



Instituto de Investigaciones Dr. José María Luis Mora

Secretaría General

**Subdirección de Tecnologías de la Información
y Comunicaciones**

**Manual de Procedimientos de
Tecnologías de la Información y
Comunicaciones**

2020

Índice

Introducción

I. Objetivo del Manual

II. Procedimientos

1. Procedimiento del uso de la sala de computo

- 1.1 Propósito del Procedimiento
- 1.2 Alcance
- 1.3 Referencia
- 1.4 Responsabilidades
- 1.5 Definiciones
- 1.6 Método de trabajo:
 - a) Políticas y Lineamientos
 - b) Descripción de actividades
 - c) Diagrama de flujo del procedimiento
 - d) Formatos e Instructivos
 - e) Anexos

2. Procedimiento de Atención de Incidentes y Solicitudes de Servicios.

- 2.1 Propósito del Procedimiento
- 2.2 Alcance
- 2.3 Referencia
- 2.4 Responsabilidades
- 2.5 Definiciones
- 2.6 Método de trabajo:
 - a) Políticas y Lineamientos
 - b) Descripción de actividades
 - c) Diagrama de flujo del procedimiento
 - d) Formatos e Instructivos
 - e) Anexos

3. Procedimiento de planeación estratégica de TIC.

- 3.1 Propósito del Procedimiento
- 3.2 Alcance
- 3.3 Referencia
- 3.4 Responsabilidades
- 3.5 Definiciones
- 3.6 Método de trabajo:
 - a) Políticas y Lineamientos

- b) Descripción de actividades
- c) Diagrama de flujo del procedimiento
- d) Formatos e Instructivos
- e) Anexos

4. Procedimiento de la integración de archivos de expedientes de contratos en materia de TIC

- 4.1 Propósito del Procedimiento
- 4.2 Alcance
- 4.3 Referencia
- 4.4 Responsabilidades
- 4.5 Definiciones
- 4.6 Método de trabajo:
 - a) Políticas y Lineamientos
 - b) Descripción de actividades
 - c) Diagrama de flujo del procedimiento
 - d) Formatos e Instructivos
 - e) Anexos

5. Procedimiento para la contratación de bienes o servicios en materia de TIC.

- 5.1 Propósito del Procedimiento
- 5.2 Alcance
- 5.3 Referencia
- 5.4 Responsabilidades
- 5.5 Definiciones
- 5.6 Método de trabajo:
 - a) Políticas y Lineamientos
 - b) Descripción de actividades
 - c) Diagrama de flujo del procedimiento
 - d) Formatos e Instructivos
 - e) Anexos

6. Procedimiento para acceder a la red inalámbrica del Instituto Mora

- 6.1 Propósito del Procedimiento
- 6.2 Alcance
- 6.3 Referencia
- 6.4 Responsabilidades
- 6.5 Definiciones
- 6.6 Método de trabajo:

- a) Políticas y Lineamientos
- b) Descripción de actividades
- c) Diagrama de flujo del procedimiento
- d) Formatos e Instructivos
- e) Anexos

7. Procedimiento para generación de contraseñas de usuarios administradores

- 7.1 Propósito del Procedimiento
- 7.2 Alcance
- 7.3 Referencia
- 7.4 Responsabilidades
- 7.5 Definiciones
- 7.6 Método de trabajo:
 - a) Políticas y Lineamientos
 - b) Descripción de actividades
 - c) Diagrama de flujo del procedimiento
 - d) Formatos e Instructivos
 - e) Anexos

Introducción

El Instituto de Investigaciones Dr. José María Luis Mora fue creado por Decreto Presidencial publicado en el Diario Oficial de la Federación el 30 de septiembre de 1981, y reestructurado también por Decreto Presidencial el 30 de agosto de 2000. Tiene por objeto fomentar la investigación científica y la formación de profesores y especialistas en el campo de la historia

y otras ciencias sociales, así como conservar y acrecentar el acervo bibliográfico de obras representativas de la cultura mexicana.

La Secretaría General tiene dentro de sus funciones la de coordinar en colaboración con la Subdirección de Tecnologías de la Información y Comunicaciones, la generación y operación actualizada de bases de datos, sistemas de trabajo automatizados o semi automatizados, paqueterías; y en general garantizar la funcionalidad de la arquitectura informática de suministro de servicios de voz y datos para la operación del Instituto.

Es por ello que la Subdirección de Tecnologías de la Información y Comunicaciones tiene la responsabilidad de elaborar y mantener actualizado el manual de procedimientos, el cual, por su contenido, resulta un instrumento elemental para apoyar el cumplimiento de las atribuciones encomendadas a esta unidad administrativa, y al mismo tiempo en un instrumento de apoyo administrativo y comunicación para las diversas unidades administrativas que conforman el Instituto Mora.

Objetivo del Manual

1. General

Estandarizar y eficientar la gestión de los servicios de Tecnologías de la Información que se prestan en el Instituto a fin de propiciar una cultura de servicio con enfoque a la mejora continua y consolidar las áreas que los gestionan, haciendo énfasis en la calidad y seguridad de la información.

Dirigir, supervisar, controlar y evaluar las actividades, programas, objetivos y metas de la Subdirección de Tecnologías de la Información y Comunicaciones.

Determinar técnicamente las características de los bienes y servicios en materia de tecnologías de la información y comunicaciones que deban ser adquiridos o contratados y administrar la infraestructura y los servicios de tecnologías de la información y comunicaciones que se proporcionen a las áreas sustantivas, de apoyo sustantivo y de apoyo administrativo del Instituto.

También tiene a su cargo dirigir y administrar un sistema de gestión de seguridad de la información en medios tecnológicos. de conformidad con las disposiciones jurídicas aplicables, para mantener la seguridad de la información y comunicaciones del Instituto, con la finalidad de asegurar la calidad, la disponibilidad e integridad de los datos.

2. Objetivos Específicos

1. Establecer una cultura orientada a procesos, usuarios y resultados.
2. Implementar un modelo de control interno en Tecnologías de la Información y Comunicaciones.
3. Formalizar y estandarizar los procedimientos de trabajo en materia de Tecnologías de la Información y Comunicaciones.
4. Implementar un modelo de gobierno en Tecnologías de la Información y Comunicaciones.
5. Establecer una estrategia para impulsar la innovación tecnológica a través de administrar el rumbo y los dominios tecnológicos.
6. Entregar consistentemente servicios de TI con los "niveles de servicios" establecidos.
7. Eficientar la transición de la operación de las soluciones tecnológicas y componentes de Tecnologías de la Información.
8. Identificar los procedimientos de cada una de los dominios tecnológicos que conforman la Subdirección de Tecnologías de Información y Comunicaciones.
9. Establecer las actividades de cada uno de los procedimientos.
10. Determinar a los responsables de la atención y desahogo de cada una de las actividades de los procedimientos.
11. Ejecutar de una forma correcta las actividades correspondientes a cada etapa de los procedimientos.

12. Apoyar el ejercicio de las funciones de los servidores públicos de la Subdirección de Tecnologías de Información y Comunicaciones.

**1. Procedimiento para el uso de las salas de
cómputo
(MP/SG/STIC/01/2020)**

1.1. **Propósito del Procedimiento**

Con fundamento en el artículo 9º, fracción VI del Decreto por el cual se reestructura el Instituto de Investigaciones Dr. José María Luis Mora, y con el objeto de regular el uso de las salas de cómputo del Instituto.

1.2. **Alcance**

El equipo localizado en las salas de cómputo es para uso exclusivo de los alumnos inscritos en los programas académicos, de los profesores-investigadores y personal del Instituto Mora, por lo que no se permite la entrada a personas externas, a excepción de las que autoricen los titulares de área, en el marco de sus atribuciones y las disposiciones aplicables, de común acuerdo con la Subdirección de Tecnologías de la Información y Comunicaciones.

1.3. **Referencia o Marco normativo**

Marco normativo

- a) Decreto de reestructuración del Instituto de Investigaciones Dr. José María Luis Mora.
- b) Estatuto Orgánico.
- c) Manual General de Organización.
- d) Manual Administrativo de Aplicación General en Materia de Tecnologías de Información y Comunicaciones y de Seguridad de la Información

1.4. **Responsables**

- Subdirección de Tecnologías de la Información y Comunicaciones
- Departamento de Servicios Escolares

1.5. **Definiciones**

Activo de información: Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para la Institución, debe ser protegido para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.

Acuerdo: el Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones y en la de Seguridad de la Información, así como establecer el Manual Administrativo de Aplicación General en dichas materias.

Acuerdo de nivel de servicio SLA: El acuerdo de nivel de servicio que se compromete con la unidad administrativa solicitante, al entregar un aplicativo de cómputo o servicio de TIC (*Service Level Agreement*, por sus siglas en inglés).

Acuerdo de nivel operacional OLA: El acuerdo de nivel operacional entre los responsables de los diversos componentes de la arquitectura tecnológica de un aplicativo de cómputo o servicio de TIC, que se debe definir y cumplir para responder a los acuerdos de nivel de servicio SLA comprometidos (*Operational Level Agreement* por sus siglas en inglés).

Ambiente de trabajo: El conjunto de herramientas, utilerías, programas, aplicaciones, información, facilidades y organización que un usuario tiene disponible para el desempeño de sus funciones de manera controlada, de acuerdo con los accesos y privilegios que tenga asignados por medio de una identificación única y una contraseña.

Amenaza: A cualquier posible acto que pueda causar algún tipo de daño a los activos de información de la Institución.

Análisis de riesgos: El uso sistemático de la información para identificar las fuentes de vulnerabilidades y amenazas a los activos de TIC, a la infraestructura crítica o a los activos de información, así como efectuar la evaluación de su magnitud o impacto y estimar los recursos necesarios para eliminarlas o mitigarlas.

Área contratante: A la facultada en la Institución para realizar procedimientos de contratación, a efecto de adquirir o arrendar bienes o contratar la prestación de servicios.

Área requirente: A la que, en la Institución, solicite o requiera formalmente la adquisición o arrendamiento de bienes o la prestación de servicios, o aquélla que los utilizará.

Área solicitante o usuaria: A la que, en la Institución, efectúa originalmente la petición a la Subdirección de Tecnologías de la Información y Comunicaciones para obtener un bien o servicio de TIC y/o que hará uso del mismo.

Área técnica: A la que, en la Institución, elabora las especificaciones técnicas que se deberán incluir en el procedimiento de contratación, evalúa la propuesta técnica de las proposiciones y es responsable de responder en la junta de aclaraciones las preguntas que sobre estos aspectos realicen los licitantes. El área técnica podrá tener también el carácter de área requirente.

Arquitectura tecnológica: A la estructura de hardware, software y redes requerida para dar soporte a la implementación de los aplicativos de cómputo, soluciones tecnológicas o servicios de TIC de la Institución.

Disponibilidad: La característica de la información de permanecer accesible para su uso cuando así lo requieran individuos o procesos autorizados.

Entregable: El producto adquirido, desarrollado o personalizado, con características cuantificables y medibles en términos de su valor, integralidad, funcionalidad y capacidades.

Evento: El suceso que puede ser observado, verificado y documentado, en forma manual o automatizada, que puede llevar al registro de incidentes.

Funcionalidad: Las características de los aplicativos de cómputo, soluciones tecnológicas o de un servicio de TIC, que permiten cubrir las necesidades o requerimientos de un usuario.

Gestión de riesgos: La identificación, valoración y ejecución de acciones, para el control y minimización de los riesgos que afecten a los activos de TIC, a la infraestructura crítica o a los activos de información de la Institución.

Impacto: Al grado de los daños y/o de los cambios sobre un activo de información, por la materialización de una amenaza.

Incidente: A la afectación o interrupción a los activos de TIC, a las infraestructuras críticas, así como a los activos de información de una Institución, incluido el acceso no autorizado o no programado a éstos.

Infraestructuras críticas: Las instalaciones, redes, servicios y equipos asociados o vinculados con activos de TIC o activos de información, cuya afectación, interrupción o destrucción tendría un impacto mayor, entre otros, en la salud, la seguridad, el bienestar económico de la población o en el eficaz funcionamiento de las Instituciones.

Infraestructura de TIC: el hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar los servicios de TIC.

Integridad: La acción de mantener la exactitud y corrección de la información y sus métodos de proceso

Mesa de servicios: El punto de contacto único, en el cual se reciben las solicitudes de servicio de los usuarios de equipos y servicios de TIC en la Institución.

Objetivos estratégicos de TIC: El conjunto de resultados que se prevé alcanzar y que se integran en el PETIC, los cuales describen el alcance de las acciones que serán llevadas a cabo por la Subdirección de Tecnologías de la Información y Comunicaciones.

PETIC: el Plan Estratégico de Tecnologías de la Información y Comunicaciones que elaboran las Instituciones en los términos señalados en el MAAGTICSI;

Problema: La causa de uno o más incidentes, del cual se plantea una solución alterna en espera de una solución definitiva.

Proyectos de TIC: el esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado de TIC;

Requerimientos funcionales: La característica que requiere cumplir un producto o entregable asociado a una función en un proceso o servicio automatizado, o por automatizar.

Riesgo: La posibilidad de que una amenaza pueda explotar una vulnerabilidad y causar una pérdida o daño sobre los activos de TIC, las infraestructuras críticas o los activos de información de la Institución.

Sistema informático: El conjunto de componentes o programas construidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso, de acuerdo a requerimientos previamente definidos.

TIC: las tecnologías de información y comunicaciones que comprenden el equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.

Usuarios: Los servidores públicos o aquéllos terceros que han sido acreditados o cuentan con permisos para hacer uso de los servicios de TIC.

Validación: La actividad que asegura que un servicio de TIC, producto o entregable, nuevo o modificado, satisface las necesidades acordadas previamente con la unidad administrativa solicitante.

Verificación: La actividad que permite revisar si un servicio de TIC o cualquier otro producto o entregable, está completo y acorde con su especificación de diseño.

Vulnerabilidades: Las debilidades en la seguridad de la información dentro de una organización que potencialmente permite que una amenaza afecte a los activos de TIC, a la infraestructura crítica, así como a los activos de información.

1.6. Lineamientos y Políticas

Del registro de usuarios

- 1) Para utilizar el equipo de cómputo de la Sala, los usuarios deberán registrarse con su cuenta y clave asignada previamente por la Subdirección de Tecnologías de la Información y Comunicaciones.
- 2) Queda prohibido registrarse con la cuenta de otro usuario.
- 3) Queda prohibido reservar equipos.
- 4) Queda estrictamente prohibido consumir cualquier tipo de alimento o bebida dentro de las Salas de Cómputo.

De las instalaciones

- 1) Las instalaciones de las Salas de Cómputo deberán ser conservadas limpias y en orden.
- 2) Las Salas de Cómputo son un área de trabajo, por lo que no se permite la reunión de grupos en torno a un equipo, esto con la finalidad de evitar molestias a los demás usuarios.
- 3) En el caso de que se desarrollen cursos o eventos en las Salas de Cómputo, se deberá respetar el horario especificado para ellos.
- 4) Igualmente se deberá respetar el programa de mantenimiento correctivo y preventivo que se aplica a los equipos de las Salas.
- 5) Todo anuncio relacionado con las Salas de Cómputo deberá ser colocado en el tablero localizado fuera de las Salas, donde también se deberán anunciar los calendarios para eventos o cursos.
- 6) El horario de las Salas de Cómputo es de 8:30 a 21.00 horas, de lunes a viernes y los sábados, previa solicitud a la responsable del Departamento de Servicios Escolares, de 9:00 a 15:00 horas.

- 7) El personal de la Subdirección de Tecnologías de la Información y Comunicaciones no se responsabiliza por ningún objeto olvidado ni por ningún archivo de usuario almacenado en los equipos; el usuario es el único responsable de su información, por lo que se recomienda respaldar sus archivos en su espacio de almacenamiento en la nube o dispositivo portátil (CD, memoria USB, disco duro externo u otro compatible con el equipo de que se trate).
- 8) El teléfono deberá ser usado exclusivamente para reportar incidentes a la Subdirección de Tecnologías de la Información y Comunicaciones por lo que no se permite su utilización con ningún otro propósito.
- 9) Todo usuario deberá tener cuidado extremo con el equipo que utilice.
- 10) Queda prohibido dejar encendido el equipo con procesos activos, cuando el usuario haya finalizado el uso o se tome un receso.
- 11) Todo dispositivo de almacenamiento (CD, memoria USB, disco duro externo, etc.) que se use en los equipos deberá ser revisado previamente con el antivirus. Esta medida evitará interrupciones de servicio que pueden afectar a todos los usuarios.
- 12) Queda prohibido instalar o borrar algún programa, así como cambiar la configuración del equipo. Si se requiere el uso de algún software en particular, se deberá solicitar su instalación al personal de la Subdirección de Tecnologías de la Información y Comunicaciones.

De la impresión

- 1) Cada usuario deberá traer papel para la impresión de sus trabajos.
- 2) Para garantizar el correcto funcionamiento de los equipos de impresión no se permite utilizar papel preimpreso o reciclado.
- 3) El tipo de papel a utilizar será bond de 75 gr. tamaño carta, oficio o doble carta; no se permite la impresión en otro tamaño o tipo de papel sin la autorización expresa de la Subdirección de Tecnologías de la Información y Comunicaciones.
- 4) En caso de que el papel se atore se deberá solicitar la asistencia del personal del área, por ningún motivo el usuario podrá abrir las charolas.

De las fallas de equipo

- 1) En caso de detectar falla en algún equipo o componente, ésta deberá ser reportada al personal de la Subdirección de Tecnologías de la Información y Comunicaciones vía telefónica.
- 2) En caso de no funcionar temporalmente algún dispositivo, la Subdirección de Tecnologías de la Información y Comunicaciones se encargará de su mantenimiento, y mientras esto sucede, se suspenderá el servicio del dispositivo en cuestión.

De las sanciones

- 1) La no observancia a lo dispuesto en estos Lineamientos será sancionado de acuerdo a la gravedad de la falta, conforme a lo que establezca el Comité de Informática.
- 2) La responsabilidad por daños y perjuicios se aplicará a los autores materiales e intelectuales.

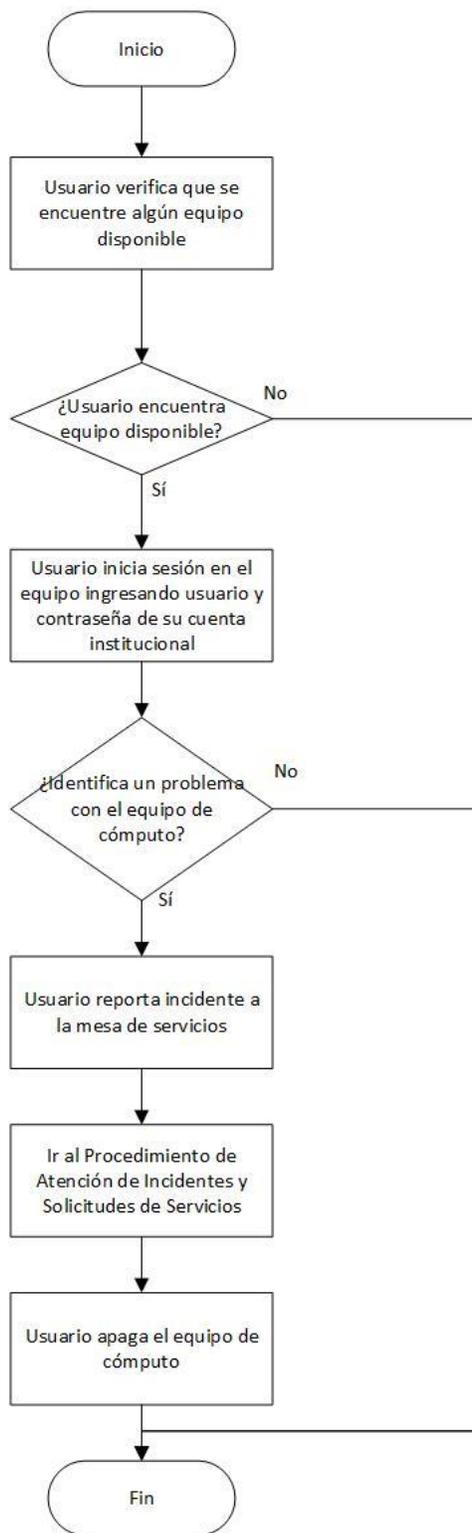
De lo no previsto

- 1) Lo no previsto por estos Lineamientos será resuelto por el Comité de Informática, de acuerdo a la normatividad vigente.

	Descripción de Actividades		Clave:
			Fecha:
	Nombre de Procedimiento: Procedimiento de la sala de cómputo		Versión: 1.0
			Página: 1/
Unidad Administrativa: Subdirección de Tecnologías de la Información y comunicaciones		Área Responsable: Soporte técnico	

Paso	Responsable	Actividad	Documento de trabajo (Clave)
1	Usuario	1. El usuario verifica que se encuentre algún equipo de cómputo disponible.	
2		2. El usuario inicia sesión en el equipo ingresando usuario y contraseña de su cuenta institucional.	
3		3. El usuario identifica un problema relacionado con el equipo de cómputo que está usando Si: Continúa en actividad 4. No: Continúa en actividad 5.	
4		4. El usuario afectado reporta incidente a la mesa de servicios vía telefónica utilizando la extensión telefónica instalada en la sala de cómputo o al correo electrónico asistenciatic@mora.edu.mx .	
5		5. Ir a Procedimiento de Atención de Incidentes y Solicitudes de Servicios	
6		6. Al concluir su actividad, el usuario apaga el equipo de cómputo.	
FIN DEL PROCEDIMIENTO			

Diagrama de flujo del procedimiento



2. Procedimiento de Atención de Incidentes y Solicitudes de Servicios.

(MP/SG/STIC/02/2020)

2.1. Propósito del Procedimiento

Establecer y operar un punto único de contacto para que las y los usuarios hagan llegar sus solicitudes de servicios e incidentes de tecnologías de información y comunicaciones (TIC),

a efecto de que las mismas sean atendidas de acuerdo a los niveles de servicio establecidos, restaurando la operación normal de los servicios de TIC elevado con ello la disponibilidad de los servicios de TIC del Instituto.

2.2. Alcance

Todo servicio provisto por la Subdirección de Tecnologías de la Información y Comunicaciones deberá ser registrado en el Catálogo de Servicios, así como tener definidos los tiempos de respuesta para la atención de incidentes y solicitudes. El catálogo de servicios será actualizado trimestralmente.

2.3. Referencia o Marco normativo

Marco normativo

- a) Decreto de reestructuración del Instituto de Investigaciones Dr. José María Luis Mora.
- b) Estatuto Orgánico.
- c) Manual General de Organización.
- d) Manual Administrativo de Aplicación General en Materia de Tecnologías de Información y Comunicaciones y de Seguridad de la Información

2.4. Responsables

Subdirección de Tecnologías de la Información y comunicaciones

2.5. Definiciones

Activo de información: Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para la Institución, debe ser protegido para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.

Acuerdo: el Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones y en la de Seguridad de la Información, así como establecer el Manual Administrativo de Aplicación General en dichas materias.

Acuerdo de nivel de servicio SLA: El acuerdo de nivel de servicio que se compromete con la unidad administrativa solicitante, al entregar un aplicativo de cómputo o servicio de TIC (*Service Level Agreement*, por sus siglas en inglés).

Acuerdo de nivel operacional OLA: El acuerdo de nivel operacional entre los responsables de los diversos componentes de la arquitectura tecnológica de un aplicativo de cómputo o

servicio de TIC, que se debe definir y cumplir para responder a los acuerdos de nivel de servicio SLA comprometidos (*Operational Level Agreement* por sus siglas en inglés).

Ambiente de trabajo: El conjunto de herramientas, utilerías, programas, aplicaciones, información, facilidades y organización que un usuario tiene disponible para el desempeño de sus funciones de manera controlada, de acuerdo con los accesos y privilegios que tenga asignados por medio de una identificación única y una contraseña.

Amenaza: A cualquier posible acto que pueda causar algún tipo de daño a los activos de información de la Institución.

Análisis de riesgos: El uso sistemático de la información para identificar las fuentes de vulnerabilidades y amenazas a los activos de TIC, a la infraestructura crítica o a los activos de información, así como efectuar la evaluación de su magnitud o impacto y estimar los recursos necesarios para eliminarlas o mitigarlas.

Área contratante: A la facultada en la Institución para realizar procedimientos de contratación, a efecto de adquirir o arrendar bienes o contratar la prestación de servicios.

Área requirente: A la que, en la Institución, solicite o requiera formalmente la adquisición o arrendamiento de bienes o la prestación de servicios, o aquélla que los utilizará.

Área solicitante o usuaria: A la que, en la Institución, efectúa originalmente la petición a la Subdirección de Tecnologías de la Información y Comunicaciones para obtener un bien o servicio de TIC y/o que hará uso del mismo.

Área técnica: A la que, en la Institución, elabora las especificaciones técnicas que se deberán incluir en el procedimiento de contratación, evalúa la propuesta técnica de las proposiciones y es responsable de responder en la junta de aclaraciones las preguntas que sobre estos aspectos realicen los licitantes. El área técnica podrá tener también el carácter de área requirente.

Arquitectura tecnológica: A la estructura de hardware, software y redes requerida para dar soporte a la implementación de los aplicativos de cómputo, soluciones tecnológicas o servicios de TIC de la Institución.

Disponibilidad: La característica de la información de permanecer accesible para su uso cuando así lo requieran individuos o procesos autorizados.

Entregable: El producto adquirido, desarrollado o personalizado, con características cuantificables y medibles en términos de su valor, integralidad, funcionalidad y capacidades.

Evento: El suceso que puede ser observado, verificado y documentado, en forma manual o automatizada, que puede llevar al registro de incidentes.

Funcionalidad: Las características de los aplicativos de cómputo, soluciones tecnológicas o de un servicio de TIC, que permiten cubrir las necesidades o requerimientos de un usuario.

Gestión de riesgos: La identificación, valoración y ejecución de acciones, para el control y minimización de los riesgos que afecten a los activos de TIC, a la infraestructura crítica o a los activos de información de la Institución.

Impacto: Al grado de los daños y/o de los cambios sobre un activo de información, por la materialización de una amenaza.

Incidente: A la afectación o interrupción a los activos de TIC, a las infraestructuras críticas, así como a los activos de información de una Institución, incluido el acceso no autorizado o no programado a éstos.

Infraestructuras críticas: Las instalaciones, redes, servicios y equipos asociados o vinculados con activos de TIC o activos de información, cuya afectación, interrupción o destrucción tendría un impacto mayor, entre otros, en la salud, la seguridad, el bienestar económico de la población o en el eficaz funcionamiento de las Instituciones.

Infraestructura de TIC: el hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar los servicios de TIC.

Integridad: La acción de mantener la exactitud y corrección de la información y sus métodos de proceso

Mesa de servicios: El punto de contacto único, en el cual se reciben las solicitudes de servicio de los usuarios de equipos y servicios de TIC en la Institución.

Objetivos estratégicos de TIC: El conjunto de resultados que se prevé alcanzar y que se integran en el PETIC, los cuales describen el alcance de las acciones que serán llevadas a cabo por la Subdirección de Tecnologías de la Información y Comunicaciones.

PETIC: el Plan Estratégico de Tecnologías de la Información y Comunicaciones que elaboran las Instituciones en los términos señalados en el MAAGTICSI;

Problema: La causa de uno o más incidentes, del cual se plantea una solución alterna en espera de una solución definitiva.

Proyectos de TIC: el esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado de TIC;

Requerimientos funcionales: La característica que requiere cumplir un producto o entregable asociado a una función en un proceso o servicio automatizado, o por automatizar.

Riesgo: La posibilidad de que una amenaza pueda explotar una vulnerabilidad y causar una pérdida o daño sobre los activos de TIC, las infraestructuras críticas o los activos de información de la Institución.

Sistema informático: El conjunto de componentes o programas construidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso, de acuerdo a requerimientos previamente definidos.

TIC: las tecnologías de información y comunicaciones que comprenden el equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.

Usuarios: Los servidores públicos o aquéllos terceros que han sido acreditados o cuentan con permisos para hacer uso de los servicios de TIC.

Validación: La actividad que asegura que un servicio de TIC, producto o entregable, nuevo o modificado, satisface las necesidades acordadas previamente con la unidad administrativa solicitante.

Verificación: La actividad que permite revisar si un servicio de TIC o cualquier otro producto o entregable, está completo y acorde con su especificación de diseño.

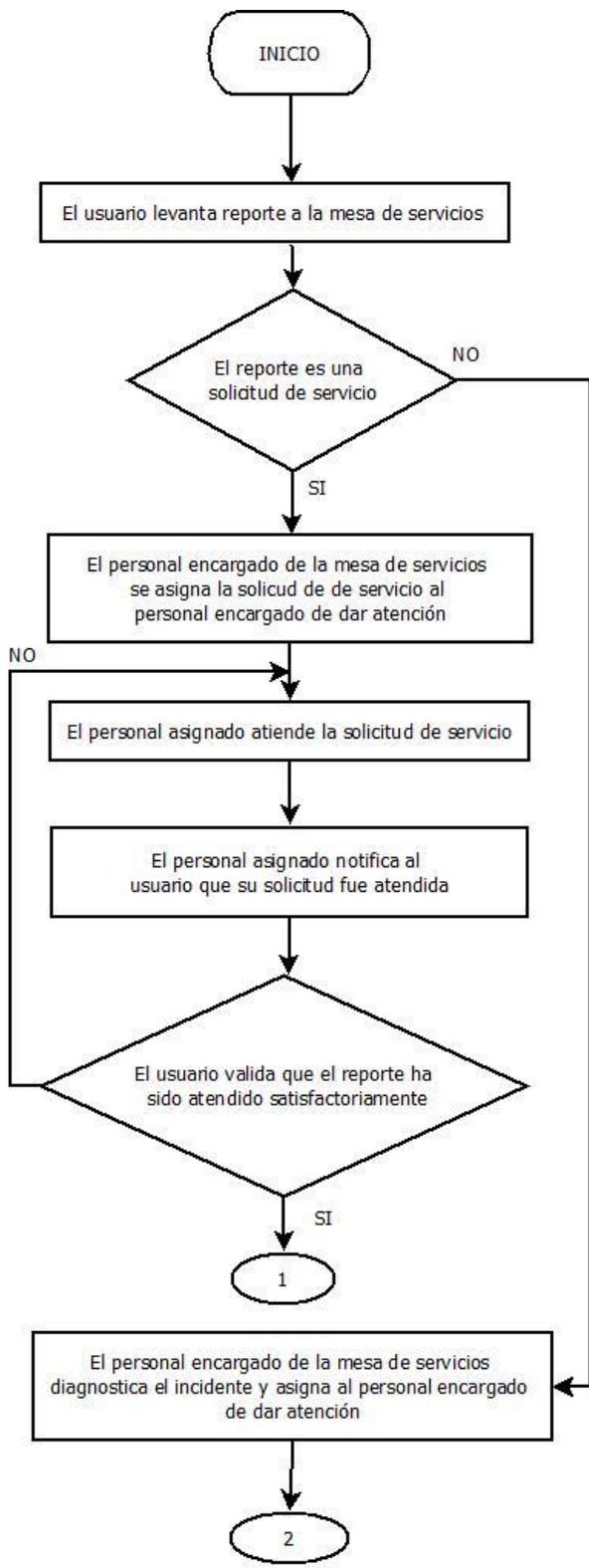
Vulnerabilidades: Las debilidades en la seguridad de la información dentro de una organización que potencialmente permite que una amenaza afecte a los activos de TIC, a la infraestructura crítica, así como a los activos de información.

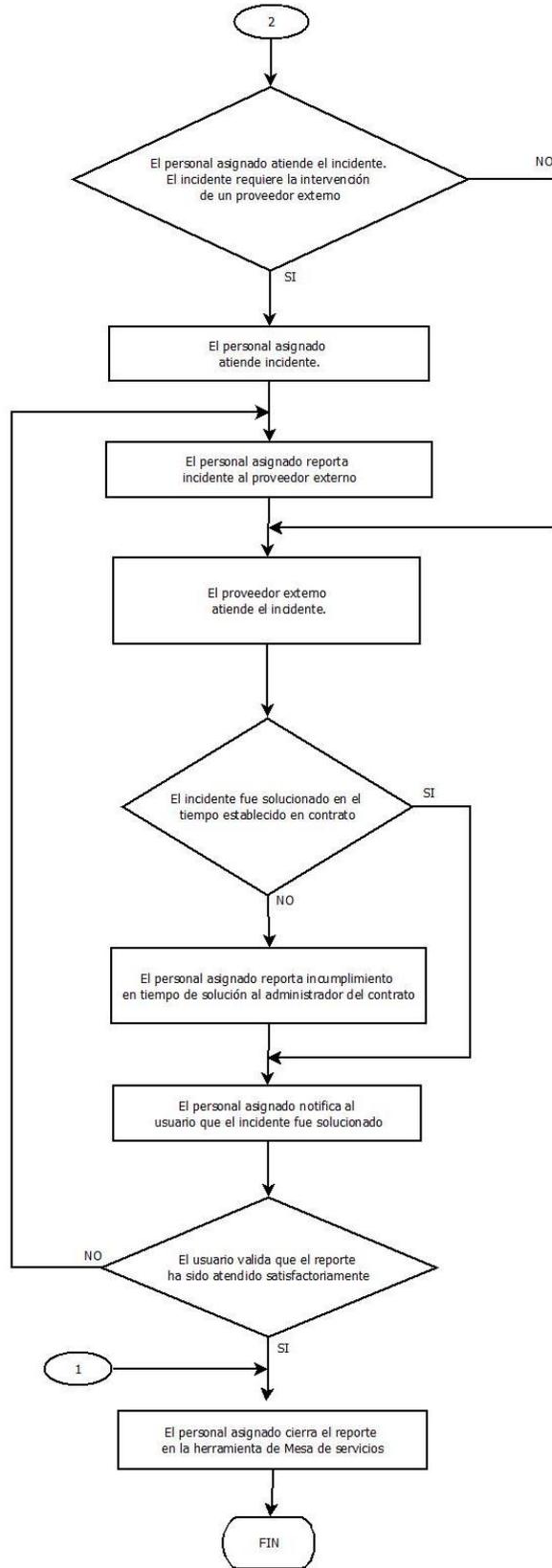
	Descripción de Actividades	Clave:
		Fecha:
	Nombre de Procedimiento: Procedimiento de Atención de Incidentes y Solicitudes de Servicios	Versión: 1.0
		Página: 1/
Unidad Administrativa: Subdirección de Tecnologías de la Información y comunicaciones		Área Responsable: Soporte técnico

Paso	Responsable	Actividad	Documento de trabajo (Clave)
1	Usuario	1. El usuario levanta reporte a la mesa de servicios vía telefónica a la extensión 1313 o al correo electrónico asistenciatic@mora.edu.mx .	
2	Encargado(a) de la mesa de servicios	2. El personal encargado de la mesa de servicios recibe el reporte. ¿El reporte es una solicitud de servicio? Sí: continúa en la actividad 3 No: continúa en la actividad 8	
3	Encargado(a) de la mesa de servicios	3. El personal encargado de la mesa de servicios asigna solicitud de servicio al personal encargado de dar atención.	
4	Personal asignado	4. El personal asignado atiende la solicitud de servicio.	
5	Personal asignado	5. El personal asignado notifica al usuario que su solicitud fue atendida.	
6	Usuario	6. El usuario valida que el reporte ha sido atendido satisfactoriamente. Sí: Continúa en actividad 16. No: continúa en actividad 4.	
7	Encargado(a) de la mesa de servicios	7. El personal encargado de la mesa de servicios diagnostica el incidente y asigna al personal encargado de dar atención.	
8	Personal asignado	8. El personal asignado atiende el incidente. El incidente requiere la intervención de un proveedor externo. Sí: continúa en la actividad 11	

Paso	Responsable	Actividad	Documento de trabajo (Clave)
9	Personal asignado	No: continúa en la actividad 10 9. El personal asignado atiende incidente.	
10	Personal asignado	10. El personal asignado reporta incidente al proveedor externo. Continúa en la actividad 15	
11	Proveedor externo	11. El proveedor externo atiende el incidente.	
12	Personal asignado	12. El incidente fue solucionado en el tiempo establecido en contrato. Si: Continúa en actividad 14 No: El Continúa en actividad 13	
13	Personal asignado	13. El personal asignado reporta incumplimiento en tiempo de solución al administrador del contrato.	
14	Personal asignado	14. El personal asignado notifica al usuario que el incidente fue solucionado.	
15	Usuario	15. El usuario valida que el reporte ha sido atendido satisfactoriamente. Sí: Continúa en actividad 16. No: continúa en actividad 10.	
16	Personal asignado	16. El personal asignado cierra el reporte en la herramienta de Mesa de servicios. FIN DEL PROCEDIMIENTO	

Diagrama de flujo del procedimiento





3. Procedimiento de planeación estratégica de TIC.

(MP/SG/STIC/03/2020)

3.1. **Propósito del Procedimiento**

Establecer un modelo de gobierno de TIC en la Institución, para efectuar, entre otras acciones, el análisis de las oportunidades de aprovechamiento de las TIC, la planeación estratégica de TIC y asegurar la adecuada organización al interior de la Subdirección de Tecnologías de la Información y Comunicaciones para la gestión de sus procesos y vinculación ordenada con sus usuarios.

3.2. **Alcance**

Identificar las necesidades en materia de TIC para establecer una Cartera Ejecutiva de proyectos para el ejercicio presupuestal siguiente.

3.3. **Referencia o Marco normativo**

Marco normativo

- a) Decreto de reestructuración del Instituto de Investigaciones Dr. José María Luis Mora.
- b) Estatuto Orgánico.
- c) Manual General de Organización.
- d) Manual Administrativo de Aplicación General en Materia de Tecnologías de Información y Comunicaciones y de Seguridad de la Información

3.4. **Responsables**

Subdirección de Tecnologías de la Información y comunicaciones

3.5. **Definiciones**

Activo de información: Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para la Institución, debe ser protegido para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.

Acuerdo: el Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones y en la de Seguridad de la Información, así como establecer el Manual Administrativo de Aplicación General en dichas materias.

Acuerdo de nivel de servicio SLA: El acuerdo de nivel de servicio que se compromete con la unidad administrativa solicitante, al entregar un aplicativo de cómputo o servicio de TIC (*Service Level Agreement*, por sus siglas en inglés).

Acuerdo de nivel operacional OLA: El acuerdo de nivel operacional entre los responsables de los diversos componentes de la arquitectura tecnológica de un aplicativo de cómputo o servicio de TIC, que se debe definir y cumplir para responder a los acuerdos de nivel de servicio SLA comprometidos (*Operational Level Agreement* por sus siglas en inglés).

Ambiente de trabajo: El conjunto de herramientas, utilerías, programas, aplicaciones, información, facilidades y organización que un usuario tiene disponible para el desempeño de sus funciones de manera controlada, de acuerdo con los accesos y privilegios que tenga asignados por medio de una identificación única y una contraseña.

Amenaza: A cualquier posible acto que pueda causar algún tipo de daño a los activos de información de la Institución.

Análisis de riesgos: El uso sistemático de la información para identificar las fuentes de vulnerabilidades y amenazas a los activos de TIC, a la infraestructura crítica o a los activos de información, así como efectuar la evaluación de su magnitud o impacto y estimar los recursos necesarios para eliminarlas o mitigarlas.

Área contratante: A la facultada en la Institución para realizar procedimientos de contratación, a efecto de adquirir o arrendar bienes o contratar la prestación de servicios.

Área requirente: A la que, en la Institución, solicite o requiera formalmente la adquisición o arrendamiento de bienes o la prestación de servicios, o aquélla que los utilizará.

Área solicitante o usuaria: A la que, en la Institución, efectúa originalmente la petición a la Subdirección de Tecnologías de la Información y Comunicaciones para obtener un bien o servicio de TIC y/o que hará uso del mismo.

Área técnica: A la que, en la Institución, elabora las especificaciones técnicas que se deberán incluir en el procedimiento de contratación, evalúa la propuesta técnica de las proposiciones y es responsable de responder en la junta de aclaraciones las preguntas que sobre estos aspectos realicen los licitantes. El área técnica podrá tener también el carácter de área requirente.

Arquitectura tecnológica: A la estructura de hardware, software y redes requerida para dar soporte a la implementación de los aplicativos de cómputo, soluciones tecnológicas o servicios de TIC de la Institución.

Disponibilidad: La característica de la información de permanecer accesible para su uso cuando así lo requieran individuos o procesos autorizados.

Entregable: El producto adquirido, desarrollado o personalizado, con características cuantificables y medibles en términos de su valor, integralidad, funcionalidad y capacidades.

Evento: El suceso que puede ser observado, verificado y documentado, en forma manual o automatizada, que puede llevar al registro de incidentes.

Funcionalidad: Las características de los aplicativos de cómputo, soluciones tecnológicas o de un servicio de TIC, que permiten cubrir las necesidades o requerimientos de un usuario.

Gestión de riesgos: La identificación, valoración y ejecución de acciones, para el control y minimización de los riesgos que afecten a los activos de TIC, a la infraestructura crítica o a los activos de información de la Institución.

Impacto: Al grado de los daños y/o de los cambios sobre un activo de información, por la materialización de una amenaza.

Incidente: A la afectación o interrupción a los activos de TIC, a las infraestructuras críticas, así como a los activos de información de una Institución, incluido el acceso no autorizado o no programado a éstos.

Infraestructuras críticas: Las instalaciones, redes, servicios y equipos asociados o vinculados con activos de TIC o activos de información, cuya afectación, interrupción o destrucción tendría un impacto mayor, entre otros, en la salud, la seguridad, el bienestar económico de la población o en el eficaz funcionamiento de las Instituciones.

Infraestructura de TIC: el hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar los servicios de TIC.

Integridad: La acción de mantener la exactitud y corrección de la información y sus métodos de proceso

Mesa de servicios: El punto de contacto único, en el cual se reciben las solicitudes de servicio de los usuarios de equipos y servicios de TIC en la Institución.

Objetivos estratégicos de TIC: El conjunto de resultados que se prevé alcanzar y que se integran en el PETIC, los cuales describen el alcance de las acciones que serán llevadas a cabo por la Subdirección de Tecnologías de la Información y Comunicaciones.

PETIC: el Plan Estratégico de Tecnologías de la Información y Comunicaciones que elaboran las Instituciones en los términos señalados en el MAAGTICSI;

Problema: La causa de uno o más incidentes, del cual se plantea una solución alterna en espera de una solución definitiva.

Proyectos de TIC: el esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado de TIC;

Requerimientos funcionales: La característica que requiere cumplir un producto o entregable asociado a una función en un proceso o servicio automatizado, o por automatizar.

Riesgo: La posibilidad de que una amenaza pueda explotar una vulnerabilidad y causar una pérdida o daño sobre los activos de TIC, las infraestructuras críticas o los activos de información de la Institución.

Sistema informático: El conjunto de componentes o programas construidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso, de acuerdo a requerimientos previamente definidos.

TIC: las tecnologías de información y comunicaciones que comprenden el equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.

Usuarios: Los servidores públicos o aquéllos terceros que han sido acreditados o cuentan con permisos para hacer uso de los servicios de TIC.

Validación: La actividad que asegura que un servicio de TIC, producto o entregable, nuevo o modificado, satisface las necesidades acordadas previamente con la unidad administrativa solicitante.

Verificación: La actividad que permite revisar si un servicio de TIC o cualquier otro producto o entregable, está completo y acorde con su especificación de diseño.

Vulnerabilidades: Las debilidades en la seguridad de la información dentro de una organización que potencialmente permite que una amenaza afecte a los activos de TIC, a la infraestructura crítica, así como a los activos de información.

3.6. Lineamientos y Políticas

El PETIC se integrará con las Iniciativas y Proyectos de TIC atendiendo lo siguiente:

- I. Favorecer el uso del cómputo en la nube para el aprovechamiento de la economía de escala, eficiencia en la gestión gubernamental y estandarización de las TIC, teniendo en consideración la seguridad de la información;
- II. Privilegiar la aplicación de Tecnologías Verdes;
- III. Establecer una ficha técnica base para cada una de las Iniciativas y Proyectos de TIC, en la cual se registre el presupuesto estimado y, de ser el caso, el presupuesto autorizado para el ejercicio fiscal, así como necesidades adicionales en este rubro;
- IV. Identificar Iniciativas y Proyectos de TIC que aporten mayores beneficios a la población o cuenten con alto impacto en el cumplimiento de los objetivos institucionales, de la EDN y del Decreto, en el ámbito de sus atribuciones, identificándolos como estratégicos;
- V. Identificar las estrategias, líneas de acción y habilitadores de la EDN contenidas en el Programa, a las cuales contribuirán para su cumplimiento;
- VI. Relacionar las características, especificaciones y estándares generales de los principales componentes por cada dominio tecnológico;
- VII. Determinar Iniciativas y Proyectos de TIC para la digitalización de los trámites y servicios registrados en el CNTSE, considerando estrategias de interoperabilidad con aplicativos de cómputo de otras Instituciones que resulten necesarios para la prestación de esos trámites y servicios;
- VIII. Establecer estrategias de interoperabilidad al interior de la propia Institución y con otras Instituciones que requieran compartir datos que obren en su posesión, puedan o no formar parte de un mismo proceso, y

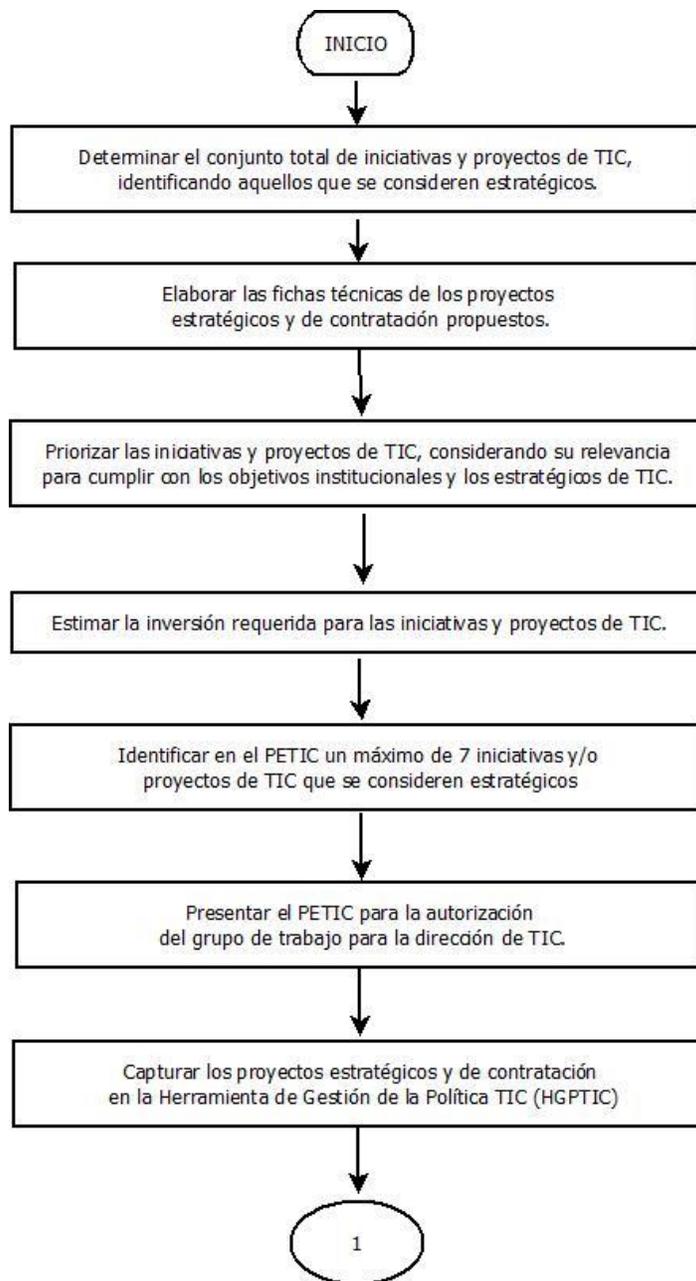
- IX. Someter a la aprobación de la Unidad las aplicaciones de cómputo para dispositivos móviles que planeen desarrollar.

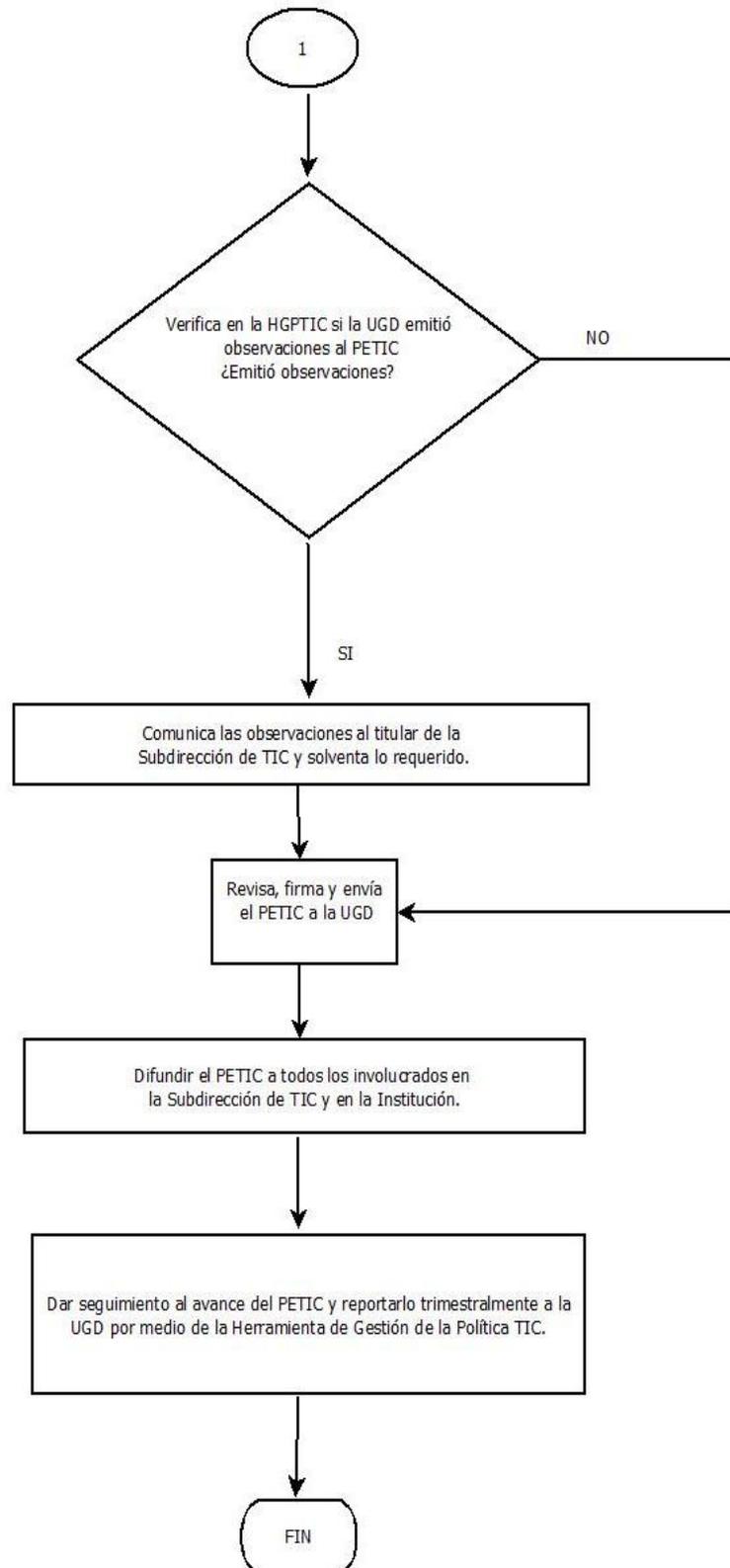
	Descripción de Actividades	Clave:
		Fecha:
	Nombre de Procedimiento: Procedimiento de planeación estratégica de TIC	Versión: 1.0

Paso	Responsable	Actividad	Documento de trabajo (Clave)
1	Titular de la Subdirección de TIC	Determinar el conjunto total de iniciativas y proyectos de TIC, identificando aquellos que se consideren estratégicos, e integrar cada iniciativa y proyecto de TIC, incluyendo su descripción, alcance, línea base y programa de trabajo.	Cartera ejecutiva de proyectos (F-03-01)
2	Administrador de proyectos de TIC	Elaborar las fichas técnicas de los proyectos estratégicos y de contratación propuestos.	Ficha técnica (F-03-02)
3	Titular de la Subdirección de TIC	Priorizar las iniciativas y proyectos de TIC, considerando su relevancia para cumplir con los objetivos institucionales y los estratégicos de TIC.	
4	Administrador de proyectos de TIC	Estimar la inversión requerida para las iniciativas y proyectos de TIC, desagregando de ésta al menos los rubros de recursos financieros, materiales y humanos.	
5	Titular de la Subdirección de TIC	Identificar en el PETIC un máximo de 7 iniciativas y/o proyectos de TIC que se consideren estratégicos, aplicando como criterio preferente para su identificación que aporten mayores beneficios a la población o cuenten con alto impacto en el cumplimiento de los objetivos institucionales, del Decreto y la EDN; debiendo asegurar que éstos se integren al portafolio de proyectos de TIC que se establece en el Proceso Administración de Proyectos (ADP).	
6	Titular de la Subdirección de TIC	Presentar el PETIC para la autorización del grupo de trabajo para la dirección de TIC.	Cartera ejecutiva de proyectos (F-03-01)
7	Administrador de proyectos de TIC Titular de la Subdirección de TIC	Capturar los proyectos estratégicos y de contratación en la Herramienta de Gestión de la Política TIC (HGPTIC) Revisar, firmar y enviar el PETIC a la Unidad de Gobierno Digital (UGD) para obtener autorización.	

Paso	Responsable	Actividad	Documento de trabajo (Clave)
8	Administrador de proyectos de TIC	Verifica en la HGPTIC si la UGD emitió observaciones al PETIC ¿Emitió observaciones? Sí: Continúa en la actividad 9 No: Continúa en la actividad 11	
9	Administrador de proyectos de TIC	Comunica las observaciones al titular de la Subdirección de TIC y solventa lo requerido.	
10	Titular de la Subdirección de TIC	Revisa, firma y envía el PETIC a la UGD. Continúa en actividad 8.	
11	Titular de la Subdirección de TIC	Difundir el PETIC a todos los involucrados en la Subdirección de TIC y en la Institución.	
12	Administrador de proyectos de TIC	Dar seguimiento al avance del PETIC y reportarlo trimestralmente a la UGD por medio de la Herramienta de Gestión de la Política TIC o el sistema informático que la UGD determine para ello.	Documento de seguimiento de PETIC (F-03-03)
FIN DEL PROCEDIMIENTO			

Diagrama de flujo del procedimiento





FORMATOS

Cartera ejecutiva de proyectos (F-03-01)

PE-CEPTIC, CARTERA EJECUTIVA DE PROYECTOS DE TIC

Objetivo:

Identificar y categorizar el conjunto de proyectos de TIC que integrarán la Cartera Ejecutiva de proyectos de TIC considerando proyectos estratégicos y proyectos de contratación de bienes y servicios de TIC.

Asegurar que el Instituto cuente con una Cartera Ejecutiva de Proyectos de TIC actualizada.

Alinear las prioridades de la Cartera Ejecutiva de Proyectos de TIC con las prioridades institucionales.

Verificar que las principales inversiones en materia de TIC se encuentren alineadas a los objetivos estratégicos de la institución.

Alcance:

El titular de la UTIC, en la fecha que se determina en el Acuerdo, deberá:

- Revisar y validar la Cartera Ejecutiva.
- Presentar la Cartera Ejecutiva para la autorización del grupo de trabajo para la dirección de TIC o a quien el titular designe.
- Registrar y enviar a la Unidad la Cartera Ejecutiva, a través de la Herramienta de Gestión de la Política TIC.

El responsable de la planeación estratégica de la UTIC deberá:

- Verificar que se obtenga la autorización de la Cartera Ejecutiva por parte de la Unidad.
- Difundir la Cartera Ejecutiva a todos los involucrados para su cumplimiento en la UTIC y en la Institución.

Proyectos Estratégicos en materia de TIC

Identificador	Proyecto	Área solicitante	Prioridad

Proyectos de contratación en materia de TIC

Identificador	Partida	Nombre del proyecto de contratación	Monto presupuestado a erogar en 2020	Área requirente	Procedimiento de contratación propuesto	Prioridad determinada por el área requirente

Firmas y fechas de elaboración, revisión y autorización

Elaboró

Vo.Bo.

Autorizó

**Ficha técnica
(F-03-02)**

- **Clasificación de la iniciativa del proyecto**

Nombre del proyecto:

Identificador del proyecto (número interno):

¿Es iniciativa o proyecto?:

Riesgo:

Alto

Medio

Bajo

Categoría:

Optimización

Simplificación

Digitalización

Racionalización

¿Planea desarrollar aplicativos móviles?:

Antecedentes:

Justificación:

Objetivo estratégico del proyecto:

Alcance:

Fecha inicio:

Fecha término:

Presupuesto del Proyecto:

Partidas

Actividades

Actividad	Fecha de inicio	Fecha de término	(%) Porcentaje asignado
Fecha de Obtención de Dictamen técnico de la UGD.			
Firma del Contrato.			

Artículo 5

I. ¿La Iniciativa o proyecto favorece el cómputo en la nube?:

II. ¿La Iniciativa o Proyecto privilegia la aplicación de Tecnologías Verdes?:

VII. ¿La Iniciativa o Proyecto considera la digitalización de trámites o servicios de CNTS?:

¿La Iniciativa o Proyecto considera la optimización de trámites o servicios?:

Unidad solicitante:

Líder de proyecto:

Fase actual:

<input type="checkbox"/>	Anteproyecto
<input type="checkbox"/>	Definición
<input type="checkbox"/>	Planeación
<input type="checkbox"/>	Ejecución
<input type="checkbox"/>	Cierre
<input type="checkbox"/>	Completado
<input type="checkbox"/>	Congelado
<input type="checkbox"/>	Cancelado

VI. Dominios tecnológicos

a) Seguridad

- **Características:**
- **Especificaciones:**
- **Estándares:**

b) Cómputo de usuario final

- **Características:**
- **Especificaciones:**
- **Estándares:**

c) Comunicaciones

- **Características:**
- **Especificaciones:**
- **Estándares:**

d) Internet / Intranet

- **Características:**
- **Especificaciones:**
- **Estándares:**

e) Aplicativos

- **Características:**
- **Especificaciones:**
- **Estándares:**

f) Bases de Datos y Datawarehousing

- **Características:**
- **Especificaciones:**
- **Estándares:**

Análisis de Fortalezas, Oportunidades, Debilidades y Amenazas (FODA)

Fortalezas:

Oportunidades:

Debilidades:

Amenazas:

**Documento de seguimiento de PETIC
(F-03-03)**

PETIC	Proyectos	Planeación		Inicio del Proyecto		Desarrollo		Cierre del proyecto		Avance general por subproyecto	Reporte	Entregables
	Linea base	25%	25%	25%	25%	25%	25%	100%				

4. Procedimiento de la integración de archivos de expedientes de contratos en materia de TIC.

(MP/SG/STIC/04/2020)

4.1. **Propósito del Procedimiento**

Integrar la documentación generada en los procedimientos de contratación, así como la formalización, operación y cierre de los contratos de servicios de la Subdirección de Tecnologías de la Información y Comunicaciones.

4.2. **Alcance**

Establecer los mecanismos para el debido resguardo de la documentación que integra los expedientes de los proyectos de contratación en materia de TIC y aquellos en los que la Subdirección de Tecnologías de la Información y Comunicaciones funge como administrador de contrato.

4.3. **Referencia o Marco normativo**

Marco normativo

- a) Decreto de reestructuración del Instituto de Investigaciones Dr. José María Luis Mora.
- b) Estatuto Orgánico.
- c) Manual General de Organización.
- d) Manual Administrativo de Aplicación General en Materia de Tecnologías de Información y Comunicaciones y de Seguridad de la Información

4.4. **Responsables**

Subdirección de Tecnologías de la Información y Comunicaciones

4.5. **Definiciones**

Activo de información: Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para la Institución, debe ser protegido para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.

Acuerdo: el Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones y en la de Seguridad de la Información, así como establecer el Manual Administrativo de Aplicación General en dichas materias.

Acuerdo de nivel de servicio SLA: El acuerdo de nivel de servicio que se compromete con la unidad administrativa solicitante, al entregar un aplicativo de cómputo o servicio de TIC (*Service Level Agreement*, por sus siglas en inglés).

Acuerdo de nivel operacional OLA: El acuerdo de nivel operacional entre los responsables de los diversos componentes de la arquitectura tecnológica de un aplicativo de cómputo o

servicio de TIC, que se debe definir y cumplir para responder a los acuerdos de nivel de servicio SLA comprometidos (*Operational Level Agreement* por sus siglas en inglés).

Ambiente de trabajo: El conjunto de herramientas, utilerías, programas, aplicaciones, información, facilidades y organización que un usuario tiene disponible para el desempeño de sus funciones de manera controlada, de acuerdo con los accesos y privilegios que tenga asignados por medio de una identificación única y una contraseña.

Amenaza: A cualquier posible acto que pueda causar algún tipo de daño a los activos de información de la Institución.

Análisis de riesgos: El uso sistemático de la información para identificar las fuentes de vulnerabilidades y amenazas a los activos de TIC, a la infraestructura crítica o a los activos de información, así como efectuar la evaluación de su magnitud o impacto y estimar los recursos necesarios para eliminarlas o mitigarlas.

Área contratante: A la facultada en la Institución para realizar procedimientos de contratación, a efecto de adquirir o arrendar bienes o contratar la prestación de servicios.

Área requirente: A la que, en la Institución, solicite o requiera formalmente la adquisición o arrendamiento de bienes o la prestación de servicios, o aquélla que los utilizará.

Área solicitante o usuaria: A la que, en la Institución, efectúa originalmente la petición a la Subdirección de Tecnologías de la Información y Comunicaciones para obtener un bien o servicio de TIC y/o que hará uso del mismo.

Área técnica: A la que, en la Institución, elabora las especificaciones técnicas que se deberán incluir en el procedimiento de contratación, evalúa la propuesta técnica de las proposiciones y es responsable de responder en la junta de aclaraciones las preguntas que sobre estos aspectos realicen los licitantes. El área técnica podrá tener también el carácter de área requirente.

Arquitectura tecnológica: A la estructura de hardware, software y redes requerida para dar soporte a la implementación de los aplicativos de cómputo, soluciones tecnológicas o servicios de TIC de la Institución.

Disponibilidad: La característica de la información de permanecer accesible para su uso cuando así lo requieran individuos o procesos autorizados.

Entregable: El producto adquirido, desarrollado o personalizado, con características cuantificables y medibles en términos de su valor, integralidad, funcionalidad y capacidades.

Evento: El suceso que puede ser observado, verificado y documentado, en forma manual o automatizada, que puede llevar al registro de incidentes.

Funcionalidad: Las características de los aplicativos de cómputo, soluciones tecnológicas o de un servicio de TIC, que permiten cubrir las necesidades o requerimientos de un usuario.

Gestión de riesgos: La identificación, valoración y ejecución de acciones, para el control y minimización de los riesgos que afecten a los activos de TIC, a la infraestructura crítica o a los activos de información de la Institución.

Impacto: Al grado de los daños y/o de los cambios sobre un activo de información, por la materialización de una amenaza.

Incidente: A la afectación o interrupción a los activos de TIC, a las infraestructuras críticas, así como a los activos de información de una Institución, incluido el acceso no autorizado o no programado a éstos.

Infraestructuras críticas: Las instalaciones, redes, servicios y equipos asociados o vinculados con activos de TIC o activos de información, cuya afectación, interrupción o destrucción tendría un impacto mayor, entre otros, en la salud, la seguridad, el bienestar económico de la población o en el eficaz funcionamiento de las Instituciones.

Integridad: La acción de mantener la exactitud y corrección de la información y sus métodos de proceso

Mesa de servicios: El punto de contacto único, en el cual se reciben las solicitudes de servicio de los usuarios de equipos y servicios de TIC en la Institución.

Objetivos estratégicos de TIC: El conjunto de resultados que se prevé alcanzar y que se integran en el PETIC, los cuales describen el alcance de las acciones que serán llevadas a cabo por la Subdirección de Tecnologías de la Información y Comunicaciones.

Problema: La causa de uno o más incidentes, del cual se plantea una solución alterna en espera de una solución definitiva.

Requerimientos funcionales: La característica que requiere cumplir un producto o entregable asociado a una función en un proceso o servicio automatizado, o por automatizar.

Riesgo: La posibilidad de que una amenaza pueda explotar una vulnerabilidad y causar una pérdida o daño sobre los activos de TIC, las infraestructuras críticas o los activos de información de la Institución.

Sistema informático: El conjunto de componentes o programas construidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso, de acuerdo a requerimientos previamente definidos.

Usuarios: Los servidores públicos o aquéllos terceros que han sido acreditados o cuentan con permisos para hacer uso de los servicios de TIC.

Validación: La actividad que asegura que un servicio de TIC, producto o entregable, nuevo o modificado, satisface las necesidades acordadas previamente con la unidad administrativa solicitante.

Verificación: La actividad que permite revisar si un servicio de TIC o cualquier otro producto o entregable, está completo y acorde con su especificación de diseño.

Vulnerabilidades: Las debilidades en la seguridad de la información dentro de una organización que potencialmente permite que una amenaza afecte a los activos de TIC, a la infraestructura crítica, así como a los activos de información.

	Descripción de Actividades		Clave:
			Fecha:
	Nombre de Procedimiento: Procedimiento de la Integración de Archivos de Expedientes de Contratos en Materia de TIC		Versión: 1.0
			Página: 1/
Unidad Administrativa: Subdirección de Tecnologías de la Información y comunicaciones		Área Responsable: Administración de proyectos y cumplimiento normativo	

Paso	Responsable	Actividad	Documento de trabajo (Clave)
1	Administrador de proyectos	Recaba la documentación requerida para la contratación de servicios o adquisición de bienes de TIC que realice la Subdirección de Tecnologías de la Información y Comunicaciones y lo resguarda en el repositorio de información (Sharepoint).	
2		Integra copia digitalizada de contratos firmados y formalizados en el expediente de la contratación en el repositorio de información.	
3		Reúne la información, evidencias y entregables generados durante la administración del contrato hasta su cierre y las registra en el expediente correspondiente dentro del repositorio de información.	ADP1 ADP2 ADP3
4		Verifica la integración completa del expediente una vez que haya concluido el servicio, constatando que se cuente con toda la documentación establecida.	
5		Determina el espacio físico del almacenamiento de los expedientes de las contrataciones en materia TIC e instruye al área competente según la materia lleve a cabo el resguardo de estos.	
6		Archiva y resguarda los expedientes de los contratos en materia TIC en el espacio físico determinado, y realiza una copia digital.	
FIN DEL PROCEDIMIENTO			

Diagrama de flujo del procedimiento



FORMATOS

Acta de constitución del proyecto (ADP1)

Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información Comunicaciones
y Seguridad de la Información (MAAGTICSI)

Subdirección de Informática

 Instituto Mora	Instituto de Investigaciones Dr. José María Luis Mora	HOJA	47 de 1
	Acta de constitución del proyecto <i>Nombre del proyecto</i>	FECHA	
		ADP1	

ADP- Proceso de administración de proyectos

Acta de constitución del proyecto. **Formato ADP 1**

Acta de constitución de proyecto de TIC

Código/Identificación del Proyecto	Fecha	Revisión

Nombre y Objetivo del proyecto

Justificación general del proyecto

Datos generales del proyecto

Identificación del proyecto:	
Nombre del proyecto:	
Unidad administrativa solicitante:	

Unidad
administrativa
impulsora:

Necesidades del área a la que va dirigido

--

Objetivos del área a la que va dirigido

Objetivos del área	Objetivos estratégicos en el PETIC

Descripción del proyecto

--

Alcance del proyecto

--

Firmas, revisión y aprobación de ejecución del proyecto

Elaboró
*Nombre del administrador de
proyectos que elabora*
Administrador de Proyectos de TIC

Aprobó
*Nombre del Subdirector de Tecnologías de la
Información y Comunicaciones*
Subdirector de Informática

Acta de aceptación de entregables (ADP2)

Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información Comunicaciones y Seguridad de la Información (MAAGTICSI)

Subdirección de Informática

 Instituto Mora	Instituto de Investigaciones Dr. José María Luis Mora	HOJA	49 de 1
	Acta de aceptación de entregables del Proyecto	FECHA	
	<i>Nombre del proyecto</i>	ADP2	

ADP- Proceso administración de proyectos

Acta de aceptación de entregables. **Formato ADP 2**

Acta de aceptación de entregables del Proyecto

Nombre del proyecto

Identificador del Entregable	Descripción del Entregable	Fecha compromiso de entrega	Fecha de verificación del entregable	Fecha real de entrega	Responsable de aceptación	Observaciones

Aceptación

Identificación y descripción breve del Entregable	Proveedor/ responsable de la entrega	Fecha de entrega-recepción	Nombre, cargo y firma autógrafa	Observaciones

Firmas de revisión y aprobación

Elaboró
Nombre del administrador de proyectos que elabora
Administración de Proyectos

Aprobó.
Nombre del Subdirector de Tecnologías de la Información y Comunicaciones
Subdirector de Informática

Acta de aceptación de cierre del proyecto (ADP3)

Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información Comunicaciones y Seguridad de la Información (MAAGTICSI)

Subdirección de Informática

	Instituto de Investigaciones Dr. José María Luis Mora	HOJA	50 de 1
	Acta de cierre de proyecto	FECHA	
	<i>Nombre del proyecto</i>	ADP3	

ADP- Proceso de administración de proyectos

Acta de cierre de proyecto. Formato ADP 3

Acta de Cierre de proyecto de TIC		
Código/Identificación del Proyecto	Fecha	Revisión

Descripción del proyecto

Fecha de inicio programada y real del proyecto

Fecha de término programada y real del proyecto

Descripción de entregables concluidos

Relación documental de la administración del proyecto

Firmas de Aceptación del cierre, de elaboración, revisión y aprobación del Acta

Elaboró

*Nombre del administrador de
proyectos que elabora*
Administración de Proyectos

Aprobó

*Nombre del Subdirector de
Tecnologías de la Información y
Comunicaciones*
Subdirector de Informática

5. Procedimiento para la contratación de bienes o servicios en materia de TIC.

(MP/SG/STIC/05/2020)

5.1. **Propósito del Procedimiento**

Describir los pasos a seguir por el área requirente para la realización y validación de la documentación de una contratación de un bien o servicio en materia de TIC.

5.2. **Alcance**

Coordinar las acciones para el ejercicio del presupuesto destinado a las TIC, a fin de maximizar su aplicación en las contrataciones de TIC requeridas por la Institución, así como las acciones para efectuar el acompañamiento necesario a las unidades facultadas para realizar los procedimientos de contrataciones en la Institución, de manera que se asegure su ejecución en tiempo y forma, alineado al presupuesto autorizado; así como el seguimiento a los contratos que se celebren.

5.3. **Referencia o Marco normativo**

Marco normativo

- a) Decreto de reestructuración del Instituto de Investigaciones Dr. José María Luis Mora.
- b) Estatuto Orgánico.
- c) Manual General de Organización.
- d) Manual Administrativo de Aplicación General en Materia de Tecnologías de Información y Comunicaciones y de Seguridad de la Información

5.4. **Responsables**

Subdirección de Tecnologías de la Información y Comunicaciones

5.5. **Definiciones**

Activo de información: Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para la Institución, debe ser protegido para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.

Acuerdo: el Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones y en la de Seguridad de la Información, así como establecer el Manual Administrativo de Aplicación General en dichas materias.

Acuerdo de nivel de servicio SLA: El acuerdo de nivel de servicio que se compromete con la unidad administrativa solicitante, al entregar un aplicativo de cómputo o servicio de TIC (*Service Level Agreement*, por sus siglas en inglés).

Acuerdo de nivel operacional OLA: El acuerdo de nivel operacional entre los responsables de los diversos componentes de la arquitectura tecnológica de un aplicativo de cómputo o

servicio de TIC, que se debe definir y cumplir para responder a los acuerdos de nivel de servicio SLA comprometidos (*Operational Level Agreement* por sus siglas en inglés).

Ambiente de trabajo: El conjunto de herramientas, utilerías, programas, aplicaciones, información, facilidades y organización que un usuario tiene disponible para el desempeño de sus funciones de manera controlada, de acuerdo con los accesos y privilegios que tenga asignados por medio de una identificación única y una contraseña.

Amenaza: A cualquier posible acto que pueda causar algún tipo de daño a los activos de información de la Institución.

Análisis de riesgos: El uso sistemático de la información para identificar las fuentes de vulnerabilidades y amenazas a los activos de TIC, a la infraestructura crítica o a los activos de información, así como efectuar la evaluación de su magnitud o impacto y estimar los recursos necesarios para eliminarlas o mitigarlas.

Área contratante: A la facultada en la Institución para realizar procedimientos de contratación, a efecto de adquirir o arrendar bienes o contratar la prestación de servicios.

Área requirente: A la que, en la Institución, solicite o requiera formalmente la adquisición o arrendamiento de bienes o la prestación de servicios, o aquélla que los utilizará.

Área solicitante o usuaria: A la que, en la Institución, efectúa originalmente la petición a la Subdirección de Tecnologías de la Información y Comunicaciones para obtener un bien o servicio de TIC y/o que hará uso del mismo.

Área técnica: A la que, en la Institución, elabora las especificaciones técnicas que se deberán incluir en el procedimiento de contratación, evalúa la propuesta técnica de las proposiciones y es responsable de responder en la junta de aclaraciones las preguntas que sobre estos aspectos realicen los licitantes. El área técnica podrá tener también el carácter de área requirente.

Arquitectura tecnológica: A la estructura de hardware, software y redes requerida para dar soporte a la implementación de los aplicativos de cómputo, soluciones tecnológicas o servicios de TIC de la Institución.

Disponibilidad: La característica de la información de permanecer accesible para su uso cuando así lo requieran individuos o procesos autorizados.

Entregable: El producto adquirido, desarrollado o personalizado, con características cuantificables y medibles en términos de su valor, integralidad, funcionalidad y capacidades.

Evento: El suceso que puede ser observado, verificado y documentado, en forma manual o automatizada, que puede llevar al registro de incidentes.

Funcionalidad: Las características de los aplicativos de cómputo, soluciones tecnológicas o de un servicio de TIC, que permiten cubrir las necesidades o requerimientos de un usuario.

Gestión de riesgos: La identificación, valoración y ejecución de acciones, para el control y minimización de los riesgos que afecten a los activos de TIC, a la infraestructura crítica o a los activos de información de la Institución.

Impacto: Al grado de los daños y/o de los cambios sobre un activo de información, por la materialización de una amenaza.

Incidente: A la afectación o interrupción a los activos de TIC, a las infraestructuras críticas, así como a los activos de información de una Institución, incluido el acceso no autorizado o no programado a éstos.

Infraestructuras críticas: Las instalaciones, redes, servicios y equipos asociados o vinculados con activos de TIC o activos de información, cuya afectación, interrupción o destrucción tendría un impacto mayor, entre otros, en la salud, la seguridad, el bienestar económico de la población o en el eficaz funcionamiento de las Instituciones.

Integridad: La acción de mantener la exactitud y corrección de la información y sus métodos de proceso

Mesa de servicios: El punto de contacto único, en el cual se reciben las solicitudes de servicio de los usuarios de equipos y servicios de TIC en la Institución.

Objetivos estratégicos de TIC: El conjunto de resultados que se prevé alcanzar y que se integran en el PETIC, los cuales describen el alcance de las acciones que serán llevadas a cabo por la Subdirección de Tecnologías de la Información y Comunicaciones.

Problema: La causa de uno o más incidentes, del cual se plantea una solución alterna en espera de una solución definitiva.

Requerimientos funcionales: La característica que requiere cumplir un producto o entregable asociado a una función en un proceso o servicio automatizado, o por automatizar.

Riesgo: La posibilidad de que una amenaza pueda explotar una vulnerabilidad y causar una pérdida o daño sobre los activos de TIC, las infraestructuras críticas o los activos de información de la Institución.

Sistema informático: El conjunto de componentes o programas construidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso, de acuerdo a requerimientos previamente definidos.

Usuarios: Los servidores públicos o aquéllos terceros que han sido acreditados o cuentan con permisos para hacer uso de los servicios de TIC.

Validación: La actividad que asegura que un servicio de TIC, producto o entregable, nuevo o modificado, satisface las necesidades acordadas previamente con la unidad administrativa solicitante.

Verificación: La actividad que permite revisar si un servicio de TIC o cualquier otro producto o entregable, está completo y acorde con su especificación de diseño.

Vulnerabilidades: Las debilidades en la seguridad de la información dentro de una organización que potencialmente permite que una amenaza afecte a los activos de TIC, a la infraestructura crítica, así como a los activos de información.

5.6. **Lineamientos y Políticas**

1. El responsable del seguimiento del presupuesto autorizado, de los procedimientos de contratación de TIC y de los contratos celebrados en materia de TIC, deberá ser designado por el titular de la UTIC, y tener un nivel jerárquico inmediato inferior al de éste.
2. El responsable del proceso deberá asegurarse que éste se ejecute con apego a las disposiciones que en materia presupuestaria resulten aplicables, así como a los procesos de las unidades administrativas facultadas para administrar los recursos financieros y elaborar el anteproyecto anual de presupuesto de la Institución.
3. El responsable de este proceso deberá asegurarse que éste se efectúe con apego a las disposiciones en materia de adquisiciones y arrendamiento de bienes muebles y servicios, al Acuerdo por el que se expide el MAAGMAASSP, al Acuerdo y aquellas en materia presupuestaria, que resulten aplicables.
4. El titular de la UTIC, deberá designar a un representante con los conocimientos técnicos suficientes que permitan dar respuesta clara y precisa a las solicitudes de aclaración de los licitantes en las juntas de aclaraciones de los procedimientos de contratación a los que fuere convocada la UTIC como área técnica.
5. Cuando otras áreas o unidades administrativas de la Institución diversas a la UTIC, tengan asignados recursos financieros para la contratación de bienes o servicios de TIC necesarios para el cumplimiento de sus funciones, deberán contar previo al inicio del procedimiento de contratación de que se trate, con la aprobación por escrito de la UTIC, por medio de un dictamen técnico.
6. En el supuesto a que se refiere la regla anterior, corresponderá al área o unidad administrativa de que se trate, fungir como área técnica, por lo que la UTIC deberá proporcionar el apoyo técnico que le sea requerido por ésta.
7. En aquellos casos en que se integren o adicionen componentes de software a un aplicativo de cómputo o a un servicio de TIC ya existente, el responsable del proceso se deberá asegurar de que se consideren las siguientes pruebas: integrales, de funcionalidad, estrés, volumen, aceptación del usuario y de seguridad, con el propósito de comprobar que la funcionalidad del aplicativo de cómputo o servicio de TIC existente se mantiene inalterada y que la relativa al componente integrado o adicionado es consistente.
8. El responsable de este proceso deberá verificar que cada vez que se suscriba un contrato para la adquisición, arrendamiento o servicios de TIC, éste sea registrado en el sistema electrónico de compras gubernamentales denominado CompraNet, con apego a la normatividad aplicable.
9. El titular de la UTIC será el responsable de la firma de aprobación del formato F2 APCT, así como de su trámite ante la Unidad.

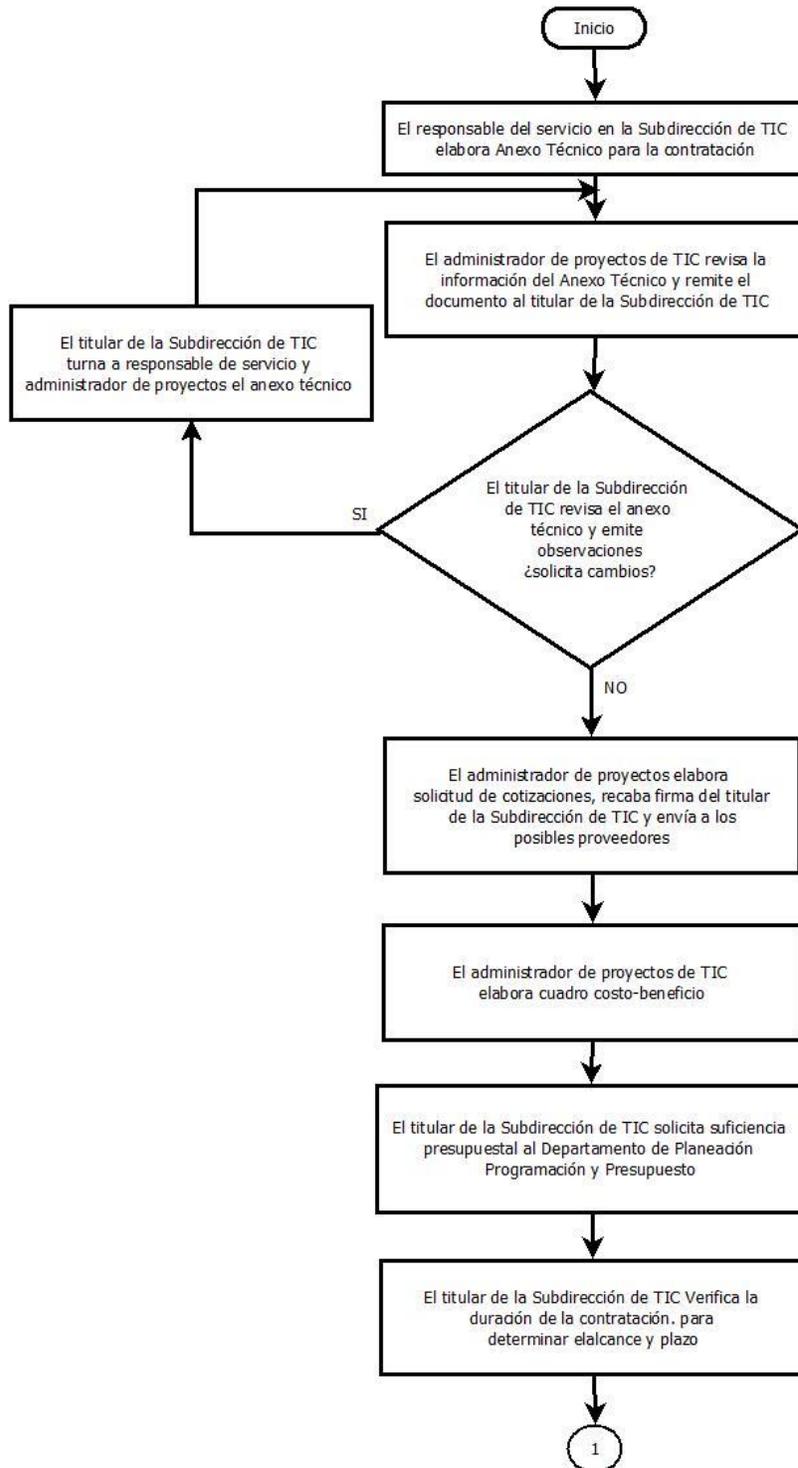
 <p>Instituto Mora</p>	Descripción de Actividades		Clave:
			Fecha:
	Nombre de Procedimiento: Procedimiento de la Validación de Documentos de Contratación de Servicios o Bienes en Materia de TIC		Versión: 1.0
			Página: 1/
Unidad Administrativa: Subdirección de Tecnologías de la Información y comunicaciones		Área Responsable: Administración de proyectos y cumplimiento normativo	

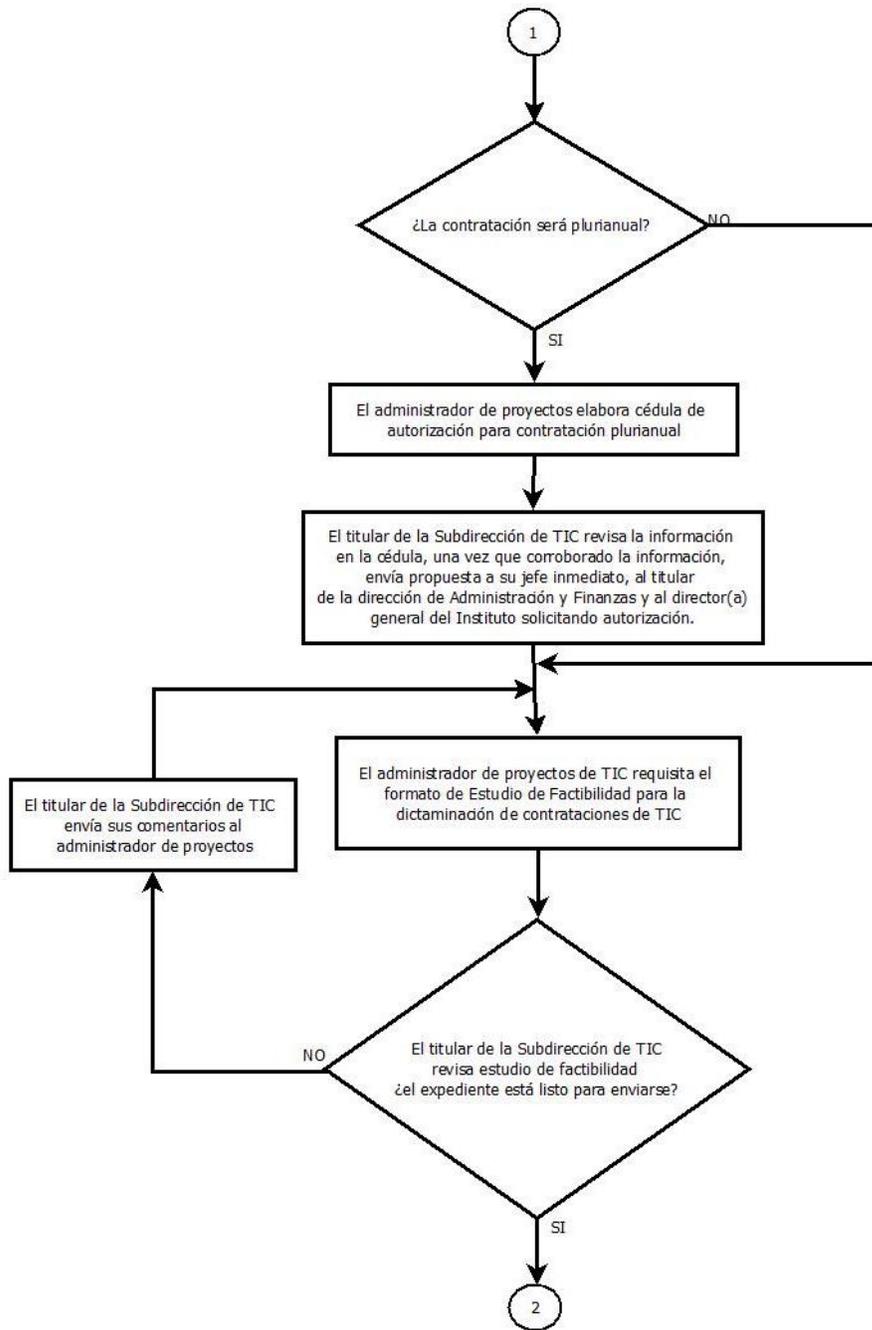
Paso	Responsable	Actividad	Documento de trabajo (Clave)
1	Responsable del servicio dentro de la Subdirección de TIC	Elabora Anexo Técnico para la contratación.	Anexo técnico (F-05-01)
2	Administrador de proyectos de TIC	Revisa la información descrita en el Anexo Técnico y remite documento al titular de la Subdirección de TIC	
3	Titular de la Subdirección de TIC	Revisa anexo técnico y emite observaciones ¿solicita cambios? Sí: Turna a responsable de servicio y administrador de proyectos. Continúa en actividad 1. No: Continúa en 4	
4	Administrador de proyectos de TIC	Elabora solicitud de cotizaciones, recaba firma del titular de la Subdirección de TIC y envía a los posibles proveedores.	Solicitud de cotizaciones (FO-CON-04)
5	Administrador de proyectos de TIC	Con la información de las cotizaciones presentadas por los posibles proveedores elabora cuadro costo-beneficio.	
6	Titular de la Subdirección de TIC	Con base en la investigación de mercado solicita suficiencia presupuestal al Departamento de Planeación Programación y Presupuesto (DPPP).	
7	Titular de la Subdirección de TIC	Verifica la duración de la contratación. para determinar el alcance y plazo. ¿La contratación será plurianual? Sí. continúa en la actividad 8. No. continúa en la actividad 10.	

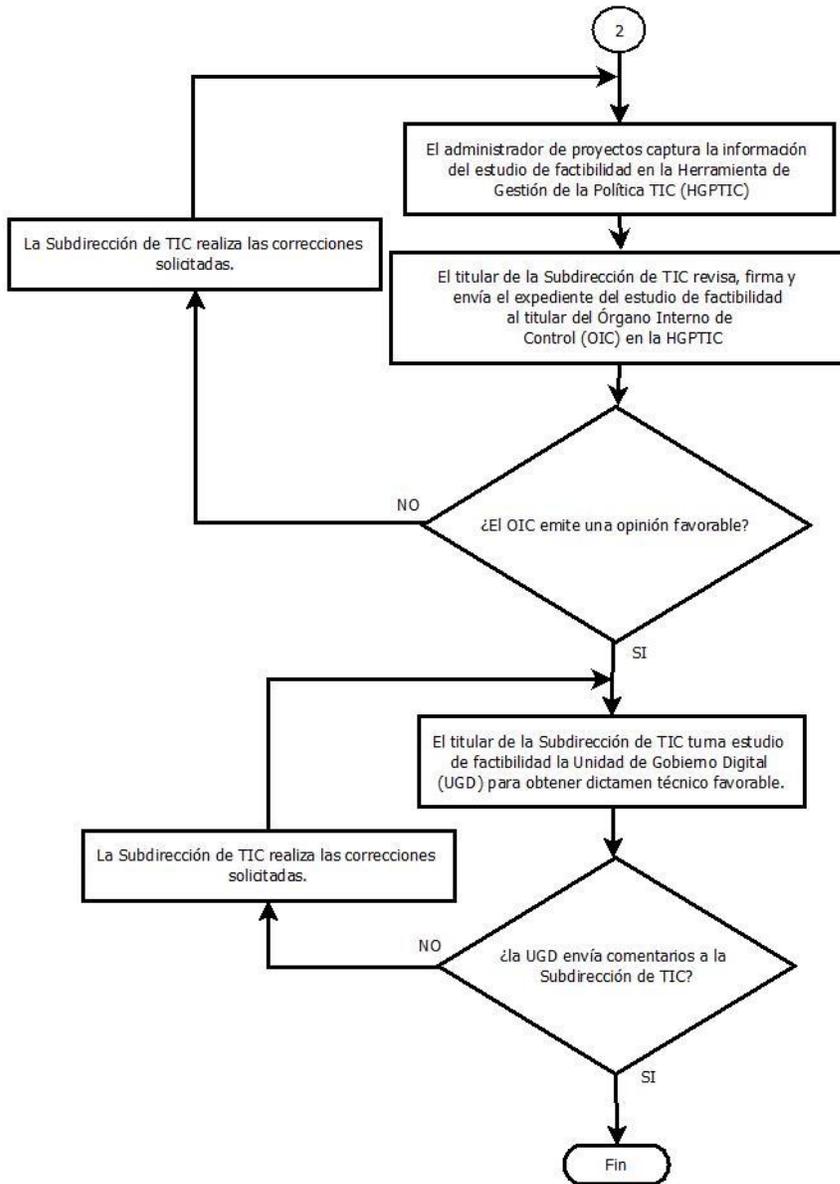
Paso	Responsable	Actividad	Documento de trabajo (Clave)
8	Administrador de proyectos de TIC	Elabora cédula de autorización para contratación plurianual	Cedula de autorización de contratación plurianual (F-05-02)
9	Titular de la Subdirección de TIC	Revisa la información descrita en la cédula de autorización de contratación plurianual, una vez que se haya corroborado que la información en el mismo es válida, envía propuesta a su jefe inmediato, al titular de la dirección de Administración y Finanzas y al director(a) general del Instituto solicitando autorización.	
10	Administrador de proyectos de TIC	Requisita el formato de Estudio de Factibilidad para la dictaminación de contrataciones de TIC	Estudio de factibilidad (APCT-F2)
11	Titular de la Subdirección de TIC	Revisa estudio de factibilidad ¿el expediente está listo para enviarse? Sí: Envía sus comentarios al administrador de proyectos Continúa en actividad 10. No: Continúa en 12.	
12	Administrador de proyectos de TIC	Captura la información del estudio de factibilidad en la Herramienta de Gestión de la Política TIC (HGPTIC).	
13	Titular de la Subdirección de TIC	Revisa, firma y envía el expediente del estudio de factibilidad al titular del Órgano Interno de Control (OIC) en la HGPTIC	
14		¿El OIC emite una opinión favorable? Sí: Continúa en actividad 16 No: Continúa en actividad 15	
15		La Subdirección de TIC realiza las correcciones solicitadas.	

Paso	Responsable	Actividad	Documento de trabajo (Clave)
16	Titular de la Subdirección de TIC	Continua en actividad 12	
17	Titular de la Subdirección de TIC	El titular de la Subdirección de TIC turna estudio de factibilidad la Unidad de Gobierno Digital (UGD) para obtener dictamen técnico favorable.	
	Titular de la Subdirección de TIC	<p>¿La UGD emite un dictamen técnico favorable?</p> <p>Sí: Fin del procedimiento</p> <p>No: Continúa en actividad 17</p>	
	Titular de la Subdirección de TIC	La Subdirección de TIC realiza las correcciones solicitadas.	
FIN DEL PROCEDIMIENTO			

Diagrama de flujo del procedimiento







FORMATOS

Anexo técnico (F-05-01)

 <p>Instituto Mora</p>	<p>INSTITUTO DE INVESTIGACIONES DR. JOSÉ MARÍA LUIS MORA SECRETARIA GENERAL SUBDIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES</p> <p>ANEXO TÉCNICO</p>	<p>Versión 1.0</p> <p>Fecha de elaboración: DD/MM/AAAA</p>
---	---	--

1. DESCRIPCIÓN DEL SERVICIO

2. CONDICIONES DE PAGO

3. TIEMPO MÁXIMO DE ENTREGA

4. VIGENCIA DE LA CONTRATACIÓN

5. PROPUESTA ECONÓMICA

Solicitud de cotizaciones
(FO-CON-04)



Secretaría General
Subdirección de Tecnologías de la Información y Comunicaciones

Ciudad de México, a DD de MM del AAAA

ASUNTO: SOLICITUD DE COTIZACIÓN.

P r e s e n t e .

El Instituto de Investigaciones Dr. José María Luis Mora, como dependencia del Gobierno Federal, requiere para sus actividades de suministro, arrendamiento y/o prestación de servicios, mismas que se encuentran reguladas por la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP) y su reglamento, obtener información para contratar bajo las mejores condiciones disponibles para el Estado.

En este sentido y en términos de lo previsto en el artículo 2 fracción X de la LAASSP, usted ha sido identificado por este ente público, como un posible prestador de servicios.

Por lo antes mencionado y con el objeto de conocer posibles proveedores a nivel nacional y el precio estimado de lo requerido, nos permitimos solicitar su valioso apoyo a efecto de proporcionarnos una cotización para la contratación _____ de acuerdo a lo siguiente:

-
-
-
-
-

Dicha cotización se requiere la remita en documento, debidamente firmada por la persona interesada y dirigida a nombre de _____, Subdirector de Tecnologías de la Información y Comunicaciones..

Agradeceré que en su respuesta se incluya lugar y fecha de cotización y vigencia de la misma.

Para el caso de dudas, comentarios y/o aclaraciones, remitidas al correo: _____.

La fecha límite para presentar la cotización será el día de *mes* de *año* a las 00:00 horas.

NOTA: Vencido el plazo de recepción de cotizaciones, el Instituto de Investigaciones Dr. José María Luis Mora, con fundamento en lo previsto en el artículo 26 de la LAASSP, se definirá el procedimiento a seguir para la contratación, el cual puede ser: LICITACIÓN PÚBLICA, INVITACIÓN A CUANDO MENOS TRES PERSONAS y/o ADJUDICACIÓN DIRECTA, mismo que se informará a las personas que presentaron su cotización.

Este documento no genera obligación alguna para la dependencia o entidad.

A t e n t a m e n t e,

Titular de la Subdirección de Tecnologías de la
Información y Comunicaciones

(Para efectos de control interno, en el caso de no recibir respuesta o manifestar un inconveniente o imposibilidad, procederá a hacer la anotación respectiva en nuestros registros, circunstancias que deberán ser consideradas al momento de definir el tipo de procedimientos de contratación.)

PARA FORMULAR COTIZACIÓN, DEBERÁ CONSIDERAR LOS SIGUIENTES ASPECTOS:

Datos que en su caso, se deben proporcionar para que el destinatario de la solicitud conteste:

1.- Se requiere la _____ de acuerdo a lo siguiente:

-
-
-
-

2.- Condiciones de ejecución:

3.- Considerar en su cotización que el pago es a los 20 días naturales posteriores a la entrega de la factura que reúna los requisitos fiscales que señala la Ley de la materia, así como el informe detallado de los trabajos realizados. Los pagos se efectuarán en 4 exhibiciones.

4.- Señalar en su caso, el porcentaje del anticipo

5.- El porcentaje de garantía de cumplimiento será del ___ %

6.- Penas convencionales por atraso en la realización del servicio será del 1% por cada día de atraso hasta un máximo de 20 días naturales.

7.- En su caso, los métodos de prueba que empleará el ente público para determinar el cumplimiento de las especificaciones solicitadas.

8.- Origen de los bienes (nacional o país de importación) y nacionalidad de los posibles proveedores.

9.- En caso de bienes de importación la moneda en que cotiza.

10.- En caso de que el proceso de fabricación de los bienes requeridos sea superior a 60 días, señale el tiempo que correspondería a su producción.

11.- En su caso, especificar si el costo incluye:

- Instalación.
- Capacitación.
- Puesta en marcha.

12.- Otras garantías que se debe considerar, indicar el o los tipos de garantía, o de responsabilidad civil señalando su vigencia.

Cedula de autorización de contratación plurianual (F-05-02)



Dirección General
Autorización de contratación plurianual

Fecha:

Nombre de la iniciativa o proyecto:	
Dirección de área solicitante:	
Área requiriente:	
Descripción / Objeto de la contratación:	
Período de la contratación:	
Orígen del Recurso:	
Análisis Costo-Beneficio plurianual vs un solo ejercicio	
<i>El desglose del gasto por año a precio corriente</i>	
Fundamento	
Soporte presupuestal	
Administrador de la iniciativa o proyecto:	

Firmas y fechas de elaboración, revisión y autorización

Autoriza	Vo.Bo
Nombre	Nombre
Puesto	Puesto
Correo electrónico	Correo electrónico
<i>Firma</i>	<i>Firma</i>

Area requirente
Nombre
Puesto
Correo electrónico
<i>Firma</i>

Formato al que se alude en el Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como establecer el Manual Administrativo de Aplicación General en dichas materias.

En caso de que el Proyecto que se desea sustentar mediante este formato, esté referido a un Contrato Marco vigente, no deberá considerar la información que se solicita al respecto de la Investigación de Mercado.

1.1. DESCRIPCIÓN DEL PROYECTO / SERVICIO PROPUESTO.

1.1.1. Nombre del proyecto / servicio.

--

1.1.2. Duración del proyecto / servicio.

<i>Fecha Inicio</i>	
<i>Fecha Fin</i>	

1.1.3. Describa en qué consiste el proyecto / servicio señalando la importancia del mismo.

<p>Alcance</p> <p>Objetivo</p> <p>Alineación</p> <p>Diagrama Conceptual</p>
--

1.1.4. Señale los riesgos que pudieran afectar el éxito del proyecto / servicio.

Descripción del riesgo o problema potencial	Probabilidad de ocurrencia (alta, media, baja)	Impacto al proyecto / servicio (alto, medio, bajo)

1.1.5. Marque con una X si la contratación del proyecto / servicio promoverá la interoperabilidad de diferentes sistemas y/o bases de datos al interior de la institución, y/o entre instituciones.

SI		NO	
----	--	----	--

1.1.6. Marque con una X si el proyecto será registrado en el Plan Estratégico de Tecnologías de Información y Comunicación (PETIC).

SI		NO	
----	--	----	--

1.2. ANÁLISIS DE LA SITUACIÓN ACTUAL.

1.2.1. Describa los antecedentes y situación actual, explicando la problemática y/o necesidad que será resuelta con la contratación del proyecto / servicio propuesto.

--

1.2.2. Describa el análisis de las contrataciones vigentes.

--

1.2.3. Marque con una X si se considera pertinente realizar una CONTRATACIÓN CONSOLIDADA.

SI		NO	
----	--	----	--

En caso negativo, señale los motivos.

--

[Para conocer la conveniencia de realizar una contratación consolidada, favor de remitirse a la siguiente liga: <http://www.funcionpublica.gob.mx/index.php/ua/sracp/upcp/compras-consolidadas.html>, y dar clic en el link "Programación de Procedimientos Consolidados de Adquisición de Bienes, Arrendamientos y Servicios que realizarán las dependencias y entidades de la Administración Pública Federal.....".]

En caso de haber respondido afirmativamente y/o de no existir el bien o servicio en la liga anterior, se deberá realizar la consulta al Oficial Mayor o equivalente a fin de dar cumplimiento a lo establecido en el numeral 20 de los LINEAMIENTOS.

1.2.4. Marque con una X si la contratación tendrá un impacto en materia de Seguridad Pública o Seguridad Nacional.

SI		NO	x
----	--	----	---

En caso afirmativo, describa el impacto según aplique.

Impacto en seguridad pública: <i>No Aplica</i> Impacto en seguridad nacional: <i>No Aplica</i>

En caso negativo, se da por hecho que el proyecto / servicio que se está contratando no está en ninguno de los supuestos que establece la Ley de Seguridad Nacional, Título Primero Disposiciones Generales, Capítulo Único, Artículo 5.

1.3. CARACTERÍSTICAS DEL PROYECTO / SERVICIO PROPUESTO

1.3.1. Marque con una X el tipo de contratación sugerida.

ADQUISICIÓN		ARRENDAMIENTO		SERVICIOS	
-------------	--	---------------	--	-----------	--

1.3.2. Marque con una X la naturaleza de contratación sugerida.

RENOVACIÓN DE CONTRATO		NUEVO CONTRATO	
------------------------	--	----------------	--

1.3.3. En relación a los trámites realizados ante la Secretaría de Hacienda y Crédito Público, marque con una X si dada la naturaleza del proyecto / servicio, ya cuenta con los siguientes registros:

REGISTRO DE PLURIANUALIDAD		REGISTRO DE PROGRAMAS Y PROYECTOS DE INVERSIÓN (PPI)	
----------------------------	--	--	--

En caso de haber marcado alguna o ambas opciones de registro, por favor llene los siguientes espacios según corresponda:

REGISTRO PLURIANUALIDAD	FOLIO DE REGISTRO	
REGISTRO DE PROGRAMAS Y PROYECTOS DE INVERSIÓN (PPI)	CLAVE REGISTRO PPI	
	NUM. SOLICITUD PPI	-

1.4. IMPACTO FINANCIERO.

1.4.1. Justificación del Gasto

Razón:

Fundamento

Causa

Erogación Presupuestaria:

1.4.2. Estudio Costo / Beneficio del proyecto propuesto.

1.4.3. Marque con una X si cuenta con suficiencia presupuestaria para el proyecto / servicio.

SI		NO	
----	--	----	--

En caso afirmativo, señale el presupuesto asignado para el proyecto / servicio.

PARTIDA	IMPORTE	TIPO DE CAMBIO	PESOS
---------	---------	----------------	-------

--	--	--	--

1.5. CALENDARIO ESTIMADO DEL PROYECTO.

--

1.6. IMPACTO OPERATIVO Y OTROS REQUERIMIENTOS.

1.6.1. *Describa el impacto de NO realizar la contratación propuesta.*

--

1.6.2. *Marque con una X si la Dependencia o Institución cuenta con personal clave con experiencia y conocimientos para realizar la gestión y administración del proyecto / servicio y contrato.*

SI		NO	
----	--	----	--

En caso afirmativo, señale en el siguiente cuadro al responsable de administrar el contrato y/o dirigir el proyecto por parte del área de TI; así como al responsable de la operación del proyecto / servicio.

Responsable del:	Nombre	Cargo	Correo electrónico institucional	Teléfono y extensión:
Contrato				
Proyecto				
Operación				

Responsable del:	Nombre	Certificaciones en mejores prácticas		
Contrato				
Proyecto				
Operación				

[Deberá anexar los documentos que acrediten las certificación que se anoten en la tabla anterior.]

En caso de NO contar con capacidad de personal clave con experiencia y conocimientos, describa cómo se atenderá la gestión y administración del contrato y/o proyecto:

--

1.6.3. *Solicita que el proveedor esté certificado en normas internacionales o mejores prácticas.*

Norma o mejor práctica	Actividad en la que se requiere

1.6.4. *Describa la justificación para la solicitud del apartado anterior e indique que certificaciones tiene la Institución.*

1.7. CONCLUSIONES.

1.7.1. *Con base en lo descrito anteriormente, señale la opción recomendada y la justificación de la(s) razón(es) en que se sustenta la opción de contratación.*

Firmas y fechas de elaboración, revisión y aprobación de la Revisión trimestral del Programa

Fecha
<p>Subdirección de Tecnologías de la Información y Comunicaciones</p> <p>_____</p> <p>Nombre del Titular la Subdirección de TIC</p>

Notas:

- a). La firma de aprobación de este documento deberá ser la del Titular de la UTIC.
- b). Incluir los anexos que necesarios haciendo referencia a la sección que corresponde cada anexo, por ejemplo: "Anexo de la Sección 1.1."

**6. Procedimiento para acceder a la red
inalámbrica del Instituto Mora
(MP/SG/STIC/06/2020)**

6.1. Propósito del Procedimiento

Gestionar el acceso que se da a usuarios para conectarse a la Red Inalámbrica del Instituto Mora (RIIM) en cualquiera de sus sedes.

6.2. Alcance

El Instituto de Investigaciones Dr. José María Luis Mora, a través de la Subdirección de Tecnologías de la Información y Comunicaciones, brinda el servicio de acceso a la Red Inalámbrica a toda la comunidad del Instituto para desarrollar, comunicar, intercambiar, investigar, difundir y consultar el material que cada usuario requiera para desempeñar sus actividades dentro de la institución.

6.3. Referencia o Marco normativo

Marco normativo

- a) Decreto de reestructuración del Instituto de Investigaciones Dr. José María Luis Mora.
- b) Estatuto Orgánico.
- c) Manual General de Organización.
- d) Manual Administrativo de Aplicación General en Materia de Tecnologías de Información y Comunicaciones y de Seguridad de la Información

6.4. Responsables

Subdirección de Tecnologías de la Información y Comunicaciones

6.5. Definiciones

Activo de información: Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para la Institución, debe ser protegido para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.

Acuerdo: el Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones y en la de Seguridad de la Información, así como establecer el Manual Administrativo de Aplicación General en dichas materias.

Acuerdo de nivel de servicio SLA: El acuerdo de nivel de servicio que se compromete con la unidad administrativa solicitante, al entregar un aplicativo de cómputo o servicio de TIC (*Service Level Agreement*, por sus siglas en inglés).

Acuerdo de nivel operacional OLA: El acuerdo de nivel operacional entre los responsables de los diversos componentes de la arquitectura tecnológica de un aplicativo de cómputo o

servicio de TIC, que se debe definir y cumplir para responder a los acuerdos de nivel de servicio SLA comprometidos (*Operational Level Agreement* por sus siglas en inglés).

Ambiente de trabajo: El conjunto de herramientas, utilerías, programas, aplicaciones, información, facilidades y organización que un usuario tiene disponible para el desempeño de sus funciones de manera controlada, de acuerdo con los accesos y privilegios que tenga asignados por medio de una identificación única y una contraseña.

Amenaza: A cualquier posible acto que pueda causar algún tipo de daño a los activos de información de la Institución.

Análisis de riesgos: El uso sistemático de la información para identificar las fuentes de vulnerabilidades y amenazas a los activos de TIC, a la infraestructura crítica o a los activos de información, así como efectuar la evaluación de su magnitud o impacto y estimar los recursos necesarios para eliminarlas o mitigarlas.

Área contratante: A la facultada en la Institución para realizar procedimientos de contratación, a efecto de adquirir o arrendar bienes o contratar la prestación de servicios.

Área requirente: A la que, en la Institución, solicite o requiera formalmente la adquisición o arrendamiento de bienes o la prestación de servicios, o aquélla que los utilizará.

Área solicitante o usuaria: A la que, en la Institución, efectúa originalmente la petición a la Subdirección de Tecnologías de la Información y Comunicaciones para obtener un bien o servicio de TIC y/o que hará uso del mismo.

Área técnica: A la que, en la Institución, elabora las especificaciones técnicas que se deberán incluir en el procedimiento de contratación, evalúa la propuesta técnica de las proposiciones y es responsable de responder en la junta de aclaraciones las preguntas que sobre estos aspectos realicen los licitantes. El área técnica podrá tener también el carácter de área requirente.

Arquitectura tecnológica: A la estructura de hardware, software y redes requerida para dar soporte a la implementación de los aplicativos de cómputo, soluciones tecnológicas o servicios de TIC de la Institución.

Disponibilidad: La característica de la información de permanecer accesible para su uso cuando así lo requieran individuos o procesos autorizados.

Entregable: El producto adquirido, desarrollado o personalizado, con características cuantificables y medibles en términos de su valor, integralidad, funcionalidad y capacidades.

Evento: El suceso que puede ser observado, verificado y documentado, en forma manual o automatizada, que puede llevar al registro de incidentes.

Funcionalidad: Las características de los aplicativos de cómputo, soluciones tecnológicas o de un servicio de TIC, que permiten cubrir las necesidades o requerimientos de un usuario.

Gestión de riesgos: La identificación, valoración y ejecución de acciones, para el control y minimización de los riesgos que afecten a los activos de TIC, a la infraestructura crítica o a los activos de información de la Institución.

Impacto: Al grado de los daños y/o de los cambios sobre un activo de información, por la materialización de una amenaza.

Incidente: A la afectación o interrupción a los activos de TIC, a las infraestructuras críticas, así como a los activos de información de una Institución, incluido el acceso no autorizado o no programado a éstos.

Infraestructuras críticas: Las instalaciones, redes, servicios y equipos asociados o vinculados con activos de TIC o activos de información, cuya afectación, interrupción o destrucción tendría un impacto mayor, entre otros, en la salud, la seguridad, el bienestar económico de la población o en el eficaz funcionamiento de las Instituciones.

Integridad: La acción de mantener la exactitud y corrección de la información y sus métodos de proceso

Mesa de servicios: El punto de contacto único, en el cual se reciben las solicitudes de servicio de los usuarios de equipos y servicios de TIC en la Institución.

Objetivos estratégicos de TIC: El conjunto de resultados que se prevé alcanzar y que se integran en el PETIC, los cuales describen el alcance de las acciones que serán llevadas a cabo por la Subdirección de Tecnologías de la Información y Comunicaciones.

Problema: La causa de uno o más incidentes, del cual se plantea una solución alterna en espera de una solución definitiva.

Requerimientos funcionales: La característica que requiere cumplir un producto o entregable asociado a una función en un proceso o servicio automatizado, o por automatizar.

Riesgo: La posibilidad de que una amenaza pueda explotar una vulnerabilidad y causar una pérdida o daño sobre los activos de TIC, las infraestructuras críticas o los activos de información de la Institución.

Sistema informático: El conjunto de componentes o programas construidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso, de acuerdo a requerimientos previamente definidos.

Usuarios: Los servidores públicos o aquéllos terceros que han sido acreditados o cuentan con permisos para hacer uso de los servicios de TIC.

Validación: La actividad que asegura que un servicio de TIC, producto o entregable, nuevo o modificado, satisface las necesidades acordadas previamente con la unidad administrativa solicitante.

Verificación: La actividad que permite revisar si un servicio de TIC o cualquier otro producto o entregable, está completo y acorde con su especificación de diseño.

Vulnerabilidades: Las debilidades en la seguridad de la información dentro de una organización que potencialmente permite que una amenaza afecte a los activos de TIC, a la infraestructura crítica, así como a los activos de información.

6.6. Lineamientos y Políticas

Políticas de Uso de la Red Inalámbrica del Instituto Mora (RIIM)

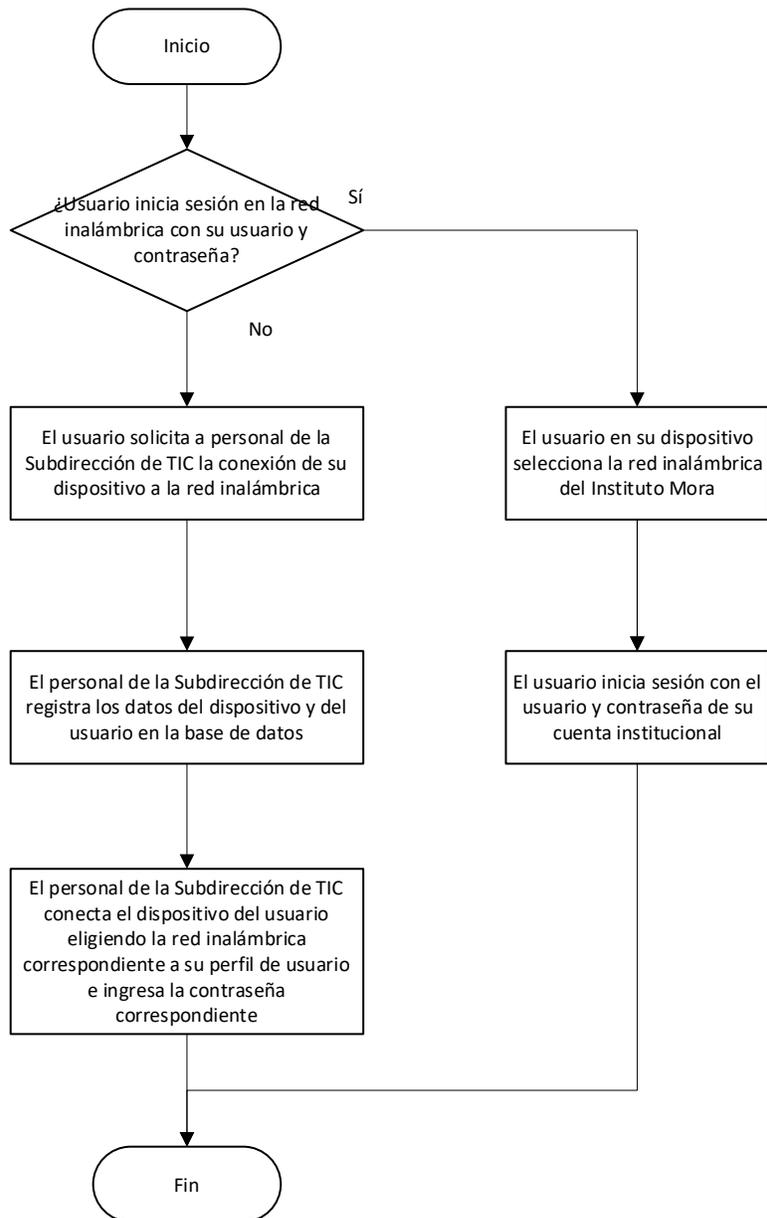
1. Las presentes políticas establecen las pautas generales para hacer uso de la RIIM y son aplicables a todos los usuarios de este servicio. Los usuarios autorizados (en adelante, "la Comunidad") son los siguientes:
 - a) Alumnos inscritos a cualquier programa académico o educación continua impartido por el Instituto.
 - b) Profesores-investigadores activos.
 - c) Visitantes a la Biblioteca y eventos académicos.
 - d) Personal administrativo y de apoyo activo.
2. La red inalámbrica está disponible para toda la Comunidad, y es de uso exclusivo para las actividades académicas, administrativas y de apoyo del Instituto.
3. Será responsabilidad de cada usuario el buen uso de la red Inalámbrica. La Subdirección de Tecnologías de la Información y Comunicaciones no se hace responsable por un mal uso por parte de los usuarios.
4. Será causa de baja temporal del servicio de RIIM a los usuarios que:
 - a) Generen tráfico excesivo en la RIIM de forma involuntaria.
 - b) Distribuyan virus, gusanos o código malicioso de forma voluntaria o involuntaria.
5. Toda vez que sean corregidas las causas del punto anterior y el usuario compruebe que ya no representa un riesgo para la RIIM, su cuenta será reactivada nuevamente.
6. A los usuarios que sean sorprendidos realizando las siguientes actividades serán dados de baja de forma definitiva del servicio RIIM:
 - a) Realizar actividades delictivas.
 - b) Envió de virus, gusanos, spam, código malicioso de forma voluntaria o con conocimiento de la actividad.
 - c) Ataques a otros puntos en la red por cualquier medio (denegación de servicio, *phishing*, etc.).
 - d) Enviar a través de la red, contenido inapropiado a cualquier pantalla del Instituto.
7. Cada usuario podrá conectar un máximo de 3 dispositivos simultáneamente a la red inalámbrica.
8. La Subdirección de Tecnologías de la Información y Comunicaciones restringirá el servicio de RIIM a aquellos usuarios que intentan violar la seguridad de cualquier equipo de cómputo o de red.

9. Al usuario que sea detectado usando software que invada la privacidad de alumnos, profesores, personal o equipo computacional se le restringirá el servicio de red.
10. Cada usuario es responsable por los sitios que visite en Internet.
11. El usuario es responsable de la información (audio, video, documentos, etc.) que baje de internet o intranet y deberá respetar los derechos de autor. En caso de no hacerlo responderá por el uso la información de la cual no cuente con la licencia o autorización respectiva antes las autoridades que lo requieran.
12. Es responsabilidad del usuario conocer las políticas de uso de la red.
13. El no tener conocimiento de estas políticas no es justificante para evitar respetarlas.

	Descripción de Actividades		Clave:
			Fecha:
	Nombre de Procedimiento: Procedimiento para acceder a la red inalámbrica del Instituto Mora		Versión: 1.0
			Página: 1/
Unidad Administrativa: Subdirección de Tecnologías de la Información y comunicaciones		Área Responsable: Soporte Técnico, Redes y Comunicaciones	

Paso	Responsable	Actividad	Documento de trabajo (Clave)
1	Usuario	1. El usuario inicia sesión en la red inalámbrica con su usuario y contraseña: Sí: continua en la actividad 2 No: continua en la actividad 4	
2			
3		2. El usuario en su dispositivo selecciona la red inalámbrica del Instituto Mora.	
		3. El usuario inicia sesión con el usuario y contraseña de su cuenta institucional.	
4		Fin del procedimiento	
		4. El usuario solicita a personal de la Subdirección de TIC la conexión de su dispositivo a la red inalámbrica.	
5	Soporte técnico / Redes y comunicaciones	5. El personal de la Subdirección de TIC registra los datos del dispositivo y del usuario en la base de datos.	
		6. El personal de la Subdirección de TIC conecta el dispositivo del usuario eligiendo la red inalámbrica correspondiente a su perfil de usuario e ingresa la contraseña correspondiente.	
FIN DEL PROCEDIMIENTO			

Diagrama de flujo del procedimiento



**7. Procedimiento para generación de contraseñas
de usuarios administradores
(MP/SG/STIC/07/2020)**

7.1. Propósito del Procedimiento

Establecer políticas y recomendaciones del uso, manejo y resguardo que deben contar las contraseñas para evitar que estas sean vulnerables además de salvaguardar la información contra uso y acceso no autorizado, divulgación o revelación, modificación, daño o pérdida.

7.2. Alcance

Establecer un estándar para la creación de contraseñas fuertes, favorecer su protección, así como estimular el cambio frecuente de las mismas.

7.3. Referencia o Marco normativo

Marco normativo

- a) Decreto de reestructuración del Instituto de Investigaciones Dr. José María Luis Mora.
- b) Estatuto Orgánico.
- c) Manual General de Organización.
- d) Manual Administrativo de Aplicación General en Materia de Tecnologías de Información y Comunicaciones y de Seguridad de la Información

7.4. Responsables

Subdirección de Tecnologías de la Información y Comunicaciones

7.5. Definiciones

Activo de información: Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para la Institución, debe ser protegido para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.

Acuerdo: el Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones y en la de Seguridad de la Información, así como establecer el Manual Administrativo de Aplicación General en dichas materias.

Acuerdo de nivel de servicio SLA: El acuerdo de nivel de servicio que se compromete con la unidad administrativa solicitante, al entregar un aplicativo de cómputo o servicio de TIC (*Service Level Agreement*, por sus siglas en inglés).

Acuerdo de nivel operacional OLA: El acuerdo de nivel operacional entre los responsables de los diversos componentes de la arquitectura tecnológica de un aplicativo de cómputo o servicio de TIC, que se debe definir y cumplir para responder a los acuerdos de nivel de servicio SLA comprometidos (*Operational Level Agreement* por sus siglas en inglés).

Ambiente de trabajo: El conjunto de herramientas, utilerías, programas, aplicaciones, información, facilidades y organización que un usuario tiene disponible para el desempeño de sus funciones de manera controlada, de acuerdo con los accesos y privilegios que tenga asignados por medio de una identificación única y una contraseña.

Amenaza: A cualquier posible acto que pueda causar algún tipo de daño a los activos de información de la Institución.

Análisis de riesgos: El uso sistemático de la información para identificar las fuentes de vulnerabilidades y amenazas a los activos de TIC, a la infraestructura crítica o a los activos de información, así como efectuar la evaluación de su magnitud o impacto y estimar los recursos necesarios para eliminarlas o mitigarlas.

Área contratante: A la facultada en la Institución para realizar procedimientos de contratación, a efecto de adquirir o arrendar bienes o contratar la prestación de servicios.

Área requirente: A la que, en la Institución, solicite o requiera formalmente la adquisición o arrendamiento de bienes o la prestación de servicios, o aquélla que los utilizará.

Área solicitante o usuaria: A la que, en la Institución, efectúa originalmente la petición a la Subdirección de Tecnologías de la Información y Comunicaciones para obtener un bien o servicio de TIC y/o que hará uso del mismo.

Área técnica: A la que, en la Institución, elabora las especificaciones técnicas que se deberán incluir en el procedimiento de contratación, evalúa la propuesta técnica de las proposiciones y es responsable de responder en la junta de aclaraciones las preguntas que sobre estos aspectos realicen los licitantes. El área técnica podrá tener también el carácter de área requirente.

Arquitectura tecnológica: A la estructura de hardware, software y redes requerida para dar soporte a la implementación de los aplicativos de cómputo, soluciones tecnológicas o servicios de TIC de la Institución.

Disponibilidad: La característica de la información de permanecer accesible para su uso cuando así lo requieran individuos o procesos autorizados.

Entregable: El producto adquirido, desarrollado o personalizado, con características cuantificables y medibles en términos de su valor, integralidad, funcionalidad y capacidades.

Evento: El suceso que puede ser observado, verificado y documentado, en forma manual o automatizada, que puede llevar al registro de incidentes.

Funcionalidad: Las características de los aplicativos de cómputo, soluciones tecnológicas o de un servicio de TIC, que permiten cubrir las necesidades o requerimientos de un usuario.

Gestión de riesgos: La identificación, valoración y ejecución de acciones, para el control y minimización de los riesgos que afecten a los activos de TIC, a la infraestructura crítica o a los activos de información de la Institución.

Impacto: Al grado de los daños y/o de los cambios sobre un activo de información, por la materialización de una amenaza.

Incidente: A la afectación o interrupción a los activos de TIC, a las infraestructuras críticas, así como a los activos de información de una Institución, incluido el acceso no autorizado o no programado a éstos.

Infraestructuras críticas: Las instalaciones, redes, servicios y equipos asociados o vinculados con activos de TIC o activos de información, cuya afectación, interrupción o destrucción tendría un impacto mayor, entre otros, en la salud, la seguridad, el bienestar económico de la población o en el eficaz funcionamiento de las Instituciones.

Integridad: La acción de mantener la exactitud y corrección de la información y sus métodos de proceso

Mesa de servicios: El punto de contacto único, en el cual se reciben las solicitudes de servicio de los usuarios de equipos y servicios de TIC en la Institución.

Objetivos estratégicos de TIC: El conjunto de resultados que se prevé alcanzar y que se integran en el PETIC, los cuales describen el alcance de las acciones que serán llevadas a cabo por la Subdirección de Tecnologías de la Información y Comunicaciones.

Problema: La causa de uno o más incidentes, del cual se plantea una solución alterna en espera de una solución definitiva.

Requerimientos funcionales: La característica que requiere cumplir un producto o entregable asociado a una función en un proceso o servicio automatizado, o por automatizar.

Riesgo: La posibilidad de que una amenaza pueda explotar una vulnerabilidad y causar una pérdida o daño sobre los activos de TIC, las infraestructuras críticas o los activos de información de la Institución.

Sistema informático: El conjunto de componentes o programas construidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso, de acuerdo a requerimientos previamente definidos.

Usuarios: Los servidores públicos o aquéllos terceros que han sido acreditados o cuentan con permisos para hacer uso de los servicios de TIC.

Validación: La actividad que asegura que un servicio de TIC, producto o entregable, nuevo o modificado, satisface las necesidades acordadas previamente con la unidad administrativa solicitante.

Verificación: La actividad que permite revisar si un servicio de TIC o cualquier otro producto o entregable, está completo y acorde con su especificación de diseño.

Vulnerabilidades: Las debilidades en la seguridad de la información dentro de una organización que potencialmente permite que una amenaza afecte a los activos de TIC, a la infraestructura crítica, así como a los activos de información.

7.6. Lineamientos y Políticas

Políticas de uso y generación de contraseñas para usuarios administradores del Instituto Mora.

- 1) Todas las contraseñas de sistema (cuentas de administrador, cuentas de administración de aplicaciones, etc.) deberán cambiarse con una periodicidad de al menos una vez cada seis meses.
- 2) Ante cualquier sospecha de que una contraseña de administrador haya sido comprometida, se deberá cambiar de forma inmediata, además se procederá a avisar del incidente de seguridad al responsable de la Seguridad de la Información (Subdirector de Tecnologías de la Información y Comunicaciones).
- 3) Si se trata de una contraseña para acceder a un sistema o servidor delicado se debe procurar limitar el número de intentos de acceso.
- 4) Sólo habrá tres responsables de la administración de las contraseñas: el Subdirector de Tecnologías de la Información y Comunicaciones, una persona del equipo de administración de proyectos y una persona del equipo de infraestructura.
- 5) Cuando una persona que tuvo acceso a una o más cuentas de usuario administrador termine su relación contractual con la institución se deberá solicitar el cambio de contraseñas a las que tuvo acceso.
- 6) Cuando las contraseñas sean enviadas vía correo electrónico éste deberá estar cifrado para asegurar que llegue al destinatario correcto.
- 7) Cuando se ejecute el algoritmo para la generación de contraseñas el usuario responsable del procedimiento deberá asegurarse de estar completamente desconectado de la red (WiFi o Ethernet).
- 8) Anualmente se deberán cambiar las memorias USB para evitar daños o pérdidas por fallas de éstas.

	Descripción de Actividades	Clave:
		Fecha:
	Nombre de Procedimiento: Procedimiento para generación de contraseñas de usuarios administradores	Versión: 1.0
		Página: 1/
Unidad Administrativa: Subdirección de Tecnologías de la Información y comunicaciones		Área Responsable: Administración de Proyectos y Cumplimiento Normativo, Redes y Comunicaciones, Infraestructura y Desarrollo.

Paso	Responsable	Actividad	Documento de trabajo (Clave)
1	Usuario administrador	1. Usuario administrador envía al equipo de administración de proyectos la petición de contraseñas que necesita crear y/o modificar.	
2	Administrador de proyectos responsable de administrar contraseñas	2. El responsable de la administración de las contraseñas se desconecta completamente de la red (WI-FI o Ethernet).	Bitácora de contraseñas
3		3. El responsable de la administración de las contraseñas creará la(s) contraseña(s) con el algoritmo para la generación de contraseñas.	
4		4. El responsable de la administración de las contraseñas llenará la bitácora de contraseñas en formato electrónico.	
5		5. El responsable de la administración de las contraseñas almacenará en 2 CD's y 2 memorias USB la bitácora de contraseñas actualizada y almacenará en un CD o memoria USB las contraseñas solicitadas. En el caso de los CD's deberán de grabarse con formato mastered o no regrabable y deberán de destruirse cada que se actualice el archivo de contraseñas.	
6		6. Una vez que se tengan las contraseñas, deberá enviar el CD o memoria USB con el listado de contraseñas solicitadas en sobre cerrado al usuario administrador solicitante quien será el responsable de salvaguardar la información contenida en el archivo.	

Paso	Responsable	Actividad	Documento de trabajo (Clave)
7	Usuario administrador	7. El usuario administrador aplicará el cambio de contraseñas. FIN DEL PROCEDIMIENTO	

Diagrama de flujo del procedimiento

