PODER EJECUTIVO
PRESIDENCIA DE LA REPUBLICA

ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal.

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- MÉXICO.- Presidencia de la República.- Coordinación de Estrategia Digital Nacional.

El suscrito Carlos Emiliano Calderón Mercado, en mi carácter de Coordinador de Estrategia Digital Nacional de la Oficina de la Presidencia de la República, con fundamento en lo dispuesto por el artículo 8, segundo y tercer párrafo, fracción I de la Ley Orgánica de la Administración Pública Federal y los artículos 2, fracciones II y VI, 3 fracción IX y 36, fracciones I, II, III, IV, VII, VIII, X, XI, XIV y XVI del Reglamento de la Oficina de la Presidencia de la República, y

CONSIDERANDO

Que el Ejecutivo Federal cuenta con la atribución de definir las políticas del Gobierno Federal en los temas de informática, tecnologías de la información, comunicación y de gobierno digital, en términos de las disposiciones aplicables, como lo dispone el artículo 8, segundo y tercer párrafo, fracción I de la Ley Orgánica de la Administración Pública Federal, tarea que ha delegado a la Coordinación de Estrategia Digital Nacional (CEDN) a través del Reglamento de la Oficina de la Presidencia de la República, publicado en el Diario Oficial de la Federación (DOF) el 09 de diciembre de 2019;

Que la CEDN es una Unidad de Apoyo Técnico de la Oficina de la Presidencia de la República, con atribuciones para emitir disposiciones administrativas, manuales, guías, instructivos y demás instrumentos análogos para el desarrollo de sus funciones, así como elaborar y coordinar la Estrategia Digital Nacional, darle seguimiento y evaluarla; requerir a las dependencias y entidades de la Administración Pública Federal (APF) la información necesaria para el desarrollo de sus funciones, así como participar en coordinación con las dependencias y entidades competentes, en el diseño y formulación de las especificaciones y estándares para las adquisiciones y arrendamientos de bienes o prestación de servicios de tecnologías de la información y comunicación; entre otras relativas a gobierno digital, así como al uso y aprovechamiento de las tecnologías de la información y comunicación;

Que la honradez y honestidad son principios rectores comprendidos en el Plan Nacional de Desarrollo 2019-2024, mismos que orientan los objetivos y acciones del Programa Nacional de Combate a la Corrupción y a la Impunidad, y de Mejora de la Gestión Pública 2019-2024, en que participa la CEDN para promover el uso intensivo de las tecnologías de la información y comunicación, la mejora del marco jurídico, el impulso y fomento de la interacción de los sistemas informáticos de la APF de manera transversal, la implementación de nuevas soluciones tecnológicas basadas en software libre para una mejor operación de los sistemas, así como el intercambio de conocimientos y recursos técnicos entre las Instituciones, con la finalidad de materializar el mandato constitucional del artículo 134, el cual dispone que los recursos económicos de que disponga la Federación se administren con eficiencia, eficacia, economía, transparencia y honradez para satisfacer los objetivos a que están destinados.

Que la priorización en el uso del Software Libre es una medida de austeridad republicana contemplada en la Ley Federal de Austeridad Republicana y; que la Ley General de Mejora Regulatoria publicada en el DOF el 18 de mayo de 2018, prevé la conformación del Expediente para Trámites y Servicios cuyos Lineamientos señalan los mecanismos técnicos para su implementación, tarea en que participa la CEDN en el ejercicio de sus atribuciones y a través de la Estrategia Digital Nacional.

Que las presentes políticas y disposiciones tienen como objetivo fortalecer el uso del software libre y los estándares abiertos, fomentar el desarrollo de aplicaciones institucionales con utilidad pública, lograr la autonomía, soberanía e independencia tecnológicas dentro de la APF, consolidar una base tecnológica robusta y homogénea en las Instituciones del Estado, así como lograr una mayor eficiencia basada en la reducción de tiempos y costos en los procesos de contratación en materia de tecnologías de la información y comunicación, descartando aquellos productos o servicios que no sean estrictamente indispensables para el funcionamiento y operación de cada Institución; así como establecer las directrices para el uso y aprovechamiento de las Tecnologías de la Información y Comunicación en las Dependencias y Entidades de la Administración Pública Federal, se expide el siguiente:

ACUERDO POR EL QUE SE EMITEN LAS POLÍTICAS Y DISPOSICIONES PARA IMPULSAR EL USO Y APROVECHAMIENTO DE LA INFORMÁTICA, EL GOBIERNO DIGITAL, LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN, Y LA SEGURIDAD DE LA INFORMACIÓN EN LA ADMINISTRACIÓN PÚBLICA FEDERAL

TÍTULO PRIMERO

DEL OBJETO Y ÁMBITO DE APLICACIÓN

CAPÍTULO I

DISPOSICIONES PRELIMINARES

Artículo 1.- El presente Acuerdo tiene por objeto emitir las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información, que serán de observancia obligatoria en la Administración Pública Federal.

Estarán exceptuadas de su aplicación, las Secretarías de la Defensa Nacional y de Marina, así como el Centro Nacional de Inteligencia.

Artículo 2.- Para los efectos de este Acuerdo, sin perjuicio de su referencia en plural o singular, se entenderán las siguientes definiciones, siglas y acrónimos:

A. Definiciones

I. **Acuerdo:** el Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información, en la Administración Pública Federal;

II. **Activo de información:** la información, los datos y los recursos que la contienen, procesan y transmiten, que por su importancia y el valor que representa para una Institución, deben ser protegidos;

III. **Acuerdo de confidencialidad:** el instrumento que se celebra entre partes para restringir el uso o divulgación pública o hacia terceros de la información o conocimiento que se trate con motivo de la relación existente;

IV. **Activo de información esencial:** el activo de información cuya destrucción, pérdida, alteración o falla tendría un grave impacto o consecuencia en la funcionalidad de la infraestructura de TIC o en los servicios que soporta;

V. **Amenaza:** el posible acto o circunstancia interna o externa que puede explotar, de manera intencional o circunstancial, la debilidad presente en un activo de información. Una amenaza puede tener diferente nivel de riesgo de acuerdo con los escenarios en los que se presente;

VI. **Arquitectura Institucional:** el enfoque mediante el cual se estructuran los componentes de la Institución (procesos, información, arquitectura tecnológica y personas) delineando sus relaciones y evolución en el tiempo, permite a las áreas de TIC entender y atender sus necesidades desde una perspectiva integral y estratégica, aportando valor;

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

VIII. **Autenticación electrónica:** el procedimiento informático que permite identificar de manera individual e inequívoca los atributos de un usuario, con la finalidad de que éste pueda acceder a un aplicativo de cómputo o a un servicio electrónico;

IX. **Borrado seguro:** el proceso mediante el cual se elimina de manera permanente y de forma irrecuperable la información contenida en medios de almacenamiento digital;

X. **Centro de Datos:** el espacio físico donde se concentran los recursos necesarios, consistentes en equipo informático y redes de comunicaciones para el procesamiento de la información de una Institución o proveedor de servicios;

XI. **Componente tecnológico**: el producto de hardware o software con una funcionalidad específica que permite satisfacer una necesidad y que, junto con otros elementos tecnológicos proporcionan un beneficio integral o mayor funcionalidad técnica;

XII. **Contrato marco de TIC:** instrumento celebrado entre la Oficialía Mayor de la SHCP y posibles proveedores de TIC, con el apoyo técnico de la CEDN para estandarizar las características y precios sobre adquisiciones, arrendamientos y servicios de TIC;

XIII. **Contrataciones consolidadas:** la integración de los procedimientos de contratación de bienes o servicios tecnológicos, entre entes públicos;

XIV. **Contrataciones anticipadas:** la excepción otorgada por la Secretaría de Hacienda y Crédito Público para que las dependencias o entidades, de forma previa a la autorización de sus presupuestos, puedan convocar, adjudicar y formalizar contratos cuya vigencia inicie en el ejercicio fiscal siguiente de aquel en el que se formalizan, de conformidad con lo señalado en el segundo párrafo del artículo 25 de la LAASSP;

XV. **Controles de seguridad de la información:** las medidas establecidas para preservar la confidencialidad, integridad y disponibilidad de los activos de información Institucionales contra las amenazas latentes o existentes y, que coadyuvan en la gestión de riesgos inherentes a su uso;

XVI. **Controles mínimos de seguridad de la información:** los controles de seguridad de la información mínimos, indispensables y obligatorios establecidos por la CEDN para la protección de los activos de información;

XVII. **Datos abiertos:** los datos digitales de carácter público que pueden ser usados, reutilizados y redistribuidos por cualquier interesado;

XVIII. **Estrategia Digital Nacional:** El plan de acción del Ejecutivo Federal para aprovechar el potencial de las tecnologías de la información y comunicación, incluidos los servicios de banda ancha e Internet, como elemento catalizador del desarrollo del país, mediante su incorporación a la vida cotidiana de las personas, y a la Administración Pública Federal, mediante el uso de la informática y el desarrollo del gobierno digital;

XIX. **Estándares abiertos:** Los desarrollados o aprobados, y mantenidos a través de un proceso impulsado por la colaboración y el consenso, facilitan la interoperabilidad y el intercambio de datos entre los diferentes productos o servicios, y están destinados para la adopción generalizada;

XX. **Estándares técnicos:** las características técnicas de bienes y servicios de TIC definidas por la CEDN, así como las mejores prácticas aplicables a la gestión de las TIC que deberán ser consideradas por las Instituciones en los diferentes procesos de contratación para la adquisición, el arrendamiento de bienes o la prestación de servicios en materia de TIC y de seguridad de la información, y en los proyectos de desarrollo que se realicen con recursos humanos internos, a fin de homologar la capacidad tecnológica, garantizar la interoperabilidad entre éstas, y fomentar el ahorro en el ejercicio del gasto público;

XXI. **Firma Electrónica Avanzada:** el conjunto de datos y caracteres que permite la identificación del firmante, creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa;

XXII. **Gobierno Digital:** las actividades basadas en tecnologías de información y comunicación que el Estado desarrolla para aumentar la eficiencia de la gestión pública, mejorar los servicios ofrecidos a los ciudadanos y dar transparencia a las acciones de gobierno;

XXIII. **Herramienta de Gestión de Política TIC:** la plataforma web administrada por la CEDN disponible para el control y gestión de las actividades que realicen las Instituciones establecidas en el presente Acuerdo;

XXIV. **Incidente de seguridad de la información:** el evento o serie de eventos de seguridad de la información no deseados o inesperados, con probabilidad significativa de comprometer las funciones esenciales de la Institución y amenazar la seguridad de la información;

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

XXVI. **Instituciones:** las dependencias y entidades integrantes de la Administración Pública Federal;

XXVII. **Instrumento de colaboración:** acuerdo o convenio formalizado entre Instituciones para establecer acciones que mejoren el aprovechamiento de las TIC, su infraestructura o recursos, con base en los principios de austeridad y eficiencia;

XXVIII. **Interoperabilidad:** la capacidad de organizaciones y sistemas dispares y diversos, para interactuar con objetivos consensuados y comunes con la finalidad de obtener beneficios mutuos, en donde la interacción implica que las Instituciones compartan infraestructura, información y conocimiento mediante el intercambio de datos entre sus respectivos sistemas de tecnología de información y comunicación;

XXIX. **Inventario Institucional de bienes y servicios de TIC:** el listado que comprende el equipo de cómputo, aplicaciones, software, bases de datos, servicios e infraestructura de cada Institución; constituye uno de los elementos de la Arquitectura Institucional;

XXX. **Inventario de bienes y servicios de TIC de la APF:** el listado que integra los Inventarios Institucionales de bienes y servicios de TIC, concentrado por la CEDN;

XXXI. **Niveles de servicio**: el establecimiento de las características y parámetros de un servicio contratado incluyendo al menos la definición, disponibilidad, calidad, tiempos de respuesta y solución;

XXXII. **Oficio de pronunciamiento del OCF:** el documento mediante el cual el OCF en la Institución que planea llevar a cabo la contratación, emite su pronunciamiento favorable o sugerencias u observaciones de manera fundada y motivada respecto de la contratación de que se trate;

XXXIII. **Plan de continuidad de operaciones:** al instrumento Institucional que indica los insumos técnicos, humanos, roles específicos y organización interna que garanticen la continuidad de las operaciones tecnológicas en las Instituciones**;**

XXXIV. **Plan de recuperación ante desastres:** al instrumento Institucional que marca las pautas para la estabilización y restauración de los servicios o activos de información esenciales a partir de un estado de contingencia o interrupción, provocado por la naturaleza o por el ser humano;

XXXV. **Procesamiento de Datos**: el tratamiento de datos (elementos básicos de información) que se lleva a cabo de manera automática por medio de sistemas o aplicativos de cómputo;

XXXVI. **Proceso esencial:** el que está relacionado con la generación y entrega de valor a los ciudadanos, ya sea en forma de productos o servicios; representa las actividades clave de la Institución para alcanzar sus objetivos;

XXXVII. **Programa de gestión de vulnerabilidades:** al proceso de identificación, clasificación y priorización para la atención y remediación o mitigación de vulnerabilidades encontradas en los activos de información de la Institución en un periodo determinado;

XXXVIII. **Proyecto estratégico de TIC:** el que requiere un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado de TIC, que puede o no requerir la contratación de bienes o servicios en materia de TIC para su ejecución y cuya implementación contribuye significativamente al logro de los objetivos estratégicos y metas de la Institución;

XXXIX. **Proyecto operativo de TIC:** el proyecto no considerado como estratégico que requiere de un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado de TIC que soporta la operación diaria de la Institución; puede o no requerir la contratación de bienes o servicios en materia de TIC para su ejecución;

XL. **Riesgo:** la probabilidad de que una amenaza pueda explotar una vulnerabilidad, generando un impacto sobre la infraestructura de TIC y los activos de información de la Institución;

XLI. **Repositorio de software de la APF:** el espacio administrado por la CEDN para concentrar el código fuente de las aplicaciones o programas desarrollados o con titularidad de las Instituciones, que les permita usar, estudiar, compartir y modificar el software con la finalidad de mejorar la calidad y seguridad de la gestión de la información, fomentando el desarrollo colaborativo entre instituciones para cubrir sus necesidades comunes y generar ahorros en el gasto público;

XLII. **Seguridad de la Información:** la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma;

XLIII. **Seguridad Nacional**: las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano, de conformidad con lo señalado en el Artículo 3 de la Ley de Seguridad Nacional;

XLIV. **Servicios en la Nube:** al modelo de provisión externa de servicios de cómputo bajo demanda que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente, que se encuentren localizados fuera o dentro del territorio nacional, en instalaciones del Estado o en instalaciones privadas;

XLV. **Software Libre:** el programa informático cuyo código fuente cumple con las cuatro Libertades del Software Libre y por ende se encuentra disponible para ser ejecutado, estudiado, modificado o distribuido libremente, independientemente de su costo o gratuidad;

XLVI. **Tecnologías de la Información y Comunicación:** el equipo de cómputo, software, dispositivos de impresión, infraestructura y servicios que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video;

XLVII. **Visto bueno de la CEDN:** la aprobación que otorga la CEDN a las UTIC de las Instituciones, a partir del cumplimiento que éstas realicen de las políticas, disposiciones, lineamientos, criterios técnicos, metodologías, guías, instructivos y demás instrumentos análogos que sean emitidos por la CEDN, y

XLVIII. **Vulnerabilidad:** a la debilidad presente en un activo de información que potencialmente permitirá que una amenaza lo impacte de manera negativa, con posibles afectaciones para la seguridad de la información dentro de la Institución.

B. Siglas y Acrónimos

ASN (*Autonomous System Number)*: Número de Sistema Autónomo;

CEDN: Coordinación de Estrategia Digital Nacional de la Oficina de la Presidencia de la República;

CNI: Centro Nacional de Inteligencia, Órgano Administrativo Desconcentrado de la Secretaría de Seguridad y Protección Ciudadana;

ERISC: Equipo de Respuesta a Incidentes de Seguridad en TIC;

Herramienta: Herramienta de Gestión de la Política TIC;

IPv4 o IPv6 (Internet Protocol version 4 or 6): Protocolo de Internet versión 4 ó 6;

LAASSP: Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público;

MGSI: Marco de Gestión de Seguridad de la Información;

NIC (Network Information Center): Autoridad que se encarga de administrar los nombres de dominio de un país y de asignarlos a quien los solicita; así como la asignación de ASN o bloques de IPv4 ó IPv6;

OCF: Órgano de Control y Fiscalización de las Instituciones, el cual considera a los Órganos Internos de Control y/o análogos dependientes de la Secretaría de la Función Pública;

POTIC: Portafolio de proyectos de Tecnologías de la Información y Comunicación;

PNCCIMGP: Programa Nacional de Combate a la Corrupción y a la Impunidad, y de Mejora de la Gestión Pública;

RSI: Responsable de la Seguridad de la Información de cada Institución;

SI: Seguridad de la Información;

SHCP: Secretaría de Hacienda y Crédito Público;

TIC: Tecnologías de la Información y Comunicación;

UPCP: Unidad de Política y Control Presupuestario de la SHCP; y

UTIC: Unidad de Tecnologías de Información y Comunicaciones o área responsable de las TIC en cada Institución.

CAPÍTULO II

DE LAS POLÍTICAS TECNOLÓGICAS GENERALES

Artículo 3.- Para todos los proyectos institucionales que comprendan servicios e implementaciones tecnológicas y de seguridad de la información, la persona titular de la UTIC deberá atender las siguientes políticas y disposiciones generales:

I. Procurar el ahorro y el uso eficiente de los recursos atendiendo las disposiciones establecidas en la Ley Federal de Austeridad Republicana;

II. Privilegiar la realización de contratos específicos que deriven de contratos marco vigentes, o la realización de contrataciones consolidadas o licitaciones públicas que garanticen las mejores condiciones para el Estado;

III. Priorizar el aprovechamiento de los recursos tecnológicos disponibles con que cuentan otras Instituciones, o los registrados en el Inventario de bienes y servicios de TIC de la APF, celebrando los instrumentos de colaboración pertinentes;

IV. Considerarse entre Instituciones, la celebración de todo tipo de acuerdos que permitan el desarrollo de proyectos conjuntos en materia de TIC.

V. Privilegiar el alojamiento de la información en territorio nacional y en instalaciones del Estado.

VI. Observar los Estándares Técnicos emitidos por la CEDN, así como la acreditación de estándares o modelos reconocidos por el sector como las mejores prácticas, y el cumplimiento de normas oficiales;

VII. Privilegiar el almacenamiento e intercambio de información en formatos basados en estándares abiertos;

VIII. Atender las disposiciones normativas en materia de protección de datos personales, transparencia y rendición de cuentas;

IX. Sujetarse a la normatividad aplicable en materia de planeación, presupuesto y adquisiciones; y

X. Priorizar los mecanismos que faciliten la participación de los Centros Públicos de Investigación y de las Empresas Productivas del Estado en su desarrollo e implementación; al tratarse de contrataciones de adquisiciones, arrendamientos o servicios de TIC y SI, deberá incluirse la participación de éstos en las investigaciones de mercado que se efectuen, siempre que estén en posibilidades de proveer los bienes o servicios requeridos.

Adicionalmente, tratándose de contrataciones, deberá considerar que, al menos, se cuente con:

a) Acreditación de la experiencia técnica especializada del personal del proveedor;

b) Políticas y Acuerdos de Confidencialidad;

c) Obligaciones de los proveedores para comunicar inmediatamente sobre posibles incidentes de seguridad que pudieran afectar directa o indirectamente a la Institución;

d) Obligación de coadyuvancia con las autoridades ante investigaciones por incidentes de seguridad, infracciones o delitos; y

e) Considerar medidas de rescisión y/o responsabilidades legales en caso de que los proveedores o su personal transgredan las políticas y acuerdos de confidencialidad o realicen actividades que, sin autorización de la Institución, expongan la información institucional o incumplan con la legislación en materia de protección de datos personales.

Artículo 4.- En los procesos de gestión de las TIC institucionales, la UTIC deberá:

I. Identificar y actualizar cuando menos una vez al año, la información relativa a la Arquitectura Institucional que soporte la estrategia de TIC en la Institución;

II. Registrar la Arquitectura Institucional a través de la Herramienta, integrando al menos los elementos relativos a la estructura organizacional, planeación, procesos y las tecnologías de información y comunicación; y

III. Coordinar las acciones para integrar y mantener actualizado el Inventario Institucional de bienes y servicios de TIC, así como revisar el Inventario de bienes y servicios de TIC de la APF para evitar la duplicación de esfuerzos o contrataciones.

Artículo 5.- Las Instituciones procurarán que las personas servidoras públicas que colaboren en la gestión, desarrollo e implementación de proyectos de TIC y SI cuenten con formación o experiencia técnica especializada y fomentarán su capacitación en la materia.

TÍTULO SEGUNDO

DE LA PLANEACIÓN DE LAS TIC

CAPÍTULO I

DEL PORTAFOLIO DE PROYECTOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Artículo 6.- Todos los proyectos de TIC que las Instituciones pretendan ejecutar a través de prácticas de desarrollo, implementación propia, o a través de contrataciones, deben apegarse a un proceso de planeación estratégica alineado a las disposiciones del Plan Nacional de Desarrollo y programas que de él deriven, la Estrategia Digital Nacional, así como a la legislación en materia de desarrollo nacional, presupuesto, austeridad y transparencia.

El proceso de planeación de TIC se formaliza con la integración y registro del Portafolio de Proyectos de Tecnologías de la Información y Comunicación (POTIC).

Artículo 7.- El POTIC es el conjunto de proyectos estratégicos y operativos en materia de TIC y de SI que las Instituciones planean llevar a cabo en el siguiente ejercicio fiscal.

Artículo 8.- El POTIC deberá incluir los proyectos que se desarrollen con recursos técnicos y humanos con que cuente la Institución, así como aquellos que requieran ser contratados.

Artículo 9.- A través del POTIC, las Instituciones buscarán, de forma enunciativa mas no limitativa:

1) Contribuir al logro de los objetivos institucionales;
2) Contribuir a la autonomía e independencia tecnológica;
3) Optimizar los recursos técnicos, humanos y económicos;
4) Ser transparente en la gestión gubernamental de las TIC;
5) Fortalecer sus capacidades tecnológicas;
6) Establecer una cultura de seguridad de la información y garantizar la operación;
7) Propiciar un ambiente de innovación basado en el uso de estándares abiertos;
8) Digitalizar trámites previamente simplificados;
9) Dar cumplimiento al marco legal que corresponda;
10) Incorporar las mejores prácticas aplicables a la gestión de las TIC; y
11) Considerar la reducción del impacto ambiental en la definición de los proyectos.

Artículo 10.- En la integración del POTIC, cada Institución definirá la metodología a usar, tomando en consideración, al menos:

a) El tamaño y requerimientos de la Institución;
b) Los mecanismos de coordinación entre Unidades Administrativas;
c) Impacto institucional de las TIC;
d) Arquitectura tecnológica requerida;
e) Activos de información y el MGSI;
f) Sus capacidades técnicas y operativas existentes; y
g) Los Estándares Técnicos de la CEDN.

Artículo 11.- Cada proyecto integrante del POTIC debe concebirse de forma integral, a partir de un estudio completo que permita su correcta definición; y deberá plantearse, al menos con la siguiente información:

a) **Antecedentes.** Descripción del contexto previo al origen del proyecto;
b) **Planteamiento del problema.** Exposición clara y breve del asunto que se requiere atender, incluyendo un diagnóstico general de la problemática;
c) **Justificación.** Descripción puntual de los motivos por los que se debe realizar el proyecto, explicando cómo se determinó el alcance del mismo;
d) **Objetivo.** Descripción de los resultados que se esperan alcanzar mediante la ejecución de las actividades que forman parte del proyecto;
e) **Impacto.** Descripción puntual de la contribución o efecto significativo que producirá la implementación del proyecto en el cumplimiento de los objetivos del Plan Nacional de Desarrollo, el PNCCIMGP, la Estrategia Digital Nacional, así como a los objetivos institucionales y su aporte a la ciudadanía;
f) **Criterios de evaluación.** Descripción de las características observables y medibles definidas por la UTIC, que permitan monitorear y evaluar el logro de los objetivos del proyecto;
g) **Alcance.** Definición general del producto, servicio o resultado que se logrará al término del proyecto;
h) **Arquitectura tecnológica**. Listado detallado de los bienes y servicios de TIC que son considerados como componentes del proyecto;

i) **Fecha de inicio y cierre del proyecto.** Fechas que indican el plazo fijado para la ejecución del proyecto;

j) **Fecha de evaluación del proyecto.** Fecha en la cual se evaluarán los resultados del proyecto;

k) **Presupuesto estimado.** Plan de asignación de recursos financieros para el desarrollo del proyecto, por partida presupuestal; y

l) **Cronograma de hitos del proyecto.** Resumen de las fases del proyecto definidas por la UTIC.

Artículo 12.- Para cada proyecto del POTIC se nombrará un responsable, que deberá cerciorarse de la documentación de cada etapa, su ejercicio en tiempo y forma, así como la aplicación de metodologías adecuadas.

Artículo 13.- Una vez integrado el conjunto de proyectos institucionales de TIC que conformará el POTIC, la persona titular de la UTIC deberá presentarlo ante sus superiores jerárquicos, a fin de revisar que dichos proyectos responden a las prioridades institucionales y, en su caso, realizará los ajustes necesarios.

Artículo 14.- Una vez definido el POTIC, se seguirá el siguiente procedimiento:

I. La UTIC registrará el conjunto de los proyectos integrantes del POTIC en la Herramienta, durante el mes de julio de cada año;

II. La CEDN realizará la revisión correspondiente y en caso de existir observaciones al mismo, podrá requerir a la UTIC para que las solvente en un plazo máximo de 15 días hábiles;

III. La CEDN contará con 15 días hábiles para emitir, en su caso, nuevas observaciones; y

IV. De no existir observaciones por solventar, la CEDN emitirá su Visto Bueno al POTIC a más tardar el 31 de octubre del ejercicio previo a su ejecución.

Artículo 15.- El POTIC que cuente con el Visto Bueno de la CEDN no deberá modificarse, salvo circunstancias excepcionales plenamente justificadas ante la CEDN, por causas tecnológicas o de operación, para lo cual se seguirá el siguiente procedimiento:

I. La UTIC deberá presentar el POTIC modificado a la CEDN entre el 01 de noviembre y el 10 de diciembre del ejercicio previo a su ejecución;

II. La CEDN realizará la revisión y en caso de existir observaciones al mismo, podrá requerir a la UTIC, mismas que deberán ser solventadas en un plazo máximo de 15 días hábiles;

III. La CEDN contará con 15 días hábiles para emitir, en su caso, nuevas observaciones; y

IV. De no existir observaciones por solventar, la CEDN emitirá su Visto Bueno al POTIC a más tardar el 31 de diciembre del ejercicio previo a su ejecución.

Asimismo, las Instituciones podrán presentar modificaciones al POTIC autorizado, durante los primeros 5 días hábiles de cada mes de su ejercicio, teniendo la CEDN un plazo máximo de 15 días hábiles para emitir una respuesta, de emitirse observaciones, se atenderá lo señalado en los numerales II y III de este Artículo.

Artículo 16.- Cuando el POTIC incluya proyectos cuyo inicio se encuentre previsto para el primer trimestre del ejercicio, se estará en el supuesto de una contratación anticipada en términos de la LAASSP; en estos casos, las Instituciones deberán darle prioridad a su registro, atendiendo las siguientes circunstancias:

a) La Institución, deberá remitir a través de la Herramienta, en conjunto todos sus proyectos que impliquen una contratación anticipada durante los primeros 10 días hábiles del mes de julio del ejercicio previo a su ejecución;

b) La CEDN podrá emitir el Visto Bueno a este tipo de proyectos, a más tardar el 31 de agosto siguiente;

c) Las observaciones que pudieran existir a los mismos, deberán ser atendidas por las Instituciones dentro de los 15 días hábiles siguientes a su emisión a través de la Herramienta; una vez solventadas, la CEDN emitirá un nuevo pronunciamiento dentro de los 15 días hábiles siguientes; y

d) De requerirse modificaciones a los proyectos autorizados por la CEDN, se abrirá un periodo para gestionarlas entre el 1 y 30 de septiembre, las cuales podrán ser aprobadas por la CEDN, que emitirá una respuesta a más tardar el 31 de octubre; de no emitirse el Visto Bueno, la CEDN podrá emitir observaciones procediendo en los términos del inciso anterior, que de no atenderse, ocasionará un tratamiento acorde al artículo 15.

Artículo 17.- El POTIC autorizado por la CEDN será el instrumento base y de referencia indispensable para el análisis de las solicitudes de Dictamen Técnico para las contrataciones que en materia de TIC y SI la Institución pretenda llevar a cabo en el ejercicio siguiente.

Artículo 18.- La persona titular de la UTIC tendrá, entre otras, las siguientes responsabilidades respecto del POTIC autorizado con el Visto Bueno de la CEDN:

a) Deberá realizar acciones para la difusión institucional de los proyectos que lo conforman;

b) Dar seguimiento para vigilar la correcta ejecución del POTIC;

c) Asegurarse que las contrataciones que pretendan efectuarse estén consideradas en el POTIC autorizado; así como

d) Instrumentar los mecanismos necesarios para hacer transparente y público el POTIC autorizado.

Artículo 19.- La UTIC deberá observar las siguientes acciones en la ejecución de cada proyecto:

a) El cumplimiento de los hitos de cada proyecto del POTIC deberá actualizarse a través de la Herramienta, dentro de los 10 días hábiles posteriores a la fecha prevista para cada hito; y

b) Remitir un informe final de la implementación en que se incluyan los resultados obtenidos a partir de la evaluación realizada por la UTIC, a través de la Herramienta y dentro de los 3 meses posteriores al cierre de cada proyecto, entendiéndose por éste la aceptación de la totalidad de entregables del mismo.

TÍTULO TERCERO

DE LOS PROCEDIMIENTOS DE CONTRATACIONES DE TECNOLOGÍAS Y SEGURIDAD DE LA INFORMACIÓN

CAPÍTULO I

DEL DICTAMEN TÉCNICO

Artículo 20. El Dictamen Técnico es el documento que emite la CEDN a un proyecto de contratación en materia de TIC y SI que pretenda celebrar una Institución; parte del análisis integral del proyecto y es un requisito indispensable para dar inicio al proceso de contratación.

Artículo 21. Estarán exceptuadas de Dictamen Técnico:

a) Las adquisiciones, arrendamiento y servicios cuyo costo total sea inferior a trescientas veces el valor de la Unidad de Medida y Actualización vigente (UMA); y

b) La adquisición de consumibles y periféricos.

En ambos casos, la Institución deberá comunicar a la CEDN sobre estos supuestos, a través del Informe de Contratación que se señala en el artículo 43 de este Acuerdo.

Artículo 22. Para la emisión del Dictamen Técnico es necesario que la persona titular de la UTIC efectúe la solicitud correspondiente ante la CEDN, adicionalmente, es requisito indispensable que:

I. La UTIC haya enviado a la CEDN el POTIC del ejercicio fiscal al que corresponda, éste se encuentre autorizado por la CEDN y no presente observación alguna pendiente de subsanar;

II. La UTIC haya remitido a la CEDN los Informes de contratación de TIC y SI del ejercicio inmediato anterior; y

III. La contratación para la que se solicita el Dictamen Técnico se encuentre alineada a un proyecto de los que conforman el POTIC correspondiente.

Artículo 23. El trámite para la obtención del Dictamen Técnico iniciará con el registro de la totalidad de los siguientes documentos a través de la Herramienta:

a) **Justificación.** Documento en que se exponen ampliamente los antecedentes, la situación actual y las causas que dan origen a la contratación;

b) **Anexo Técnico.** Documento técnico que describe de forma detallada las especificaciones técnicas y de calidad, así como el alcance de la adquisición, arrendamiento o servicio a contratar;

c) **Resultado de la investigación de mercado.** Documento emitido por el área especializada existente en la dependencia o entidad en que consta el análisis de la información obtenida a partir de la investigación de mercado para la contratación de los servicios, arrendamiento o adquisición de que se trate. Ésta deberá permitir la identificación de los precios estimados de cada componente tecnológico requerido;

d) **Estudio costo beneficio**. Es el documento mediante el cual se analizan las opciones posibles de contratación para adquisiciones, arrendamientos o servicios en particular y se demuestra su viabilidad;

e) **Estudio de factibilidad.** Es el documento que contiene la determinación sobre la conveniencia de adquirir, arrendar bienes o contratar servicios, el cual comprende entre otros, los siguientes elementos: el análisis de las contrataciones vigentes y, en su caso, la procedencia de su renovación; la conveniencia de efectuar su contratación a través de contratos marco o de forma consolidada; así como los costos de mantenimiento, soporte y operación que se deriven de la contratación, vinculados con el factor de temporalidad más adecuado;

f) **Documento de suficiencia presupuestal.** Es el documento emitido por el área de programación y presupuesto u homólogo en las Instituciones, mediante el cual se valida que la unidad ejecutora del gasto calendarizó recursos suficientes en las partidas presupuestales correspondientes, y por lo tanto cuenta con suficiencia de recursos para destinar al compromiso de pago que se derive de una contratación que se pretenda realizar. El presupuesto planeado debe estar en concordancia con el resultado de la investigación de mercado. En el caso de contrataciones anticipadas, podrá suplirse el documento de suficiencia presupuestal con un documento de evidencia de la aprobación presupuestal para la contratación anticipada;

Artículo 24.- En aquellos casos en que el proyecto de contratación que se somete a Dictamen Técnico abarque más de un ejercicio fiscal, deberá remitir adicionalmente el documento de autorización de plurianualidad, o en su caso, aquél que acredite el inicio del trámite para su obtención ante la Unidad Administrativa que corresponda.

Artículo 25.- Cuando por el carácter exclusivo de la contratación de una adquisición, arrendamiento o servicio de TIC y SI exista un único proveedor con la capacidad de ofrecerlo, su participación en el proceso de contratación deberá acreditarse mediante el documento de exclusividad correspondiente, de conformidad con los artículos 41, fracción I de la LAASSP y 72, fracción II de su Reglamento.

Artículo 26.- Cuando se trate de proyectos relacionados con la seguridad de la información, la Institución deberá acreditar y justificar la necesidad de su implementación con base en el MGSI de la Institución.

Artículo 27.- En el caso de Instituciones que pretendan realizar proyectos en materia de TIC y de SI con el carácter de seguridad nacional, será necesario que la información relacionada con los mismos sea valorada por el CNI, a efecto de que éste emita su opinión sobre dicho carácter. Lo anterior, sin perjuicio de la responsabilidad de la Institución solicitante respecto de la veracidad y términos de la justificación presentada.

La opinión emitida por el CNI invariablemente deberá ser incluida en el estudio de factibilidad correspondiente, en el entendido de que, de no justificarse el carácter de seguridad nacional, la institución solicitante deberá reformular su estudio con un carácter distinto.

Lo anterior, con independencia del análisis técnico que realice la CEDN de las especificaciones de las plataformas de hardware y/o software, con la finalidad de determinar su pertinencia, por lo cual, deberán presentar las especificaciones técnicas y documentación señalada en los artículos que anteceden, para emitir el Dictamen Técnico correspondiente.

Artículo 28.- Cuando existan razones justificadas que no permitan a la Institución apegarse a los Estándares Técnicos, deberá contemplarse su justificación dentro del Estudio de Factibilidad de la contratación de que se trate.

Artículo 29.- Una vez integrados dichos documentos, la UTIC deberá remitirlos al OCF respectivo para que los examine y en su caso, emita el oficio de pronunciamiento favorable, o en su defecto las sugerencias u observaciones debidamente fundadas y motivadas, en un plazo de 8 días posteriores a su remisión. Dicho pronunciamiento estará orientado exclusivamente al cumplimiento de los procedimientos y normatividad aplicable en la materia, respetando la competencia técnica de la CEDN.

Artículo 30.- Recibido el pronunciamiento favorable del OCF, podrá dar paso a la solicitud de Dictamen Técnico ante la CEDN, adicionando el oficio de pronunciamiento del OCF a través de la Herramienta.

Artículo 31.- La CEDN analizará cada solicitud de Dictamen Técnico que reciba, en un período máximo de 15 días hábiles, y comunicará su respuesta a la UTIC, la cual podrá ser en los siguientes sentidos:

a) Favorable, con la cual la Institución podrá dar continuidad al proceso de contratación que corresponda;

b) No favorable, en cuyo caso la Institución deberá presentar una nueva solicitud y atender los tiempos señalados para ello;

c) Solicitud de modificación en el alcance; o

d) Requerimiento de Aclaración.

En los supuestos señalados para los incisos c y d, las Instituciones contarán con hasta 15 días hábiles para efectuar la modificación o aclaración que se solicite, en ambos casos la CEDN tendrá hasta 15 días hábiles para efectuar la revisión y emitir una nueva respuesta.

Artículo 32.- Existirá un mecanismo de Dictamen Técnico automático aplicable a contrataciones cuyo importe total se encuentre en el rango de 300 a 1200 UMAS, así como refacciones y suscripciones a revistas o periódicos en línea de cualquier monto; en este caso, la Institución comunicará bajo protesta de decir verdad que cumple y cuenta con los requisitos necesarios señalados en el artículo 23 de este Acuerdo para la contratación expedita del requerimiento, dicho procedimiento se desahogará a través de la sección correspondiente en la Herramienta y será verificado por la CEDN.

Artículo 33.- Cuando se trate de proyectos que por su complejidad operativa o trascendencia, requieran un análisis más amplio, la CEDN podrá convocar la participación del Grupo Técnico, pudiendo ampliar su respuesta para la emisión del Dictamen Técnico hasta por 30 días hábiles.

Artículo 34.- Los Dictámenes Técnicos tendrán vigencia a partir de la fecha de su emisión y hasta el 31 de diciembre del año en que fueron emitidos, perdiendo su validez cuando la Institución solicitante altere o modifique las características técnicas contenidas en el Anexo Técnico y/o la vigencia de la contratación no inicie en el ejercicio fiscal planteado para la ejecución del proyecto, o el periodo considerado para la contratación anticipada.

Artículo 35.- En el caso de contrataciones para adquisiciones, se procederá de conformidad con los Lineamientos en materia de Austeridad Republicana de la APF, remitiéndose a través de la Herramienta, la documentación y el Dictamen Técnico a la Subsecretaría de Egresos de la SHCP para que en el ámbito de sus atribuciones emita el pronunciamiento correspondiente.

CAPÍTULO II

DEL GRUPO TÉCNICO

Artículo 36.- El Grupo Técnico, estará conformado por:

I. Integrantes permanentes, que serán:

- Una persona servidora pública de la CEDN que lo presidirá y será designada por la persona titular de la CEDN;
- Dos personas servidoras públicas de la CEDN, designadas por la presidencia del Grupo Técnico.
- Representante de la Oficialía Mayor de la SHCP;

II. Integrantes invitados, convocados a instancia del presidente del Grupo Técnico, que podrán ser:

- Personas servidoras públicas designadas por la CEDN;
- Titular de la Unidad de Tecnologías de Información y Comunicación de la Institución de que se trate u homólogo;
- Servidores públicos del área contratante de la Institución de que se trate (en caso de ser distinta a la UTIC);
- Titular de la Unidad de Tecnologías de la Información y Comunicación de la cabeza de sector de que se trate u homólogo (en caso de ser aplicable);
- Titular de la Unidad de Administración y Finanzas de la Institución de que se trate u homólogo;
- Titular del OCF de la Institución de que se trate;
- Representante de la Empresa Productiva Subdiaria de la Comisión Federal de Electricidad, CFE Telecomunicaciones e Internet para todos.

Los integrantes permanentes tendrán derecho a voz y voto, mientras que los integrantes invitados solo podrán hacer uso de la voz.

En caso de ausencia plenamente justificada, los servidores públicos invitados deberán nombrar a sus respectivos suplentes para la reunión, mismos que deberán tener el nivel o rango jerárquico inmediato inferior.

Artículo 37.- El Grupo Técnico será convocado a instancia de la presidencia del Grupo Técnico, quien deberá señalar fecha, hora y lugar o medio remoto en que se efectúe la reunión.

Artículo 38.- La reunión del Grupo Técnico, deberá contar con mayoría simple de integrantes permanentes. Los acuerdos se tomarán por mayoría de votos; y en caso de empate, el presidente del Grupo Técnico tendrá voto de calidad.

Artículo 39.- Para cada reunión se elaborará una minuta en que consten los acuerdos tomados, misma que estará firmada por todos los asistentes de manera autógrafa o a través de la Firma Electrónica Avanzada y formará parte de la documentación soporte del Dictamen Técnico de que se trate.

CAPÍTULO III

DE LAS DISPOSICIONES APLICABLES A LOS PROCEDIMIENTOS DE CONTRATACIONES DE TECNOLOGÍAS Y SEGURIDAD DE LA INFORMACIÓN

Artículo 40.- Las contrataciones que las Instituciones realicen para la adquisición de bienes, arrendamientos o prestación de servicios en materia de TIC y SI, deberán contar con un Dictamen Técnico favorable expedido por la CEDN.

Artículo 41.- La persona titular de la UTIC, tendrá en el ámbito de los procedimientos de contrataciones de TIC y SI, entre otras, las siguientes responsabilidades:

a) Coordinar las acciones necesarias para el adecuado ejercicio del presupuesto destinado a las contrataciones de TIC y de SI que realice;

b) Vigilar que los procedimientos de aprobación del POTIC, dictamen técnico y contrataciones se efectúen en tiempo y forma;

c) Acompañar a las unidades contratantes de su Institución en el desarrollo de las contrataciones de TIC y SI;

d) Dar seguimiento al cumplimiento de los contratos de TIC y SI, así como a la normativa aplicable; y

e) La designación de responsables para el seguimiento de cada proyecto que conforme el POTIC.

Artículo 42.- El responsable de cada proyecto del POTIC deberá verificar el cumplimiento de las obligaciones contraídas por el proveedor, realizar la evaluación correspondiente y remitirla a la CEDN a través de la Herramienta de forma semestral, o al término de la contratación si ésta tuviera una duración inferior.

Artículo 43.- La UTIC integrará a través de la Herramienta, un Informe de Contratación con datos de cada uno de los procedimientos de adquisiciones, arrendamientos o servicios de TIC y SI que lleve a cabo, el cual deberá complementar y remitir en los plazos, conforme lo siguiente:

a) Sobre contrataciones formalizadas, la digitalización del contrato, dentro de los 30 días hábiles siguientes a su suscripción;

b) Sobre adquisiciones, arrendamientos o servicios que no impliquen la emisión de un Dictamen Técnico por encontrarse en la excepción señalada en el artículo 21 de este Acuerdo, la documentación que permita comprobar su realización, dentro de los 30 días hábiles siguientes; y

c) Sobre contrataciones que, contando con Dictamen Técnico favorable no se concretaran, la información sobre las razones que impidieron su realización, en el mes de enero del ejercicio fiscal siguiente.

Artículo 44.- De forma periódica y según corresponda a cada proceso de facturación y pago por concepto de adquisiciones, arrendamientos o servicios, la UTIC remitirá constancia fiscal de cada uno de los pagos que efectúe, dentro de los 30 días posteriores a su realización, a través de la Herramienta; los cuales podrán ser verificados con los antecedentes registrados y con los registros que posean otras Instituciones, como medida de transparencia y rendición de cuentas en el ejercicio del presupuesto público correspondiente a las TIC.

TÍTULO CUARTO

POLÍTICAS TECNOLÓGICAS APLICABLES A LOS PROYECTOS DE TIC Y SI

CAPÍTULO I

SERVICIOS EN UN CENTRO DE DATOS

Artículo 45.- Se entenderá por servicios en un centro de datos, el hospedaje de la infraestructura, almacenamiento y procesamiento de datos, conectividad y gestión de aplicativos de cómputo, incluidos servicios en la nube, y la ejecución de respaldos que garanticen la continuidad operativa de la Institución.

Artículo 46.- Las Instituciones deberán privilegiar la operación de Centros de Datos gubernamentales; en caso de no contar con Centros de Datos propios será posible solicitar a otra Institución, preferentemente de su mismo sector, recursos tecnológicos para el alojamiento de su infraestructura, para lo cual deberán formalizarse los instrumentos de colaboración que resulten necesarios.

En caso de no contar con esta disponibilidad, podrán contratarse servicios de Centros de Datos a terceros, procurando que la información se aloje en territorio nacional.

En casos específicos, podrá requerirse la contratación de Servicios en la Nube Pública, en este supuesto, deberán aportarse datos que justifiquen la contratación, dentro del Estudio de Factibilidad.

Artículo 47.- En la operación y administración de servicios de Centros de Datos, las Instituciones deberán observar al menos, lo siguiente:

a) Identificar la capacidad utilizada de su infraestructura, haciendo del conocimiento de la CEDN sus planes de crecimiento y operación, así como la capacidad excedente que pueda ser compartida de manera temporal con otra Institución;

b) Procurar una infraestructura basada en estándares abiertos, compatible con el uso de máquinas virtuales y contenedores, que permita la portabilidad y migración de aplicativos entre Centros de Datos;

c) Establecer la infraestructura y administración de la seguridad de la información en zonas de seguridad física y lógica, considerando identidad, perfiles y privilegios para todo el personal involucrado, de conformidad con los controles de seguridad de la información definidos por cada Institución; así como

d) Asegurar el acceso total y sin restricciones a la información y a los datos de la Institución o bajo su resguardo.

Artículo 48.- En la contratación para el arrendamiento o servicios de hospedaje, gestión u operación de Centros de Datos, se deberán considerar al menos, los siguientes elementos:

a) Usuarios y contraseñas de acceso a las consolas aplicables;

b) La posibilidad de efectuar una migración completa o parcial, hacia un proveedor diferente, hacia infraestructura propia o de otro ente gubernamental;

c) Que durante la contratación y durante la etapa de migración, el proveedor permita a las Instituciones contratantes, el acceso y disposición sin restricciones a la información y datos comprendidos en los servicios objeto del contrato; y

d) Que al término de la contratación, el proveedor entregue a la Institución:

   i. La totalidad de la información y datos comprendidos en los servicios contratados;

   ii. El inventario de servicios, usuarios, grupos y roles actualizados, incluyendo contraseñas vigentes a todas las consolas que forman parte de los servicios contratados; así como

   iii. Las Arquitecturas, diagramas y documentación de soporte de los servicios contratados.

Artículo 49.- Las migraciones que las Instituciones lleven a cabo desde su infraestructura hacia la infraestructura de un proveedor, o bien entre las infraestructuras de diferentes proveedores, o en su caso, de la infraestructura de un proveedor hacia infraestructura gubernamental, deberán considerar como mínimo los aspectos técnicos que aseguren a favor de la Institución la adecuada prestación de los servicios y la correcta ejecución de la migración, considerando al menos, los siguientes aspectos:

a) Continuidad de sus servicios tecnológicos, sin interrupciones;

b) La adecuada planeación administrativa que permita disponer de la infraestructura propia o contratada para efectuar la migración de servicios tecnológicos en los tiempos programados;

c) Autonomía técnica para efectuar la migración por sí o a través de terceros; y

d) Que se genere una memoria técnica de la migración en la cual se detallen las conexiones, arquitectura y otros elementos técnicos que permitan replicar el proceso, de considerarse necesario.

CAPÍTULO II

REDES DE DATOS Y SERVICIOS DE INTERNET

Artículo 50.- Los servicios de internet corporativo o de internet de oficinas remotas que contraten las Instituciones deberán cumplir con los Estándares Técnicos de la CEDN.

Artículo 51.- Las instituciones deberán adoptar las medidas para migrar sus servicios de telecomunicaciones hacia el protocolo de internet IPV6, de conformidad con la guía que para tal efecto emita la CEDN; mientras tanto, podrán utilizar el Protocolo de Internet IPv4 en aquellos servicios que sean expuestos tales como correo electrónico, transferencia de archivos, conexiones seguras y aplicaciones web.

Artículo 52.- Todas las Instituciones deberán solicitar ante la autoridad NIC México el número de ASN de IPv6; y deberán solicitar a sus proveedores de servicios la capacidad de ruteo de ASN. La gestión de la solicitud deberá notificarse a la CEDN a través de la Herramienta, adicionalmente, registrarán la solicitud de los nombres en el dominio gob.mx especificando su vigencia y propósito.

Artículo 53.- Las Instituciones deberán privilegiar la implementación de servicios de redes de telecomunicaciones proporcionados por otras Instituciones que cuenten con la capacidad técnica para hacerlo, con apego a los Estándares Técnicos de la CEDN.

Artículo 54 .- Las instituciones deberán, ante el uso compartido de redes de comunicaciones, considerar al menos los siguientes elementos:

a) Mecanismos y políticas de seguridad;

b) Protocolos de actuación en contingencias;

c) Niveles de servicios;

d) Identificación de vulnerabilidades; así como

e) Requisitos de gestión de todos los servicios de red.

Los cuales deberán estar contemplados en los Instrumentos de colaboración y contratos de servicios de red que se celebren.

Artículo 55.- Las redes institucionales deberán segmentarse, separando los servicios de información, usuarios y sistemas en diferentes redes.

Artículo 56.- El intercambio de información que utilice la red de internet como transporte, debe hacerse a través de mecanismos de autenticación y cifrado mediante firmas digitales, certificados digitales o infraestructura de llaves públicas;

CAPÍTULO III

CORREO ELECTRÓNICO

Artículo 57.- Los servicios institucionales de correo electrónico deberán considerar al menos:

a) La inserción de una leyenda de confidencialidad de la información en los correos institucionales emitidos;

b) El control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios;

c) Soluciones de filtrado para correo no deseado o correo no solicitado, así como programas informáticos que protejan del envío y recepción de correos electrónicos con software malicioso;

d) Técnicas de autenticación de correo electrónico que permita al receptor comprobar que un correo electrónico fue enviado y autorizado por la Institución poseedora del dominio;

e) Que el envío por internet se realice con mecanismos de cifrado de la información; así como

f) Contar con los mecanismos necesarios para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos.

Adicionalmente, cuando los servicios de correo electrónico sean contratados a un proveedor, éste deberá garantizar, al menos:

I. Que la Institución podrá acceder y tener a su disposición la totalidad de los correos contenidos en las carpetas de los usuarios, durante la vigencia de la contratación y al término de ésta, en el formato establecido en los Estándares Técnicos; y entregar un respaldo de los mismos en medio no editable;

II. La suscripción de un Acuerdo de Confidencialidad respecto de la información y datos personales relacionados con los correos electrónicos y usuarios del servicio prestado, el cual deberá prevenir efectos legales durante y después de la vigencia del contrato;

III. Que concluida la vigencia de los servicios contratados y una vez entregado el respaldo a la Institución, se elimine toda información y contenido de los correos electrónicos institucionales en la infraestructura del proveedor; y

IV. Que los procedimientos de borrado seguro se efectúen ante la supervisión de servidores públicos de la Institución y se genere evidencia de su realización.

CAPÍTULO IV

APLICATIVOS DE CÓMPUTO

Artículo 58.- Se entenderá por Aplicativo de Cómputo, el software y/o los sistemas informáticos que se conforman por un conjunto de componentes o programas construidos con herramientas que habilitan una funcionalidad o digitalizan un proceso, de acuerdo con los requerimientos previamente definidos;

Artículo 59.- La persona titular de la UTIC será responsable de que todos los aplicativos de cómputo desarrollados o financiados por la Institución se encuentren registrados en el Inventario de bienes y servicios de TIC de la APF y su código fuente se encuentre siempre actualizado y disponible en el repositorio de software de la APF.

Artículo 60.- En todo proyecto relacionado con el desarrollo y mantenimiento de aplicativos de cómputo, deberá considerarse el Inventario de bienes y servicios de TIC de la APF y el repositorio de software de la APF, a fin de evitar duplicidades y maximizar el aprovechamiento de los existentes;

Artículo 61.- Las Instituciones podrán implementar aplicativos de cómputo de propósito general provenientes de repositorios públicos de software libre, siempre que tengan las características requeridas para el ejercicio de las funciones públicas y representen un beneficio tecnológico que genere ahorros reales para el Estado mexicano. A su vez, las Instituciones podrán colaborar con proyectos e iniciativas de desarrollo de software libre de conformidad con la normatividad mexicana en la materia.

Artículo 62.- La titularidad y disposición de los aplicativos de cómputo y la totalidad de sus componentes tales como el código fuente, el código objeto, el diseño físico y lógico, los diagramas de operación y de la arquitectura tecnológica, la imagen institucional, los manuales técnicos y de usuario, desarrollados por personal de la Institución o por terceros que se financien con recursos públicos federales, deberá asegurarse en favor del Estado Mexicano, el cual podrá a su vez, otorgar licencias de uso, copia, modificación y/o distribución, de conformidad con la legislación aplicable en la materia.

Artículo 63.- Cuando se trate de desarrollos basados en software libre, se respetarán las condiciones de su licenciamiento original, y las Instituciones deberán documentar la contribución que en el ámbito de sus atribuciones efectuaron a dicho software libre, justificando la utilidad pública de dicha intervención.

Artículo 64.- En las actividades de desarrollo y mantenimiento de aplicativos de cómputo que se realicen por personal interno de la Institución o por proveedores, deberán aplicarse las metodologías más adecuadas en función de las características del proyecto, considerando en los casos que se determine viable, un enfoque de desarrollo ágil de software que permita generar entregas tempranas de software funcional, seguro y con integración continua, favoreciendo la obtención de productos que se implementen en el corto plazo.

En todos los casos, deberá generarse la documentación indispensable que mantenga y enlace el diseño, la codificación y la calidad del software.

Artículo 65.- Los procesos de desarrollo y mantenimiento de aplicativos de cómputo deberán seguir un modelo de arquitectura de software que genere aplicaciones reutilizables e interoperables entre las áreas de la Institución y otras Instituciones, asimismo, deberán privilegiar el uso de lenguajes de programación y las plataformas de desarrollo basadas en software libre y estándares abiertos que se establezcan en los Estándares Técnicos.

Artículo 66.- Las Instituciones deberán observar en sus procesos de desarrollo y mantenimiento de aplicativos de cómputo, los estándares técnicos en materia de datos abiertos, con el propósito de homologar sus características y facilitar su acceso, uso, reutilización y distribución para cualquier fin, conforme con los ordenamientos jurídicos aplicables.

Artículo 67.- Los proyectos de servicios de desarrollo o mantenimiento de software deberán incluir el diseño detallado o conceptual del aplicativo a desarrollar, que comprenda por lo menos:

a) Requerimientos del negocio;

b) Mecanismos o esquemas de seguridad de la información;

c) Políticas de privacidad y protección de datos personales, de conformidad con la legislación aplicable;

d) Alcance de los módulos;

e) Perfiles de usuario;

f) Matriz de trazabilidad;

g) Protocolos de pruebas y;

h) Mecanismos de autenticación a través de la Firma Electrónica Avanzada (e-firma), cuando resulte aplicable.

Artículo 68.- Los nuevos desarrollos de software deberán considerar la información estructurada disponible en la Institución, a fin de disminuir su dispersión y duplicidad. Para ello deberán fomentarse bases de datos institucionales que concentren, compartan y estandaricen la información de los sistemas gubernamentales.

Artículo 69.- Los aplicativos de cómputo que operen sobre datos críticos, confidenciales o sensibles, deberán garantizar que el procesamiento y transferencia de la información se realice a través de mecanismos que garanticen su seguridad e integridad, como priorizar su alojamiento en territorio nacional. Para ello, deberán atender los Estándares Técnicos emitidos por la CEDN, la legislación en materia de protección de datos personales y las disposiciones que sean emitidas en materia de Seguridad Nacional.

Artículo 70.- El desarrollo de sistemas electrónicos de trámites y servicios deberá priorizar los procesos de digitalización que permitan proveer trámites digitales simplificados y con utilidad social, así como los que formen parte del Expediente de Trámites y Servicios que se deriva de la Ley General de Mejora Regulatoria.

Artículo 71.- Los aplicativos de cómputo o servicios de TIC y de seguridad de la información, deberán contemplar como campo llave para su interoperabilidad, la Clave Única de Registro de Población (CURP) o el RFC al tratarse de personas físicas o el Folio Mercantil en el caso de personas morales y, en su caso, otros atributos que permitan realizar la autenticación electrónica correspondiente, como lo es la Firma Electrónica Avanzada (e-firma), en todos los casos, deberán preverse medidas de protección a los datos personales, de conformidad con la legislación aplicable.

Artículo 72.- El diseño de nuevas soluciones tecnológicas y servicios de TIC deberá cumplir con la normativa técnica de domicilios geográficos del Instituto Nacional de Estadística y Geografía (INEGI).

CAPÍTULO V

PLATAFORMAS DIGITALES DE PÁGINAS WEB

Artículo 73.- Todas las Instituciones deberán estandarizar la estructura e imagen de sus sitios web apegándose a la identidad gráfica del gobierno federal, de acuerdo con las guías, manuales y documentos técnicos emitidos por la Coordinación General de Comunicación Social y la CEDN.

Artículo 74.- La implementación de todos los servicios de plataformas digitales de páginas web que realicen las Instituciones, deberá observar, al menos lo siguiente:

I. Considerar la aplicación de los Estándares Técnicos de la CEDN en materia de arquitecturas de desarrollo e interoperabilidad, y servicios de hospedaje;

II. Aplicar las mejores prácticas para el desarrollo de plataformas web, como los estándares y recomendaciones del Consorcio de la Red Informática Mundial (W3C, World Wide Web Consortium) relativos a uso de lenguajes de marcado, hojas de estilo, accesibilidad web y validadores;

III. Compatibilidad con todos los navegadores actuales y de nuevas generaciones, así como con sistemas operativos móviles y sus navegadores;

IV. Contar con versiones de páginas web adaptables a las resoluciones de dispositivos móviles;

V. Incluir funciones de accesibilidad para personas con discapacidad, de conformidad con los Estándares Técnicos de la CEDN;

VI. Incluir Aviso de privacidad, así como términos y condiciones de uso claros y actualizados, en los términos de la legislación aplicable; así como

VII. Garantizar que el acceso a las plataformas digitales de páginas web se realice a través de mecanismos de autenticación y cifrado mediante certificados digitales.

CAPÍTULO VI

SEGURIDAD DE LA INFORMACIÓN

Artículo 75.- Las Instituciones deberán contar con un Marco de Gestión de Seguridad de la Información (MGSI) alineado a la política general de SI, que procure los máximos niveles de confidencialidad, integridad y disponibilidad de la información generada, recibida, procesada, almacenada y compartida por dichas Instituciones, a través de sus sistemas, aplicaciones, infraestructura y personal; dicho MGSI deberá contribuir al cumplimiento de los objetivos institucionales, de TIC, regulatorios, organizacionales, operativos y de cultura de la seguridad de la información.

La política general de seguridad de la información está orientada a garantizar certidumbre en la continuidad de la operación y la permanencia e integridad de la información institucional.

Artículo 76.- El MGSI deberá conformarse, al menos por los siguientes elementos:

a) El establecimiento de objetivos alineados a la política general de seguridad de la información;

b) La identificación de los procesos y activos esenciales de la Institución, a través de un diagnóstico que involucre a las áreas que participan en la gestión de la información;

c) Elaboración de un análisis de riesgos para identificar las amenazas y vulnerabilidades;

d) La implementación de los controles mínimos de seguridad de la información, con base en la clasificación de los activos de información institucionales, y de conformidad con los Estándares Técnicos de la CEDN;

e) Programa de gestión de vulnerabilidades, que incluya su identificación, evaluación y corrección. La identificación de las mismas deberá partir de un análisis de vulnerabilidades al interior de la Institución, así como de las alertas o investigaciones de seguridad divulgadas por fuentes externas;

f) Un protocolo de respuesta ante incidentes de seguridad de la información, que contemple la conformación de un Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC), acciones de preparación, detección y análisis, contención, erradicación y recuperación, así como actividades posteriores al incidente, de conformidad con el Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;

g) Plan de continuidad de operaciones y plan de recuperación ante desastres que consideren los aspectos para el restablecimiento de la operación de TIC, la información y los servicios;

h) Los mecanismos de supervisión y evaluación que permitan medir la efectividad de los controles de SI y de madurez institucional en la gestión de SI;

i) Un Programa de formación en la cultura de la seguridad de la información para las personas servidoras públicas de la Institución; así como

j) Un Programa de implementación del MGSI que considere los incisos anteriores.

Lo anterior, con base en procesos de planeación, implementación, supervisión y mejora continua.

Con la información y documentos generados, la UTIC deberá completar la información requerida a través de la Herramienta en la sección correspondiente al MGSI.

Artículo 77.- En cada Institución, la persona titular de la UTIC tendrá el rol de Responsable de la Seguridad de la Información (RSI), a excepción de las Instituciones que por su legislación específica o estructura organizacional cuenten con un área de Seguridad de la Información que no dependa de la UTIC, en dichos casos el rol de Responsable recaerá en la persona titular del área de Seguridad de la Información.

Artículo 78.- El RSI creará grupos de trabajo para la definición, implementación y evaluación del MGSI, los cuales se conformarán por la persona titular de la UTIC, los servidores públicos involucrados en la operación institucional y procesos relacionados con la seguridad de la información, y el RSI cuando este rol no recaiga en la persona titular de la UTIC. Cada grupo de trabajo documentará sus objetivos, actividades y definirá los roles de los servidores públicos que formen parte del mismo.

Artículo 79.- El RSI, tendrá entre otras, las siguientes responsabilidades:

I. Dar seguimiento a la conformación del MGSI, así como a su implementación y al cumplimiento de los controles mínimos de seguridad;

II. Presentar a sus superiores jerárquicos, incluido el titular de la Institución, un informe sobre la integración del MGSI, con la finalidad de comunicar su contenido y mecanismos de ejecución. En la presentación deberá considerarse la presencia de la persona titular de la UTIC cuando el rol de RSI no recaiga en éste;

III. Dar aviso inmediato a la CEDN sobre los incidentes de seguridad de la información que se presenten, y asegurarse del cumplimiento del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;

IV. Implementar un programa de evaluaciones, que contemple al menos, una evaluación trimestral del MGSI para verificar el desempeño de los controles de seguridad y determinar acciones de mejora;

V. Hacer del conocimiento del OCF en la institución y/o de las autoridades competentes, las irregularidades u omisiones en cumplimiento del MGSI, o delitos relacionados con la seguridad de la información en que incurran las personas servidoras públicas, y en su caso los proveedores y su personal, obligados a su observancia; así como

VI. Mantener un proceso de mejora continua del MGSI para cumplir con las disposiciones aplicables.

Artículo 80.- En aquellos casos en que la Institución requiera, para su operación y adecuada implementación del MGSI, efectuar una contratación para la adquisición, arrendamiento o prestación de servicios en materia de SI, dicha contratación deberá ser justificada y realizarse de conformidad con el proceso de planeación y dictamen que se detallan en los Títulos Segundo y Tercero de este Acuerdo.

Artículo 81.- El proceso de mejora continua del MGSI será revisado por la CEDN bajo las siguientes directrices:

I. En enero y julio de cada ejercicio, la Institución deberá actualizar en la Herramienta, la documentación del MGSI, e incorporar, adicionalmente, un informe que contenga el resultado de las evaluaciones efectuadas a los controles de seguridad y la descripción de las acciones de mejora implementadas en el último semestre;

II. Dicha información será revisada por la CEDN, que podrá emitir en cualquier momento, las observaciones que considere pertinentes, otorgando a las Instituciones, un plazo de hasta 15 días para solventarlas;

III. La CEDN podrá sugerir a las Instituciones la realización de evaluaciones técnicas adicionales, así como su colaboración para efectuarlas, con la finalidad de favorecer los máximos umbrales posibles en la eficacia del MGSI; así como

IV. Las recomendaciones que emita la CEDN deberán ser atendidas por la Institución.

TÍTULO QUINTO

DISPOSICIONES SUPLEMENTARIAS

CAPÍTULO I

INTERPRETACIÓN, SEGUIMIENTO Y VIGILANCIA

Artículo 82.- La interpretación del presente Acuerdo, para efectos administrativos, así como la resolución de los casos no previstos en el mismo, corresponderá a la CEDN.

Artículo 83.- La persona titular de la CEDN podrá auxiliarse y/o delegar en el personal que considere necesario, las funciones y/o atribuciones en materia de Gobierno Digital para la ejecución y supervisión de las políticas y disposiciones contenidas en el presente Acuerdo.

Artículo 84.- La CEDN podrá proporcionar asistencia en la aplicación de las disposiciones contenidas en el presente Acuerdo, conforme a los criterios técnicos, metodologías, guías, y demás instrumentos análogos que emita para tal efecto.

Artículo 85.- La CEDN, en ejercicio de sus atribuciones, podrá modificar, ampliar o suspender las fechas y términos previstos en este Acuerdo, así como definir los mecanismos de operación alternativos al uso de la Herramienta en caso de requerirse, lo que deberá comunicar oportunamente a las Instituciones.

Artículo 86.- Las recomendaciones que emita la CEDN derivadas de la aplicación y validación de las disposiciones contenidas en este Acuerdo son de carácter técnico y de ninguna manera sustituyen disposiciones generales y específicas que deba implementar la Institución para dar cumplimiento a lo establecido en la normativa, así como la atención de auditorías y otros instrumentos de fiscalización o rendición de cuentas.

Artículo 87.- La CEDN actualizará al menos una vez al año los Estándares Técnicos que estarán disponibles en el sitio https://www.gob.mx/wikiguias/ para lo cual podrá convocar la participación de servidores públicos adscritos a las unidades de TIC y de SI de las Instituciones.

Artículo 88.- La CEDN emitirá los manuales, guías, instructivos y demás instrumentos análogos que se deriven o complementen las políticas y disposiciones señaladas en el presente Acuerdo, y establecerá los medios de comunicación o herramientas para su operación.

Artículo 89.- En todos los casos, la CEDN podrá solicitar a la UTIC los informes que considere necesarios, entre ellos los relativos al POTIC, contrataciones e implementación de proyectos.

Artículo 90.- La CEDN podrá, por incumplimiento de las disposiciones contenidas en el presente Acuerdo, dar vista a las autoridades competentes para que éstas inicien las investigaciones correspondientes.

Artículo 91.- Los OCF y los Titulares de Administración y Finanzas u homólogos de las Instituciones, vigilarán en el ámbito de sus atribuciones, el cumplimiento de lo dispuesto por el presente Acuerdo.

TRANSITORIOS

PRIMERO.- El presente Acuerdo entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

SEGUNDO.- Se abroga el Acuerdo por el que se expide el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, publicado en el Diario Oficial de la Federación el 08 de mayo de 2014 y sus reformas del 04 de febrero de 2016 y del 23 de julio de 2018, así como su ANEXO ÚNICO "Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información".

TERCERO.- Quedan sin efecto las disposiciones administrativas que se opongan a lo establecido en este Acuerdo.

CUARTO.- Las referencias que en cualquier guía, manual, lineamiento o disposición administrativa se hacen al Acuerdo que se abroga o a sus reformas, se entenderán hechas al Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal.

Las disposiciones y políticas de las Instituciones relativas al uso y aprovechamiento de la informática, el gobierno digital y las tecnologías de la información y comunicación, deberán armonizarse al contenido de este Acuerdo, dentro de los 120 días siguientes a su publicación.

QUINTO.- Las Instituciones que a la entrada en vigor del presente Acuerdo, cuenten con contratos vigentes en materia de TIC y SI, se sujetarán a lo establecido en los mismos, así como a las disposiciones conforme a las cuales se hayan celebrado.

SEXTO.- Todos los procesos, proyectos, trámites, autorizaciones y demás actos iniciados durante la vigencia del Acuerdo que se abroga deberán concluirse conforme a lo previsto en el mismo y a las disposiciones que resulten aplicables.

SÉPTIMO.- La Cartera Ejecutiva de Proyectos de TIC aprobada para el ejercicio fiscal en curso continuará vigente hasta la conclusión del mismo, sin embargo, las Instituciones deberán llevar a cabo el proceso de planeación y la integración del POTIC señalados en este Acuerdo conforme los plazos indicados, los cuales excepcionalmente, pueden ser modificados en el primer año de su aplicación, circunstancia que será comunicada por la CEDN a las Instituciones. Para tal efecto, la CEDN definirá las plataformas o mecanismos que serán utilizados.

OCTAVO.- El primer Informe de Contratación que realicen las Instituciones deberá comprender la totalidad de los procedimientos para la adquisición, arrendamientos y servicios de TIC y SI realizados en el ejercicio fiscal que corresponda a la entrada en vigor de este Acuerdo.

NOVENO.- El MGSI de cada Institución deberá integrarse y remitirse a través de la Herramienta en un plazo de 120 días hábiles a partir de la publicación de este Acuerdo.

DÉCIMO.- La CEDN emitirá la Guía para la migración al Protocolo de Internet versión 6; dentro de los tres meses posteriores a la publicación de este Acuerdo, a partir de esa fecha, las Instituciones contarán con un plazo de 2 años para concretar la migración de sus servicios de telecomunicaciones.

DÉCIMO PRIMERO.- A partir de la publicación de este Acuerdo, las Instituciones deberán iniciar la conformación del Inventario de bienes y servicios de TIC con la información que derive de sus contratos vigentes, el cual actualizarán con los bienes y servicios de TIC propiedad de la Institución y los que corresponda a sus proyectos de desarrollo propio durante los 6 meses posteriores a su entrada en vigor.

DÉCIMO SEGUNDO.- Las Instituciones realizarán la primera actualización de la Arquitectura Institucional, dentro de los 3 meses posteriores a la publicación de este Acuerdo.

Ciudad de México, a 15 de agosto de 2021.- El Coordinador de Estrategia Digital Nacional de la Oficina de la Presidencia de la República, **Carlos Emiliano Calderón Mercado**.- Rúbrica.