



# **MANUAL DE POLÍTICAS DE TRATAMIENTO DE DATOS PERSONALES Y DE USO Y PUBLICACIÓN DE INFORMACIÓN EN EL PORTAL WEB INSTITUCIONAL**

**Enero de 2023**



ISO 9001

icontec

SC6793-1



CO-SC6793-1



# **INSTITUTO TOLIMENSE DE FORMACIÓN TÉCNICA PROFESIONAL – “ITFIP”**

## **MANUAL DE POLÍTICAS DE TRATAMIENTO DE DATOS PERSONALES Y DE USO Y PUBLICACIÓN DE INFORMACIÓN EN EL PORTAL WEB INSTITUCIONAL.**

**Versión 1.3**

**Wilson Mauricio Pimiento Cárdenas**  
Coordinador de Sistemas

**LUIS ALBERTO VASQUEZ GUERRA**  
Direccionamiento Estratégico – G.I.T. Sistemas

**MARIO FERNANDO DÍAZ PAVA**  
Rector

**El Espinal - Tolima**  
**Enero 13 de 2023**

**Contenido**

|                                                                                   | Pág. |
|-----------------------------------------------------------------------------------|------|
| I. DISPOSICIONES LEGALES.....                                                     | 4    |
| II. CONDICIONES GENERALES.....                                                    | 4    |
| III. IDENTIFICACIÓN DEL RESPONSABLE DEL TRATAMIENTO NOMBRE DE LA INSTITUCIÓN..... | 5    |
| IV. DEFINICIONES .....                                                            | 5    |
| V. TRATAMIENTO DE LO DATOS PERSONALES .....                                       | 6    |
| 1. Tratamiento .....                                                              | 6    |
| 4. Área responsable de la garantía de derechos del titular .....                  | 9    |
| 5. Política de cookies .....                                                      | 9    |
| 5.1. Qué son las Cookies .....                                                    | 9    |
| 5.2. Cookies utilizadas en este sitio web .....                                   | 10   |
| 5.3. Cómo deshabilitar el uso de Cookies.....                                     | 10   |
| 5.4. Actualización y cambios en la política de cookies .....                      | 10   |
| VI. POLÍTICAS DE USO Y PUBLICACIÓN DE INFORMACIÓN EN EL PORTAL WEB .....          | 11   |
| 1. De las Pautas Generales .....                                                  | 11   |
| 2. De la Publicación de Contenidos .....                                          | 11   |
| 3. De los Servicios.....                                                          | 12   |
| 3.1. Correo Electrónico.....                                                      | 12   |
| 3.1.1. Nombre de usuario del correo o Nick.....                                   | 12   |
| 3.1.2. Responsabilidades y uso correcto del correo electrónico.....               | 12   |
| 3.1.5 Abuso del correo electrónico.....                                           | 13   |
| 3.1.6 Recomendaciones para el uso del correo electrónico .....                    | 14   |
| 3.2 Chat Ayuda Online .....                                                       | 14   |
| 3.2.1. Uso correcto y responsabilidades del Chat Ayuda Online.....                | 15   |
| 3.3. Blog Institucional .....                                                     | 15   |
| 3.3.1. Uso correcto y responsabilidades del Blog Institucional.....               | 16   |
| 3.4. Foro Institucional.....                                                      | 16   |
| 3.4.1. Uso correcto y responsabilidades del Foro Institucional.....               | 16   |
| 3.4.2. Normas de publicación de mensajes en el Foro Institucional.....            | 17   |
| 3.5 Plataforma GUIA .....                                                         | 18   |
| 3.6 Aplicativo para PQR.....                                                      | 18   |
| 3.7 Uso de redes abiertas .....                                                   | 18   |
| 3.8 Aulas virtuales .....                                                         | 19   |
| 3.8 Reglas para el uso de las aulas virtuales.....                                | 19   |
| 3.9 Redes Sociales .....                                                          | 19   |
| 3.9 Reglas para el uso de las redes sociales.....                                 | 20   |
| VII. POLÍTICA Y ACCIONES PARA CONSTRUIR CLAVES DE ACCESO SEGURAS.....             | 21   |
| 1. Lineamientos generales .....                                                   | 21   |
| 2. Recomendaciones generales para la selección de claves de acceso.....           | 21   |
| 3. Recomendaciones para la protección de las claves de acceso .....               | 22   |
| 4. Asignación de nombre de usuario.....                                           | 23   |
| REFERENCIAS .....                                                                 | 23   |
| ANEXO 1 .....                                                                     | 24   |

## **PRESENTACIÓN**

Este documento contiene todos los lineamientos que sigue el Instituto Tolimense de formación técnica profesional “ITFIP” para el tratamiento de la información, servicios electrónicos y de datos personales que tiene en custodia bien sea producida por el mismo ITFIP como también, por la que las diferentes personas dejan al cuidado y uso de la institución.

Con estos lineamientos el ITFIP manifiesta que garantiza los derechos de habeas data, la privacidad, la intimidad, el buen nombre y la autonomía Institucional, en el tratamiento de los datos personales y de información. En consecuencia, todas sus actuaciones se regirán por los principios de buena fe, de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

Todas las personas que, en desarrollo de diferentes actividades culturales, académicas, contractuales, comerciales, laborales, entre otras, sean permanentes u ocasionales, llegaran a suministrar al ITFIP cualquier tipo de información o dato personal, podrá conocerla, actualizarla y rectificarla.

## **I. DISPOSICIONES LEGALES**

La Constitución Política reconoce a los ciudadanos, en su artículo 15, los derechos al buen nombre, habeas data, intimidad personal y familiar, así como el derecho a solicitar respecto a los datos personales su actualización y rectificación. Las leyes estatutarias 1266 de 2008 y 1581 de 2012 desarrollaron dichos derechos constitucionales que fueron a su vez reglamentados por los decretos 1727 de 2009, 2952 de 2010, 1377 de 2013 y 886 de 2014.

Los principios de libertad, legalidad, veracidad o calidad de los datos, finalidad, circulación restringida, temporalidad, interpretación integral, seguridad, transparencia y confidencialidad se interpretarán en concordancia con el derecho a la educación, su función social, reglamentación y con el principio de autonomía universitaria que atañe a las universidades (arts. 67, 68 y 69 C. P.).

El tratamiento de la información personal de aspirantes, inscritos, estudiantes y graduados se adelantará de conformidad con los principios antes indicados y en el marco de lo dispuesto por la Ley 30 de 1992, los decretos reglamentarios 1767 de 2006 y 4968 de 2009 y la Resolución 1780 del Ministerio de Educación Nacional.

Respecto a los niños, niñas y adolescentes se actuará conforme a las disposiciones constitucionales (art. 44) y legales descritas en el Código de la Infancia y la Adolescencia, en pleno reconocimiento de sus derechos fundamentales, en especial al libre desarrollo de la personalidad e intimidad.

## **II. CONDICIONES GENERALES**

Es interés del ITFIP, la salvaguardia de la privacidad de la información personal del Usuario obtenida a través de sus aplicaciones o sistemas informáticos, para lo cual se compromete a adoptar una política de confidencialidad de acuerdo con lo que se establece a continuación:

- El Usuario reconoce que el ingreso de información personal, lo realiza de manera voluntaria.
- El Usuario acepta que, a través del registro en las aplicaciones o sistemas informáticos, la institución recoge datos personales, los cuales no se cederán a terceros sin su conocimiento, ya que se manejan como propiedad del cliente.



- La recolección y tratamiento automatizado de los datos personales, como consecuencia de la navegación y/o registro por las aplicaciones o sistemas informáticos y que tiene como finalidades las detalladas a continuación:
  - La adecuada gestión y administración de los servicios ofrecidos en las aplicaciones o sistemas informáticos, en los que el Usuario decida darse de alta, utilizar o contratar.
  - El estudio cuantitativo y cualitativo de las visitas y de la utilización de los servicios por parte de los usuarios.
  - El envío por medios tradicionales y electrónicos de información relacionados con los servicios que presta el ITFIP.

### III. IDENTIFICACIÓN DEL RESPONSABLE DEL TRATAMIENTO NOMBRE DE LA INSTITUCIÓN

El ITFIP, que en adelante se denominará la Institución, creada mediante Decreto 3462 del 24 de diciembre de 1980, como una Institución pública de carácter académico, del orden nacional, con personería jurídica, autonomía administrativa y patrimonio independiente adscrito al Ministerio de Educación Nacional, identificado con NIT 800.173.719-0, ubicada en DOMICILIO Y DIRECCIÓN: Calle 18 Cra. 1ª B/Arkabal. CORREO ELECTRÓNICO: [info@itfip.edu.co](mailto:info@itfip.edu.co), Celular: 57+3166254592. Página web: [www.itfip.edu.co](http://www.itfip.edu.co)

### IV. DEFINICIONES

Para los efectos de la presente política y en concordancia con la normatividad vigente en materia de protección de datos personales, se tendrán en cuenta las siguientes definiciones:

- **Aplicaciones informáticas:** es un programa informático diseñado como una herramienta para realizar operaciones o funciones específicas. Generalmente, son diseñadas para facilitar ciertas tareas complejas y hacer más sencilla la experiencia informática de las personas.
- **Base de Datos:** Conjunto organizado de datos personales que sea objeto de tratamiento.
- **Confidencialidad:** propiedad por la que la información no está disponible o divulgada a personas no autorizadas, entidades o procesos.
- **Contenidos:** implican todas las formas de información o datos que se divulgan en la página web, entre los que se encuentran: textos, imágenes, fotos, logos, diseños, animaciones.
- **Dato personal:** cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Derechos de Propiedad Intelectual:** Incluye lo relativo a marcas, nombres comerciales, logos, enseñas, lemas, nombres de dominio, secretos empresariales, saber-hacer, diseños industriales, patentes, modelos de utilidad y derecho de autor.
- **Disponibilidad:** Propiedad de ser accesibles y utilizables bajo pedido por una entidad autorizada.
- **Foro:** Servicio automatizado de mensajes, a menudo moderado por un propietario, a través del cual los suscriptores reciben mensajes dejados por otros suscriptores por un tema dado. Los mensajes se envían por correo electrónico.
- **Integridad:** Propiedad de la salvaguarda de la integridad de los activos. Completitud de la información.

- **Internet:** Herramienta de comunicación con decenas de miles de redes de computadoras unidas por el protocolo TCP/IP. Sobre esta red se pueden utilizar múltiples servicios como por ejemplo correos electrónicos, www, etc.
- **Página web:** Resultado en hipertexto o hipermedia que proporciona un navegador del www después de obtener la información solicitada. Su contenido puede ir desde un texto corto a un voluminoso conjunto de textos, gráficos estáticos o en movimiento, sonido, etc.
- **Publicar:** Hacer que un documento sea visible desde el Sitio Web.
- **Servicios:** Son las ayudas e información en línea que la Institución provee actualmente o que piensa proveer en el futuro a los usuarios, por medio de esta página web, como publicación de noticias o actividades propias de la gestión institucional; trámites en línea; consultas; foros y buzón de quejas y reclamos, entre otros.
- **Sistemas informáticos:** conjunto de técnicas que nos permite almacenar, procesar información y garantizar la seguridad de la misma, mediante una serie de partes (hardware, software y el personal) interrelacionadas.
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- **Usuario:** Es toda persona que ingresa al Sitio Web. Puede registrarse en caso de que requiera realizar un trámite o recibir un servicio de la entidad; o para poner una queja mediante el uso del buzón de Quejas y Reclamos, creado para este efecto.

## V. TRATAMIENTO DE LO DATOS PERSONALES

### 1. Tratamiento

La recolección, uso, circulación y supresión de datos personales por parte del ITFIP tienen como fin el desarrollo de procesos administrativos, financieros y académicos propios de su actividad, la difusión de los productos de investigación y de los programas con oferta para el respectivo ciclo lectivo, y las demás actividades afines a la misión educativa. En aquellos casos en que no exista mandato legal que así lo supla, el ITFIP hará la solicitud de autorización al titular cuando los suministre a terceros según el procedimiento descrito en la ley, para el manejo de los datos personales de acuerdo con la finalidad que desarrolla la política aquí descrita.

Para el cumplimiento de los fines institucionales y cuando así se requiera, el ITFIP podrá contratar para que los servicios sean prestados por terceros, en estos casos la información que pueda contener datos de la comunidad ITFIP se trasladará con la suscripción de cláusulas de privacidad que permitan salvaguardar la intimidad del titular y la correcta prestación del servicio, y el cumplimiento de los demás deberes legales y constitucionales.

Es importante precisar que los datos derivados de la actividad educativa (institucionales, población estudiantil, recurso humano, entre otros) hacen parte del Sistema Nacional de Información de la Educación Superior a cargo del Ministerio de Educación Nacional y por tanto seguirán las reglas descritas en las normas previstas en el marco legal de esta política.

De conformidad con lo expuesto el ITFIP aplica los siguientes principios específicos, los cuales constituyen los lineamientos a seguir en la recolección, manejo, uso, tratamiento, almacenamiento e intercambio, de datos personales. Esto es:



- **Principio de legalidad.** En el uso, captura, recolección y tratamiento de datos personales, se dará aplicación a las disposiciones vigentes y aplicables que rigen el tratamiento de datos personales y demás derechos fundamentales conexos.
- **Principio de libertad.** El, uso, captura, recolección y tratamiento de datos personales sólo puede llevarse a cabo con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal, estatutario, o judicial que releve el consentimiento.
- **Principio de finalidad.** El uso, captura, recolección y tratamiento de datos personales a los que tenga acceso y sean acopiados y recogidos por el ITFIP, estarán subordinados y atenderán una finalidad legítima, la cual debe serle informada al respectivo titular de los datos personales.
- **Principio de veracidad o calidad.** La información sujeta a uso, captura, recolección y tratamiento de datos personales debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
- **Principio de transparencia.** En el uso, captura, recolección y tratamiento de datos personales debe garantizarse el derecho del Titular a obtener del ITFIP, en cualquier momento y sin restricciones, información acerca de la existencia de cualquier tipo de información o dato personal que sea de su interés o titularidad.
- **Principio de acceso y circulación restringida.** Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados. Para estos propósitos la obligación del ITFIP, será de medio.
- **Principio de seguridad.** Los datos personales e información usada, capturada, recolectada y sujeta a tratamiento por el ITFIP, será objeto de protección en la medida en que los recursos técnicos y estándares mínimos así lo permitan, a través de la adopción de medidas tecnológicas de protección, protocolos, y todo tipo de medidas administrativas que sean necesarias para otorgar seguridad a los registros y repositorios electrónicos evitando su adulteración, modificación, pérdida, consulta, y en general en contra de cualquier uso o acceso no autorizado.
- **Principio de confidencialidad.** Todas y cada una de las personas que administran, manejen, actualicen o tengan acceso a informaciones de cualquier tipo que se encuentre en Bases o Bancos de Datos, se comprometen a conservar y mantener de manera estrictamente confidencial y no revelarla a terceros, todas las informaciones personales, comerciales, contables, técnicas, comerciales o de cualquier otro tipo suministradas en la ejecución y ejercicio de sus funciones. Todas las personas que trabajen actualmente o sean vinculadas a futuro para tal efecto, en la administración y manejo de bases de datos, deberán suscribir un documento adicional u otrosí a su contrato laboral o de prestación de servicios para efectos de asegurar tal compromiso. Esta obligación persiste y se mantiene inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento.

En el tratamiento se requiere la autorización previa, expresa e informada del titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta y verificación posterior. Sin perjuicio de las excepciones previstas en la ley, hay algunos casos en los que no se requiere la autorización del titular cuando se trate de:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.



- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las Personas.

## 2. Dato sensible

Se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos, entre otros, la captura de imagen fija o en movimiento, huellas digitales, fotografías, iris, reconocimiento de voz, facial o de palma de mano, etc. Se podrá hacer uso y tratamiento de los datos catalogados como sensibles cuando:

- El Titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.
- El Tratamiento sea necesario para salvaguardar el interés vital del titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
- El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del titular.
- El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

### 2.1. Autorizaciones y consentimiento

La recolección, almacenamiento, uso, circulación o supresión de datos personales por parte del ITFIP, requiere del consentimiento libre, previo, expreso e informado del titular de los mismos.

### 2.2. Medio y manifestaciones para otorgar la autorización

La autorización puede constar en un documento físico, electrónico, mensaje de datos, Internet, Sitios Web, en cualquier otro formato que permita garantizar su posterior consulta, o mediante un mecanismo técnico o tecnológico idóneo, que permita manifestar u obtener el consentimiento vía clic o doble clic, mediante el cual se pueda concluir de manera inequívoca, que, de no haberse surtido una conducta del titular, los datos nunca hubieren sido capturados y almacenados en la base de datos. La autorización será generada por el ITFIP y será puesta a disposición del titular (Ver Anexo).

### 2.3. Revocatoria de la autorización

Los titulares de los datos personales pueden revocar el consentimiento al tratamiento de sus datos personales en cualquier momento, siempre y cuando no lo impida una disposición legal o contractual. Para ello, el ITFIP deberá establecer mecanismos sencillos y gratuitos que permitan al titular revocar su consentimiento.

Se deberá tener en cuenta que existen dos modalidades en las que la revocación del consentimiento puede darse. La primera, puede ser sobre la totalidad de las finalidades consentidas, esto es, que el ITFIP deba



dejar de tratar por completo los datos del titular. La segunda, puede ocurrir sobre tipos de tratamiento determinados, como por ejemplo para fines publicitarios o de estudios de mercado. Con la segunda modalidad, esto es, la revocación parcial del consentimiento, se mantienen a salvo otros fines del tratamiento que el responsable, de conformidad con la autorización otorgada puede llevar a cabo y con los que el titular está de acuerdo.

### 3. Derechos del Titular

El titular de los datos puede hacer uso de su facultad legal para:

- Conocer en cualquier tiempo la información que sobre su persona esté depositada en las bases de datos sujetas a tratamiento del ITFIP.
- Solicitar la rectificación y actualización de sus datos de las bases de datos sujetas a tratamiento por del ITFIP.
- Revocar la autorización de tratamiento de aquellos datos contenidos en las bases de datos a cargo del ITFIP y que no hagan parte del Sistema Nacional de Información de la Educación Superior.
- Ser informado de la solicitud de terceros, distinto a autoridades judiciales o administrativas, de obtener sus datos y a consentir, mediante autorización expresa, o negar la entrega de los mismos.
- Ejercer ante las autoridades competentes las acciones derivadas del incumplimiento de la política de tratamiento aquí descrita.
- Los demás que le sean otorgados por la Constitución y la ley.

### 4. Área responsable de la garantía de derechos del titular

El área responsable de garantizar los derechos del titular de los datos que consten en las bases de datos a cargo del ITFIP es la Oficina de Gestión Jurídica.

En el caso de que el titular considere que se ha dado un uso inapropiado, se han incumplido las finalidades antes descritas o se han desconocido los mandatos legales o sus derechos fundamentales, el procedimiento que debe seguir es el siguiente:

1. El titular del dato o su representante deberá presentar comunicación por escrito donde conste su calidad, informe su interés y exprese de manera clara los fundamentos de su solicitud.
2. La misma deberá ser radicada en la unidad de atención al ciudadano o remitida al correo electrónico [info@itfip.edu.co](mailto:info@itfip.edu.co)
3. La oficina de Jurídica procederá a dar respuesta en un término máximo de cinco (5) días hábiles. En ella se señalará las medidas adoptadas con el fin de salvaguardar los derechos del titular.

### 5. Política de cookies

La utilización de sitios web implica el conocimiento y la aceptación a la instalación de las Cookies a las que se refiere esta Política de Cookies.

#### 5.1. Qué son las Cookies

Una cookie es un fichero que se descarga en su ordenador al acceder del Usuario a determinadas páginas web. Las cookies permiten a una página web, entre otras cosas, almacenar y recuperar información sobre los hábitos de navegación de un usuario o de su equipo y, dependiendo de la información que contengan y de la forma en que utilice su equipo, pueden utilizarse para reconocer al usuario.



Las Cookies, en función de quién gestiona el equipo o dominio desde los que se envían, pueden dividirse en Cookies propias (gestionadas por un equipo o dominio gestionado por el propio editor del sitio web) o Cookies de terceros (gestionados por terceras entidades que tratan los datos obtenidos a través de éstas).

## 5.2. Cookies utilizadas en este sitio web

El ITFIP en sus sitios web, además de las cookies técnicas estrictamente necesarias que permiten al usuario la navegación a través de nuestras páginas Web y el uso de las diferentes opciones o servicios que ofrecemos, se utilizan los siguientes tipos de cookies:

- Cookies de análisis: Son aquellas que bien tratadas por nosotros o por terceros, nos permiten cuantificar el número de usuarios y así realizar la medición y análisis estadístico de la utilización que hacen los usuarios del servicio ofertado. Para ello se analiza su navegación en nuestra página web con el fin de introducir mejoras en el funcionamiento del sitio web y/o mejorar la oferta de productos o servicios que le ofrecemos.
- Cookies de análisis: son aquellas que se usan para optimizar el manejo del contenido del sitio web del ITFIP, así como también para mejorar la visualización en los navegadores y para el análisis estadístico.

## 5.3. Cómo deshabilitar el uso de Cookies

El usuario puede en cualquier momento deshabilitar el funcionamiento de las cookies del sitio web y revocar el consentimiento prestado para su utilización mediante la configuración del navegador, pero puede que esto afecte a la capacidad de navegar por la web o a la correcta utilización de algunas de las funciones de la web.

Puedes consultar como hacerlo en cada navegador siguiendo los siguientes links:

| NAVEGADOR         | LINK                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Google Chrome     | <a href="http://support.google.com/chrome/bin/answer.py?hl=es&amp;answer=95647">http://support.google.com/chrome/bin/answer.py?hl=es&amp;answer=95647</a>                                                                                                                                                                                                                                                                                         |
| Internet Explorer | <a href="https://support.microsoft.com/es-es/office/habilitar-las-cookies-6b018d22-1d24-43d9-8543-3d35ddb2cb52">https://support.microsoft.com/es-es/office/habilitar-las-cookies-6b018d22-1d24-43d9-8543-3d35ddb2cb52</a>                                                                                                                                                                                                                         |
| Microsoft Edge    | <a href="https://support.microsoft.com/es-es/topic/ver-las-cookies-en-microsoft-edge-a7d95376-f2cd-8e4a-25dc-1de753474879#:~:text=Abre%20Microsoft%20Edge%20y%20luego,controles%20espec%C3%ADficos%20para%20las%20cookies.">https://support.microsoft.com/es-es/topic/ver-las-cookies-en-microsoft-edge-a7d95376-f2cd-8e4a-25dc-1de753474879#:~:text=Abre%20Microsoft%20Edge%20y%20luego,controles%20espec%C3%ADficos%20para%20las%20cookies.</a> |
| Mozilla Firefox   | <a href="https://support.mozilla.org/es/kb/Deshabilitar%20cookies%20de%20terceros">https://support.mozilla.org/es/kb/Deshabilitar%20cookies%20de%20terceros</a>                                                                                                                                                                                                                                                                                   |
| Safari            | <a href="https://support.apple.com/es-co/guide/safari/ibrw850f6c51/16.1/mac/13.0">https://support.apple.com/es-co/guide/safari/ibrw850f6c51/16.1/mac/13.0</a>                                                                                                                                                                                                                                                                                     |

## 5.4. Actualización y cambios en la política de cookies

Los sitios Web del ITFIP se reserva el derecho a introducir modificaciones en esta Política de Cookies, por ello se aconseja a los Usuarios que la visiten periódicamente.

Cuando se produzcan cambios significativos en esta Política de Cookies, se comunicarán a los Usuarios para su aceptación mediante avisos en el Portal o a través de correo electrónico o bien través de cualquier otro procedimiento adecuado según las circunstancias.

Si tiene dudas sobre esta Política de Cookies, puede contactar con nosotros en este correo electrónico: [info@itfip.edu.co](mailto:info@itfip.edu.co).



## VI. POLÍTICAS DE USO Y PUBLICACIÓN DE INFORMACIÓN EN EL PORTAL WEB

Se enuncian en el presente documento los “Términos y Políticas del portal web de la institución [www.itfip.edu.co](http://www.itfip.edu.co)”, esperando que los usuarios de este conozcan cómo funciona, los usos aceptados y los que deben evitar.

Se entenderá que toda persona que utilice el portal web institucional conoce y acepta los términos, condiciones y reglamentación vigente sobre el acceso y uso del portal. El desconocimiento de esta regulación no lo exonera de la responsabilidad a la que haya lugar.

### 1. De las Pautas Generales

En reconocimiento de la importancia dada a la privacidad de información, esta política de privacidad concierne a todos los servicios y sitios web ofrecidos por la institución, exceptuando los enlaces que lleva a otros sitios.

La administración y publicación de la información del portal web [www.itfip.edu.co](http://www.itfip.edu.co) es responsabilidad de la persona encargada.

### 2. De la Publicación de Contenidos

- Los contenidos dentro de la Web institucional deben reflejar el respeto por la dignidad e integridad de otras entidades y de las personas en general, evitando transgredir las leyes, normas y buenas costumbres.
- Todas las publicaciones que se realicen en el portal web deberán ser autorizadas por la oficina de comunicaciones o quien haga sus veces.
- Los contenidos de las publicaciones deberán ser siempre de carácter institucional y de interés para toda la comunidad tanto del ITFIP como el público en general.
- Toda publicación debe respetar la normatividad colombiana vigente en materia de derechos de autor, así como las normas internacionales de Copyright, registro de marcas y otras relacionadas.
- El contenido del Sitio Web no puede ser de carácter pornográfico, político, militar o subversivo.
- El formato y la presentación de la información que se publique deben ser siempre consistente con los colores, las fuentes, tamaños y logos institucionales.
- Se podrá publicar documentos en formatos como .doc, xlsx, pdf, gif, .jpg, png. En el caso de documentos o textos extensos y se desplieguen en línea, éstos deben usar el formato .pdf.
- Por ningún motivo se podrán publicar ficheros binarios para la descarga directa. Un archivo binario es aquel que contiene información (texto formateado o fotografías, o archivos ejecutables que contienen programas), codificada en binario.
- La información publicada debe estar completa, no se debe escribir en un artículo “Sitio en Construcción”.
- Los enlaces deben ser claros, reconocibles y sin lugar a ambigüedades.



- Se debe cuidar la redacción y ortografía de la información que se publique.

### 3. De los Servicios

El portal institucional “[www.itfip.edu.co](http://www.itfip.edu.co)”, ofrece diferentes servicios con el fin de informar y mantener al tanto del desarrollo de todas las actividades y obligaciones en el desarrollo del objeto social de la institución, así como compartir e interactuar con la comunidad en general.

#### 3.1. Correo Electrónico

Una cuenta de correo electrónico permite la mensajería entre las personas y las entidades con la institución. La mensajería está asociada a una dirección única o cuenta de usuario de correo electrónico en el ámbito de la institución como en internet. En términos generales, el correo electrónico en la institución seguirá la reglamentación establecida en la ley 527 de 1999. Ley, que permite la seguridad electrónica de los usuarios, por medio del reglamento para el acceso y uso del servicio, el comercio electrónico, y de las firmas digitales, estableciendo las entidades de certificación y se dictan otras disposiciones.

Para la creación y uso de las cuentas de correo electrónico en la institución se siguen los siguientes criterios.

##### 3.1.1. Nombre de usuario del correo o Nick

La forma común de una cuenta de correo electrónico es:

[usuario@itfip.edu.co](mailto:usuario@itfip.edu.co)

El nombre de usuario (**usuario**) para la cuenta de correo se construye o se forma utilizando los siguientes criterios.

- La primera letra del primer nombre del usuario.
- El primer apellido completo.
- Los 2, 3 o 4 últimos dígitos del documento de identidad dependiendo del caso.
- Los caracteres con tilde son sustituidos por los mismos, pero sin tilde.

##### 3.1.2. Responsabilidades y uso correcto del correo electrónico

Los usuarios tendrán las siguientes responsabilidades al momento de hacer correo.

- Los usuarios son responsables de todas las actividades realizadas con las cuentas de correo electrónico proporcionado por la Institución.

Los usuarios deberán tener mucho cuidado con los recursos que integran dicha cuenta y, particularmente con elementos, como la contraseña, que pueden permitir el acceso a la cuenta de correo y recursos personales que utilicen con ese Nick.

- No están permitidos los mecanismos y sistemas que intenten ocultar la identidad del emisor de correo.
- Está prohibida la suplantación de identidad de otra persona en el envío de mensajes de correo electrónico, actividad tipificada como infracción en la Ley.



- Las cuentas de correo individuales son de carácter personal e intransferible. El usuario es totalmente responsable de todas las actividades realizadas con dicha cuenta.
- Se debe tener en cuenta que los procesos de administración de servidores, podrán implicar el movimiento temporal y/o definitivo de sus correos, mas no de su edición y no es responsabilidad por parte del administrador de la información que se encuentre en los buzones.
- Las cuentas de correo electrónico y sus contenidos son propiedad de la Institución y ella dispondrá de conformidad con las disposiciones legales vigentes su uso y tenencia.
- La Institución establece que la cuota de almacenamiento disponibles en cada una de las cuentas de correo es de 3GB. Este almacenamiento deber ser para uso exclusivo de las activades propias de la institución. Cualquier otra información la institución procederá a eliminarla.
- Si se supera la cuta de almacenamiento asignada el servicio del correo y sus aplicaciones conexas se verán afectas. Por lo que se recomienda a los usuarios sacar copias de la información y administrar juiciosamente su espacio del almacenamiento disponible.
- Las cuentas de correo que por dos años o más no sean usadas, estas serán eliminadas de oficio por la institución. En este caso también se incluyen las cuentas que están suspendidas por dos años o más.

### **3.1.3 Copias de seguridad de los correos.**

No se realizan copias de seguridad de los buzones de usuario, siendo responsabilidad de éstos guardar una copia local en caso de almacenar los mensajes en el servidor.

### **3.1.4 Activación y desactivación de cuentas de correo**

El uso inapropiado o el abuso en el servicio de correo electrónico pueden ocasionar la desactivación temporal o permanente de las cuentas. Las acciones en este sentido pueden llevarse a cabo en función de incidencias que puedan suponer un problema para el buen funcionamiento del servicio o para la imagen de la Institución.

La desactivación de la cuenta lleva consigo el borrado de todos los mensajes de correo que estén en ese momento en el servidor y la imposibilidad de recibir nuevos mientras no vuelva a ser activada.

En cualquier caso, la política de activación y desactivación en circunstancias normales será en función del tipo de cuenta y lo hará la institución de conformidad con la necesidad que se presente.

Cuentas del personal Estudiantil: Será activada en el momento en que el estudiante de primer semestre realice la matricula académica, y se mantendrá activa mientras sean estudiante. Si pierde la calidad de estudiante la cuenta será desactivada y después de dos años será eliminada. La Institución mantendrá comunicación con sus egresados por medio de los correos personales que ellos deben suministrar en el momento de diligenciar la ficha de egresado.

Cuentas del personal de contrato: será desactivada y/o eliminadas permanente cuando finalice la relación contractual del usuario con la Institución.

### **3.1.5 Abuso del correo electrónico**



Determinadas prácticas en el uso de la cuenta de correo electrónico están catalogadas como Abuso del Correo Electrónico. Estas actividades están especialmente perseguidas por la comunidad Internet, y suelen ocasionar un grave deterioro de la imagen de la Institución.

Cuando la institución se vea afectada por actividades de este tipo, y sea posible determinar el origen y los responsables, la institución puede decidir bloquear y rechazar todos los mensajes de correo pertenecientes a otra organización.

Los abusos de correo pueden agruparse en las siguientes categorías:

- **Difusión de contenido inadecuado.** Contenido ilegal por naturaleza (todo el que constituya complicidad con hechos delictivos). Ejemplos: apología del terrorismo, programas piratas, amenazas, estafas, esquemas de enriquecimiento piramidal, virus o código malicioso.
- **Difusión masiva no autorizada.** El uso de correos propios o ajenos para enviar masivamente mensajes electrónicos no solicitados por el destinatario o por la institución, sean o no publicitarios o de cualquier índole, no están permitidos.

### 3.1.6 Recomendaciones para el uso del correo electrónico

En el uso de este servicio se debe hacer sin perder de vista las siguientes recomendaciones o directrices, con las que se pretende que los usuarios del correo salvaguarden y empleen de forma adecuada el servicio. Éstas son:

- No responder al correo no solicitado (spam).
- No difundir correo no solicitado.
- No envíe mensajes a muchas personas en el campo "Para".
- Dar nuestra dirección con moderación.
- Diferenciar entre correo profesional y personal.
- Usar un estilo de redacción adecuado al destinatario.
- Limite el tamaño de los mensajes y el uso de adjuntos.
- Limite el tamaño de las firmas automáticas.
- No utilice estilos ni adornos innecesarios.
- Respete la privacidad de los mensajes y el destinatario.
- Utilice contraseñas seguras para el acceso a su cuenta de correo.
- No descargue archivos adjuntos si no está seguro de su procedencia.
- En lo posible bloquear la visualización de imágenes en el cuerpo de los mensajes de sus correos.
- Configure su cliente de correo electrónico con un filtro anti-spam.
- Por ningún motivo no olvidar cerrar las sesiones al finalizar el trabajo.

### 3.2 Chat Ayuda Online

Este servicio permite en tiempo real una conversación en línea entre el operador del chat y un usuario del portal. Este servicio es ofrecido a los usuarios con el fin de optimizar la comunicación directa desde cualquier parte del mundo. Las conversaciones versarán sobre temas institucionales.

En caso de que en el momento de ingresar al Chat el usuario no encuentra un operario disponible para que los atienda en línea, él puede escribir un mensaje en el chat y el operario después puede entrar y leerlo para posteriormente responderlo vía correo electrónico.

El operador encargado de administrar y responder los mensajes de dicho servicio de la oficina de atención al ciudadano.

### 3.2.1. Uso correcto y responsabilidades del Chat Ayuda Online

En el uso de este servicio se debe seguir las siguientes directrices:

- Para acceder al servicio, los usuarios deberán suministrar el nombre, un correo electrónico válido y en lo posible, un número celular de contacto. Esto con el fin de que el operador del chat pueda saber con quién se está comunicando. Información necesaria también, en caso de que haya dejado un mensaje fuera de línea, para que el operador pueda dar respuesta a dicho mensaje.
- Solo será permitido tratar temas de índole institucional.
- No se permiten expresiones mal intencionadas o groserías, pues ante todo está la educación ética y moral. En caso de que se reporte este tipo de conducta, la persona pierde el uso de este servicio.
- Está prohibida la suplantación de identidad de otra persona en el envío de mensajes, actividad tipificada como infracción en la Ley.
- El usuario que utiliza este servicio, declara estar en conocimiento y aceptar los Términos y Condiciones Generales, la Política de Privacidad, los Términos y Condiciones para el uso del Correo electrónico, y las bases que se indican en este documento.
- El ITFIP no se responsabiliza por las opiniones y comentarios emitidos por los participantes; su contenido es única y exclusiva responsabilidad civil y penal de quien lo envió.
- El ITFIP se reserva el derecho de retirar en cualquier momento, y a su criterio, los mensajes que vayan en contra de las reglas del chat o de la legislación vigente.
- Todo usuario del servicio de chat se compromete a:
  - a. Mantener una conducta decente, y de respeto mutuo cuando utiliza este servicio.
  - b. No usar lenguaje ofensivo, calumnioso u ofensivo hacia los otros usuarios de este servicio.
  - c. No violar las leyes o reglamentos vigentes.
  - d. No publicar mensajes comerciales.
  - e. No enviar repetida e indiscriminadamente mensajes en el cuarto de chat, que puedan provocar una degradación del servicio.
  - f. Se reserva el derecho de modificar las reglas de uso en cualquier momento y a su solo criterio.
- No se responsabiliza por los daños que provengan del uso de este servidor.
- Recomendaciones al usuario antes de acceder al servicio de chat:
  - a. Evite dar información personal a las personas que ha conocido en el chat.
  - b. Sea consciente de que puede ser objeto de mensajes indeseados por parte de otros usuarios en el chat. Se sugiere ignorarlos y notificar este tipo de irregularidades.
  - c. La velocidad de conexión al servidor de chat depende en gran parte de la velocidad de conexión de su proveedor de acceso Internet. Tenga paciencia en caso de que los mensajes no estén llegando con la rapidez deseada.
- El ITFIP se reserva el derecho de terminar o suspender el acceso de los usuarios que infrinjan las reglas de uso del chat, de los términos y condiciones generales, de la Política de Privacidad, o cualquier otra disposición relacionada con el uso de esta herramienta.

### 3.3. Blog Institucional

Es un sitio web, aparte del portal institucional en el que uno o varios autores publican cronológicamente textos o artículos, apareciendo primero el más reciente, donde el autor conserva siempre la libertad de dejar publicado lo que crea pertinente y donde suele ser habitual que los propios lectores participen activamente a través de sus comentarios. Este blog sirve para compartir ideas y opiniones con respecto a la institución.



Si algún estudiante o funcionario desea publicar información de temas educativos o referente a la institución deberá comunicarse con la oficina de planeación para que esta autorice a la coordinación de sistemas la creación de la línea del blog.

### 3.3.1. Uso correcto y responsabilidades del Blog Institucional

Para la correcta funcionalidad y uso del blog se deben seguir los siguientes criterios.

- Normas de estilo
  - No utilices mayúsculas en el título ni abusos de ellas en el contenido. En internet equivale a gritar y es muy desagradable.
  - El idioma que debes usar es el español. Evita el lenguaje soez y los localismos.
  - Intenta escribir de la manera más correcta posible. Esto no es la RAE, pero tampoco es un chat o un sms. El lenguaje es lo único que nos vincula, y si queremos que se nos entienda y no se nos malinterprete, debemos usarlo de la manera más correcta posible.
- Normas de contenido
  - No uses las bitácoras para resolver dudas.
  - No incluyas contenidos ilegales, tales como piratería o prácticas de dudosa ética o legalidad.
  - No está permitido el spam.
  - No se permite contenido racista, xenófobo, homófobo o sexista, así como insultos a otros usuarios o administradores.
  - La crítica constructiva siempre es bienvenida, no así la destructiva. Recordamos que para la primera hay una sección en el foro donde exponer las quejas o sugerencias.
  - Si quieres publicar contenido de interés para los administradores o moderadores, hazlo en el foro del portal institucional.
  - Los blogs no son el lugar adecuado para la publicación de Howto's o Comos.
  - No está permitida la publicidad o promoción directa de productos o servicios. Puedes hacer alusión a ellos en el desarrollo de una.
  - Aunque el blog es un espacio personal, no se permitirán contenidos que se desvíen de la temática general del foro ni aquellos que carezcan de la debida seriedad.
- Licencias de contenidos
  - Si vamos a publicar contenido de otras personas, siempre hay que respetar la licencia que esa persona ha puesto sobre su contenido y los permisos de derechos de autor. En caso de que no encontremos la licencia en la fuente, siempre se presupondrá que es de aplicación la licencia más restrictiva. En el caso de que la Licencia permita la cita, utilizaremos siempre las comillas o el quote para hacer ver que el contenido no es nuestro, y colocar siempre la fuente. Todo esto depende de la licencia. Algunas no permiten ni siquiera la cita, así que deberemos limitarnos a poner nuestro comentario y un enlace a la noticia o el texto. Otras permiten copiar completa e incluso modificaciones (como algunas licencias Creative Commons).

### 3.4. Foro Institucional

Servicio que tiene como propósito dar a conocer las opiniones y comentarios de los diferentes participantes alrededor de temáticas específicas de la institución. Estos foros servirán como insumo y catalizador de las inquietudes sobre las diferentes temáticas de la institución.

#### 3.4.1. Uso correcto y responsabilidades del Foro Institucional



Para el uso correcto de foro y de las responsabilidades que ello conlleva se deben seguir los siguientes lineamientos:

- Los usuarios deberán suscribirse a la página institucional, ingresando la información correspondiente, estos datos deberán ser valederos.
- Solo será permitido tratar temas de carácter institucional.
- No se permiten expresiones o temas mal intencionados o groserías, pues ante todo está la educación ética y moral. En caso de que se reporte este tipo de conducta, la persona pierde el uso de este servicio.
- Está prohibida la suplantación de identidad de otra persona en el envío de mensajes, actividad tipificada como infracción en la Ley.
- Preste atención a las buenas maneras en el foro. Los insultos y las descalificaciones personales no serán tolerados.
- Se evitará cualquier manifestación escrita o en imágenes que atenten contra las leyes vigentes o incite directa o indirectamente a la comisión de algún acto delictivo.
- Se evitará el SPAM en el foro (publicar el mismo post en foros distintos) salvo si son del personal del foro, de urgencia, o de especial interés actual.
- Solamente se permitirán encuestas relacionadas con la temática del foro. En ningún caso se podrán hacer encuestas o abrir temas de tipo religioso o político. En caso de duda, pregunte a cualquier moderador la conveniencia de la encuesta.
- Los moderadores, están aquí para mantener el correcto funcionamiento del foro. Si un mensaje tuyo es borrado, editado o cerrado no abras otro para pedir explicaciones. Se borrarán automáticamente los mensajes o hilos abiertos por este motivo. No se moderan mensajes sin ninguna razón, la explicación está en estas normas. No se permitirá el cuestionamiento público de estas normas. Si alguien tiene algún problema o sugerencia al respecto, enviar correo a [info@itfp.edu.co](mailto:info@itfp.edu.co).
- No se permiten mensajes de tipo personal en el foro.
- En caso de incumplimiento reiterado de las normas se procederá a un baneo y pérdida de nick al usuario en cuestión. Todo mensaje queda registrado con su IP y cada persona es responsable de sus palabras.
- No se publicarán fotos, hipervínculos, textos o imágenes de contenido pornográfico, pedófilo, sadomaquista o relativa a actos íntimos que vulneren la normativa vigente o justificativos de discriminación por razón alguna, ni se proporcionarán enlaces para tener acceso a este tipo de material.
- Escribe en minúsculas, en internet las mayúsculas equivalen a gritar y hacen más difícil leer los mensajes
- De la misma manera está prohibido el lenguaje tipo SMS y la escritura en negrita de la totalidad del mensaje, solo se podrá utilizar esta para resaltar algo importante. Afortunadamente los teclados disponen de todas las letras y haremos uso de ellas de la manera correcta. Cualquier mensaje que no se pueda entender con claridad podrá ser eliminado por los moderadores. Si se repitiese el autor podría ser sancionado.

### **3.4.2. Normas de publicación de mensajes en el Foro Institucional**

- Antes de realizar una consulta o plantear sus dudas revise los posts de este foro.
- Elija el subforo adecuado en el que publicar en función de la pregunta.
- Los títulos de los mensajes deben ser explicativos del contenido, no importa si son largos. Esto da velocidad al foro pues los foreros ya entran donde saben que les interesa y también ayuda mucho a la hora de hacer búsquedas.



- Antes de publicar busque en el foro a ver si ya existe algún tema relacionado con su duda y su pregunta ya está contestada. En caso de encontrar un tema relacionado con su duda, pero no encuentre en él la respuesta que busca continúe el tema ya abierto, esto hace que el foro quede más organizado, compacto y sea más útil para futuras búsquedas.
- No cambie de tema en medio de un hilo. Intente buscar un hilo similar o en su defecto abra un mensaje nuevo.

### **3.5 Plataforma GUIA**

Este servicio tiene que ver con la posibilidad que da el portal para acceder a la información académica de los estudiantes y para que la oficina de Registro y Control Académico realice gestión sobre la misma.

A la plataforma solamente podrán acceder estudiantes, docentes y administrativo de la institución y estará al servicio en Internet los 7 días de la semana, 24 horas al día.

El uso de esta aplicación está regido por todas las disposiciones legales vigentes y por las leyes Tratamiento de datos personales y por las disposiciones establecidas en el presente manual.

### **3.6 Aplicativo para PQR.**

Este servicio está orientado a facilitar los mecanismos para el reporte de las peticiones, quejas, reclamos, solicitudes y felicitaciones que los diferentes usuarios a ven tenga presentar ante la Institución. El uso de estos servicios está regido por las disposiciones legales vigentes en materia de tratamiento de datos personales y por las disposiciones establecidas en el presente manual.

### **3.7 Uso de redes abiertas**

Para los usuarios que utilicen el servicio de red de datos bien sea de forma inalámbrica o por cable debe aceptar y se comprometen estrictamente a seguir las siguientes condiciones de uso:

- Utilizar la red para fines Académicos, sin interferir con el trabajo de los demás usuarios de la misma.
- No entorpecer asuntos propios de las autoridades Institucionales.
- El usuario acepta y reconoce que hay riesgos potenciales al transmitir y recibir datos a través de un servicio de red.
- No instalar servicios tales como correo, DNS, y/o DHCP sin fines académicos.
- Respetar la integridad de los sistemas de computación. Esto significa que ningún usuario podrá adelantar acciones orientadas a infiltrarse, dañar o atacar la seguridad informática de la Institución, a través de medio físico o electrónico alguno.
- No instalar equipos activos de red, tales como repetidores, switches o Access Point, enrutadores, etc.
- Quien desee usar el servicio de red deberá hacerlo a través de los equipos de cómputo institucionales, personal o dispositivo móvil.



- Mantener instalado y actualizado un software de antimalware en el equipo de cómputo o dispositivo móvil que se utilice para conectarse a la red.
- Mantener actualizados y "parchados" tanto el sistema operativo como las aplicaciones instaladas en el equipo de cómputo o dispositivo móvil que se utilice para conectarse a la red.
- Desconectar inmediatamente de la red sus equipos de cómputo o dispositivos móviles en caso de sospechar que puedan estar infectados con virus informáticos.
- No hacer uso de herramientas que comprometan la disponibilidad, desempeño y confidencialidad de datos transportados por la red.
- La institución de educación superior ITFIP no asume ningún tipo de responsabilidad sobre el uso, visualización, creación e intercambio de la información transmitida por la red, ya que los contenidos en internet son incalculables y de naturaleza desconocida.

### 3.8 Aulas virtuales

El uso y manejo de toda la información de las aulas virtuales que se emplean en la formación que la Institución imparte a través de la TIC, estará regida por todas las disposiciones legales vigentes y por la normas y reglamentos de la institución propios del tema. Sin embargo, a continuación, se presenta una serie de reglas que se debe seguir para facilitar el uso ya la convivencia en las aulas virtuales. Son normas básicas de respeto, buena conducta, de construcción de ciudadanía y de reputación digital que nos permitirán desarrollar nuestro actuar en armonía y buenos tratos en la sociedad digital generada en las aulas.

### 3.8 Reglas para el uso de las aulas virtuales

Las normas que se presenta a continuación son la escritas y publicadas por Virginia Shea en su libro Netiquette. Ella plantea las siguientes reglas (que son las que se adoptan en el uso de las aulas virtuales) (Shea 1995):

- Nunca olvides que las personas que leen tus mensajes tienen sentimientos y pueden tener una cultura, ideología o religión diferente, así que debes ser respetuoso.
- Sigue las normas de buenos modales que se utilizan en la vida cotidiana.
- ESCRIBIR TODO EN MAYÚSCULAS ES SINÓNIMO DE GRITAR y, además, dificulta la lectura.
- Respeta el tiempo de las otras personas, por lo tanto, no envíes mensajes excesivamente extensos, con contenidos sin importancia o con archivos muy pesados (ten en cuenta esto cuando vayas a enviar un correo; evita los spams y las cadenas).
- Comportate de forma amable cuando estés en línea.
- Comparte tu conocimiento con la comunidad, esto hará que las demás personas también se animen a compartir.
- Ayuda a mantener los debates en un ambiente sano y constructivo, no te dejes llevar por las provocaciones.
- Respeta la privacidad de las personas.
- No abuses de tu poder cuando seas administrador en algún espacio virtual.
- Perdona los errores ajenos para que luego perdonen los que tú puedas cometer.

### 3.9 Redes Sociales



En las redes sociales se debe seguir normas que permitan una participación decorosa y que ayuden a la convivencia armónica de los participantes en estos espacios virtuales. Normas que se toman también del libro de la autora Virginia Shea.

### 3.9 Reglas para el uso de las redes sociales

Las normas a seguir en las redes sociales son las siguientes.

- Usa una foto en tu perfil acorde a la reputación que quieres construir en las redes, que represente lo que quieres mostrar a los demás. La foto es un dato básico de carácter público, se debe procurar que la situación que muestre en la foto sea algo que cualquier persona pueda ver.
- Es importante redactar una descripción de perfil corta, mencionando aquellas actividades, trayectoria o gustos por los cuales quieres que los demás te identifiquen. Esta es una forma de tener una carta de presentación virtual.
- Los textos que se comparten por este medio deben ser cortos.
- Evita saturar a los demás con una carga excesiva en tus publicaciones.
- Las redes sociales pueden usarse en entornos educativos de forma muy eficiente para compartir artículos, noticias, videos, eventos de interés; para esto es conveniente tener una red social para uso profesional y otra red social para uso personal, donde podrás hacer publicaciones de índole particular como contar lo que haces, piensas o sientes (asuntos que solo le interesan a tus familiares y amigos).
- Si compartes información de otros, es deseable colocar el enlace a la fuente original o un lugar donde se amplíe lo que se está comentando (siempre hay que reconocer al autor original y tener en cuenta las licencias correspondientes de uso).
- Sé selectivo con el material multimedia que compartes por estos medios, pues una vez subido se podría replicar automáticamente.
- Abstente de publicar material que muestre situaciones inadecuadas, ya que será casi imposible detenerlo, aspecto que es importante recalcar con niños y jóvenes, quienes no reflexionan mucho en las consecuencias de sus actos que pueden llegar a tener consecuencias legales.
- Cuando encuentres material indebido sobre tu persona o de otras personas, ten en cuenta que siempre tienes la posibilidad de utilizar las opciones de denuncia que ofrecen los servicios. En la mayoría de los casos el material es retirado en muy poco tiempo.
- Si no quieres que algo se sepa, nunca lo digas o publiques en Internet, ni siquiera a través de un mensaje privado.

## VII. POLÍTICA Y ACCIONES PARA CONSTRUIR CLAVES DE ACCESO SEGURAS

A continuación, se presenta un conjunto de lineamientos que buscan establecer recomendaciones que deben considerar para que al momento de crear y usar clave de acceso fuertes permitan niveles de seguridad aceptable para que la vulnerabilidad de los sistemas y servicios informáticos de la institución se la mínima posible y de esta manera se preserven y mantengan estos valiosos recursos.

El objetivo fundamental de esta política es la de establecer la forma como se deben crear, asignar, proteger y usar de la forma más segura las claves de acceso a los recursos informáticos de ITFIP. Así como también establecer las responsabilidades que los usuarios de los recursos informáticos de la institución adquieren al manejar alguna de las claves de acceso asignadas para su uso y custodia.

### 1. Lineamientos generales

Los siguientes son los lineamientos a seguir en el manejo y uso de las claves de acceso a los recursos informáticos del ITFIP<sup>1</sup>.

- Todas las claves de acceso de sistema (root, administradores red, cuentas de administración de aplicaciones, etc...) deben ser cambiados al menos una vez cada seis meses.
- Todas las claves de acceso de usuario (cuentas de email, cuentas de servicios Web, etc.) deben ser cambiadas al menos una vez cada doce meses. Sin embargo, se recomienda cambiarla con mayor frecuencia y también siempre que el usuario sospeche que la seguridad de su contraseña pueda haber sido comprometida.
- Las cuentas de usuario que tengan privilegios de sistema a través de su pertenencia a grupos o por cualquier otro medio, deben tener claves de acceso distintas del resto de cuentas mantenidas por dicho usuario en los servicios y recursos informáticos del ITFIP.
- En la medida de lo posible, las claves de acceso deberán ser generadas automáticamente con las características recomendadas en esta política y se les comunicará a los usuarios siempre en estado "expirado" para obligar al usuario a cambiarla en el primer uso que hagan de la cuenta o servicio.
- Las claves de acceso por defecto asociadas a los sistemas o aplicaciones nuevas deberán ser cambiadas antes de poner estos sistemas en producción. También se desactivarán aquellas cuentas "por defecto" que no sean imprescindibles.
- Todas las claves de acceso de sistema y de usuario de recursos y servicios del ITFIP deben respetar las recomendaciones descritas en la presente política.
- Algunos servicios en los que sea crítico el mantener la seguridad de las claves de acceso podrán determinar medidas adicionales de protección de la misma.

### 2. Recomendaciones generales para la selección de claves de acceso

Las claves de acceso son usadas con múltiples propósitos. Éstas pueden usarse en cuentas de usuario, sistema para el manejo de los recursos informáticos del ITFIP, servicios Web, cuentas de correo electrónico, protectores de pantalla, administración de dispositivos remotos, etc. Se debe poner especial atención en la selección de claves de acceso fuertes para la autenticación en todos los recursos y servicios informáticos del ITFIP. La seguridad de las claves de acceso se basa en que:

- La clave de acceso personal sólo la conoce el usuario propietario de la misma.
- La clave de acceso debe ser lo suficientemente "fuerte" como para no ser descifrada.
- Para que una clave de acceso sea considerada "fuerte" (segura):
- Debe tener mínimo 8 caracteres.

<sup>1</sup> Estos lineamientos son tomados del documento "Política de contraseñas de la universidad politécnica de valencia". Consultado en [https://www.upv.es/entidades/ASIC/normativa/politica\\_contraseñas.pdf](https://www.upv.es/entidades/ASIC/normativa/politica_contraseñas.pdf), el día y hora: 17-01-2015 a las 11:35.



- Se debe usar como mínimo los tres siguientes grupos. El cuarto (símbolos) es de uso opcional:
  1. Letras minúsculas.
  2. Letras mayúsculas.
  3. Números (por ejemplo, 1, 2, 3).
  4. Símbolos (por ejemplo, ¡, @, Ñ, =, -, etc.).
- No ser, ni derivarse de una palabra del diccionario, de la jerga o de un dialecto.
- No debe utilizar secuencias básicas de teclado (por ejemplo: "qwerty", "asdf" o las típicas en numeración: "1234" o "98765")
- No repetir los mismos caracteres en la misma clave de acceso. (ej.: "111222").
- No derivarse del nombre del usuario o de algún pariente cercano.
- No derivarse de información personal (del número de teléfono, número de identificación, fecha de nacimiento, etc...) del usuario o de algún pariente cercano.
- No podrá contener el nombre de usuario o del nombre completo de persona.
- No podrá tener espacios en blanco.

Al crear la clave de acceso, se debe tener presente que en el caso de que se use un teclado que no sean españoles, los símbolos que utiliza en sus claves de acceso pueden estar en sitios diferentes del teclado.

Las claves de acceso no deben ser almacenadas por escrito nunca. Intente crear claves de acceso que pueda recordar fácilmente. Una forma de recordarlo con facilidad es crear una clave de acceso basada en una frase fácilmente recordable. Ejemplo:

Frase: dinero llama dinero  
Clave de acceso: \$Dinero1llamaDienro2.-

### 3. Recomendaciones para la protección de las claves de acceso

No utilice la misma clave de acceso que utiliza para las cuentas de recursos y servicios informáticos del ITFIP en otras cuentas que no sean del ITFIP (acceso a su proveedor de servicios personal, acceso a servicios de su banco, etc.).

Cuando sea posible, no utilice las mismas claves de acceso en distintas cuentas y servicios informáticos del ITFIP. Por ejemplo, utilice claves de acceso distintas para su usuario de la plataforma AIDD y para su correo electrónico.

No comparta las cuentas y claves de acceso a los recursos informáticos con nadie, incluyendo administrativos, secretarías, etc. Todas las claves de acceso deben ser tratadas como información sensible y confidencial.

A continuación, se presenta una lista de recomendaciones para el buen uso de las claves de acceso:

- No revele su clave de acceso por teléfono a NADIE, incluso aunque le hablen en nombre de la Coordinación de Sistemas o de un superior suyo en la organización.
- No revele las claves de acceso en mensajes de correo electrónico ni a través de cualquier otro medio de comunicación electrónica.
- Nunca escriba las claves de acceso en papel y lo guarde. Tampoco almacene claves de acceso en archivos en el computador sin que sean encriptado o colocarles de algún mecanismo de seguridad.
- Las claves de acceso no deben ser incluidas en mensajes de correo electrónico, ni ningún otro medio de comunicación electrónica.
- Las claves no deben ser comunicadas las claves de acceso en conversaciones telefónicas.
- No de sus claves acceso a sus superiores, ni a sus colaboradores.
- No hable sobre las claves de acceso delante de otras personas.



- No revele sus claves de acceso en ningún cuestionario o formulario, independientemente de la confianza que le inspire el mismo.
- No comparta las claves de acceso con familiares.
- No revele las claves de acceso a sus compañeros cuando se marche de vacaciones.
- No se debe utilizar como clave de acceso, ni contener, el nombre de usuario asociado a la clave de acceso.
- No utilice la característica de “Recordar Contraseña o claves de acceso” existente en algunas aplicaciones.
- No escribir las claves de acceso computadores de los que se desconozca su nivel de seguridad y puedan estar monitorizados, o en computadores de uso público (bibliotecas, cibercafés, telecentros, etc.).
- Si alguien le pide la clave de acceso, refiérase a este documento o pídale que se comunique con la Coordinación de Sistemas del ITFIP.
- Si sospecha que una cuenta o alguna de sus claves de acceso pueden haber sido comprometidas, comuníquelo inmediatamente a la coordinación de Sistemas del ITFIP y cambie las claves de acceso de todas sus cuentas.
- Cambie las claves de acceso con la frecuencia recomendada para cada tipo de cuenta y servicio.

#### 4. Asignación de nombre de usuario

La asignación de usuarios y de claves de acceso para las cuentas con las que se pueden usar los recursos informáticos del ITFIP está en cabeza de los administradores de cada uno de dichos recursos y son ellos los que, de acuerdo al rol establecido en las aplicaciones y recursos informáticos, definen y administran las cuentas de los usuarios que usan los deferentes recursos.

Los nombres de usuarios asignados para las cuentas con las que se usan generalmente los recursos informáticos, se asignan de acuerdo a las necesidades de cada uno de las aplicaciones que se usan para el uso de los recursos informáticos. Sin embargo, en la medida de lo posible, para la creación de claves de acceso se debe seguir lo establecido en la política de uso de datos establecida en la institución.

#### REFERENCIAS

Shea, Virginia. Netiquettes. Disponible en  
[http://www.reynolds.edu/get\\_started/distance\\_learning/CoreRulesofNetiquette.pdf](http://www.reynolds.edu/get_started/distance_learning/CoreRulesofNetiquette.pdf). Consultado en  
27.11.2017 - 10:31

Universidad politécnica de valencia. Política de contraseñas. 2010  
[https://www.upv.es/entidades/ASIC/normativa/politica\\_contrasenyas.pdf](https://www.upv.es/entidades/ASIC/normativa/politica_contrasenyas.pdf), el día y hora: 17-01-2015 a las  
11:35



## ANEXO 1

### AUTORIZACIÓN Y REFRENDACIÓN DE USO DE DATOS PERSONALES

Con la expedición de la ley 1581 de 2012 y el Decreto 1377 de 2013, se desarrolla el principio constitucional que tienen todas las personas a conocer, actualizar y rectificar todo tipo de información recogida o, que haya sido objeto de tratamiento de datos personales en bancos o bases de datos y, en general en archivos de entidades públicas y/o privadas

El ITFIP como institución que almacena, y recolecta datos personales requiere obtener su autorización para que de manera libre, previa, expresa, voluntaria, y debidamente informada, permita a todas las dependencias académicas y/o administrativas, recolectar, recaudar, almacenar, usar, circular, suprimir, procesar, compilar, intercambiar, dar tratamiento, actualizar y disponer de los datos que han sido suministrados y que se han incorporado en distintas bases o bancos de datos, o en repositorios electrónicos de todo tipo con que cuenta la Institución. Esta información es, y será utilizada en el desarrollo de las funciones propias del ITFIP en su condición de institución de educación superior, de forma directa o a través de terceros.

El ITFIP en los términos dispuestos por el artículo 10 del decreto 1377 de 2013 queda autorizada de manera expresa e inequívoca para mantener y manejar toda su información, a no ser que usted le manifieste lo contrario de manera directa, expresa, inequívoca y por escrito a la cuenta de correo electrónico dispuesta para tal efecto: [info@itfip.edu.co](mailto:info@itfip.edu.co)

“Consiento y autorizo de manera previa, expresa e inequívoca que mis datos personales sean tratados conforme a lo previsto en el presente documento y/o autorización”.

Si usted no desea que sus datos personales sean utilizados por el ITFIP, podrá revocar de manera parcial o total tal autorización de manera expresa e inequívoca, directa, expresa y por escrito bien sea en medio físico o electrónico; o de manera oral, o por cualquier medio o conducta inequívoca que permita concluir de forma razonable que se revoca tal autorización o consentimiento.

En el evento en que usted tenga alguna observación y/o comentario sobre el manejo y uso de sus datos personales, o en caso de que usted considere que el ITFIP dio un uso contrario al autorizado y a las leyes aplicables; o no desee seguir recibiendo información relacionada con el ITFIP y sus actividades, según el presente documento, usted podrá contactarnos a través de una comunicación dirigida a la Oficina Jurídica, responsable de protección de datos en el ITFIP en:

Dirección: Calle 18 Carrera 1ª Barrio Arkabal Espinal, Tolima – Colombia  
Oficina Jurídica ITFIP  
Correo electrónico: [info@itfip.edu.co](mailto:info@itfip.edu.co)  
Atención al ciudadano: 57+3166254592