de la persona a la que se asocia dicho par de claves, haciendo con ello posible la acreditación de la autenticidad perseguida mediante su empleo.

Es obligación de la CA-UTP:

- Como Autoridad de Certificación
  1. Garantizar el cumplimiento de las obligaciones anteriormente expuestas y, específicamente, que la clave privada de CA-UTP no ha sido comprometida, a menos que se anuncie lo contrario.

  2. La generación de las llaves privadas de los usuarios a través de una frase clave.

  3. Generar la lista de revocación conteniendo los certificados revocados y la fecha y causa de revocación.

  4. Disponer de las herramientas técnicas y mecanismos seguros necesarios para garantizar la inviolabilidad de los aspectos que ambas autoridades certifican.

5. Se responsabiliza frente a su comunidad universitaria de los errores producidos por fallo de su sistema durante los procedimientos de carga de peticiones, generación, renovación y revocación de certificados.

6. Cualquier incidente o responsabilidad nacidos del compromiso de la llave privada de CA-UTP es responsabilidad única y exclusiva de la Universidad Tecnológica de Panamá.

7. Y todas aquellas obligaciones impuestas por la presente CPS, la Ley 43 de Firma Digital de Panamá y por la normativa vigente.

- Como Autoridad de Registro
  1. Es responsabilidad de la Autoridad de Registro la correcta identificación de los solicitantes, tanto para la emisión de certificados como para la revocación o suspensión.

  2. Cualquier anomalía o incidente producido entre el momento de la revocación o suspensión y el momento de la notificación de tal, a la CA-UTP es responsabilidad única y exclusiva de aquélla.

  3. Identificar y autenticar correctamente al usuario y a la unidad que represente, conforme a los procedimientos que se establecen en esta CPS.

  4. Almacenar de forma segura y por un periodo razonable la documentación aportada en el proceso de emisión del Certificado y en el proceso de revocación del mismo.

  5. Llevar a cabo cualesquiera otras funciones que le correspondan, a través del personal que sea necesario en cada caso, conforme se establece en esta CPS.

**8.2 Responsabilidad del suscriptor de un Certificado.**

1. Cualquier anomalía o incidente producidos entre el momento de la revocación, suspensión o reactivación de la frase clave privada correspondiente a un Certificado de Identidad Personal y el momento de la notificación de tal extremo a la CA-UTP es responsabilidad única y exclusiva del suscriptor.

2. Cualquier incidente o responsabilidad nacidos del compromiso de la frase clave privada asociada a un Certificado de Identidad Personal es responsabilidad única y exclusiva del suscriptor.

3. Solicitar la revocación del Certificado cuando se cumpla alguno de los supuestos previstos en el epígrafe titulado "REVOCACIÓN DE CERTIFICADOS" de la presente CPS.

4. No revelar la frase clave privada que es el código de activación del Certificado.

5. Asegurarse de que toda la información contenida en el Certificado es cierta y notificar inmediatamente a la CA-UTP en caso que se haya incluido cualquier información incorrecta o inexacta o en caso que, de forma sobrevenida, la información del Certificado no se corresponda con la realidad. Asimismo, deberá comunicar de manera inmediata el cambio o variación que haya sufrido cualquiera de los datos con los que se generó el Certificado, aunque éstos no estuvieran incluidos en el propio Certificado.

6. Informar inmediatamente a la CA-UTP acerca de cualquier situación que pueda afectar a la validez del Certificado.

7. Realizar un uso debido y correcto del Certificado, según se desprende de esta CPS.

8. Cualquier otra que se derive de la ley, del contenido de esta CPS.

## 9. SOLICITUDES.

La generación de certificados firmados por CA-UTP se realizará, de acuerdo a las siguientes cláusulas:

### 9.1 Generación automática de Certificados.

La autoridad de Registro podrá solicitar la generación de los certificados que necesite sin necesidad de solicitud individualizada por parte de los usuarios.

La generación inicial de un certificado se deberá efectuar a través de los formularios que la RA-UTP designe para ello.

Una vez generado el certificado, el usuario recibirá una copia del mismo en su correo electrónico institucional, junto a un número identificador único.

### 9.2 Solicitud de Certificados.

La orden de generación de certificados sólo la puede realizar la RA-UTP.

Los datos personales recabados por la RA-UTP y cedidos a la CA-UTP para la generación de los certificados serán los mínimos imprescindibles para identificar al usuario, su cargo y eventualmente las funciones específicas a desarrollar en la Universidad Tecnológica de Panamá.

Dichos datos solo podrán ser empleados para la emisión de los certificados electrónicos reconocidos.

### 9.3 Envío y aceptación.

La CA-UTP una vez generado el certificado correspondiente, enviará una copia en formato ascii[4] al correo del usuario. El usuario, deberá verificar, una vez que llene el formulario y envíe su solicitud de certificado, que el mismo haya llegado a su correo. En caso contrario es responsabilidad del usuario hacer los reclamos a la CA-UTP; la cual procederá a realizar las investigaciones sobre el caso.

La RA-UTP creará un documento en papel, en el que se recojan los siguientes datos: fecha de la solicitud, datos del solicitante (nombre, OU, Correo Electrónico, DNI, etc.) y datos únicos del certificado.

Llegados a este punto, al solicitante se le considera acreedor de un certificado digital de identidad como miembro de la Universidad Tecnológica de Panamá

## 10. REVOCACIONES.

### 10.1 Causas de la Revocación.

Un certificado podrá ser revocado si:

1. Ha existido pérdida, robo, modificación, divulgación no autorizada, u otro compromiso de la frase clave privada del sujeto del certificado.

2. Alguna de las partes (CA-UTP, RA-UTP, o el suscriptor) ha incumplido alguna de las obligaciones de la política.

3. Si la Universidad Tecnológica de Panamá conoce o tiene motivos para creer razonablemente que uno de los hechos representados en el certificado es falso o ha cambiado.

4. Si la Universidad Tecnológica de Panamá conoce que alguno de los requisitos de emisión del certificado no fue cumplido.

5. Si el sistema de certificación se vio comprometido de modo tal que afecta a la fiabilidad del certificado.

### 10.2 Revocación a petición del suscriptor de un Certificado de Identidad Personal.

La Universidad Tecnológica de Panamá deberá revocar un certificado si el suscriptor ha olvidado su frase clave, y se haya comprobado que la persona que realiza la solicitud de revocación es en efecto el suscriptor.

El protocolo de identificación se compondrá de los siguientes pasos:

1. El solicitante se apersonará ante la RA-UTP o la entidad que la UTP disponga, y le presentará una identificación válida (cédula, pasaporte u otro tipo de carné, cuya foto identifique al usuario), para que se verifique la autenticidad del mismo.

2. La RA-UTP comprobará que el solicitante posee un certificado firmado por CA-UTP, mediante consulta al repositorio de certificados u otro procedimiento similar.

3. Se generará una solicitud de revocación que se imprimirá en ese momento, que será firmada por el interesado y remitida a CA-UTP.

4. La CA-UTP revocará el certificado y avisará a la RA-UTP y al usuario de la revocación.

5. La CA-UTP emitirá una nueva lista de revocación que publicará en la página web de la Universidad Tecnológica de Panamá (http://www.utp.ac.pa/certificados)

[4] American Standard Code for information Interchange (Código Estadounidense Estándar para el Intercambio de Información) es un código de caracteres basado en el alfabeto latino tal como se usa en inglés moderno y otras lenguas occidentales.

## 11. PUBLICACIÓN Y DEPÓSITO.

El contenido de esta CPS, así como de toda la información que se publique, estará expuesta a título informativo en la dirección de Internet:

http:/ /www.utp.ac.pa/certificados

y los originales estarán depositados en las oficinas de la CA-UTP.

Igualmente, los Usuarios podrán tener acceso de forma fiable a la información de la CA dirigiéndose a sus oficinas, o bien, solicitándolo a la dirección de correo:

autoridad.certificacion@utp.ac.pa

A través de la cual se remitirá la información firmada con un Certificado de la CA de la Universidad Tecnológica de Panamá.

**APROBADO POR EL CONSEJO ADMINISTRATIVO EN SESIÓN EXTRAORDINARIA No. 03-2005 REALIZADA EL 22 DE JUNIO DE 2005.**