AVISO MEDIANTE EL CUAL SE INFORMA DE LA PUBLICACIÓN EN LA PÁGINA WEB/PORTAL DE TRANSPARENCIA DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES DE LAS "NORMAS PARA LA ADMINISTRACIÓN, OPERACIÓN Y MANTENIMIENTO DE SOLUCIONES DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES"

Publicación en el Diario Oficial de la Federación el 15 de noviembre de 2024

CONSIDERANDO

I. Que en cumplimiento a lo dispuesto en los artículos 57, primer párrafo y fracción VIII, y 61, fracciones IV, V y VII del Estatuto Orgánico del Instituto Federal de Telecomunicaciones esta Unidad de Administración emitió las "Normas para la Administración, Operación y Mantenimiento de soluciones de Tecnologías de la Información y Comunicaciones del Instituto Federal de Telecomunicaciones.", y

II. Que para dar cumplimiento a lo establecido en el artículo 100 del Estatuto Orgánico del Instituto Federal de Telecomunicaciones, he tenido a bien emitir el siguiente:

AVISO MEDIANTE EL CUAL SE INFORMA DE LA PUBLICACIÓN EN LA PÁGINA WEB/PORTAL DE TRANSPARENCIA DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES DE LAS "NORMAS PARA LA ADMINISTRACIÓN, OPERACIÓN Y MANTENIMIENTO DE SOLUCIONES DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES"

Disposición: Normas para la Administración, Operación y Mantenimiento de soluciones de Tecnologías de la Información y Comunicaciones del Instituto Federal de Telecomunicaciones.

Objeto: Establecer los procesos y disposiciones que las Unidades Administrativas del Instituto deberán considerar para la ejecución de proyectos que incluyan en su alcance total o parcial el uso o aplicación de tecnologías de la información.

Fecha de emisión: 30 de octubre de 2024.

Medio de consulta: Las siguientes ligas electrónicas:
http://www.ift.org.mx/sites/default/files/Normas-TIC-ift.pdf

Liga adicional: www.dof.gob.mx/2024/IFT/NormasTIC2024.pdf

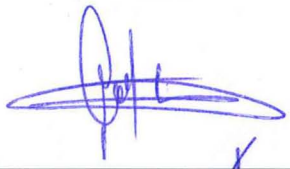
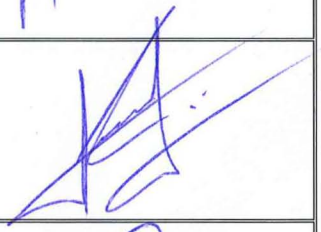
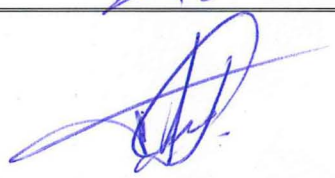
México, Ciudad de México, a 30 de octubre de 2024.- El Titular de la Unidad de Administración del Instituto Federal de Telecomunicaciones, **Oscar Everardo Ibarra Martínez**.- Rúbrica.

INSTITUTO FEDERAL DE TELECOMUNICACIONES

UNIDAD DE ADMINISTRACIÓN
DIRECCIÓN GENERAL DE TECNOLOGÍAS
DE LA INFORMACIÓN Y COMUNICACIONES

"NORMAS PARA LA ADMINISTRACIÓN, OPERACIÓN Y MANTENIMIENTO DE SOLUCIONES DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES"

Fecha de autorización: 04-11- 2024

AUTORIZACIÓN	
Titular de la Unidad de Administración Mtro. Oscar Everardo Ibarra Martínez	
VALIDACIÓN	
Director General de Tecnologías de la Información y Comunicaciones C. Abraham Adán Orduña Cortés	
Director de Seguridad de la Información C. Christian Cisneros Pedraza,	
Director de Infraestructura Tecnológica C. Julio César Álvarez Castillo	
Director de Desarrollo de Sistemas C. Francisco Javier Aguilar Salas	

Director de Gobierno y Adquisiciones de TIC C. Marco Antonio Reyes Arriaga	

INSTITUTO FEDERAL DE TELECOMUNICACIONES

NORMAS PARA LA ADMINISTRACIÓN, OPERACIÓN Y MANTENIMIENTO DE SOLUCIONES DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES

Última modificación publicada DOF 04-11-2024

TÍTULO PRIMERO
DISPOSICIONES GENERALES
CAPÍTULO ÚNICO

Artículo 1.- Las presentes normas tienen por objeto instrumentar las medidas que las Unidades Administrativas (UA) del Instituto Federal de Telecomunicaciones (IFT) deberán considerar para la ejecución de Proyectos que incluyan, en su alcance total o parcial, el uso o aplicación de tecnologías de la información y comunicaciones (TIC), así como aquellas que aseguren la correcta transición e implementación de las Soluciones Tecnológicas a la operación y mantenimiento por parte de la Dirección General de Tecnologías de la Información y Comunicaciones del Instituto Federal de Telecomunicaciones (DGTIC).

Para mejor entendimiento de la definición de los conceptos utilizados en el presente documento normativo y sus anexos, se debe consultar el "Glosario" (Anexo A)

Artículo 2.- Las presentes normas son de observancia general y obligatoria para todas las UA que integran el IFT, cuando en el cumplimiento de sus funciones requieran diseñar, construir, implementar u operar soluciones que, a través del uso total o parcial de las TIC, satisfagan sus necesidades y las apoyen en el cumplimiento de sus atribuciones, incluyendo aquellas que son realizadas por un proveedor o tercero.

Artículo 3.- Con el fin de vigilar el cumplimiento de las presentes normas, la DGTIC realizará las actividades de seguimiento o monitoreo necesarias, conforme a las atribuciones que le confiere el artículo 61 del Estatuto Orgánico del Instituto Federal de Telecomunicaciones, así mismo, resolverá cualquier situación, en materia de TIC, no prevista en las mismas.

Artículo 4.- Para los proyectos realizados por entes proveedores o terceros, la aceptación y liberación de los proyectos y el pago de estos, sin dar cumplimiento a las presentes normas, será responsabilidad del Administrador del Contrato de la UA correspondiente, por lo que la DGTIC no será responsable de atender las fallas y/o deficiencias de la Solución Tecnológica, ni estará obligada a desplegar la solución tecnológica en la infraestructura productiva del Instituto.

TÍTULO SEGUNDO
ADMINISTRACIÓN DEL PORTAFOLIO DE PROYECTOS DE TIC
CAPÍTULO PRIMERO
OFICINA DE PROYECTOS DE TIC

Artículo 5. La Oficina de Proyectos de la DGTIC (OP) tiene como objetivo establecer y verificar la implementación y cumplimiento de las metodologías, herramientas y técnicas para estandarizar la gestión de proyectos de TIC en el IFT, así como su control y seguimiento.

Artículo 6. La OP, es la responsable de la administración centralizada del portafolio, programas y proyectos de TIC para garantizar que estén orientados hacia el logro de los objetivos institucionales; para ello, será la responsable de ponderar todas las iniciativas de TIC del IFT para priorizar su ejecución.

Artículo 7. La OP tendrá las siguientes funciones:

I. Establecer metodologías y estándares, basados en mejores prácticas, para la gestión de proyectos de TIC.
II. Proporcionar soporte administrativo y técnico a las personas Líderes de Proyecto y personas Líderes de Negocio.
III. Coordinar y asignar recursos de manera eficiente entre diferentes proyectos de TIC.
IV. Realizar seguimiento del progreso de los proyectos de TIC y asegurar que se cumplan los plazos, presupuesto y alcance definidos.
V. Gestionar el portafolio de proyectos de TIC.
VI. Priorizar y seleccionar iniciativas de TIC a ser ejecutadas.
VII. Realizar estimaciones de proyectos de TIC.
VIII. Facilitar la comunicación y presentar informes a las partes interesadas sobre el estado y el rendimiento de los proyectos de TIC.
IX. Dar seguimiento a proyectos contratados con proveedores que, en su alcance, total o parcial, incluyan TIC.

Artículo 8. La OP tiene competencia para supervisar, coordinar y estandarizar la ejecución todos los proyectos que incluyan, en su alcance total o parcial, el uso de TIC.

CAPÍTULO SEGUNDO
CLASIFICACIÓN DE PROYECTOS DE TIC

Artículo 9. De acuerdo con la naturaleza de las contrataciones y proyectos de TIC, se establece la siguiente clasificación:

Tipo de proyecto	Sub-tipo
Adquisición de servicios que incluyen TIC	No aplica.
Licenciamiento o suscripción de software	No aplica.
Adquisición o arrendamiento de hardware	Equipo de cómputo personal, periféricos, dispositivos móviles, entre otros Equipo de procesamiento, almacenamiento, transmisión de datos y ciberseguridad
Sistema Informático (sistema, portal, micrositio o aplicación móvil)	Nuevo sistema informático. Mantenimiento mayor a un sistema existente. Mantenimiento menor a un sistema existente.
Servicio de nube	Software como Servicio (SaaS) Plataforma como Servicio (PaaS) Infraestructura como Servicio (IaaS) Contenedores como Servicio (Caas)
Analítica de datos	Captura y procesamiento de datos Almacenamiento de datos Análisis de datos Tableros de datos
Tecnología emergente	Cualquier proyecto que involucre una tecnología no usada en el IFT

Tabla 1. Tipología general de proyectos de Soluciones Tecnológicas

Cada tipo de proyecto se describe a continuación:

I. **Adquisición de servicios que incluyen TIC:** corresponde a la contratación de cualquier servicio que incluya en su alcance, total o parcial, el uso de TIC.

II. **Licenciamiento o suscripción de software:** corresponde a la adquisición o suscripción de algún tipo de software o licencia existente en el mercado, así como a su instalación dentro de los centros de datos, servicios de nube, o equipos de cómputo personal administrados por la DGTIC, pudiendo ser de tipo comercial o de código abierto. En caso de que la DGTIC cuente con el software y el número de licencias requeridas, la UA solicitante deberá solicitarlas apegándose a lo estipulado en las "Políticas para el uso de los recursos de TIC"; de lo contrario, la DGTIC acompañará a la UA en el proceso de evaluación y adquisición que resulte necesario. Adicionalmente se tendrá que validar que su despliegue se realice adecuadamente.

III. **Adquisición o arrendamiento de hardware:** consiste en la adquisición o arrendamiento, instalación y configuración de equipamiento tecnológico dentro de los centros de datos y/o servicios de nube administrados por la DGTIC. Si la DGTIC cuenta con el tipo de hardware requerido, la UA solicitante deberá solicitarlo apegándose a lo estipulado en las "Políticas para el uso de los recursos de TIC". En caso contrario, la DGTIC acompañará a la UA en el proceso de adquisición que resulte necesario y realizará su revisión para asegurar que su instalación y uso no pongan en riesgo la Seguridad de la Información del Instituto, así como para validar que su despliegue se realice adecuadamente.

IV. **Sistema informático:** se refiere al desarrollo o contratación de una nueva Solución Tecnológica o al mantenimiento de una ya existente. Si se trata del desarrollo de un nuevo sistema, la DDS) lo evaluará para identificar si se trata de un sistema informático, portal, micrositio o aplicación móvil. En caso de un cambio o actualización de un sistema informático existente, el mantenimiento se puede clasificar en 4 tipos:

   a) Correctivo: se deriva de fallos o errores que afectan la funcionalidad del sistema, portal, micrositio o aplicación móvil.
   b) Preventivo: se refiere a realizar cambios necesarios, actualizaciones y adaptaciones que pueden originar algunos problemas mayores en un futuro.
   c) Perfectivo: se refiere a ajustar el sistema, portal, micrositio o aplicativo móvil agregando nuevas funcionalidades y/o eliminando funcionalidades que son irrelevantes.
   d) Adaptable: se refiere al cambio de tecnologías, tales como el sistema operativo, almacenamiento en la nube, entre otros.

   Se entenderá por mantenimiento mayor aquellos mantenimientos que incluyen cambios que afectan el flujo de trabajo, actualización del sistema informático, portal, micrositio, aplicaciones móviles o infraestructura tecnológica y/o que requieren un tiempo de ejecución superior a 400 horas-persona tomando en cuenta todo el ciclo de vida del proyecto; son cambios más profundos y complejos que pueden afectar significativamente la estructura, funcionalidad o componentes fundamentales del sistema. Algunos cambios que pueden caer en este tipo de mantenimiento pueden ser, de forma enunciativa mas no limitativa, descritos de la siguiente forma:

   - Modificar el flujo de sistemas o de reglas de negocio.
   - Agregar nuevos perfiles o roles.
   - Modificar la funcionalidad del sistema informático, portal, micrositio o aplicaciones móviles.
   - Actualizar catálogos del sistema informático, portal, micrositio o aplicaciones móviles.
   - Agregar módulos.
   - Incrementar el número de transacciones u operaciones que deba realizar un sistema.

   Se entenderá por mantenimiento menor, aquellos mantenimientos a sistemas informáticos, portales, micrositios o aplicaciones móviles instalados en la infraestructura del IFT, en ambiente productivo, cuyos cambios requieren un tiempo de ejecución menor o igual a 400 horas persona,

tomando en cuenta todo el ciclo de vida del proyecto. Los mantenimientos menores consideran modificaciones que no alteran profundamente la estructura o funcionalidad general del sistema, estos tipos de cambios suelen estar enfocados en mejorar, corregir o ajustar aspectos relativamente pequeños y específicos del sistema. Este tipo de mantenimientos deberán ser solicitados a través de un ticket de "Mantenimiento Menor" a la Mesa de Servicio Institucional. Los mantenimientos menores pueden ser, de forma enunciativa mas no limitativa, descritos de la siguiente forma:

- Corrección de errores
- Actualización de interfaces de usuario
- Mejoras de rendimiento
- Ajustes a la lógica de negocio
- Actualización de compatibilidad
- Optimización de bases de datos
- Implementación de pequeños módulos o funcionalidades
- Para los mantenimientos menores, las UA no requerirán notificarlos en la respuesta a la solicitud de información realizada por la DGTIC para la elaboración del Programa Anual de Proyectos de TIC.

V. **Servicio de nube**: consiste en utilizar infraestructura, plataformas y/o software que alojan proveedores externos para satisfacer diversas necesidades tecnológicas del Instituto, lo cual permite a los usuarios acceder a recursos computacionales de manera flexible y escalable.

VI. **Analítica de datos**: uso de herramientas, plataformas, y servicios especializados para la recolección, procesamiento, análisis, visualización, y uso de datos dentro del Instituto, las cuales están diseñados para ayudar a extraer valor de los datos, facilitando la toma de decisiones basada en información precisa y oportuna.

VII. **Tecnología emergente**: implementación, gestión y provisión de tecnologías que aún no han sido adoptadas en el Instituto. Estas tecnologías ofrecen nuevas oportunidades para mejorar procesos, aumentar la eficiencia, o habilitar capacidades que antes no estaban disponibles.

CAPÍTULO TERCERO
PORTAFOLIO DE PROYECTOS DE TIC

Artículo 10.- El Portafolio de Proyectos de TIC se compone del Programa Anual de Proyectos de TIC (PAP) y el Programa de Desarrollo Informático (PDI). El portafolio permite una visión general de todos los proyectos de TIC del Instituto para comprender como se relacionan entre sí, con la finalidad de priorizarlos, optimizar recursos, determinar su alineación con los objetivos estratégicos del Instituto, gestionar los riesgos y ayudar en la toma de decisiones.

PROGRAMA ANUAL DE PROYECTOS DE TIC (PAP)

Artículo 11.- La DGTIC conformará en cada ejercicio fiscal el PAP, el cual es un inventario de los proyectos por atender de las UA del Instituto, que en su alcance total o parcial incluyan TIC. El PAP, se conforma por 4 etapas que a continuación se describen:

I. Identificación de iniciativas de TIC.

Durante el último trimestre de cada año, la DGTIC realizará un análisis a efecto de identificar las iniciativas a ser proyecto con alcance total o parcial de TIC considerando la Estrategia de Gobierno Electrónico, el Anteproyecto del Plan Anual de Trabajo (PAT), el Anteproyecto del Presupuesto Egresos de la Federación (PEF) y el PAP del ejercicio fiscal en curso, así como cualquier otra fuente de información que facilite la identificación de posibles iniciativas de TIC.

Por medio de oficio, la DGTIC solicitará a las UA la confirmación respecto a las iniciativas a ser proyecto que serán programadas para el siguiente ejercicio fiscal, y de ser el caso, notifiquen si existen iniciativas adicionales que se deban considerar para su registro en el PAP.

Las UA tendrán 15 días hábiles a partir de la recepción del oficio para enviar su respuesta mediante oficio, el cual podrá ser firmado por la persona Titular de la Unidad a través de la Firma Electrónica de Documentos Internos (FEDI) o de forma autógrafa. Dicho oficio, deberá contener todas las iniciativas a ser proyecto por parte de la UA a efecto de que éstas se consideren para ser integradas como parte del PAP.

Por cada iniciativa a ser proyecto, la UA deberá proporcionar la información suficiente que permita su identificación, análisis y evaluación, para tal efecto, la DGTIC establecerá la forma en la que se deberá recabar dicha información. Concluido el plazo, se dará por finalizada esta etapa, por lo que las iniciativas a ser proyecto que requieran ser registradas posterior a la fecha límite y durante el ejercicio fiscal siguiente, serán identificadas como "Iniciativas extemporáneas" y su atención estará sujeta a la priorización descrita en la etapa de "Priorización de iniciativas" del presente artículo.

II. Análisis y clasificación de las iniciativas de TIC.

Durante esta etapa, la DGTIC realizará el análisis de la información proporcionada por las UA para cada una de las iniciativas a ser proyecto con la finalidad de clasificarlas conforme a su naturaleza y fuente de financiamiento. Para tal efecto, se considerará lo siguiente:

a) Iniciativas de contratación de hardware, software o servicios a través de recursos del Presupuesto de Egresos de la Federación (PEF) o del Fideicomiso de Infraestructura y Equipamiento del Instituto Federal de Telecomunicaciones (FIE). Para tal efecto, en el marco de la integración del Programa Anual de Adquisiciones y Servicios del IFT (PAAAS), la DGTIC obtendrá la información de los proyectos que en su alcance total o parcial incluyan TIC.
b) Iniciativas a ser proyecto que no cuentan con presupuesto asignado en el PEF o del FIE, y que las UA esperan sean atendidas por medio de los recursos a cargo de la DGTIC.

III. Priorización de iniciativas.

Para determinar aquellas iniciativas a ser proyecto que podrán ser atendidas con los recursos a cargo de la DGTIC, se realizará una evaluación y priorización con la finalidad de elaborar una propuesta de atención de las iniciativas.

Los criterios considerados son los siguientes:

a) Cobertura Institucional. Este criterio identifica el posible impacto que tendrá la ejecución y puesta en marcha de la iniciativa en evaluación, considerando cuántas áreas del Instituto serán beneficiadas y/o cuántas entidades concesionarias, personas usuarias o agentes externos impactará. Se considera que las iniciativas que tienen una cobertura al exterior del Instituto tendrán mayor peso. Asimismo, este criterio considera si la Solución Tecnológica automatizará o mejorará algún trámite o proceso.
b) Impacto y alineación con los objetivos estratégicos del Instituto. Se trata de determinar si la iniciativa impactará de forma directa al logro de los objetivos estratégicos del Instituto. Principalmente, se deberá identificar si forma parte del PAT del IFT, o en su defecto, determinar la contribución de la iniciativa con base en los objetivos que se encuentren descritos en la "Planeación Estratégica" del IFT. En ambos casos, se deberá considerar la versión más actualizada de la documentación antes referida.
c) Riesgos. El objetivo de este criterio es identificar si las iniciativas a evaluar apoyaran a mitigar riesgos institucionales, como la afectación a servicios proporcionados a las entidades de

gobierno, a la ciudadanía y/o a empresas reguladas, el incumplimiento en la protección de Datos Personales y el daño a la Transparencia institucional, la afectación actual a los procesos y/o la operación interna o afectación a la reputación e imagen del IFT.

d) Cumplimiento regulatorio/normativo. Este criterio considera aspectos del tiempo en que se requiere tener la iniciativa de TIC a disposición de la UA o bien de los entes externos o fiscalizadores del Instituto. Deberá identificarse si la urgencia deriva de una disposición regulatoria o normativa que delimite un tiempo específico de cumplimiento. En este último caso, el proyecto tendrá un mayor peso y, por lo tanto, cobrará mayor prioridad.
e) Beneficios/impacto/valor al Instituto. Este criterio evalúa el impacto que tendrá la iniciativa en:
   - La alineación a políticas de conversión digital de los trámites y servicios que ofrece el Instituto a sus áreas internas y a los entes externos;
   - El valor que aporten al Ecosistema Digital institucional.
   - La optimización de los recursos involucrados en la ejecución de los procesos de las UA (tecnológicos, financieros, y materiales).
f) Viabilidad técnica. Este criterio evalúa la posibilidad del inicio inmediato y el nivel de complejidad del desarrollo de la iniciativa. En caso de que la iniciativa en cuestión se trate de un mantenimiento a un sistema o portal existente, se tendrá en cuenta el nivel histórico de visitas a éste y se privilegiarán aquellos que están dirigidos a la ciudadanía o a los concesionarios del sector de telecomunicaciones y radiodifusión.

Con el resultado de la priorización de las iniciativas a ser proyecto, la DGTIC realizará una propuesta de atención de éstas, la cual será presentada al Grupo de evaluación de iniciativas de TIC a efecto de validar que el PAP guarde consistencia con la planeación estratégica, el gobierno electrónico, el gobierno de datos y la agenda de transformación digital del IFT.

Posterior a dicha validación, las iniciativas a ser proyecto que podrán ser atendidas a través de los recursos a cargo de la DGTIC serán comunicadas a las personas Titulares de las UA por medio de correo electrónico, indicando también aquellas iniciativas que deberán esperar para ser atendidas.

El total de las iniciativas de contratación de hardware, software o servicios con recursos presupuestales del PEF o del FIE no serán objeto de priorización toda vez que cuentan con recursos propios para su ejecución a través de un proveedor o tercero.

IV. Integración del Programa Anual de Proyectos de TIC.

El PAP incluirá las iniciativas de contratación de hardware, software o servicios con recursos presupuestales del PEF o del FIE y que estén registradas en el PAAS. En este caso, las UA contarán con el apoyo y participación técnica por parte de la DGTIC conforme a lo establecido en las Políticas y Bases en materia de Adquisiciones, Arrendamientos y Contratación de Servicios de cualquier naturaleza del Instituto Federal de Telecomunicaciones (POBAS).

Asimismo, considerará las iniciativas a ser proyecto que podrán ser atendidas a través de los recursos a cargo de la DGTIC conforme al resultado de la priorización de iniciativas.

La DGTIC formalizará el PAP y lo compartirá por correo electrónico al Grupo de evaluación de iniciativas de TIC, a la persona Titular de la Unidad de Administración y a las personas interesadas.

PROGRAMA DE DESARROLLO INFORMÁTICO (PDI)

Artículo 12. Con fundamento en la fracción II del artículo 61 del Estatuto Orgánico del Instituto, la DGTIC tiene la atribución de elaborar y administrar el programa institucional de desarrollo informático anual, mismo que deberá reflejar la estrategia en materia de tecnologías de la información y comunicaciones

del Instituto, a fin de mantener actualizada la infraestructura tecnológica del mismo. Con la finalidad de dar cumplimiento a lo anterior, la DGTIC realizará lo siguiente:

I. En el último trimestre de cada año, las Direcciones de Área adscritas a la DGTIC identificarán las iniciativas a ser proyecto que atiendan las necesidades de TIC del IFT. Dicho proceso deberá considerar, de manera enunciativa pero no limitativa, los siguientes aspectos:

   a) Renovación de iniciativas de contratación de hardware, software o servicios con fuente de financiamiento PEF o FIE.
   b) Los proyectos identificados en el Programa de Desarrollo Institucional (PDI) del ejercicio fiscal en curso que no hayan concluido, así como aquellos cuyo plan de trabajo esté programado para concluir en ejercicios fiscales posteriores.
   c) El resultado de la planeación estratégica vigente de la DGTIC, alineado a los objetivos institucionales y a las necesidades emergentes del IFT.
   d) Los proyectos propuestos por las Direcciones de Área de la DGTIC, en función de su impacto y contribución a los objetivos Institucionales.

II. Una vez finalizado el proceso de identificación, se consolidará una lista completa de las iniciativas que hayan sido consideradas viables para su desarrollo como proyectos TIC.

III. La DGTIC evaluará la lista consolidada de iniciativas y determinará cuáles de ellos serán considerados prioritarios para su inclusión en el PDI del ejercicio fiscal siguiente, en función de su impacto y contribución a los objetivos institucionales.

IV. La DGTIC procederá a la elaboración del documento que formalice el PDI correspondiente, mismo que deberá contener los resultados obtenidos respecto al PDI del año en curso, así como el desarrollo de los siguientes puntos para cada uno de los proyectos aprobados:

   a) Los antecedentes del proyecto, detallando la justificación y el contexto en el que se inscribe.
   b) El alcance del proyecto, definiendo los objetivos específicos y el marco temporal de su ejecución.
   c) El mapa de ruta o cronograma de actividades, incluyendo las fases clave del desarrollo del proyecto.
   d) Los principales hitos o entregables, que permitan medir el grado de cumplimiento de los objetivos del proyecto.
   e) Los beneficios esperados, tanto en términos cualitativos como cuantitativos.

El PDI deberá ser validado y autorizado por la DGTIC, la persona Titular de la Unidad de Administración, y tendrá una vigencia de 12 meses año calendario. La OP realizará la difusión del PDI a todo el personal de la DGTIC.

Artículo 13.- Para asegurar el correcto desarrollo de los proyectos asociados al PDI, la OP realizará el seguimiento y monitoreo correspondiente, atendiendo lo descrito en las siguientes fracciones:

I. Cada persona Líder de Proyecto deberá generar informes de avance mensual, que serán enviados a la DGTIC y a la OP con la finalidad de conocer el estado del proyecto.
II. De manera trimestral la OP generará un documento con el reporte de avance de cada uno de los proyectos, en el que identifique el porcentaje de avance real, la fase en la que se encuentra el proyecto, los principales hitos alcanzados, los riesgos y cualquier otro indicador que se considere de valor para el seguimiento del proyecto.
III. Al finalizar el año, se realizará un informe de cierre que integre cada uno de los proyectos que conforman el PDI, considerando:

a) Evaluación de resultados.
b) Descripción general de las actividades realizadas.
c) Resultados o beneficios obtenidos.

Dicho informe de cierre deberá incluirse como parte inicial del PDI del ejercicio fiscal siguiente.

CAPÍTULO CUARTO
SEGUIMIENTO DEL PORTAFOLIO DE PROYECTOS DE TIC

Artículo 14.- La OP le asignará una clave o identificador único dentro del portafolio a cada uno de los proyectos que integren el PAP y el PDI, lo anterior, con el fin de facilitar su trazabilidad y seguimiento.

Artículo 15.- En el transcurso del ejercicio fiscal, la DGTIC podrá sostener reuniones con la DGARMSG y la DGFPC a efecto de identificar la cancelación, cambios en la fuente de financiamiento o integración de forma extemporánea de nuevas iniciativas de TIC en el PAAAS.

En caso de que una iniciativa de contratación de hardware, software o servicios, originalmente planteada para ser atendida con recursos del PEF o FIE, requiera ser atendida a través de los recursos a cargo de la DGTIC, quedará sujeta a lo dispuesto en la fracción III del artículo 11 de las presentes Normas.

Artículo 16.- Como parte del control y seguimiento del portafolio, la OP informará mensualmente a las personas Titulares de cada UA el estado que guarden sus proyectos de TIC que formen parte del PAP.

Las Fases en las que se podrán notificar los proyectos son:

I. **Inicio.** Se refiere a proyectos que están programados en el PAP para su ejecución y que cuentan con una fecha de inicio planeada que permitirá dar seguimiento a su ejecución.
II. **Planeación.** Se refiere a que el proyecto está siendo revisado por parte del equipo de la DGTIC con el objetivo de obtener el Documento de Entendimiento y Propuesta de Solución aprobados por la UA solicitante, mismos que deberán ser firmados a través de la FEDI o de forma autógrafa.
III. **Ejecución.** Se refiere a proyectos que fueron formalizados mediante la realización de la junta de arranque y un acta constitutiva misma que deberá ser firmada a través de la FEDI o de forma autógrafa. Esta fase se mantendrá hasta que el proyecto pase al ambiente productivo.
IV. **Cierre.** Se refiere a proyectos en los cuales se concluyeron todas las actividades y se formaliza con la firma de las y los interesados en la documentación de cierre, cabe mencionar que esta documentación podrá ser firmada a través de la FEDI o de forma autógrafa a excepción de la encuesta de satisfacción. Los documentos que corresponden a este estado son los siguientes:
    a) Acta de cierre del proyecto,
    b) Acta de aceptación de entregables, cuando aplique y,
    c) Encuesta de satisfacción.
V. **Cancelado.** Se refiere a iniciativas o proyectos en los que la UA decide cancelar su ejecución; al haber analizado la vigencia de su necesidad, los riesgos asociados a su ejecución, o la disponibilidad de recursos, entre otros elementos relevantes. La UA deberá informar a la DGTIC cuando decida la cancelación de algún proyecto, indicando las causas que la motivaron a tomar dicha decisión.
VI. **Reprogramado.** Se refiere a iniciativas o proyectos donde la UA decide que su ejecución se llevará a cabo para el siguiente ejercicio fiscal, considerando para ello, la vigencia de su necesidad, los riesgos asociados a su ejecución y/o la disponibilidad de recursos, entre otros supuestos. Esta

decisión deberá ser informada a la DGTIC indicando las causas que dieron origen a la reprogramación.

VII. En espera. Se refiere a iniciativas a ser proyectos que deberán esperar a ser atendidas. Dichas iniciativas podrán considerar su ejecución una vez concluidos los proyectos del PAP en curso.

Artículo 17.- Para el seguimiento a los proyectos del PAP que son atendidos por medio de los recursos a cargo de la DGTIC y son desarrollados a través de una metodología tradicional o en cascada, los porcentajes establecidos para cada una de las fases serán los siguientes:

Etapa o Fase	Porcentaje mínimo	Porcentaje Máximo
Inicio	0%	10%
Planeación	11%	20%
Construcción	21%	75%
Pruebas de QA	76%	90%
Pruebas de UAT	91%	95%
Despliegue	96%	98%
Cierre	99%	100%

Tabla 2. Porcentajes por fase para metodología tradicional o en cascada

Artículo 18.- Para el seguimiento a los proyectos del PAP que son atendidos por medio de los recursos a cargo de la DGTIC y son desarrollados a través de una metodología de entrega de valor constante (iterativo o ágil), el avance del proyecto se medirá con, entre otras, las siguientes herramientas:

I. Burn Down Chart: Gráfica que muestra el trabajo restante en el tiempo y que ayudará a visualizar cuánto trabajo queda por hacer y si el equipo está en camino de completar el proyecto a tiempo.
II. Burn Up Chart: Gráfica que muestra el trabajo completado frente al trabajo total planificado y que proporcionará una visión clara del progreso del equipo hacia la finalización del proyecto y permite ver si se han añadido nuevas tareas.
III. Velocidad del equipo: Medida de la cantidad de trabajo completado en un sprint que ayudará a predecir cuánto trabajo puede completar el equipo en futuros sprints, ajustando la planificación y expectativas.
IV. Definición de hecho (Definition of Done - DoD): Lista de criterios que deben cumplirse para que una historia de usuario se considere completada y que asegurará que todo el trabajo entregado cumpla con los estándares de calidad y funcionalidad.
V. Entrega de funcionalidad completa: Verificación de que cada entrega incluye una funcionalidad completa y utilizable y que garantizará que cada entrega agrega valor y puede ser utilizada por las personas usuarias finales, incluso si las entregas no son periódicas.
VI. Métricas de calidad: Criterios y medidas utilizadas para evaluar la eficiencia del proyecto, incluye pruebas automatizadas, revisiones de código, y análisis de deuda técnica que ayudará a mantener y mejorar la calidad del código y la funcionalidad entregada.
VII. Feedback de las personas usuarias finales: Opiniones y comentarios de las personas usuarias finales sobre la funcionalidad entregada que permitirán ajustar el producto según las necesidades y expectativas reales de las personas usuarias.
VIII. Índice de satisfacción de las y los clientes: Medida de la satisfacción de las y los clientes con la funcionalidad entregada, esta proporcionará una métrica directa de cómo el trabajo del equipo está cumpliendo con las expectativas del cliente.
IX. Análisis de Valor Negocio: Evaluación de cómo cada entrega contribuye al valor general del negocio y ayudará a priorizar las tareas y entregas que más impactan en los objetivos del negocio.

TÍTULO TERCERO
GESTIÓN DE PROYECTOS DE TIC
CAPÍTULO PRIMERO
METODOLOGÍAS PARA LA GESTIÓN DE PROYECTOS DE TIC

Artículo 19.- Para garantizar que las Soluciones Tecnológicas alcancen los objetivos para los cuales son creadas, la DGTIC implementó una metodología basada en buenas prácticas, para homologar la gestión de los proyectos de TIC. Esta metodología consta de las siguientes fases.

I. Inicio: En esta fase se define el propósito y los objetivos del proyecto. Se identifican los interesados clave y se establecen sus expectativas. Se crea un documento formal el proyecto denominado Caso de Negocio.

II. Planeación: Se genera el documento de entendimiento donde se define el alcance y la forma en que se atenderá la solución tecnológica por la DGTIC. Se realiza el análisis y diseño de la solución, cronograma detallado que incluye todos los aspectos del proyecto, como el alcance, el costo, la calidad y los recursos. Se detallan los entregables del proyecto y se establecen los límites del mismo. Se identifican las actividades necesarias para completar el proyecto. Se establecen los mecanismos y métodos para la comunicación efectiva entre los interesados del proyecto. Se identifican los riesgos potenciales, se analizan y se planifican las respuestas adecuadas. Finalmente, se genera el documento denominado Propuesta de solución.

III. Ejecución: La fase inicia con la reunión de arranque del proyecto y se formaliza el proyecto con el Acta de constitución. Se llevan a cabo las actividades del proyecto según el cronograma del proyecto de acuerdo al modelo de desarrollo seleccionado.

IV. Monitoreo y Control: Se supervisa el progreso del proyecto y se comparan los resultados reales con el cronograma del proyecto. Se gestionan los cambios en el proyecto de manera controlada y se asegura que se implementen de manera efectiva. Se supervisa el alcance del proyecto y se gestionan los cambios en el alcance. Se asegura que la información del proyecto se comunique de manera efectiva y oportuna.

V. Cierre: Se finalizan todas las actividades del proyecto o fase y se obtienen las aprobaciones formales de los interesados. Se documentan las lecciones aprendidas durante el proyecto y se archivan para referencia futura. Se entregan los productos finales del proyecto a los interesados y se asegura que cumplan con los requisitos y expectativas. Se formalizan los documentos: Acta de cierre de proyecto y encuesta de satisfacción.

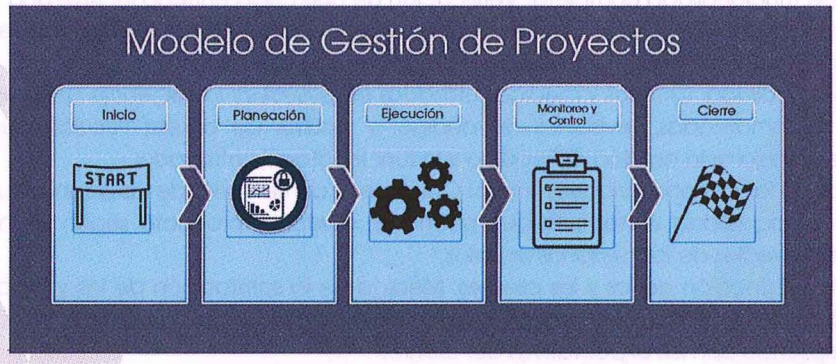


Ilustración 1 Modelo de Gestión de Proyectos

Artículo 20.- Para comenzar la fase de Inicio de los proyectos aprobados, la OP elaborará y enviará un proyecto de **Caso de Negocio** a la UA para que sea complementado y, en su caso, aprobado. El caso de negocio será elaborado con base en la información que la UA proporcione del proyecto durante el levantamiento preliminar del "Programa Anual de Proyectos de TIC" (PAP). Un Caso de Negocio se considera un estudio documentado acerca de la viabilidad de un proyecto indicando principalmente:

I. Problema de negocio/oportunidad identificada
II. Propuesta de solución
III. Propuesta de valor
IV. Ventaja competitiva
V. Entrega de valor a través de ciclos
VI. Objetivos de la iniciativa
VII. Impacto en cantidad de usuarios
VIII. Métricas claves identificadas a mejorar
IX. Flujo o modelo conceptual
X. Riesgos identificados si no existe esta solución

Una vez finalizada la revisión y aprobación del Caso de Negocio del proyecto, por parte de la UA y la OP, esta última, lo enviará a la DDS, con lo que se dará por finalizada la fase de inicio.

Artículo 21. Para el caso de proyectos con recursos a cargo de la DGTIC, la persona Analista de Negocio, deberá realizar la gestión de requerimientos necesarios para la solución tecnológica, elaborando el Documento de Entendimiento del proyecto y estableciendo la línea base de este, considerando entre otros puntos importantes, los requerimientos funcionales, no funcionales y reglas de negocio. El Documento de Entendimiento se modelará mediante las rondas de trabajo que sean necesarias junto con la persona Líder de Negocio de la UA solicitante hasta obtener la aprobación de éste. La formalización del mismo no deberá exceder de 5 días hábiles. La OP formalizará a firma el Documento de Entendimiento, el cual podrá ser firmado a través de la FEDI o de forma autógrafa.

Artículo 22. La estimación de esfuerzo para cada proyecto será realizada por el equipo de la DDS, dicha estimación deberá ser aprobada por la persona a cargo de la DDS, quien podrá solicitar una estimación de control y validación a la OP para determinar la sobreestimación o subestimación de un proyecto.

Artículo 23. Para el caso de Licenciamientos y adquisición de hardware, la OP dará seguimiento al cronograma de trabajo, específicamente, a las actividades relacionadas con los servicios proporcionados por la DGTIC y que estén dentro del alcance del proyecto.

Artículo 24. **Acta de Constitución del proyecto.** Este documento será elaborado por la OP. Dicho documento deberá identificar el detalle de actividades necesarias para crear la solución tecnológica como son: descripción, objetivo, alcance, tiempos y costos estipulados que se hayan presentado en la propuesta de solución tecnológica. El Acta Constitutiva deberá ser aprobada y firmada por el Titular de la UA solicitante y el líder de negocio para dar inicio a la ejecución del proyecto. Este documento podrá ser firmado a través de la FEDI o de forma autógrafa.

Artículo 25. **Control de cambios.** La OP dará seguimiento a todos los proyectos con recursos a cargo de la DGTIC, en caso de encontrar alguna desviación, la OP identificará y plasmará aquellos riesgos identificados y solicitará a la persona Líder de Proyecto el plan de mitigación correspondiente.

Si la OP, identifica alguna desviación mayor al 10% en el avance del proyecto, solicitará a la persona Líder de Proyecto elaborar el documento de control de cambios correspondiente.

Para la elaboración del control de cambios, la persona Líder de Proyecto deberá tomar en cuenta lo siguiente:

I. Incluir la justificación, además de especificar el impacto en tiempo, costo y el cambio al alcance cuando aplique.
II. El control de cambios de un proyecto no podrá exceder el 15% del esfuerzo total estimado en su planeación inicial, sin importar si es un solo control de cambios o de varios.
III. Si el control de cambios solicitado supera el 15% del esfuerzo original planeado, la UA requirente deberá reducir el alcance del cambio solicitado, o dividirlo en fases, para atender y dar continuidad al proyecto para su salida a ambiente productivo. Los nuevos requerimientos serán solventados en una segunda fase o como un proyecto de mantenimiento o mejora. Esto no exime a la persona Líder de Negocio de firmar la documentación de cierre del proyecto conforme al alcance pactado, el cual podrá ser firmado a través de la FEDI o de forma autógrafa.
IV. La responsable de la validación del documento de control de cambios será la OP. Los responsables de aprobar el control de cambios serán conjuntamente, la persona titular de la UA solicitante y la persona titular de la DGTIC. El documento podrá ser firmado a través de la FEDI o de forma autógrafa.
V. Una vez aprobado el control de cambios, la OP lo hará del conocimiento de las personas interesadas en el proyecto.
VI. Para proyectos contratados con proveedores o terceros, el control de cambios deberá llevarse a cabo conforme a las Normas en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Telecomunicaciones y sus Lineamientos.

Artículo 26. Matriz de riesgos. La persona Líder de Proyecto, será responsable de generar la matriz de riesgos iniciales del proyecto con la finalidad de tener identificados aquellos riesgos potenciales a convertirse en un problema, para ello, deberá realizar el registro de los mismos, identificar la probabilidad de impacto y ocurrencia, así como asignar la severidad y al responsable de su atención, quien deberá de elaborar el plan de mitigación.

La OP deberá monitorear y gestionar en conjunto con la persona Líder de Proyecto los riesgos asociados al proyecto, a efecto de mitigar el impacto de estos en caso de materializarse. De igual forma, deberá dar seguimiento a la implementación de acciones para su tratamiento.

Artículo 27. Cédulas de avance: Para mantener los registros del monitoreo y asegurar que éstos son comunicados a las personas interesadas en el proyecto, la persona Líder del Proyecto deberá generar informes programados o cédulas de avance, los cuales además deberá difundir y mantener disponibles para su consulta.

Para todos los proyectos, se deberán generar cédulas de avance de forma semanal con corte al viernes y deberán ser enviadas a la OP a más tardar el siguiente día hábil para su revisión, aprobación y envío. Una vez aprobadas, la OP será la encargada de enviar dichos documentos a las y los interesados.

Artículo 28. Acta de cierre de proyecto y encuesta de satisfacción. Durante el proceso de cierre, la persona Líder de Proyecto, en conjunto con la OP, deberá asegurar que todas las actividades del proyecto han sido concluidas, incluyendo liberación a producción y que se ha generado la solución tecnológica que dio origen al proyecto, bajo las condiciones y criterios de aceptación acordados.

Posteriormente, la OP podrá formalizar el cierre del proyecto, mediante el Acta de Cierre donde se hará constar la aceptación del proyecto por parte de la persona Líder de Negocio. Para el caso de proyectos contratados con proveedores o terceros, la documentación de cierre deberá apegarse a lo establecido en las POBAS.

Una vez concluidos la aprobación y firma de la documentación relacionada con el cierre, la OP enviará la encuesta de satisfacción, la cual permitirá generar una base de conocimiento para la mejora continua.

CAPITULO SEGUNDO
MODELADO DE NEGOCIO DE INICIATIVAS DE TIC DESARROLLADAS POR PROVEEDORES O TERCEROS

Artículo 29. El modelado de Negocio tiene como objetivo enriquecer las contrataciones que lleven a cabo las UA que incluyan en su alcance total o parcial el uso a aplicación de TIC, con la finalidad de:

I. Incrementar los beneficios al invertir en TIC como herramientas para hacer más eficiente las funciones de las UA;
II. Alinear las necesidades tecnológicas de las UA con los beneficios esperados a través de la solución tecnológica a adquirir o desarrollar;
III. Reutilizar servicios, sistemas y/o componentes de TIC existentes en el Instituto que se puedan aprovechar a fin de solventar de forma total o parcial las necesidades de las UA;
IV. Asegurar que, desde el dimensionamiento inicial, se consideren los procedimientos, estándares y políticas vigentes establecidos por la DGTIC;
V. Asegurar que, desde el planteamiento de las necesidades de la solución tecnológica se consideren los procedimientos, estándares y políticas vigentes establecidos por el Gobierno de Datos del Instituto, de modo que se asegure la gestión de los datos con base en los marcos de referencia de la materia;
VI. Prevenir y proyectar las necesidades de TIC del Instituto;
VII. Fortalecer técnicamente la documentación de la solución tecnológica requerida mediante el Anexo Técnico, y
VIII. Recomendar los estándares apropiados en materia de TIC aplicables a la solución tecnológica.

Para dar inicio al Modelado de Negocio para iniciativas de contratación de hardware, software o servicios con recursos presupuestales del PEF o del FIE, la UA deberá enviar al correo proyectos.tic@ift.org.mx, el Anexo Técnico y el oficio de solicitud de visto bueno dirigido a la persona titular de la DGTIC y firmado a través de la FEDI preferentemente o de forma autógrafa, donde se solicite formalmente a la DGTIC la revisión y Visto Bueno del cumplimento normativo de TIC, lo anterior con el fin de iniciar los ciclos de revisión que sean necesarios para brindar el apoyo y participación técnica por parte de la DGTIC conforme a lo establecido en las POBAS.

Al concluir la fase de modelado de negocio, la OP enviará el Anexo Técnico aprobado para la firma de la UA, lo cual podrá ser a través de la FEDI preferentemente o de forma autógrafa. Una vez que se cuente con el Anexo Técnico firmado, la DGTIC emitirá el Oficio de Visto Bueno de cumplimiento normativo de TIC con lo cual la UA podrá continuar, en cada caso, con el proceso de contratación.

Artículo 30.- Los proveedores que resulten adjudicados en el desarrollo de soluciones tecnológicas deberán apegarse a lo dispuesto en las "Normas Específicas para Soluciones Tecnológicas Desarrolladas por Terceros" (Anexo B).

CAPÍTULO TERCERO
MARCO DOCUMENTAL ASOCIADO A LAS SOLUCIONES TECNOLÓGICAS

Artículo 31.- Acorde al tipo de proyecto definido y a la selección del método de desarrollo de la solución tecnológica, se deberán desarrollar los documentos (técnicos y de gestión de proyecto) aplicables, conforme a lo establecido en la "Relación del marco documental aplicable por tipo de proyecto y su método de desarrollo" (Anexo C).

Artículo 32.- La DGTIC, proveerá las plantillas estándar que se deberán utilizar para dar cumplimiento al marco documental citado anteriormente.

Artículo 33.- Toda la documentación técnica de la solución tecnológica podrá ser revisada por la DGTIC, teniendo la facultad de solicitar los cambios y/o mejoras necesarias, las cuales, deberán ser atendidas por el proveedor hasta que la misma cumpla con los requisitos solicitados por la DGTIC.

TÍTULO CUARTO
DESARROLLO DE SOLUCIONES TECNOLÓGICAS
CAPÍTULO PRIMERO
CONSIDERACIONES PARA EL DISEÑO DE SOLUCIONES TECNOLÓGICAS

Artículo 34.- Las consideraciones para el diseño de soluciones tecnológicas son las siguientes:

I. Arquitectura de la Solución Tecnológica. Se deberá considerar como parte de la arquitectura de la Solución Tecnológica la conceptualización de al menos, una capa de presentación (servidores de presentación), una capa de negocio (servidor de aplicaciones web, servidores de contenido o servidor de reglas de negocio) y una capa de datos (almacenamiento en base de datos o de archivos electrónicos), tal y como se ilustra en el diagrama anexo.

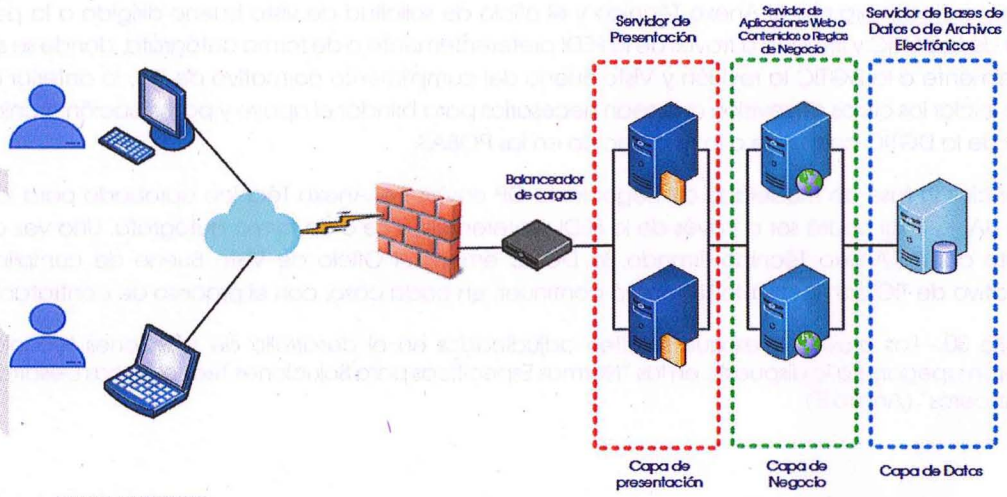


Ilustración 2 Arquitectura de la Solución Tecnológica

La distribución de los componentes a nivel red, así como el número de servidores que formarán parte de la arquitectura tecnológica deberá acordarse entre la persona Líder de Proyecto del proveedor y la DGTIC.

II. Comunicación con otras Soluciones Tecnológicas. Se deberá identificar la interoperabilidad de la Solución Tecnológica requerida con otras Soluciones Tecnológicas existentes en el Instituto o en otras organizaciones. Para ello, la persona Líder de Negocio será la responsable de identificar los puntos de comunicación de la Solución Tecnológica y comunicárselos a la persona Líder del Proyecto del proveedor, quien con apoyo de la DGTIC deberá describir todos los parámetros de configuración y conexión, e incluir un diagrama detallado de interoperabilidad, en donde se visualicen todos los componentes de TIC involucrados y su interrelación.

III. Interoperabilidad entre sistemas. Los protocolos de interoperabilidad se deberán validar con la DGTIC para cada uno de los sistemas con los que se pretenda comunicar la Solución Tecnológica, siendo los protocolos base SOAP o REST.

IV. Ambientes independientes: Desarrollo, pruebas y producción. Deberán existir ambientes independientes de producción, pruebas y desarrollo de Software, de tal forma que no compartan recursos tecnológicos entre sí. Las versiones de sistema operativo, base de datos y servidores de aplicación deberán ser idénticos en todos los ambientes que formen parte de la Solución Tecnológica.

Será responsabilidad del proveedor proporcionar todos los elementos correspondientes al ambiente de desarrollo, así como su instalación y configuración. Dicho ambiente podrá ubicarse en las instalaciones del proveedor o en cualquier otra ubicación, diferente a los Centros de Datos del IFT, que al mismo le convenga.

Los ambientes de pruebas y producción deberán ser instalados y configurados en los Centros de Datos del IFT, siendo la DGTIC la responsable de proveer los servidores y sistema operativo acordes a la arquitectura definida. La instalación y configuración de estos ambientes será responsabilidad conjunta entre el proveedor y la DGTIC. Para realizar los despliegues en los ambientes que se encuentren dentro de la Infraestructura del Instituto, se deberá estar a los dispuesto en el procedimiento de "Gestión de Versiones y Despliegue" y el "Procedimiento de Gestión de Cambios" cuando aplique.

Los servidores que por defecto proporciona la DGTIC cuentan con las siguientes características:

a) Servidores virtualizados.
b) Unidad de almacenamiento para el sistema operativo de 100 GB.
c) Memoria instalada 4GB en RAM.
d) Procesador de 2 Cores.

En caso de requerir características adicionales, la persona Líder de Negocio en conjunto con la persona Líder del Proyecto del proveedor deberá presentar la justificación técnica de la solicitud, la cual será revisada por la DGTIC, para verificar la disponibilidad de recursos existentes y la viabilidad técnica del requerimiento.

De acuerdo con la naturaleza y requerimientos de la Solución Tecnológica, en los casos justificados, revisados y aprobados por la DGTIC, se podrán tener los ambientes de desarrollo, pruebas y producción fuera de los centros de Datos del IFT.

V. Nombre de dominio del sistema (DNS). La estructura del nombre de dominio del sistema que deberá considerarse para los ambientes de desarrollo, calidad y productivo es la siguiente

Productivo:

Nombre del sistema. dominio institucional

Desarrollo:

Dev.nombre del sistema. dominio institucional

Calidad:

Qa.nombre del sistema. dominio institucional

El dominio institucional es estático, siendo: ift.org.mx

El dominio no podrá contener la nomenclatura de "www" derivado del certificado SSL, wildcard. De lo contrario cada dominio con www tendrá un costo asociado al mismo.

VI. Plataformas tecnológicas soportadas. Con la finalidad de estandarizar las plataformas tecnológicas utilizadas en el Instituto, la DGTIC ha aprobado el uso de lo siguiente:

Sistema Operativo:	RedHat Enterprise Linux 9.x o superior
Base de Datos:	MySQL 8.0
Servidor de Aplicaciones Web:	Apache Web Server en su versión más estable y sin vulnerabilidades
Servidor de Presentación:	NGINX 1.14 o superior.Apache o traefik.
Lenguaje de Programación:	• PHP 8 o superior • Yii • HTML 5 • CSS 3 • JQuery

	• JavaScript • Bootstrap • Angular
Sistema de Administración de Contenidos:	CMS Drupal

Tabla 3. Portales Web

	Microsoft	Open Source
Sistema Operativo:	Windows Server 2022 R2 o superior	RedHat Enterprise Linux 9.x o superior
Base de Datos:	SQL Server 2019	MySQL 8.0
Servidor de Aplicaciones:	Internet Information Services versión 10 o superior	Apache Web Server en su versión más estable y sin vulnerabilidades
Servidor de presentación	Internet Information Services versión 10 o superior	NGINX 1.14 o superior.Apache o traefik.
Lenguaje de Programación:	• HTML 5 • CSS 3 • JQuery • NET • .NET Framework 4.7 o superior	• PHP 8 o superior • HTML 5 • CSS 3 • JQuery • JavaScript • Bootstrap Angular
Sistema de Administración de Contenidos / Colaboración:	Microsoft SharePoint 2016 o superior	• CMS Drupal

Tabla 4. Aplicaciones Web internas

	Oracle	Microsoft
Sistema Operativo:	RedHat Enterprise Linux 9.x o superior	Windows Server 2022R2 o superior
Base de Datos:	Oracle 21c o superior	SQL Server 2019

Servidor de Aplicaciones:	Oracle WebLogic 14c o superior Apache Tomcat 10.1 o superior	Internet Information Services (IIS 10)
Servidor de presentación	NGINX 1.14 o superior y Apache	NGINX 1.14 o superior y Apache
Lenguaje de Programación:	• Vista • HTML 5 • CSS 3 • JQuery • JavaScript • Bootstrap • JSF 2.0 • Prime Faces • Controlador Java • EJB 3 o superior • Spring MVC • Modelo • Hibernate • MyBatis • Spring JDBC	• C# última versión • VB.NET última versión estable • Web Forms • ADO • Entity Framework • JDK 17 o superior • Python

Tabla 5. Sistemas Transaccionales

Las herramientas y plataformas sobre las que se desarrolle y ponga en operación la Solución Tecnológica deberán ser las versiones más actuales y estables de acuerdo a los criterios establecidos por la DGTIC[1]. Dichas versiones deberán ser establecidas en conjunto con la persona Analista de Negocio, la DIT y el Líder de Negocio (en caso de aplicar) en la etapa de planeación y deberán corresponder con la plataforma tecnológica aceptada en el Instituto.

VII. Cifrado y comunicación segura. El intercambio de información sensitiva (cuentas de personas usuarias, contraseñas, datos personales, información confidencial, información reservada, etc.) entre la Solución Tecnológica y las personas usuarias, deberá realizarse a través de medios seguros utilizando mecanismos de cifrado basados en los protocolos SSL/TLS de al menos 128 bits, con algoritmo de firma

[1] *El licenciamiento con el que cuente el Instituto o la versión libre utilizada.
*Que las plataformas o herramientas se encuentren instalada en la infraestructura del IFT (únicamente en Sistemas Operativos).

SHA-256 y longitud de llaves de 2048 bits. Los certificados deberán ser expedidos por una autoridad certificadora de confianza y tener una vigencia máxima de 397 días naturales.

El Instituto se reserva el derecho de solicitar al proveedor el apoyo necesario para la adquisición e implementación de los certificados digitales SSL/TLS necesarios para el funcionamiento del sistema.

VIII. Interfaz Gráfica. Como parte de los requerimientos no funcionales de la Solución Tecnológica, deberá especificarse la aplicabilidad de los requerimientos gráficos, los cuales pueden ser:

a) Alineación a la norma de accesibilidad emitida por la W3C[2].

b) Alineación al Manual de Identidad vigente en el Instituto.[3]

c) Los diferentes navegadores web en los que se deberá visualizar deberán ser al menos Microsoft EDGE, Google Chrome y Safari en sus versiones más recientes.

d) Compatibilidad con dispositivos móviles (sistemas responsivos).

IX. Modelo entidad – relación (Modelo Físico). El diseño de todas las bases de datos de los sistemas desarrollados para el Instituto debe considerar el tipo de información que se requiere almacenar, asegurando la consistencia e integridad de las tablas y los registros.

El modelo entidad- relación debe explicar gráficamente por lo menos la interacción existente entre los objetos de la base de datos como; entidad, atributo, relación, conjunto de relaciones, restricciones y llaves. Se deberá incluir un diagrama de tablas, con el detalle de todos sus elementos. Este modelo se deberá considerar como parte de los entregables y es responsabilidad del proveedor su elaboración y de la persona Líder de Negocio asegurar la entrega del mismo a la DGTIC.

Para definir un modelo de datos deberá solicitar a la DGTIC el documento anexo "Estándares de Bases de Datos". (Anexo D)

X. Diccionario de Datos. El diccionario de datos incluye las reglas para la estandarización de nomenclaturas, tipo y longitud de los campos, facilitando la identificación y administración de los componentes.

a) Descripción de la nomenclatura utilizada.

b) Detalles de los datos.

c) Nombre.

d) Descripción.

e) Tipo de dato.

f) Longitud.

g) Valor por defecto.

h) Estructura.

[2] https://www.w3.org/WAI/standards-guidelines

[3] http://www.conexion.ift.org.mx/intranet/index.php/component/k2/itemlist/search?searchword=manual+de+identidad&categories=

i) Restricciones.

El Diccionario de Datos debe coincidir con lo establecido en el Modelo entidad-relación y ser lo más descriptivo posible. Se deberá considerar como parte de los entregables y será responsabilidad del proveedor su elaboración y de la persona Líder de Negocio asegurar la entrega del mismo a la DGTIC.

Para definir un modelo de datos deberá solicitar a la DGTIC el documento "Estándares de Bases de Datos"(Anexo D)

Artículo 35.- Las consideraciones para la funcionalidad estándar de las soluciones tecnológicas son las siguientes:

I. Administración de usuarios. Cuando la Solución Tecnológica requiera la Gestión de personas Usuarias, deberá darse prioridad a la integración con el Directorio Activo Institucional del IFT. En caso contrario, la Solución Tecnológica deberá contener un módulo de administración de personas usuarias (alta, baja, cambios) que permita validar la identidad de las personas usuarias a través de un mecanismo de autenticación basado en contraseñas y niveles de permisos (Roles).

El acceso a dicho módulo deberá estar limitado a la red de datos interna del Instituto, de tal forma que ninguna persona usuaria pueda acceder al módulo de administración desde Internet a menos que utilice una VPN configurada por el área responsable en el Instituto.

El módulo de administración de personas usuarias deberá configurarse de manera que permita cumplir con los siguientes requisitos para la administración de contraseñas:

a) Reglas configurables para asignar la complejidad de las contraseñas (longitud mínima de caracteres, uso de mayúsculas, minúsculas, números y símbolos).
b) Cambio periódico de contraseñas.
c) Bloqueo automático del acceso a la cuenta de la persona usuaria después de un número determinado de intentos fallidos.
d) Reinicio de contraseñas por parte de la persona administradora del sistema a solicitud de una persona usuaria.
e) Almacenamiento seguro de contraseñas a través de los algoritmos de cifrado SHA2 o AES 128 o 256 bits.

II. Autenticación de personas usuarias. Para aplicaciones que requieran autenticar personas usuarias internas del Instituto, se deberá utilizar el Directorio Activo Institucional, como medio de autenticación a las mismas. En caso contrario, la solución deberá contar con un mecanismo de seguridad para la autenticación de los mismos.

Para el caso de aplicaciones que se encuentren publicadas en Internet, se deberán utilizar mecanismos de autenticación basados en persona usuaria y contraseña, considerando lo establecido en los requisitos para la administración de contraseñas citadas del numeral anterior.

Adicionalmente, con la finalidad de proteger de abusos a las aplicaciones (particularmente las que se encuentren públicas en Internet), en las etapas de diseño y construcción, se deberán implementar mecanismos tipo CAPTCHA de nueva generación que minimicen los riesgos de ataque de diccionario por sistemas automatizados o robots.

III. Matriz de roles y privilegios. El módulo de administración de personas usuarias de la Solución Tecnológica deberá contar con un mecanismo de autorización basado en roles o perfiles, que permita al sistema verificar qué roles tienen permisos sobre qué recursos; qué opciones de menú configurar; o qué información mostrar en tiempo de ejecución.

Se debe considerar como un entregable una matriz con los roles que pueden acceder a los distintos recursos que provee el sistema y con qué privilegios pueden hacerlo, y es responsabilidad de la persona Líder de Negocio asegurar la entrega de la misma por parte del proveedor.

La matriz deberá presentar de forma clara los perfiles creados para las personas usuarias, los módulos a los que tienen acceso y los permisos sobre cada objeto del sistema, así como una breve descripción de cada uno de estos elementos.

La Solución Tecnológica deberá asegurar que los recursos puedan ser accedidos conforme a los roles y privilegios establecidos y por las personas usuarias autorizadas.

Una copia del entregable de la matriz de roles y privilegios deberá ser entregado a la DGTIC por parte de la persona Líder de Negocio.

IV. Se recomienda almacenar la información sensitiva (como contraseñas) en lugares a los que sólo el aplicativo pueda acceder y cifrar dicha información. Los algoritmos para el cifrado de la información deberán ser acordados entre la Dirección de Seguridad de la Información (DSI) y el proveedor de tal forma que no impacte el rendimiento de la plataforma del sistema.

V. El proveedor de la Solución Tecnológica deberá asegurar que el uso de cookies para identificar a una persona usuaria no permita la lectura de cookies desde el lado de la persona usuaria, sólo desde el servidor y preferentemente utilizando un identificador único temporal asociado con la persona usuaria.

En caso de que la Solución Tecnológica utilice cookies para recabar información concerniente a las personas usuarias, se deberá notificar por medio de un aviso en la interfaz gráfica o mediante una ventana emergente.

VI. Manejo de sesiones. La Solución Tecnológica deberá ser capaz de limitar a una, el número de sesiones concurrentes de una misma persona usuaria.

La Solución Tecnológica deberá contar con un mecanismo que permita identificar y notificar a la persona usuaria con respecto de otra sesión abierta con sus datos de acceso en otro dispositivo y solicitarle su cierre.

VII. Validación de datos de entrada. La validación de los datos de entrada deberá realizarse y parametrizarse en los diferentes módulos que conformen la Solución Tecnológica, de tal forma que se mitiguen ataques tales como: inyección de código (SQL, LDAP o XPath), así como ataques de sitios cruzados (XSS).

a. SQL Injection. Se recomienda validar todos los campos por medio de listas blancas. De esta forma, sólo se aceptarán caracteres no peligrosos. Es importante normalizar la entrada para evitar las evasiones por medio de codificaciones en los parámetros. De ser posible, se recomienda el uso de "prepared statements" con algún framework de

desarrollo para construir sentencias SQL con parámetros externos. En caso de una propuesta diferente, se deberá hacer una evaluación con la DSI.

b. Cross Site Scripting. Como regla general, no se debe confiar en información recibida por la persona usuaria. Resulta peligroso utilizar, en la generación de páginas de respuesta, datos recibidos directamente de la persona usuaria sin realizar la codificación adecuada según el caso. Se recomienda el uso de algún antivirus y tener actualizado el navegador web.

c. Buffer Overflow. Por norma general, cualquier operación que conlleve copia de datos sobre un área de memoria, debe de ser realizada con especial cuidado, a fin de garantizar que el área de memoria destino reservada será suficiente para albergar los datos que se quieren copiar.

d. Path Manipulation. Se recomienda no utilizar datos provenientes de la persona usuaria para construir el nombre de los ficheros. En caso de ser necesario, se recomienda aplicar filtrado sobre los datos recibidos, preferentemente con base en el uso de listas blancas.

VIII. Validación de datos de salida. La Solución Tecnológica deberá asegurar que los mensajes de salida devueltos a las personas usuarias al momento de la autenticación o interacción con la Solución Tecnológica no especifiquen mayor información sobre la existencia de personas usuarias o valores válidos, por ejemplo: "Error de ingreso: La combinación de persona usuaria y clave proporcionados no es válida".

Asimismo, el proveedor deberá asegurarse de enmascarar el direccionamiento IP de los servidores de aplicación Web para evitar su publicación.

IX. Bitácoras de eventos. La Solución Tecnológica, dentro de su operación, deberá generar bitácoras de eventos. Las bitácoras deberán contener al menos la siguiente información: ¿Quién lo hizo? ¿Qué hizo? ¿Cuándo lo hizo? ¿Dónde lo hizo? y una breve descripción del evento. La Solución Tecnológica deberá resguardar las bitácoras preferentemente en una instancia independiente a la base de datos del sistema.

Los criterios para determinar el grado de detalle y las transacciones a las que se aplicará dicha funcionalidad se definirán de común acuerdo entre la persona usuaria, la DSI y el equipo desarrollador del proveedor durante la etapa de análisis y diseño y dependiendo la sensibilidad de los datos que maneje la Solución Tecnológica.

X. El borrado de los registros deberá realizarse a nivel lógico, se recomienda contemplar un campo "estatus" en el cual se determine el estado como cancelado cuando se haya eliminado un registro. Se deberá justificar ante la DGTIC cualquier borrado físico de los registros.

En caso de que la plataforma tecnológica no permita resguardar las bitácoras en una instancia independiente a la Base de Datos, podrá optarse por resguardar las bitácoras en formato de texto plano. Será responsabilidad del proveedor proponer las medidas para mantener su integridad y confidencialidad, mismas que serán validadas por la DSI.

La Solución Tecnológica deberá proveer los mecanismos necesarios para garantizar que el contenido de las bitácoras no ha sido alterado a nivel de registro. Esto es, deberá garantizar que estén registrados todos los eventos y que estos eventos no hayan sido alterados, incluso por la persona administradora del Sistema. Lo anterior, será aplicable, dependiendo de la

sensibilidad de los datos que maneje la aplicación y de común acuerdo entre la persona Líder de Negocio, la DSI y el equipo de desarrollo del proveedor en la etapa de análisis y diseño.

La Solución Tecnológica deberá mantener las bitácoras disponibles y deberá mantener separadas las bitácoras de eventos de acuerdo a los componentes que lo integran (al menos: sistema operativo, base de datos y aplicativo).

El periodo que deberán mantenerse disponibles las bitácoras será establecido entre la persona Líder del Proyecto del proveedor, la DSI y la persona Líder de Negocio, tomando como base la criticidad de la información contenida en el sistema y la normatividad aplicable.

Las bitácoras deberán estar consideradas como parte de la información que deberá respaldarse.

XI. Manejo de errores. Las respuestas ante un error en la Solución Tecnológica no deberán entregar información que pudiera revelar detalles acerca de cómo está hecha o funcionan los procedimientos de ésta, por lo que se deberán utilizar siempre que sea posible controles de error (try – catch) para el manejo de excepciones o errores inesperados.

Será responsabilidad del proveedor la creación de una página personalizada que se despliegue cada vez que el sistema genere un error, por ejemplo, los errores 4xx y 5xx, y que elimine la divulgación de información relativa a la arquitectura del sistema.

Los mensajes de error deberán almacenarse en las bitácoras del sistema, de tal forma que se puedan utilizar para el análisis y resolución de problemas.

XII. Sincronización de tiempo del sistema. La Solución Tecnológica deberá de contar con un mecanismo configurable que permita la sincronización del sistema con un servicio de Network Time Protocol "NTP" definido por el IFT.

Dicho servicio de reloj deberá utilizarse como insumo de las bitácoras de eventos, inactividad de sesión y limitación del tiempo de conexión al sistema.

XIII. Finalizar sesión por inactividad. La Solución Tecnológica deberá contar con un mecanismo configurable que permita la terminación de la sesión de una persona usuaria después de un determinado tiempo de inactividad.

Una vez cerrada la sesión, se deberá notificar a la persona usuaria que su sesión ha expirado por inactividad.

XIV. Limitación del tiempo de conexión al sistema. Previo a la validación del requerimiento, la Solución Tecnológica deberá ser capaz de limitar el acceso a las personas usuarias en horarios específicos definidos por el Líder de Negocio en conjunto con la DGTIC.

La Solución Tecnológica deberá de contar con un mecanismo configurable que permita al Instituto limitar el horario de conexión al sistema de acuerdo a una fecha en específico o a un rango de tiempo definido por el Instituto.

XV. Implementar buenas prácticas de programación. El proveedor de la Solución Tecnológica debe cumplir cuando menos con lo siguiente:

a) Desarrollar Soluciones Tecnológicas aplicando mejores prácticas de programación definidas y provistas por la DDS.

b) Utilizar siempre un repositorio para el control de versiones.

La DGTIC se reserva el derecho de realizar las comprobaciones necesarias para el cumplimiento de buenas prácticas y estándares solicitados.

CAPÍTULO SEGUNDO
MODELOS DE DESARROLLO

Artículo 36.- La DGTIC realizará la gestión de Soluciones Tecnológicas de TIC basado en los siguientes tres modelos de gestión de proyectos:

I. Para proyectos en modelo de desarrollo en Cascada:

Ilustración 3. Modelo de desarrollo en cascada

II. Para proyectos en modelo de desarrollo Iterativo:

Ilustración 4. Modelo de desarrollo iterativos

III. Para proyectos en modelo de desarrollo en Ágil:

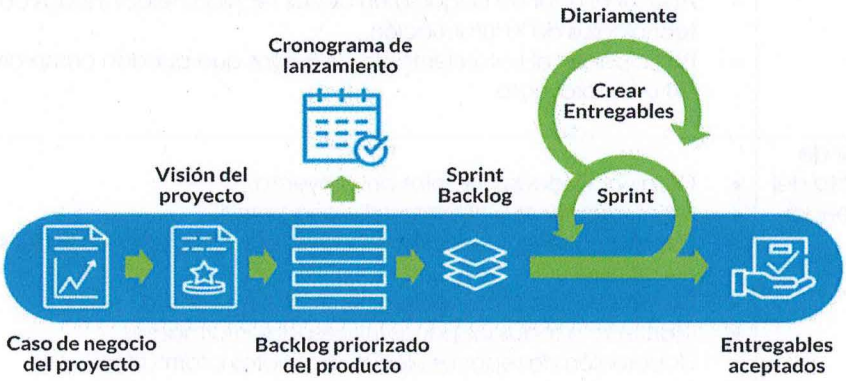


Ilustración 5. Modelo de desarrollo ágil

Articulo 37.- Para las Soluciones Tecnológicas desarrollados por la Fábrica de Software, las UA deberán apegarse a lo dispuesto en el documento de "Modelos de Desarrollo de Soluciones Tecnológicas" (Anexo E)

CAPÍTULO TERCERO

ROLES PARA EL DESARROLLO DE SOLUCIONES TECNOLÓGICAS

Artículo 38.- Para el desarrollo de soluciones tecnológicas se consideran diferentes roles de acuerdo a la fuente de financiamiento del proyecto, los cuales se describen a continuación, de forma enunciativa mas no limitativa:

- Para iniciativas de contratación de servicios que cuenten con financiamiento PEF o FIE aprobado:

Servicios con financiamiento PEF o FIE	
Administrador del Contrato	• Validar el cumplimiento de los objetivos del proyecto. • Identificar y aplicar las posibles deductivas (en caso de que apliquen).
Líder de Negocio	• Emitir su retroalimentación y/o visto bueno al proveedor con respecto a la documentación relacionada a la administración del proyecto. • Definir los criterios de aceptación que serán utilizados para validar el cumplimiento de los requisitos. • Identificar, comunicar y, en su caso, participar en el tratamiento de los riesgos que puedan comprometer el éxito del proyecto. • Ejecutar las pruebas de usuario. • Validar los despliegues para liberaciones. • Evaluar y aprobar la propuesta del control de cambio en el proyecto (en su caso). • Gestionar el cierre administrativo del proyecto.
Líder técnico	

Servicios con financiamiento PEF o FIE	
	• Apoyar al Líder de Negocio en dudas técnicas relacionadas con tecnologías de la información. • Participar en el tratamiento de los riesgos que puedan comprometer el éxito del proyecto.
Líder de Proyecto del proveedor	• Definir actividades iniciales del proyecto. • Crear, mantener y priorizar del cronograma. • Llevar a cabo la alineación con los interesados para entender sus necesidades • Garantizar que el producto se entregue en tiempo. • Mantener a todas las partes interesadas informadas. • Elaboración de reportes ejecutivos y notas informativas.
Oficina de Proyectos	• Validar y dar seguimiento al cronograma. • Monitorear y controlar el ciclo de vida del proyecto. • Dar seguimiento al cumplimiento de los acuerdos. • Gestionar las encuestas de satisfacción. • Asegurar que los interesados sigan los principios y buenas prácticas implementadas por las DGTIC.

Tabla 6 Roles para Servicios con financiamiento PEF o FIE

Para iniciativas proyectos a desarrollar con recursos a cargo de la DGTIC:

Modelo de desarrollo en cascada e iterativo	
Líder de Negocio / Responsable de la UA	• Asegurar que el Analista de Negocio tenga el entendimiento de los requerimientos solicitados. • Emitir su retroalimentación y/o visto bueno con respecto a la documentación relacionada a la administración del proyecto. • Participar en las reuniones a las que sea convocado para el seguimiento del proyecto. • Definir los criterios de aceptación que serán utilizados para validar el cumplimiento de los requisitos. • Identificar, comunicar y, en su caso, participar en el tratamiento de los riesgos que puedan comprometer el éxito del proyecto. • Ejecutar las pruebas de usuario. • Validar los despliegues para liberaciones. • Evaluar y aprobar la propuesta del control de cambio en el proyecto. • Tomar decisiones a nivel estratégico del proyecto.
Analista de Negocio (AN) / Product Owner (OP)	• Eliminar impedimentos. • Fomentar la colaboración y la mejora continua en el equipo de desarrollo. • Dirigir reuniones periódicas de seguimiento técnico y de negocio. • Asegurar que el producto tenga la calidad adecuada. • Asignar tareas y recursos. • Motivar y guiar al equipo de trabajo, fomentando la colaboración y comunicación efectiva.
Líder de Proyecto	• Identificar y documentar los requerimientos.

Modelo de desarrollo en cascada e iterativo	
(LP) / Scrum Master (SM)	• Determinar las necesidades generales del proyecto. • Definir actividades iniciales del proyecto. • Crear, mantener y priorizar del cronograma. • Llevar a cabo la alineación con los interesados para entender sus necesidades. • Validar los requisitos mediante los casos de uso, reglas de negocio y criterios de aceptación. • Garantizar que el producto se entregue en tiempo. • Apoyar al equipo de desarrollo en la definición y dudas sobre los requerimientos.
Project Manager (PM)	• Definir los objetivos, alcance y requerimientos iniciales del proyecto. • Validar y dar seguimiento al cronograma. • Monitorear y controlar el ciclo de vida del proyecto. • Mantener a todas las partes interesadas informadas. • Identificar los riesgos y problemas para apoyar en la implementación de los planes de mitigación. • Dar seguimiento al cumplimiento de los acuerdos. • Evaluar el cumplimiento de los objetivos de los proyectos. • Llevar a cabo la resolución de conflictos. • Llevar a cabo juntas para gestionar las lecciones aprendidas. • Elaboración de reportes ejecutivos y notas informativas. • Gestionar el cierre administrativo del proyecto y las encuestas de satisfacción. • Evaluar la calidad y satisfacción de los entregables. • Asegurar que los interesados sigan los principios y buenas prácticas implementadas por las DGTIC.

Tabla 7 Roles para iniciativas proyectos a desarrollar con recursos a cargo de la DGTIC (Modelo de desarrollo Cascada e Iterativo)

Modelo de desarrollo en ágil	
Líder de Negocio / Responsable de la UA	• Definir los requerimientos del proyecto. • Solicitar algún cambio en el proyecto. • Definir el alcance para que cada liberación coincida con los objetivos de la UA. • Definir los criterios de aceptación que deberán cumplir el o los objetivos del proyecto. • Identificar, comunicar y, en su caso, participar en el tratamiento de los riesgos que puedan comprometer el éxito del proyecto. • Atender las reuniones y eventos a los que sean convocados. • Asistir a las reuniones diarias definidas para el proyecto por medio del kickoff. • Validar los despliegues para liberaciones. • Validar y ejecutar los casos de prueba. • Tomar decisiones a nivel estratégico del proyecto. • Evaluar y aprobar la propuesta del control de cambio en el proyecto. • Asegurar que el Product Owner tenga el entendimiento de los requerimientos solicitados.

Modelo de desarrollo en ágil	
Analista de Negocio (AN) / Product Owner (OP)	• Colaborar activamente en la preparación del arranque del servicio. • Asegurar y colaboras con el interesado Líder de Negocio para definir aspectos del dominio de negocio. • Participar activamente e involucrar al Líder de negocio en las actividades de planeación de las liberaciones: Colaborar para determinar el alcance y número de iteraciones por cada liberación, establecer los tipos de pruebas para cada liberación, generar el cronograma de liberaciones (priorización del backlog). • Asegurar que el Líder de Negocio defina la meta de la iteración por inicio (Sprint Backlog). • Participar activamente durante la Planeación de la Iteración y asegurar la participación de los interesados (sesión Sprint Planning). • Colaborar con el equipo en la ejecución de la iteración resolviendo dudas • Participar en las acciones para mitigar riesgos y problemas de acuerdo a su competencia. • Apoyar al Líder de Negocio para refinar Historias de Usuario suficientes para la siguiente iteración. • Apoyar al Líder de Negocio para refinar/ajustar/complementar los criterios de aceptación de cada Historia de Usuario, así como la Definición de Hecho (Definition of Done (DoD, por sus siglas en inglés) en caso de ser necesario. • Contribuir de manera comprometida durante la ceremonia de Revisión de la Iteración mediante la verificación del cumplimiento de los criterios de aceptación de las Historias de Usuario implementadas proporcionando la aprobación de las mismas. • Asegurar el compromiso del Líder de Negocio para validar y otorgar su aprobación de las historias de usuario entregadas en la sesión de la ceremonia de Revisión del sprint • Participar en la actualización del Backlog del Producto de acuerdo con la retroalimentación del Líder de Negocio • Facilitar el visto bueno. de la liberación involucrando al Líder de Negocio solicitante para su revisión y aprobación conforme a los criterios de aceptación definidos. • Participar en las reuniones o eventos que sea convocado y propiciar la inclusión del Líder de Negocio en estas reuniones.
Líder de Proyecto (LP) / Scrum Master (SM)	• Determinar las necesidades generales del proyecto. • Definir actividades iniciales del proyecto. • Crear, mantener y priorizar el backlog del producto. • Validar los requisitos mediante las historias de usuario, reglas de negocio y criterios de aceptación. • Definir los criterios de aceptación que deberán cumplir el o los objetivos de las Historias de Usuario. • Tomar decisiones informadas sobre el desarrollo y el lanzamiento del producto. • Definir la meta de la Iteración e identificar las Historias de Usuario a comprometer (Sprint Backlog). • Garantizar que el producto se entregue en tiempo. • Apoyar al equipo de desarrollo scrum en la definición y dudas sobre los requerimientos.

Modelo de desarrollo en ágil	
Project Manager (PM)	• Definir los objetivos, alcance y requerimientos iniciales del proyecto. • Validar y dar seguimiento al cronograma. • Monitorear y controlar el ciclo de vida del proyecto. • Mantener a todas las partes interesadas informadas. • Identificar los riesgos y problemas para apoyar en la implementación de los planes de mitigación. • Dar seguimiento al cumplimiento de los acuerdos. • Evaluar el cumplimiento de los objetivos de los proyectos. • Llevar a cabo la resolución de conflictos. • Llevar a cabo juntas para gestionar las lecciones aprendidas. • Elaboración de reportes ejecutivos y notas informativas. • Gestionar el cierre administrativo del proyecto y las encuestas de satisfacción • Evaluar la calidad y satisfacción de los entregables. • Asegurar que los interesados sigan los principios y buenas prácticas implementadas por las DGTIC.

Tabla 8 Roles para iniciativas proyectos a desarrollar con recursos a cargo de la DGTIC (Modelo de desarrollo Ágil)

CAPÍTULO CUARTO

PRUEBAS A SOLUCIONES TECNOLÓGICAS

Artículo 39.- Para el caso de proyectos desarrollados por un proveedor o terceros, el proveedor deberá considerar la creación de una Matriz de Pruebas, a través de ésta se deberán definir y documentar las variables o condiciones, así como reglas de negocio y/o criterios de aceptación que serán revisados por el equipo de Calidad para determinar que el requerimiento ha sido cubierto de forma satisfactoria y cumpla los criterios establecidos.

Para desarrollos realizados a través de recursos humanos asignados con cargo a la DGTIC, es responsabilidad del equipo de calidad generar la matriz de prueba, independientemente de la metodología a utilizarse en el desarrollo de la Solución Tecnológica, para ello, es indispensable que las personas Líderes de Proyecto proporcionen la documentación generada debidamente versionada y en su versión final (Historias de Usuario, Casos de Uso, Interfaz de Usuario y Criterios de Aceptación) la cual fungirá como base de prueba en la elaboración de los casos de prueba, conforme a lo señalado en el apartado Documentar y validar Matriz de Pruebas.

Resultados de la ejecución de la matriz de pruebas. La totalidad de los Casos de Pruebas deben de cumplir con los criterios de aceptación definidos por la persona Líder de Negocio y la DGTIC respectivamente, por lo tanto, es necesario que todos los hallazgos detectados durante la ejecución de pruebas de calidad, funcionales de seguridad y de aceptación del usuario (UAT), sean registrados conforme se ejecuta cada iteración de prueba, con el fin de asegurar su comunicación y seguimiento, en el formato "Reporte de Hallazgos" o en la herramienta de seguimiento de errores utilizada en el Instituto, la cual, de manera enunciativa mas no limitativa, incluirá lo siguiente:

I. Nombre de la Solución Tecnológica o proyecto.
II. Versión de la Solución Tecnológica sobre la que se realiza la prueba.
III. Identificador (ID) del hallazgo.

IV. Tipo de hallazgo: Defecto / Mejora.
V. Severidad: Crítico / Alto / Medio / Bajo.
VI. Descripción.
VII. Pasos para reproducir (secuencia de acciones que lleva a su generación).
VIII. Estado: Abierto / Cerrado / No Corregido.
IX. Ruta de trazabilidad donde se ejecutó la prueba.
X. Resolución (forma en que fue atendido).
XI. Evidencia.

Artículo 40.- La DGTIC solicitará previo a la realización de pruebas de calidad las pruebas descritas a continuación:

Pruebas unitarias. Para este tipo de pruebas el líder de proyecto será responsable de entregar pruebas unitarias (en el ambiente de desarrollo) a los módulos desarrollados que conforman la Solución Tecnológica, generando las evidencias necesarias para verificar su correcta realización.

Pruebas de Integración. El líder de proyecto será responsable de entregar las pruebas de integración de aquellas soluciones tecnológicas en las que se haya solicitado el consumo de servicios de otros sistemas, generando las evidencias correspondientes.

Artículo 41.- Para comenzar con las pruebas de calidad, es indispensable que la base documental (Casos de Usos, Interfaz de Usuario, Historias de Usuario o Criterios de Aceptación) que se proporcione al equipo de calidad, presente a detalle y de forma clara los flujos, mensajes, validaciones, reglas de negocio y/o criterios de aceptación a ser validados. Para iniciar con la ejecución de las pruebas de calidad es obligatorio contar con lo siguiente:

I. Matriz de Trazabilidad de Requerimientos o Lista priorizada.
II. Matriz de pruebas finalizada o aprobada según corresponda.
III. Evidencia de ejecución de pruebas unitarias.
IV. Evidencia de ejecución de pruebas de integración (cuando aplique)
V. Información del ambiente de pruebas (Ligas de acceso y roles y credenciales de acceso a la solución tecnológica).
VI. Ambiente de pruebas con el total de las funcionalidades a probar.

Artículo 42.- Pruebas funcionales de seguridad. La DSI será la responsable de realizar pruebas funcionales de seguridad sobre la Solución Tecnológica desarrollada, con la finalidad de verificar la correcta implementación de las recomendaciones de seguridad establecidas. Será responsabilidad de la DSI reportar los hallazgos encontrados, anexando la evidencia del incumplimiento detectado. Para la liberación de la Solución Tecnológica en un ambiente productivo, será responsabilidad del Líder de proyecto asegurar que sean atendidos los defectos del sistema que hayan sido encontrados por la DSI.

Artículo 43.- Pruebas de Usuario (UAT). La persona es responsable de la ejecución de pruebas de usuario (UAT) en el momento en que se libere funcionalidad de acuerdo con el método de desarrollo de la solución y del cronograma del proyecto. Los datos de prueba utilizados para las pruebas UAT serán responsabilidad del líder de negocio en acuerdo con el líder de proyecto, y debe evitar utilizar datos clasificados o susceptibles de ser clasificados como confidenciales o reservados, bajo responsabilidad de la UA, el líder de negocio deberá dar el Visto Bueno a las pruebas de aceptación validando el total de la funcionalidad de la solución tecnológica y enviando las evidencias de ejecución de la DGTIC.

Artículo 44.- La DGTIC realizará los análisis de vulnerabilidades a todas las soluciones tecnológicas que se implementen en el Instituto, siempre que sea viable. El objetivo de estos análisis es evitar que se liberen soluciones tecnológicas con vulnerabilidades que comprometan la Seguridad de la Información del

Instituto. El líder del proyecto o el proveedor, según sea el caso, será el responsable de que se atiendan las vulnerabilidades identificadas.

De acuerdo a los niveles de disponibilidad de un sistema, la volumetría de usuarios (concurrentes) y a su promedio esperado de transacciones por usuario, la DGTIC determinará la necesidad de ejecutar pruebas de estrés a una Solución Tecnológica, previo a su puesta en producción. En el caso de un desarrollo con proveedor o tercero, dichas pruebas deberán ser solicitadas a través del líder de negocio al proveedor las cuales no deberán tener costo para el Instituto.

Artículo 45.- Durante la ejecución de las pruebas de calidad y UAT, se podrán identificar diferentes tipos de hallazgos, los cuales se describen a continuación:

I. Defectos. Se trata de una imperfección en un componente o solución que puede causar fallas al desempeñar las funciones requeridas, por ejemplo, una sentencia o una definición de datos incorrectas.
II. Mejoras. Recomendación detectada para un mejor desempeño de las funciones requeridas.
III. Nuevos requerimientos. Se refiere a una nueva funcionalidad para la Solución Tecnológica detectada por la persona líder técnico solicitante durante la ejecución de sus pruebas de aceptación. Para la posible inclusión de esta nueva funcionalidad, se deberá analizar el impacto de la misma considerando a las restricciones del proyecto y acordar entre los involucrados la aceptación o no de la misma.

A su vez, los defectos identificados se clasificarán de acuerdo con los siguientes niveles de severidad y criterio.

I. Severidad Crítica:
    a. Cuando el defecto provoca que la (s) función (es) principal (es) sea (n) inutilizable (s) o que la solución tecnológica se bloqueé o no responda con frecuencia. (Impedimento de uso)
    b. Cuando el defecto afecta la interoperabilidad en tres sistemas.
    c. Cuando el defecto causa la pérdida de datos importantes y no recuperables. (Pérdida de datos)
    d. Cuando la solución tecnológica expone vulnerabilidades de seguridad que podrían ser explotadas, como direcciones IP, puertos, nombres de base de datos, líneas de código. (Riesgo de seguridad)
II. Severidad Alta:
    a. No cumple en su totalidad con la funcionalidad esperada o regla (s) de negocio establecida (s).
    b. Cuando el defecto se presenta en 2 o más módulos o secciones de la solución tecnológica.
    c. Cuando el defecto no cumple totalmente con requisitos no funcionales establecidos, como rendimiento, usabilidad o accesibilidad.
    d. Cuando el defecto provoca la pérdida parcial de datos.
III. Severidad Media:
    a. Cuando la solución tecnológica presenta inconsistencias visuales o de texto.
    b. Cuando el defecto afecta funcionalidades secundarias o menos utilizadas de la solución tecnológica.
    c. Cuando el defecto no está relacionado con la actualización de información o se presentan funcionalidades no documentadas.
IV. Severidad Baja:

a. Cuando la solución tecnológica no corresponde con el diseño autorizado por la persona líder de Negocio o los criterios que, en su caso, establezca la DGTIC.
b. Cuando el contenido, datos o información presentan faltas de ortografía.

Artículo 46.- Todos los hallazgos identificados deberán registrarse en la herramienta institucional asignada para el seguimiento por parte de la DSI, la Subdirección de Supervisión de la Calidad de Soluciones Tecnológicas (SSCST) y los Usuarios. Para el acceso a la herramienta la DDS deberá solicitar los accesos necesarios mediante correo electrónico a la SSCST, lo anterior para su seguimiento y atención.

Artículo 47.- Ambiente de Pruebas. El líder de proyecto, con apoyo de la Subdirección de Soporte a Sistemas y Continuidad Operativa (SSSCO), deberá realizar y verificar que la implementación de la Solución Tecnológica y funcionalidades en el ambiente de calidad opere correctamente previo al inicio de las pruebas funcionales que realizará el equipo de calidad, siendo este el ambiente en el que se deberán ejecutar todas las pruebas de la UA solicitante, el área de calidad y aquellas de seguridad necesarias acorde a la naturaleza de la Solución Tecnológica.

Respecto a los despliegues de nuevas funcionalidades o correcciones al ambiente de pruebas, se podrán realizar cuando el equipo de calidad haya notificado la finalización de la iteración de pruebas, lo anterior, para evitar la inyección de defectos o falsos-positios o, en su caso, no esté siendo utilizado. Para ello el líder de proyecto, con apoyo de la SSSCO realizarán dichos despliegues al ambiente de pruebas bajo el escenario señalado anteriormente.

Artículo 48.- Para el caso de proyectos desarrollados por un proveedor o terceros, el líder de proyecto del proveedor debe de entregar la matriz de prueba al líder de negocio para su aprobación, esta matriz debe contemplar todas las reglas de negocio, criterios de aceptación y requerimientos solicitados por la UA. Una vez que se tenga la matriz aprobada, el proveedor deberá ejecutar el 100% de los casos de pruebas que la integran y deberán integrar las evidencias al documento de ejecución que se entregará al Líder de Negocio quien, a su vez, las entregará a la DGTIC previo al inicio de las pruebas de calidad. La DGTIC realizará pruebas de calidad con técnicas exploratorias en el momento en que se realice algún despliegue parcial o total de la Solución Tecnológica, considerando al menos un 30% de los casos de prueba que forman parte de la matriz de prueba aprobada por la UA. Para la ejecución de las pruebas se deberá privilegiar el uso de datos de prueba y, en su caso, resguardar cualquier dato requerido para tales fines.

Artículo 49. Para las soluciones tecnológicas desarrolladas a través de recursos a cargo de DGTIC, sólo se podrán liberar al ambiente de producción, sistemas o módulos de los que se haya atendido la totalidad de defectos clasificados con severidad "Crítica" o "Alta", debiendo tener para ello el visto bueno de la DGTIC. Este visto bueno dependerá de la entrega y aprobación de un plan de actividades para atender a los posibles defectos de tipo "Medio" o "Bajo" en estado, "Abierto" o "No corregido" o, en su caso, se notifique por correo electrónico a la SSCST la atención de estos para su validación.

Para el caso de proyectos desarrollados por un proveedor o terceros se podrán liberar al ambiente de producción, sistemas o módulos de los que se haya atendido la totalidad de defectos.

TÍTULO QUINTO

OPERACIÓN Y MANTENIMIENTO DE SOLUCIONES TECNOLÓGICAS

CAPÍTULO PRIMERO

OPERACIÓN Y MANTENIMIENTO

Para la operación y mantenimiento de soluciones tecnológicas se estará a lo dispuesto en las siguientes normas:

Artículo 50.- Respecto a la infraestructura que soporta las Soluciones Tecnológicas y con la finalidad de minimizar el número de vulnerabilidades contenidas en la infraestructura en la que se encuentran las mismas, es necesario realizar un fortalecimiento a través de actualizaciones constantes a Sistemas Operativos, Servidores de Aplicaciones y Manejadores de Bases de Datos, para lo cual se deberá considerar lo siguiente:

I. El sistema operativo deberá tener instaladas todas las actualizaciones y parches que se encuentren disponibles por parte del fabricante y dentro de los repositorios oficiales, esta actividad se podrá implementar en el momento que se necesite.
II. El servidor de aplicaciones, para los ambientes de pruebas, desarrollo y producción, deberá tener instaladas las actualizaciones y parches de seguridad que se encuentren disponibles por parte del fabricante al momento de la instalación, considerando que los 3 ambientes deberán ser idénticos en versiones y parches instaladas.
III. Se deberá realizar la instalación y configuración inicial del Manejador de Base de Datos, en cada uno de los diversos ambientes donde será utilizado.
IV. La instalación, implementación y actualización de los servidores de aplicaciones será responsabilidad de la DGTIC o, en el caso de un producto de caja cerrada, la responsabilidad será en conjunto con el proveedor.
V. La DSI proporcionará guías de fortalecimiento para su implementación. Dichas guías están orientadas a definir la configuración recomendada de los servicios, así como la eliminación y/o desactivación de los puertos, servicios y software innecesarios para el funcionamiento de la Solución Tecnológica. La DIT será responsable de implementar las guías de fortalecimiento, lo anterior, para dar cumplimiento a la "Política General de Ciberseguridad y Seguridad de la Información del IFT"

Artículo 51.- Para liberación a Producción, se deberá considerar previamente lo siguiente:

I. La persona líder de Negocio y la persona Titular de la UA deberán establecer en conjunto con la DGTIC la criticidad de la Solución Tecnológica.
II. Ambiente para liberación a producción. Consiste en la preparación y entrega del ambiente productivo de la Solución Tecnológica. La persona líder del proyecto de la DGTIC deberá mantener homologadas las mismas características de hardware y versiones de software en todos los ambientes de la Solución Tecnológica y podrá realizar el despliegue correspondiente.
III. Resguardo del código fuente del sistema. Se deberá resguardar el código fuente de la Solución Tecnológica conforme al procedimiento de Gestión de Versiones y Despliegues establecido por la DGTIC.
IV. Resguardo de llaves criptográficas. Se deberá proporcionar los parámetros de configuración, licenciamiento, contraseñas, archivos y llaves correspondientes a los certificados SSL/TLS o cualquier otro mecanismo de cifrado. Toda la información concerniente deberá ser entregada a la SSSCO. El área responsable será la DSI.
V. Memoria Técnica. Es obligatorio que la persona líder del proyecto de la DGTIC genere la memoria técnica donde incluya la descripción completa y a detalle del proceso de instalación, configuración, encendido y apagado de la Solución Tecnológica.
VI. Se deberán describir los procesos para la Instalación de la Solución Tecnológica, dicha información deberá contener al menos: arquitectura, números de licencias, números de serie, elementos de hardware, elementos de software y cualquier otra información relativa al licenciamiento y operación de la Solución Tecnológica.
VII. Plan de actividades de Instalación. Antes de la liberación de una nueva versión de una Solución Tecnológica, se deberá identificar por parte de la persona líder del proyecto de la DGTIC y la persona Líder de Negocio, las actividades, tiempos, actores y recursos para lograr de forma

exitosa su liberación a producción. La persona líder de proyecto de la DGTIC deberá definir que componentes son los que se deberán instalar, si se ejecutan scripts, el orden en que se deben ejecutar, el orden de despliegue de artefactos, así como la dependencia o interacción con otros sistemas, entre otros.

VIII. Plan de migración de la información. Si se requiere una migración de datos para poner en producción un sistema, se deberán coordinar los recursos necesarios para realizarla.

IX. El Administrador del proyecto de la DGTIC y la persona líder de Negocio deberán establecer los tiempos, recursos humanos, técnicos y administrativos (procesos) de los componentes a migrarse según los requerimientos. Para ello se deberá documentar de manera enunciativa más no limitativa lo siguiente:
   a. Información por migrar.
   b. Tamaño.
   c. Fecha de migración.
   d. Equipo de trabajo.
   e. Afectaciones.
   f. Método de migración.
   g. Plan de retorno (Roll back).
   h. Puntos de control.

X. Generación de respaldos. Se aplicarán las Políticas de Respaldo vigentes con la finalidad de garantizar la disponibilidad de la información y la continuidad de la operación de la Solución Tecnológica. Si la UA requiere periodos de respaldo distintos a los previstos en dicha política, deberá solicitarlo formalmente a la DGTIC.

XI. Documento de Mantenimiento de la Base de Datos. En este documento se describen el conjunto de actividades de mantenimiento y optimización recomendadas para su aplicación en la Base de Datos, con el propósito de mejorar el rendimiento y garantizar la integridad y resguardo de los datos que, entre otros, incluye:
   a. Optimización / reconstrucción de índices.
   b. Revisión de integridad de la base de datos.
   c. Respaldos.
   d. Proyección de crecimiento de la base de datos.
   e. Generación de estadísticas de desempeño.
   f. Organización de datos históricos.
   g. Especificación de Jobs de la base de datos.

XII. El Administrador del proyecto de la DGTIC deberá documentar el mantenimiento a la Base de Datos alineado a los "Estándares de Base de Datos" definidos por el Instituto.

XIII. Documentación de gestión de los datos. Se deberán documentar los datos como activos del Instituto, considerando al menos lo siguiente:
   a. Diccionario de datos.
   b. Modelo lógico y físico de la base de datos.
   c. Clasificación y organización de los datos.
   d. Metadatos.
   e. Reglas de calidad de los datos.
   f. Linaje de los datos.
   g. Encriptación o enmascaramiento de datos.
   h. Glosario de Negocio.

XIV. Plan de continuidad de la Solución Tecnológica (nuevas Soluciones Tecnológicas). La DGTIC se reserva el derecho de solicitar un ambiente y un plan de recuperación para alguna Solución Tecnológica que, de acuerdo con su criticidad, requiera recuperarse en el menor tiempo posible ante una contingencia.

XV. Plan de Recuperación de Desastres (Soluciones Tecnológicas productivas). La DGTIC identificará las Soluciones Tecnológicas críticas para la operación del Instituto a través de mecanismos de evaluación de riesgos y determinación de criticidad para seleccionar las aplicaciones que formaran parte del Plan de Recuperación de Desastres.

XVI. Dichas soluciones deberán contar con un ambiente y un Plan de Recuperación de Desastres para restaurar la operación en el menor tiempo posible ante una contingencia.

XVII. La persona Titular del aplicativo, en conjunto con las diferentes áreas de la DGTIC, deberá definir y documentar las acciones que se llevarán a cabo durante la contingencia, indicando el escenario para el que fue creado, el orden secuencial de actividades que deberán ejecutarse, el tiempo de recuperación aproximado y los recursos (humanos, técnicos y administrativos) requeridos para su ejecución. Adicionalmente, se deberán indicar las acciones de retorno a la operación en condiciones normales.

XVIII. Para realizar un cambio al alcance del Plan de Recuperación de Desastres se deberá informar a la persona Titular de la Unidad de Administración.

XIX. Manual de usuario. Es responsabilidad del Administrador del proyecto de la DGTIC, en conjunto con la persona líder de Negocio, realizar el manual de usuario en el que se describa de forma sencilla y entendible, las actividades que realizan los múltiples roles de usuario dentro de la Solución Tecnológica, flujos de proceso, negocio y administración. La entrega deberá ser previa a la liberación de la Solución Tecnológica. Esto aplica solo a nuevos desarrollos o aplicativos a los que el usuario operará.

XX. Planes de capacitación. En caso de requerirse, la persona líder de Negocio deberá considerar desde el Documento de Entendimiento de Solución Tecnológica la capacitación a usuarios finales y/o en su caso a usuarios que administren el sistema.

XXI. Derechos de Autor. Salvo que exista impedimento legal, la titularidad de los derechos de autor y/o de propiedad industrial de los componentes que integran la Solución Tecnológica, invariablemente se constituirán a favor del Instituto en términos de las disposiciones legales aplicables y, por tanto, tendrá la facultad exclusiva de autorizar o prohibir su reproducción, adaptación, distribución, comunicación pública, reordenación, compilación, modificación, transformación, así como cualquier otro uso o explotación parcial o total en cualquier forma o por cualquier medio conocido o por conocerse en territorio nacional y/o extranjero, reservándose el derecho de hacer su difusión.

XXII. Aceptación del usuario de la Solución Tecnológica. La persona líder del proyecto de la DGTIC deberá asegurarse que la UA solicitante acepta la Solución Tecnológica para su liberación a producción, así como obtener el visto bueno a través de los formatos Acta de aceptación de entregables y Encuesta de satisfacción del Anexo C.

Artículo 52.- Cuando se requiera el despliegue de la Solución Tecnológica en Ambiente Productivo, se deberá considerar lo estipulado en el procedimiento de control de cambios definido por la DGTIC, así como:

I. Solicitud de despliegue en producción. Para poder solicitar el despliegue en un ambiente de producción, dentro de los centros de datos del Instituto, de una Solución Tecnológica, se debe contar con las siguientes aprobaciones:
   a. Aprobación vía correo electrónico del área de Base de Datos, con la documentación y scripts, que apliquen.
   b. Aprobación vía correo electrónico del área de Calidad una vez que se cumpla con la "Ejecución de Pruebas Funcionales y de Seguridad" y de acuerdo a los criterios vigentes.
   c. Aprobación vía correo electrónico del área de Ciberseguridad una vez que se cumpla con el "Análisis de vulnerabilidades del aplicativo y la infraestructura de acuerdo con los criterios vigentes.
   d. Aprobación del área de negocio equivalente a: "Aceptación del usuario de la Solución Tecnológica", a través de la firma del documento emitido para dicho efecto, el cual podrá ser firmado a través de la FEDI o de forma autógrafa, o bien mediante una confirmación vía correo electrónico de la persona líder del negocio.

II. La obtención de estas autorizaciones deberá ser realizada a través de la persona Analista de Negocio; una vez que cuenta con todas ellas, deberá remitirlas vía correo electrónico a la

SSSCO, quien será responsable de realizar los despliegues respectivos en los ambientes productivos conforme al Proceso de Gestión de Cambios y deberá validar que se cumplan los siguientes puntos:

a. Resguardo del código fuente del sistema.
b. Resguardo de llaves criptográficas.
c. Memoria Técnica.
d. Diagrama de Despliegue y Diagrama de Arquitectura, inmersos en los manuales anteriores.
e. Registro de la infraestructura de la Solución Tecnológica en las herramientas de monitoreo con que cuente la DGTIC.
f. En su caso, registro de la Solución Tecnológica a la operación de la Mesa de Servicio Institucional, para su soporte por DGTIC.

Artículo 53.- Cuando la Solución Tecnológica se encuentre en Ambiente Productivo:

I. Soporte de la Solución Tecnológica. El soporte que brindará la DGTIC a soluciones desarrolladas bajo el financiamiento de contratos a cargo de la DGTIC se realizará a solicitud de la UA mediante un ticket en la mesa de servicio o bien si se trata de un requerimiento normativo con fecha perentoria, deberá enviar un oficio a la DGTIC, tal y como se describe en la Tabla 1. Tipología general de proyectos de Soluciones Tecnológicas.
II. Reporte y control de cambios a la Solución Tecnológica. Posterior a la puesta en producción es necesario que el Administrador del proyecto de la DGTIC, lleve un control de todos los cambios incluyendo:
    a. El cambio;
    b. La situación que lo originó, y;
    c. La Solución que se implementó.
III. Los cambios deberán aplicarse conforme al Proceso de Gestión de Cambios establecido por la DGTIC.

Artículo 54.- Los roles y responsabilidades de la Solución Tecnológica en Productivo son los siguientes:

Roles y responsabilidades. Una vez que la Solución Tecnológica ha sido aprobada para su instalación en el ambiente productivo y que se ha formalizado el inicio de su operación, se deberán asignar los siguientes roles:

I. Por la UA solicitante:
a. Persona Titular del aplicativo: quien fungirá como el dueño del aplicativo y será el principal responsable de la toma de decisiones relacionadas al mismo. Por ejemplo: autorizaciones de cambios, mejoras o mantenimientos solicitados por la UA o por la propia DGTIC. Se sugiere que el servidor público asignado se establezca desde la solicitud del PAP y se confirme en Documento de Entendimiento. En caso de algún cambio de persona, la UA deberá notificar a la OP y al Líder de Proyecto de la DGTIC.
b. Contacto de Negocio: La UA deberá definir un servidor público que funja como enlace entre la DGTIC y el titular del aplicativo, a través del cual se puedan tratar los asuntos relacionados a cambios, mejoras o mantenimientos de este. En caso de no existir una designación por la UA, se considerará al servidor público en el Documento de Entendimiento.

II. Por la DGTIC:
a. Contacto Técnico: La DGTIC deberá definir un servidor público que funja como responsable de atender a las necesidades del aplicativo en producción, así como de evaluar y en su caso ejecutar, en conjunto con el Contacto de negocio los cambios, mejoras o mantenimientos del aplicativo.
b. Se deberá mantener un directorio de información de contacto de los servidores públicos que cubran los roles anteriormente citados.

Artículo 55.- De la baja de soluciones tecnológicas.

Para optimizar el aprovechamiento de los recursos informáticos del Instituto, la DGTIC realizará un monitoreo de las soluciones tecnológicas en productivo para determinar el impacto de su uso. Dicho reporte será enviado a Comisionados y personas Titulares de cada UA con finalidad de darle una visibilidad del uso y valor que está generando al IFT.

Los criterios establecidos para que una solución tecnológica sea candidata para darse de baja son los siguientes:

I. Poco o nulo uso durante un periodo de 6 meses consecutivos.
II. Poca o nula generación de valor para el IFT o la ciudadanía.
III. Obsolescencia tecnológica y alta vulnerabilidad derivado de la falta de actualizaciones disponibles o parches de seguridad.
IV. Se extingue la necesidad por la que fue creado pudiendo ser:
   a. Obsolescencia del proceso de negocio controlado por la aplicación
   b. La solución tecnológica es reemplazada por una nueva o los módulos de la solución fueron consolidados en alguna otra solución.
V. Cambios en la regulación o fallas en su cumplimiento.
VI. Falta de Rendimiento y escalabilidad.
VII. Fallas en el cumplimiento en las disposiciones del área de Seguridad del IFT.
VIII. Pérdida de soporte por parte del fabricante de uno o varios de los componentes.

Artículo 56.- Para el caso de Soluciones Tecnológicas que serán dadas de baja de la infraestructura operativa del Instituto, se deberán tener las siguientes consideraciones:

I. La solución tecnológica se dará de baja de todos los ambientes tecnológicos en los que se encuentre.
II. Respaldo del aplicativo: generar y asegurar el respaldo de la última versión en ambiente productivo.
III. Respaldo de la base de datos: generar y asegurar el respaldo de todos los datos y esquemas relacionados con la aplicación.
IV. Evaluación del impacto: Realizar un análisis exhaustivo del impacto que la desactivación de la solución tendrá en las áreas de negocio, procesos operativos, usuarios y clientes; y que no exista interoperabilidad o dependencia del aplicativo con otras soluciones tecnológicas o plataformas.
V. Comunicación y acuerdos con las y los interesados: acordar con todas las personas interesadas sobre los cambios planeados, proveer información clara sobre las razones del cambio y el cronograma a ejecutar.
VI. Documentación completa del proceso de baja: Mantener toda la documentación detallada de todo el proceso de baja, incluyendo las razones tomadas, pasos realizados, problemas encontrados y, en su caso, soluciones aplicadas.
VII. Tiempo de resguardo: establecer con el dueño de la aplicación y conforme a la normatividad aplicable, el tiempo de resguardo de la solución tecnológica.
VIII. Baja del monitoreo, inventarios, CMDB y del catálogo de Mesa de Servicio.

Artículo 57.- La DGTIC revisará las Soluciones Tecnológicas que serán adquiridas como un producto listo para ser instalado, las cuales deberán respetar la plataforma tecnológica estándar vigente (licenciamientos y versiones). En caso de que, derivado de la naturaleza de la solución, el producto tenga una plataforma tecnológica diferente a la establecida en este capítulo, la DGTIC podrá revisar la posibilidad de su inclusión, considerando que el posible impacto a la infraestructura, arquitectura y seguridad de la información del Instituto se encuentre dentro de un nivel aceptable. De ser aprobado, la DGTIC otorgará su Visto Bueno a la UA.

Las Soluciones Tecnológicas a que se refiere este artículo invariablemente deberán someterse a las pruebas de calidad necesarias que permitan garantizar su buen funcionamiento en la infraestructura del Instituto, así como, a las pruebas funcionales de seguridad y análisis de vulnerabilidades que comprueben su alineación y cumplimiento a los estándares de seguridad definidos, además de considerar la programación de sus liberaciones a la operación diaria del Instituto, incluyendo los planes y documentación de soporte necesaria para su administración, operación y mantenimiento. La documentación requerida será acordada entre la UA solicitante, la DGTIC y el proveedor conforme al Anexo C de las presentes Normas.

Artículo 58.- Para la gestión de actualizaciones de redes de voz y datos, hardware y software, sistemas operativos, aplicativos, bases de datos y demás componentes tecnológicos en el IFT, con el fin de asegurar la continuidad del negocio, la seguridad de la información y el desempeño óptimo de los sistemas, se deberán seguir los siguientes criterios:

I. Planificación de Actualizaciones
   a. Las actualizaciones deberán planificarse previamente y aprobarse por el Grupo de Trabajo de TI.
   b. Se deberá elaborar un calendario de actualizaciones anual, revisado y aprobado trimestralmente y actualizado cada vez que sea necesario
   c. Las actualizaciones críticas de seguridad se evaluarán e implementarán urgentemente fuera del calendario regular conforme el proceso de gestión de cambios y aprobado por el ECAB.

II. Evaluación y Pruebas
   a. Antes de implementar cualquier actualización, se deberá realizar una evaluación de impacto para identificar posibles riesgos y efectos sobre otros sistemas y operaciones.
   b. Todas las actualizaciones deberán ser probadas en un entorno controlado que simule las condiciones del entorno de producción.
   c. Los resultados de las pruebas deberán ser documentados y revisados antes de la aprobación final.

III. Implementación
   a. Cuando se requiera el despliegue de la actualización en Ambiente Productivo, se deberá considerar lo estipulado en el procedimiento de control de cambios definido por la DGTIC, así como el procedimiento gestión de versión y despliegue considerando lo siguiente: Las actualizaciones deberán ser implementadas fuera de las horas laborables del IFT para minimizar el impacto en los usuarios, es decir, después de las 18:30 horas de lunes a jueves y después de las 15 horas los viernes.
   b. Un plan de respaldo y restauración deberá estar preparado y probado antes de la implementación de cualquier actualización.
   c. Se deberá comunicar a todos los usuarios afectados sobre las actualizaciones programadas y los posibles impactos en el servicio. En caso de que trate de un portal dirigido a la ciudadanía y entidades concesionarias se deberá publicar el aviso en el portal institucional 48 horas antes.

IV. Monitoreo y Verificación.
   a. Después de la implementación de cualquier actualización, se deberá realizar un monitoreo continuo para asegurar que el sistema funcione correctamente.
   b. Se deberá realizar una verificación post-implementación para asegurar que todos los componentes tecnológicos actualizados funcionen según lo esperado.
   c. Cualquier problema identificado tras la actualización deberá reportarse y resolverse inmediatamente y, en su caso, aplicar el rollback correspondiente.

V. Documentación.
   a. Toda actualización deberá ser documentada detalladamente, incluyendo el propósito, el procedimiento seguido, los resultados de las pruebas, y el plan de respaldo y restauración.

b. La documentación se almacenará en un repositorio central accesible al personal autorizado.

VI. Responsabilidades
   a. El equipo de la DIT y la DSI son responsables de la planificación, evaluación, prueba, implementación, monitoreo y documentación de todas las actualizaciones.
   b. El Grupo Asesor de Cambios es responsable de la revisión y aprobación de las actualizaciones planificadas.
   c. Los usuarios son responsables de reportar cualquier problema que experimenten después de una actualización.
   d. El Grupo Asesor de Cambios de Emergencia es responsable de la revisión y aprobación de las actualizaciones no planificadas.

Niveles de servicio

Artículo 59.- Las Soluciones Tecnológicas que se desarrollen y/o implementen deberán contar con Niveles de servicio (SLA) establecidos conforme a la criticidad y tipo de solución acordados entre la persona líder de Negocio y la DGTIC.

Los niveles de prioridad que deberán considerarse son los siguientes:

Nivel de prioridad	Descripción
Nivel de Prioridad 1 – Impacto/Urgencia Afectación critica al Negocio	El incidente ha causado una afectación impactando a todos los usuarios del servicio y no se cuenta con una solución temporal.
Nivel de Prioridad 2 – Alto Alto impacto al negocio	Un proceso de negocio es afectado de manera que las funciones del negocio son degradadas severamente, múltiples usuarios son afectados, un usuario clave es afectado, o una función crítica está operando con una capacidad o funcionalidad reducida. Una solución temporal podría estar disponible, sin embargo, la solución temporal no es fácilmente aceptada. Ejemplos: Problemas mayores de datos/ El sistema está lento, pero la carga de trabajo es manejable/administrable.
Nivel de Prioridad 3 – Medio Moderado impacto al negocio	Un proceso de negocio es afectado de manera que ciertas funciones no están disponibles a un grupo reducido usuarios finales o un sistema y/o servicio está degradado. Una solución temporal está disponible.
Nivel de Prioridad 4 – Bajo Bajo impacto al negocio	Un proceso de negocio es afectado de manera que ciertas funciones no están disponibles a un usuario final, una solución temporal está disponible.

Tabla 9 Prioridades

Mantenimientos y actualizaciones

Artículo 60.- Todos los mantenimientos y actualizaciones a soluciones tecnológicas, sin excepción, deberán cumplir con lo siguiente:

I. Generar un cronograma (Microsoft Project u otras herramientas), señalando claramente en él, las etapas, áreas involucradas y actividades a desarrollarse durante el mantenimiento o acciones acordadas para su seguimiento.
II. Generar el documento de mantenimiento correspondiente, en donde se precise a detalle los cambios solicitados, alcance, excepciones y, en su caso, flujos afectados.

III. Actualizar toda la documentación correspondiente derivado de las modificaciones o actualizaciones que sufran las Soluciones Tecnológicas.

IV. Toda actualización o mantenimiento que se les realicen a las soluciones tecnológicas, deberán ser sometidas a pruebas funcionales y análisis de vulnerabilidades, a efecto de corroborar que los cambios aplicados no hayan afectado las funcionalidades de las soluciones tecnológicas vigentes o, en su caso, se hayan inyectado vulnerabilidades.

TÍTULO SEXTO

IMPLEMENTACIÓN DE NUEVAS TECNOLOGÍAS

CAPÍTULO ÚNICO

IMPLEMENTACIÓN DE NUEVAS TECNOLOGÍAS

Artículo 61.- Como parte de las atribuciones de la DGTIC, se realiza un monitoreo continuo del mercado y las tendencias tecnológicas para identificar tecnologías emergentes que puedan generar valor al IFT. Cada tecnología identificada, será sujeta a una evaluación preliminar que incluirá análisis de beneficios potenciales, riesgos asociados, costos de implementación y alineación con los objetivos estratégicos del IFT.

En caso de que las UA requieran la implementación de Tecnologías emergentes y que no se encuentren actualmente en la infraestructura del Instituto, deberán solicitarlo mediante correo electrónico dirigido a la DGTIC o, en su caso, a la oficina de proyectos, justificando el uso de dicha tecnología, así como la funcionalidad del proyecto solicitado. La DGTIC realizará un proceso de evaluación, análisis de adopción, implementación y gobernanza de tecnologías para dichas iniciativas.

Para realizar la adopción de tecnologías nuevas, la DGTIC realizará pilotos y pruebas de concepto para evaluar la viabilidad técnica y el impacto en los procesos de negocio. Las tecnologías que pasen la fase de prueba serán revisadas y aprobadas por la alta dirección antes de su implementación en el IFT.

Para la implementación de nuevas tecnologías se desarrollará un plan detallado de implementación que incluirá cronograma, asignación de recursos, capacitación y gestión del cambio. Además, se identificarán y gestionarán los riesgos asociados a la implementación de nuevas tecnologías, incluyendo la seguridad de la información, la continuidad del negocio y el cumplimiento regulatorio. Después de la implementación, se realizará un seguimiento continuo y una evaluación periódica del rendimiento y el impacto de la nueva tecnología.

Está estrictamente prohibido que los usuarios habiliten o instalen tecnologías emergentes y/o nuevas en los equipos de cómputo e instalaciones del IFT sin previo conocimiento y aprobación de la DGTIC. En caso de algún incumplimiento de esta disposición, se procederá conforme al artículo 29 de las Políticas de TIC.

TÍTULO SÉPTIMO

GOBIERNO DE DATOS EN SOLUCIONES TECNOLÓGICAS

CAPÍTULO ÚNICO

DESARROLLO DE SOLUCIONES TECNOLÓGICAS

Artículo 62.- El presente Capítulo tiene como objetivo establecer los puntos que deberán considerarse para el Gobierno de Datos en todas las soluciones tecnológicas que sean realizadas por la DGTIC o por un tercero:

I. Todo proyecto tecnológico que se inicie en la DGTIC deberá incluir, desde su fase de planificación, un análisis de Gobierno de Datos. Este análisis identificará los tipos de datos que serán utilizados, su clasificación (públicos, sensibles, confidenciales), y las medidas de protección necesarias.

II. Todos los desarrollos de soluciones tecnológicas deberán apegarse a la definición de estándares de calidad de datos, gestión de metadatos establecidos en la política de Gobierno de Datos, Seguridad de la información y cumplimiento normativo.

III. Todos los desarrollos de soluciones tecnológicas deberán tener como premisa la explotación de la información para apoyo a la toma de decisiones.

IV. Durante el desarrollo, se implementarán controles de calidad de datos para asegurar que la información manejada sea precisa, completa y coherente, esto implica definir estructuras de datos, relaciones y restricciones que garanticen la integridad y seguridad de la información.

V. Se establecerán protocolos de seguridad para garantizar que los datos sean protegidos contra accesos no autorizados, pérdidas o alteraciones. Esto incluye el cifrado de datos en tránsito y en reposo, controles de acceso basados en roles, y la implementación de medidas para la detección y respuesta ante incidentes de seguridad.

VI. Se prohibirá el uso de datos reales de usuarios en ambientes de desarrollo y pruebas. En su lugar, se utilizarán datos anonimizados o sintéticos para evitar cualquier exposición de información sensible o confidencial. Los datos reales de ambientes productivos no deberán ser utilizados en cualquier tipo de mantenimiento de portales y sistemas.

VII. Todos los desarrollos tecnológicos deberán cumplir con las normativas aplicables en materia de protección de datos y privacidad, incluyendo las leyes nacionales e internacionales relevantes. La DGTIC realizará auditorías periódicas para asegurar el cumplimiento de estas políticas y adoptar medidas correctivas cuando sea necesario.

VIII. El personal involucrado en los desarrollos tecnológicos deberá recibir capacitación continua sobre las políticas de Gobierno de Datos y las mejores prácticas en su implementación, revisión y actualización.

TÍTULO OCTAVO

CONSIDERACIONES FINALES

CAPÍTULO PRIMERO

CUMPLIMIENTO DE LAS NORMAS

Artículo 63.- Con el fin de vigilar el cumplimiento de las presentes Normas, la DGTIC realizará las actividades de monitoreo necesarias, conforme a las atribuciones que le confiere el Estatuto Orgánico del Instituto Federal de Telecomunicaciones, así mismo las interpretará para efectos administrativos y resolverá cualquier situación no prevista en las mismas.

CAPÍTULO SEGUNDO
DISPOSICIONES TRANSITORIAS

Única. Las presentes Normas deberán publicarse en el Portal de Transparencia Institucional, sin perjuicio de publicar el aviso correspondiente sobre su publicación en dicho Portal, en el Diario Oficial de la Federación y entrarán en vigor al día hábil siguiente al de la publicación del mencionado aviso.

Las presentes "Normas para la Administración, Operación y Mantenimiento de soluciones de Tecnologías de la Información y Comunicaciones del Instituto Federal de Telecomunicaciones", se emiten con fundamento en los artículos 57, primer párrafo y fracción VIII, así como 61, fracciones IV, V y VII del Estatuto Orgánico del Instituto Federal de Telecomunicaciones, en la Ciudad de México, el día 04 de noviembre de 2024.