IEM
INSTITUTO ELECTORAL DE MICHOACÁN

MANUAL DE ORGANIZACIÓN Y PROCEDIMIENTOS

de la Coordinación de Informática del Instituto Electoral de Michoacán

Contenido

1. Introducción

Este manual ha sido diseñado para proporcionar una visión detallada de la estructura, funciones y responsabilidades de la Coordinación de Informática dentro del Instituto Electoral de Michoacán. Su objetivo principal es servir como una guía de referencia para todos los miembros del equipo, brindando información clara y precisa sobre los procesos, políticas y procedimientos específicos que se deben seguir en el ámbito informático.

En este manual, se cuenta con una descripción completa de la misión y visión de la Coordinación de Informática, así como de sus objetivos estratégicos. Asimismo, se detalla la estructura organizativa de la Coordinación de Informática, desde la persona Titular de la Coordinación hasta los diferentes equipos y roles especializados, lo que permitirá comprender cómo se toman las decisiones y cómo se gestionan los recursos y proyectos.

Además, se presenta el detalle de las políticas y procedimientos clave relacionados con la seguridad de la información, la gestión de sistemas y redes, el desarrollo de software, la adquisición de equipos y tecnología, y otras actividades relevantes. Estas directrices aseguran que todos los miembros del equipo sigan las prácticas y estándares adecuados, garantizando la integridad, confidencialidad y disponibilidad de los sistemas y datos electorales.

Este manual se mantendrá actualizado de acuerdo con los avances y cambios en el ámbito tecnológico y las necesidades del IEM. Nuestra intención es que sirva como una referencia confiable y actualizada para todos los miembros de la Coordinación de Informática y personal de Instituto, permitiéndoles desempeñar sus funciones de manera eficiente, efectiva y en línea con los principios y estándares del Instituto Electoral de Michoacán.

1.1. Propósito del Manual

El presente manual tiene como objetivo proporcionar una guía clara y estructurada sobre la Coordinación de Informática del Instituto Electoral de Michoacán. Su propósito es establecer las políticas, procedimientos y responsabilidades relacionadas con la gestión de los recursos informáticos y la infraestructura tecnológica.

1.2. Alcance del Manual

El alcance del manual abarca todas las actividades relacionadas con la Coordinación de Informática del Instituto Electoral de Michoacán, incluyendo el desarrollo y mantenimiento de sistemas, la administración de redes y comunicaciones, el soporte técnico, la seguridad de la información, la gestión de proyectos informáticos, la gestión de activos de TI y la mejora continua.

1.3. Definiciones y Acrónimos

Se incluye un glosario de términos y acrónimos relevantes en el anexo 8.1 para facilitar la comprensión de los conceptos utilizados en el manual.

2. Antecedentes

El 30 de junio de 2016 el Consejo General del Instituto Electoral de Michoacán mediante acuerdo IEM-CG/15/2016, aprobó la estructura organizacional del Instituto Electoral de Michoacán, así como las cédulas de los cargos y puestos para el personal del Servicio Profesional y de la Rama Administrativa, a fin de dar cumplimiento al artículo séptimo transitorio del Estatuto del Servicio Profesional Electoral Nacional y del personal de la Rama Administrativa; donde se hace la denominación de puestos de acuerdo con el Catálogo de cargos y puestos, estableciendo lo siguiente:

a) Las Vocalías pasan a ser Direcciones Ejecutivas
b) Las Jefaturas de Departamento pasan a ser Coordinaciones
c) Se crearon los Departamentos que dependen de las Coordinaciones, asignados como Técnicos

En atención a esta modificación orgánica el Departamento de Sistemas paso a ser la Coordinación de Informática misma que depende directamente de la Presidencia del IEM.

El 16 de julio de 2020, mediante acuerdo No. IEM-CG-30/2020, el Consejo del Instituto Electoral de Michoacán aprobó la modificación al reglamento interior del IEM, que establece la creación de 3 áreas Técnicas al interior de la Coordinación de Informática quedando estructurada como a continuación se describe:

a) Persona Técnica de Desarrollo e Innovación Tecnológica.
b) Persona Técnica de Publicación Digital, Plataformas Web y Archivo Documental.
c) Persona Técnica de Capacitación, Mantenimiento y Soporte Técnico.
d) Adicionalmente, cada técnico contará con un auxiliar para el desarrollo de sus funciones, lo que se atenderá en base a la disponibilidad presupuestal.

3. Marco Jurídico

De manera enunciativa, más no limitativa, se indican las siguientes disposiciones que sustentan las atribuciones de la Coordinación de Informática.

Constitución Política de los Estados Unidos Mexicanos (CPEUM)

Artículo 41, Base V, apartado C.

Ley General de Instituciones y Procedimientos Electorales (LGIPE)

Artículo 98, numeral 1.

Constitución Política del Estado Libre y Soberano de Michoacán de Ocampo

Sección IV, Artículo 98.

Código Electoral del Estados de Michoacán de Ocampo (CEEMO)

Artículo 29.

Ley de Gobierno Digital del Estado de Michoacán de Ocampo

Reglamento Interior del IEM

Sección 4ª Artículos 31, 32, 32 bis, 32 ter y 32 quater.

4. Estructura Organizativa

4.1. Misión de la Coordinación de Informática

La misión de la Coordinación de Informática es proporcionar servicios y soluciones tecnológicas eficientes, confiables y seguras que apoyen los procesos electorales y fortalezcan la transparencia, integridad y confiabilidad de los sistemas de información del Instituto Electoral de Michoacán.

4.2. Visión de la Coordinación de Informática

La visión de la Coordinación de Informática es ser un referente en el uso estratégico de la tecnología de la información, promoviendo la innovación, la calidad y la mejora continua en el ámbito electoral de Michoacán.

4.3. Funciones y Responsabilidades

4.3.1. De la Coordinación de Informática

La Coordinación de Informática, deberá planear, operar y vigilar el funcionamiento del sistema informático para que las diferentes áreas del Instituto cumplan

oportunamente con el desarrollo de sus actividades, a través de innovaciones en la materia, para lo cual cuenta con las siguientes atribuciones:

I. Elaborar normas y políticas en materia de informática y telecomunicaciones del Instituto;
II. Diseñar y elaborar los sistemas de información interna que se requieran, de conformidad con las prioridades del Instituto;
III. Operar los sistemas de información automatizados en las diversas áreas del Instituto y participar en la capacitación de su personal para el manejo de los equipos y la operación de los programas;
IV. Elaborar los mecanismos y procedimientos informáticos, que permitan al Instituto estar a la vanguardia en la aplicación y uso de sistemas electrónicos que favorezcan los procedimientos internos del Instituto;
V. Proponer programas que permitan modernizar, agilizar y optimizar los procesos en materia electoral;
VI. Garantizar la trasmisión de sesiones del Consejo General, a través de la página oficial del Instituto;
VII. Revisar y mantener actualizado el archivo electrónico del Instituto;
VIII. Vigilar la actualización del archivo documental electrónico del Instituto;
IX. Elaborar y programar el soporte técnico, así como el mantenimiento preventivo y correctivo de los equipos al servicio del Instituto;
X. Realizar y coordinar el trabajo, que en materia de informática y de sistemas, requieran la Secretaría Ejecutiva y las Direcciones Ejecutivas del Instituto;
XI. Auxiliar a las áreas del Instituto en la solución de problemas técnicos en materia de cómputo e informática; así como en la creación de tecnologías y proyectos informáticos;
XII. Revisar técnicamente y desahogar las consultas que, en la materia de su competencia, le planteen los Órganos Desconcentrados del Instituto;
XIII. Coadyuvar en la elaboración de la urna electrónica; así como la operación del voto electrónico de los Michoacanos en el extranjero;
XIV. Proponer y elaborar programas de mantenimiento preventivo del equipo de cómputo;

XV. Vigilar la adecuada utilización de los equipos de cómputo, la adquisición y renovación de las licencias o en su caso, regular el uso de programas, así como su actualización y mantenimiento;

XVI. Adoptar y proponer las medidas de seguridad necesarias para salvaguardar el archivo digital del Instituto cuando corresponda;

XVII. Realizar el diseño, dar mantenimiento e incluir la información que, por determinación legal, debe estar a disposición de la ciudadanía, así como la demás que sea emitida por las áreas del Instituto, respecto a la página de Internet Oficial;

XVIII. Rendir los informes que le sean solicitados por el Consejo General, los Consejeros, la Junta o el Presidente;

XIX. Coordinar la operación del sistema informático del Programas de Resultados Electorales Preliminares en concordancia con las reglas, lineamientos y criterios aplicables, en el caso de que lo implemente el Instituto;

XX. Proponer al Consejo General la utilización del modelo o sistema electrónico para la recepción del voto, cuando sea factible su utilización;

XXI. Implementar instrumentos electrónicos o tecnológicos en el desarrollo de los mecanismos de participación ciudadana que le competan, con base en las medidas de certeza y seguridad que se estimen pertinentes;

XXII. Implementar el sistema electrónico para la recepción del voto debiendo garantizar la certeza, seguridad, transparencia y apego a los principios de la integridad del voto, así como ofrecer inmediatez en los resultados y transmisión de estos;

XXIII. Realizar un estudio de viabilidad para la adquisición o arrendamiento de equipo de cómputo requerido por el Instituto;

XXIV. Supervisar y dar seguimiento a las actividades realizadas por el personal de la Coordinación; y,

XXV. Las demás que establezca la normativa aplicable.

4.3.1. De la Persona Técnica de Desarrollo e Innovación Tecnológica

La persona técnica de desarrollo e innovación tecnológica se encargará de diseñar, elaborar, implementar, sistematizar, dar mantenimiento y operar todos los sistemas que se requieran desarrollar en el Instituto, para ello contará con las siguientes atribuciones:

I. Realizar estudios, análisis, diseños, desarrollos, implementaciones, mantenimiento y expansiones para la infraestructura en materia de tecnologías de la información y comunicaciones que las distintas áreas del Instituto le soliciten;
II. Desarrollar, implementar y operar los sistemas de información que requieran las áreas que integran el Instituto, para facilitar sus tareas habituales y optimizar recursos;
III. Implementar medidas de seguridad informática en los servicios de red disponibles en el Instituto;
IV. Investigar, analizar de manera permanente, nuevas tecnologías en materia de informática y telecomunicaciones que puedan ser aplicadas en las tareas del Instituto;
V. Proponer programas que permitan modernizar, agilizar y optimizar los procesos en materia electoral;
VI. Elaborar los mecanismos y procedimientos informáticos, que permitan al Instituto estar a la vanguardia en la aplicación y uso de sistemas electrónicos que favorezcan los procedimientos internos del Instituto;
VII. Diseñar, desarrollar, implementar y dar mantenimiento a los sistemas informáticos relacionados con el Proceso Electoral;
VIII. Elaborar el sistema electrónico para la recepción del voto;
IX. Coadyuvar en la elaboración de la urna electrónica y en la operación del voto electrónico de los Michoacanos en el extranjero;
X. Implementar y desarrollar los mecanismos de seguridad necesarios a efecto de generar el Programa de Resultados Electorales Preliminares, en el caso de que lo implemente el instituto;

XI. Efectuar estudios de viabilidad para la definición de los recursos, equipo y sistemas de cómputo que requiera el Programa de Resultados Electorales Preliminares, en caso de que lo implemente el Instituto;

XII. Capacitar al personal en el uso de sistemas y equipos de comunicación relacionados con el Programa de Resultados Electorales Preliminares, en caso de que lo implemente el Instituto;

XIII. Diseñar, desarrollar, implementar y dar mantenimiento al sistema informático para la formulación de estudios y estadísticas electorales, además de coadyuvar con la Dirección Ejecutiva de Organización Electoral en su operación;

XIV. Diseñar los mecanismos técnicos en el establecimiento de las reglas y modalidades de intercambio de información en el marco del convenio de colaboración con el Instituto Nacional Electoral; y,

XV. Desarrollar las demás funciones que le encomiende el superior jerárquico, en el ámbito de su competencia.

4.3.2. De la Persona Técnica de Publicación Digital, Plataformas WEB y Archivo Documental

La persona técnica de publicación digital, plataformas web y archivo documental será el encargado de proporcionar los servicios informáticos para el mantenimiento y actualización del contenido de la información de las plataformas web y aplicaciones institucionales.

Además de coadyuvar con las áreas correspondientes en lo relativo a la gestión del archivo documental del Instituto, así como la información de oficio que debe de ser publicada en materia de transparencia. Para ello contará con las siguientes atribuciones:

I. Diseñar, actualizar, operar y dar mantenimiento a las plataformas web y aplicaciones institucionales;

II. Organizar y en su caso crear o diseñar el contenido multimedia, incluyendo la edición de textos, el diseño gráfico y otros recursos relacionados de las plataformas web y aplicaciones institucionales;

III. Apoyar en la difusión de la información de la página de internet para la sistematización del acceso a la información pública;
IV. Administrar los servidores (base de datos, aplicaciones, web, etc.) equipo de telecomunicaciones (switchs, routers, etc.), equipo de seguridad (firewall) así como los servicios de red con los que cuenta el Instituto;
V. Desarrollar e implementar las herramientas informáticas necesarias para remitir la información capturada y sistematizada en archivos de consulta pública en la página web del Instituto y los demás medios que determine el Consejo General;
VI. Coadyuvar en los procedimientos y herramientas para la trasmisión de sesiones y eventos institucionales además de supervisar la trasmisión hacia la red interna e internet;
VII. Apoyar a la Coordinación de Transparencia y Acceso a la Información para la publicación de la información pública, correspondiente a las obligaciones de transparencia;
VIII. Dar contestación a las solicitudes en materia de acceso a la información pública y protección de datos personales que le sean turnadas por parte de la Coordinación de Transparencia y Acceso a la Información;
IX. Organizar y conservar la documentación de la Coordinación relacionada con las obligaciones de transparencia;
X. Revisar y mantener actualizado el archivo electrónico del Instituto;
XI. Adoptar y proponer las medidas de seguridad necesarias para salvaguardar el archivo digital del Instituto cuando corresponda;
XII. Apoyar a la técnica de desarrollo e innovación tecnológica todas las actividades y aspectos relacionados a la programación y manejo web;
XIII. Coadyuvar en materia de tecnologías de la información y comunicaciones en los procedimientos de participación ciudadana, cuando así se requiera;
XIV. Investigar y sugerir planes para la implementación de nuevas técnicas web; y,
XV. Desarrollar las demás funciones que le encomiende el superior jerárquico, en el ámbito de su competencia.

4.3.3. De la Persona Técnica de Capacitación, Mantenimiento y Soporte Técnico

La persona técnica de capacitación, mantenimiento y soporte técnico será la encargada de mantener en operación la infraestructura informática que incluye los servicios de la red de voz y datos, equipo de cómputo y software, a través del mantenimiento correctivo y preventivo y la actualización de estos, además garantizará el óptimo funcionamiento acorde a las necesidades institucionales ordinarias y de proceso electoral. Para ello contará con las siguientes atribuciones:

I. Brindar soporte técnico a la infraestructura de cómputo y telecomunicaciones asesorando al personal de las áreas que lo requieran sobre el uso adecuado de los mismos;
II. Revisar técnicamente y desahogar las consultas que, en la materia de su competencia, le planteen los Órganos Desconcentrados del Instituto;
III. Dar seguimiento y garantizar que los sistemas informáticos estén completamente operativos;
IV. Brindar mantenimiento preventivo y correctivo al equipo de cómputo y a la red de voz y datos institucional;
V. Vigilar la adecuada utilización de los equipos de cómputo, la adquisición y renovación de las licencias o en su caso, regular el uso de programas, así como su actualización y mantenimiento;
VI. Implementar y supervisar acciones para la protección de la información y comunicaciones, como software y hardware en equipos, dispositivos y redes de comunicación, contra amenazas que puedan llegar a dañar la integridad de información almacenada en los equipos informáticos y de comunicaciones del Instituto;
VII. Administrar accesos y uso de la Red Interna, Internet, cuentas de correo institucional y servicio de impresión, así como de establecer políticas para su uso adecuado;
VIII. Mantener en óptimas condiciones los equipos informáticos y de comunicación para el correcto funcionamiento y conectividad de los equipos y dispositivos de las áreas del Instituto;

IX. Diseñar las bases de datos institucionales necesarias para los sistemas de información automatizados;

X. Elaborar instructivos, guías, manuales y demás documentos relacionados con el uso, operación y manejo de los diferentes sistemas;

XI. Capacitar al personal del Instituto para el manejo de los equipos y la operación de los programas;

XII. Proponer y elaborar programas de mantenimiento preventivo del equipo de cómputo;

XIII. Coadyuvar en el diseño y elaboración de instrumentos de apoyo académico y de consulta estadística;

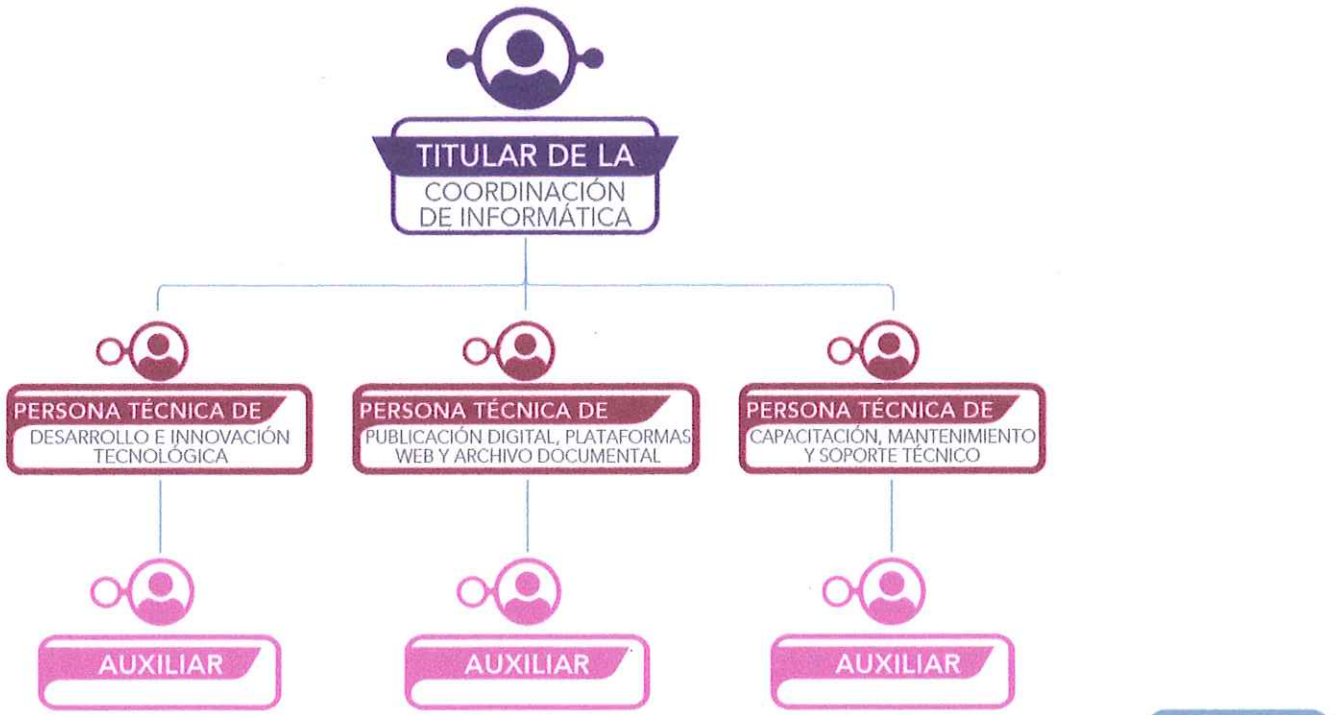
XIV. Apoyar a la técnica de desarrollo e innovación tecnológica para generar la información estadística que requieran las áreas del Instituto a partir de la información recabada por los sistemas de información; y,

XV. Desarrollar las demás funciones que le encomiende el superior jerárquico, en el ámbito de su competencia.

4.4. Organigrama

IEM
INSTITUTO ELECTORAL DE MICHOACÁN

ESTRUCTURA ORGÁNICA COORDINACIÓN DE INFORMÁTICA



5. Procesos de la Coordinación de Informática

5.1. Proceso de Desarrollo y Mantenimiento de Sistemas

El proceso de desarrollo de software es el método que usamos para crear aplicaciones informáticas de cualquier tipo, que indica qué etapas tendrá que hacer el equipo de desarrollo, qué disciplinas del desarrollo se realizarán en cada etapa y cómo se organizará el mantenimiento, una vez se haya desarrollado el software.

Con independencia del ciclo de desarrollo que se elija para cada proyecto, al menos se contará con las etapas siguientes;

- Análisis de requisitos. Como primera instancia se debe recabar información primordial de la fuente principal para tener claro el fin del proyecto a desarrollar.
- Diseño del sistema. A continuación, se hace una idea y se esquematiza el proyecto en termino macro para decidir el lenguaje de programación.
- Implementación. En este punto el trabajo de desarrollo empieza y se programa el software solicitado. Empleando códigos y elementos necesarios para su funcionamiento.
- Verificación. Una de las etapas más relevantes, se evalúa el proceso y se corrigen fallas en caso de presentar errores en el proyecto.
- Mantenimiento. Finalmente se asegura la calidad del software brindando atención oportuna, capacitación y actualizaciones que permitan añadir nuevas y mejores funcionalidades.

5.2. Proceso de Administración de Redes y Comunicaciones

La administración de redes abarca un amplio número de asuntos. En general, se suelen tratar con muchos datos estadísticos e información sobre el estado de distintas partes de la red, y se realizan las acciones necesarias para ocuparse de fallos y otros cambios. La técnica más primitiva para la monitorización de una red es hacer

ping a los hosts críticos, el cual se basa en un datagrama de echo (eco), que es un tipo de datagrama que produce una réplica inmediata cuando llega al destino.

El objetivo de la administración de redes es mantener en óptimas condiciones de operación la infraestructura de red, a través de:

- Monitoreo y control estadístico del tráfico en la red utilizando herramientas especialmente diseñadas para este fin.
- Identificación y prevención de fallas canalizando las actividades correctivas que fueran necesarias a los proveedores de este servicio.
- Análisis del impacto del crecimiento en la infraestructura de redes.
- Soporte técnico de primer nivel para diagnóstico en sitio y/o mantenimientos tanto preventivos como correctivos.
- Instalación, capacitación, configuración y utilización de herramientas de cómputo para la administración de la red.
- Planeación estratégica del crecimiento de la red de acuerdo con las necesidades reales y últimas tendencias tecnológicas disponibles.
- Administración de perfiles de usuario, cuentas de NIS, DNS.
- Configuración del ruteo interno y/o externo (intranet/extranet)
- Administración de la seguridad (FireWall)

A grandes rasgos la distribución de los servicios de red en el Instituto se realiza por medio de 3 distintas redes, la red común para todos los equipos del instituto en un primer segmento de red aislado, la red de servidores en un segundo segmento red aislado y la red de dispositivos móviles comúnmente llamada red WIFI. Adicionalmente se ha provisionado de un servicio red VPN por sus siglas en inglés (Virtual Private Network), que permite la navegación en la intranet institucional.

5.3. Proceso de Soporte Técnico

Para cubrir con las necesidades de Soporte Técnico de los usuarios del Instituto, se cuenta con 1 Técnico y 1 Auxiliar, sin embargo, cuando las necesidades de la contingencia lo requieren se canalizan los recursos humanos y tecnológicos necesarios hasta brindar la solución a cada solicitud de soporte, cabe señalar que

una vez atendida la solicitud, esta entra en una etapa de seguimiento en la cual se verifica la solución y en caso que el caso de soporte no tenga alcance el grado de satisfacción se plantea el escalamiento de soporte.

El escalamiento puede derivar en una solución mas agresiva o bien a través de un tercero se verifique la solución del caso de soporte cuando la situación lo amerite.

5.4. Proceso Gestión de Seguridad de la Información

El proceso de gestión de la seguridad informática comprende la implementación de controles definidos en el Plan de Seguridad de la Información sobre los componentes de la infraestructura tecnológica institucional y otras necesidades que permitan mantener la operación normal y segura de los servicios informáticos institucionales y finaliza con el monitoreo, que permite establecer la correcta y eficiente operación de los controles implementados.

Una estrategia de seguridad de datos exhaustiva incorpora personas, procesos y tecnologías. Establecer controles y políticas apropiados es tanto una cuestión de cultura organizativa como de implementación del conjunto correcto de herramientas. Esto significa priorizar la seguridad de la información en todas las áreas de la empresa.

El Plan de Maestro de Seguridad de la Coordinación de Informática se basa en gestión de 6 factores que se describen a continuación:

- **Seguridad física de servidores y dispositivos de usuarios**
  Independientemente de que los datos se almacenen de forma local, en un centro de datos o en el cloud público, debe asegurarse de que las instalaciones estén protegidas contra intrusos y cuenten con medidas de extinción de incendios y controles climáticos adecuados. En caso de optar por un proveedor de cloud se debe asegurar que éste asumirá la responsabilidad de estas medidas proactivas.

- **Gestión y controles de acceso**
  El principio de "privilegio mínimo" debe aplicarse en todo el entorno de TI. Esto significa otorgar acceso a las bases de datos, redes y cuentas administrativas a la menor cantidad de personas posible, y solo a quienes lo necesiten realmente para hacer su trabajo.

- **Seguridad y parcheado de aplicaciones**
  Todos los programas de software deben actualizarse con la última versión lo antes posible una vez que se estén disponibles parches o versiones nuevas.

- **Copias de seguridad**
  Se deberán mantener copias de seguridad utilizables y comprobadas minuciosamente respecto de todos los datos críticos como la estrategia de seguridad de datos sólida. Además, todas las copias de seguridad deben estar sujetas a los mismos controles de seguridad físicos y lógicos que rigen el acceso a las bases de datos principales y a los sistemas centrales.

- **Formación de los empleados**
  Capacitar a los empleados sobre la importancia de tener buenas prácticas de seguridad y contraseñas seguras, así como enseñarles a reconocer ataques de ingeniería social, este conocimiento los convertirá en un "firewall humano" que jugará un rol crítico en la protección de sus datos.

- **Supervisión y controles de seguridad de redes y endpoints**
  Implementar un conjunto exhaustivo de herramientas y plataformas de gestión, detección y respuesta a amenazas en todo su entorno local y sus plataformas cloud para mitigar los riesgos y reducir la probabilidad de una vulneración.

5.5. Proceso de Gestión de Proyectos Informáticos

La gestión de proyectos de TI se entiende como el proceso de gestionar, planificar y desarrollar proyectos de tecnología de la información. Los gerentes de proyectos pueden usar el software de gestión de proyectos de TI para pasar por las cinco fases del ciclo de vida de la gestión de proyectos y llevar a cabo tareas complejas de forma más eficiente, cabe señalar que no todos los Proyectos Informáticos implican el desarrollo de software, ya que pueden ser de tipo de infraestructura, mantenimiento, o incluso relacionados con capacitación al usuario.

Con independencia del proyecto que se trate al menos deberá cumplir con las siguientes fases:

1. **Fase de iniciación**
   Determina la necesidad y evalúa la viabilidad del proyecto.

2. **Fase de planificación**
   Establece el presupuesto, identifica los riesgos y define objetivos claros

3. **Fase de ejecución**
   Genera entregas, delega tareas y mantiene la comunicación

4. **Fase de supervisión y control**
   Da seguimiento al progreso del equipo y supervisa los proyectos con un software de gestión de proyectos

5. **Fase de cierre**
   Evalúa los éxitos y fracasos del proyecto

5.6. Proceso de Gestión de Activos de TI

El sistema de gestión de activos es un concepto muy amplio, describe cualquier proceso de la Institución para rastrear equipos y organizar inventarios. Sin embargo, para su administración se deben considerar elementos tales como:

- Obsolencia programada del hardware
- Actualizaciones de software disponibles
- Comparativa de tecnología vigente y futura
- Costos de mantenimiento
- Costos de insumos y consumibles
- Ergonomía
- Rendimiento y consumo energético
- Costos de adquisición respecto de planes de arrendamiento o leasing

El Proceso de Gestión de Activos de TI estará sujeto a lo que determine el Comité de Adquisiciones y su reglamentación, sin embargo, la Coordinación de Informática deberá plantear las soluciones de TI en función de los estándares de racionalidad y disciplina presupuestal.

5.7. Proceso de Continuidad del Negocio

Se describirá el plan de continuidad del negocio de la Coordinación de Informática, incluyendo las medidas de contingencia y los procedimientos de recuperación ante desastres.

Es importante considerar que se deben evaluar y analizar todos los procesos de negocio y no limitarse exclusivamente a los recursos e infraestructura asociado a los sistemas de información.

Como primer paso para controlar las contingencias externas o internas que pudiesen surgir durante la operación de los procesos de la Coordinación de Informática, se deberán identificar y clasificar los riesgos que afecten el plan de continuidad.

5.7.1 Clasificación de riesgos

Clase de riesgo	Nombre de riesgo	Descripción de riesgo
Información	Pérdida de información.	Se asocia con la pérdida de información física y digital de los archivos, bases de datos, servidores y sistemas de información de la Institución.
Disponibilidad	No restablecimiento de los servicios tecnológicos de la Institución.	Contempla la disponibilidad de la información y de los servicios que tiene la Institución con sus usuarios.
Imagen	Pérdida de credibilidad y confianza en la Institución.	Están relacionados con la percepción y la confianza por parte de la ciudadanía en general.
Operativo	Daño o deterioro de los activos tangibles.	Comprende el daño o deterioro de los bienes muebles o inmuebles de la Institución.
Tecnológico	Accesos no autorizados.	Se asocia con el acceso a los sistemas de información, aplicativos, bases de datos o servidores sin autorización previa.
Tecnológico	Afectación de la infraestructura tecnológica.	Está relacionado con el daño, pérdida, siniestro o deterioro a nivel de hardware, enlaces de datos entre otros.
Tecnológico	Inadecuados servicios de Tecnologías de la Información.	Contempla la pertinencia, calidad y oportunidad de los servicios de tecnología y las deficiencias en la prestación de los mismos.

Una vez identificados los riesgos, el Plan de Continuidad de Negocio debe estar orientado a la mitigación de riesgos, por lo tanto la Coordinación de Informática deberá programar capacitaciones para los usuarios en temas tales como respaldo de información, y fomentar el uso correcto de los equipos tecnológicos, en materia de servicios de internet se deberá contar con al menos 2 contratos de red de datos con distintos proveedores con el objeto de garantizar la redundancia del servicio de modo tal que la Institución cuente con la garantía del servicio de datos constante con independencia de las interrupciones de uno u otro servicio contratado.

5.8. Proceso de Publicación WEB

El sistema de publicación web o también conocido como sistema de gestión de contenidos, es un proceso que permite crear, organizar y publicar documentos y otros contenidos de forma colaborativa.

Su principal ventaja consiste en el hecho de que permite organizar y mostrar contenidos que, de acuerdo con lo establecido en los artículos 15, 16 y 17 de los Lineamientos, publiquen, modifiquen o actualicen las áreas de:

- Secretaría Ejecutiva: contenidos relacionados con el segmento de archivo en el cual se contiene la documentación oficial de consulta del portal de internet, así como toda la información que conforme a sus atribuciones deba publicar y los estrados electrónicos;
- Coordinación de Informática: contenidos que, a solicitud de las Áreas responsables, que son aquellas unidades administrativas del Instituto señaladas en el Reglamento Interior, que en cumplimiento de sus atribuciones tengan información bajo su resguardo, susceptible de ser publicada y que hayan sido validados por la Persona Técnica de publicación Digital; y,
- Coordinación de Comunicación Social: Contenidos referentes a actividades que se realizan en el Instituto, notas relevantes en materia electoral en el Estado y demás temas de trascendencia e interés para la ciudadanía y público en general.

Así el administrador clasificará los contenidos, añadirá secciones, y administrará las bases de datos de usuarios, así como la obtención de la trazabilidad de las publicaciones realizadas.

6. Políticas y Normas

6.1 Consideraciones Generales

6.1.1 Uso adecuado de las TIC

Las políticas definidas en este punto están relacionadas con los equipos de cómputo que son asignados a los usuarios, el centro de datos, aspectos relacionados con la propiedad de la información que es creada y manipulada por los usuarios del IEM y la utilización inadecuada de los recursos informáticos que el IEM pone a disposición de sus empleados para que desarrollen sus actividades. Constituye la base de las políticas que debe cumplir todo el personal.

6.1.2 Contraseñas

El cumplimiento de las políticas de contraseñas por parte de los usuarios del IEM es extremadamente importante ya que éstas constituyen la primera línea de defensa para garantizar que la información sólo sea accedida por el personal autorizado. Tanto equipos, sistemas y datos utilizan mecanismos de contraseñas para controlar el acceso, como ejemplo podemos mencionar las contraseñas definidas en el momento del arranque del equipo, para ingresar a la red institucional, para utilizar sistemas internos y externos, etc. No existe ninguna tecnología que pueda prevenir el acceso no autorizado a la información si un usuario viola esta política de ahí que sea de las más relevantes e importantes.

6.1.3 Correo electrónico e Internet

Los accesos a Internet y Correo Ele6ctrónico son servicios que actualmente son utilizados tanto en Oficinas Centrales del Instituto (por medio de la red institucional), así como por las Oficinas Alternas y los Consejos Distritales y Municipales (por medio de la internet) con los siguientes beneficios.

- Interactuar de una forma directa, ágil y eficiente, a través de la mensajería electrónica de Internet.

- Ofrecer a los usuarios una herramienta de investigación que permita realizar consultas y obtener fundamentación clara y precisa.

El Internet y correo electrónico se han convertido en medios de comunicación electrónicos prácticamente indispensables para el trabajo diario por lo que es muy importante cumplir con las políticas relacionadas con ellos. De esta forma evitamos interrupciones que podrían afectar la operatividad de las distintas áreas del IEM.

6.1.4 Uso de Software

Los programas de computadoras conocidos como software están protegidos por las Leyes de derechos de autor y por los tratados internacionales, el software tiene un valor económico, sin embargo, el software es un elemento crítico de varios aspectos de funcionamiento de la Institución y por lo tanto debe de administrarse y debe tener políticas.

Las políticas sobre el uso de Software en el IEM se crean para que sirvan como marco regulatorio en cuanto a la instalación y uso de software en el equipo de cómputo propiedad del IEM y del equipo bajo la modalidad de arrendamiento.

6.2 Alcance

Estas políticas son aplicables y actualmente efectivas para todos los empleados del Instituto Electoral de Michoacán que utilicen equipo de cómputo. Los usuarios del IEM tienen la obligación de seguir al pie de la letra las presentes políticas emitidas por la Coordinación de Informática y aprobadas por la Junta Estatal Ejecutiva.

La Coordinación de Informática es la encargada de administrar estas políticas El equipo de cómputo regulado y atendido por estas políticas es:

- El que es parte del activo fijo del IEM
- El que se encuentra en su modalidad de arrendamiento.

6.3. Políticas de Uso de Recursos de TI

1. En ninguna circunstancia los empleados de la Institución pueden utilizar los recursos informáticos para realizar actividades prohibidas por las normas establecidas en el Reglamento Interior del Instituto Electoral de Michoacán o de presente Manual de la Coordinación de Informática, así como la demás normativa aplicable

2. Para los equipos propiedad del IEM, la Coordinación de Informática es la única autorizada a realizar las actividades de soporte técnico y cambios de configuración en el equipo de cómputo. En el caso de labores de mantenimiento efectuadas por terceros éstas deben ser previamente aprobadas por la Coordinación de Informática. Para los equipos de cómputo en esquema de arrendamiento, la empresa arrendadora es la única autorizada a realizar las labores de mantenimiento y cambio de hardware o en su caso autorizar dichas labores.

3. El equipo de cómputo, propiedad del IEM o arrendado, deberá ser utilizado únicamente para actividades relacionadas con los objetivos y metas de la Institución.

4. Para el correcto funcionamiento del equipo de cómputo deberán de realizarse como mínimo dos mantenimientos preventivos al año, al equipo propiedad del IEM que no cuente con garantía del fabricante, de acuerdo con el plan de mantenimiento preventivo del equipo de cómputo anual elaborado por la Coordinación de Informática a principio de cada ejercicio.

5. La Coordinación de Informática deberá implementar las acciones necesarias para el correcto funcionamiento del equipo de cómputo, tales como actividades preventivas.

6. La Coordinación de Informática es la responsable de la asignación y distribución del equipo de cómputo.

7. La contratación de servicios de cómputo se lleva a cabo de acuerdo con los lineamientos del Decreto de Austeridad dictado por el Ejecutivo Federal basándose en la normatividad vigente que se dicte en materia de arrendamiento y adquisiciones.

8. La solicitud de refacciones y accesorios de equipo de cómputo deberá contar con el visto bueno de la Coordinación de Informática y de preferencia concentrar todos los requerimientos en una sola solicitud mensual.

9. Para conectar una computadora a la red institucional que no esté bajo el control administrativo del IEM (computadoras privadas del personal de IEM, computadoras de otras empresas o terceros en general, las cuales no están sujetas a la totalidad de las políticas de seguridad de IEM y por ende constituyen un riesgo al ser conectadas a la red institucional) se deberá solicitar permiso a la Coordinación de Informática para que ésta inspeccione el equipo, compruebe que no constituye un riesgo para la seguridad de la

institución, evalúe el porqué de la necesidad de conectar el equipo a nuestra red privada y dé la autorización en su caso.

10. Cuando exista algún incidente (robo, extravío, daño físico, etc.) que afecte de manera directa a un equipo de cómputo del IEM, deberá ser notificado de inmediato a la Coordinación de Informática.

11. Sólo el personal autorizado por la Coordinación de Informática está facultado para abrir los gabinetes de las computadoras personales o de cualquier otro equipo de cómputo propiedad del IEM. Para los equipos de cómputo en esquema de arrendamiento la empresa arrendadora es la única autorizada a abrir los gabinetes de dichos equipos o en su caso autorizar la apertura de ellos.

12. Todos los equipos de cómputo bajo la supervisión de IEM, deben contar con un software antivirus actualizado y un firewall personal administrado por el personal del área de seguridad informática, con el objetivo de proteger el equipo de programas maliciosos.

13. Todos los equipos de cómputo bajo la supervisión de IEM, deben ser actualizados de manera periódica con los últimos parches de seguridad del sistema operativo y aplicaciones instaladas en el equipo.

14. Todas las computadoras conectadas a la red IEM contarán obligatoriamente con un fondo definido por la Coordinación de Informática a fin de preservar la imagen institucional.

15. El acceso al centro de cómputo es restringido y sólo personal autorizado por la Coordinación de Informática puede tener acceso a él.

16. Sólo el personal autorizado por la Coordinación de Informática puede abrir los gabinetes de los servidores y el equipo que está dentro del centro de cómputo.

17. El acceso a los servidores del IEM, ya sea usando la consola de administración local o una consola de administración remota es restringido a personal autorizado por la Coordinación de Informática. El intento de conexión por alguna persona no autorizada a cualquier consola de administración de los servidores se considera una violación de las políticas de seguridad.

18. Los usuarios de cualquier equipo de cómputo del IEM deben estar conscientes que los datos que ellos crean y manipulan en los sistemas, aplicaciones y cualquier medio de procesamiento electrónico, durante el desarrollo normal de sus actividades laborales, son propiedad y responsabilidad del IEM.

19. Los derechos patrimoniales de un programa de computación, hojas de cálculo, archivos de Word, macros, etc. y su documentación, creados por uno o varios empleados en el ejercicio de sus actividades laborales corresponden al IEM.

20. Los respaldos que contengan información del IEM y que fueron realizados o solicitados por el usuario del equipo de cómputo, se tendrán exclusivamente bajo resguardo, debiendo de entregarlos en el momento de la finalización de la relación laboral.

6.4. Usos inadecuados (Actividades no permitidas)

1. Violar los derechos de cualquier persona o institución protegidos por derechos de autor, patentes o cualquier otra forma de propiedad intelectual. Entre otras actividades, se incluye la distribución o instalación de software sin la licencia de uso adecuada adquirida por el IEM (Políticas de Uso de Software).

2. Difundir información identificada como confidencial a través de medios que involucren el uso de la Tecnología de Información.

3. Introducir software malicioso en la red o en los servidores (virus, worms, ráfagas de correo electrónico no solicitado, etc.)

4. Utilizar la infraestructura de tecnología de información del IEM para conseguir o transmitir material con ánimo de lucro. Igualmente se prohíbe el uso del sistema de comunicaciones del IEM con el fin de realizar algún tipo de acoso, difamación, calumnia o cualquier forma de actividad hostil.

5. Hacer ofrecimientos fraudulentos de servicios cuyo origen sean los recursos o servicios propios del IEM.
6. Realizar actividades que contravengan la seguridad de los sistemas o que generen interrupciones de la red o de los servicios.

7. Monitorear puertos o realizar análisis del tráfico de la red con el propósito de evaluar vulnerabilidades de seguridad. El personal de la Coordinación de Informática, responsable de la Seguridad Informática puede realizar estas actividades siempre y cuando tenga conocimiento la misma Coordinación de Informática.

8. Ejecutar cualquier herramienta o mecanismo de monitoreo de la red de manera no autorizada.

9. Burlar mecanismos de seguridad, autenticación, autorización o de auditoría de cualquier servicio de red, aplicación, servidor o cuenta de usuario.

10. Interferir o negar el servicio a usuarios autorizados con el propósito de lesionar la prestación del servicio o la imagen del IEM (por ejemplo, ataques DoS).

11. Uso de comandos o programas para el envío de mensajes de cualquier tipo con el propósito de interferir o deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (Internet, Intranet).

12. Instalar cualquier tipo de software en los equipos de cómputo de IEM sin la previa autorización de la Coordinación de Informática.

13. Modificar la configuración del software antivirus, firewall personales o políticas de seguridad en general implantadas en los equipos de cómputo de IEM sin consultar previamente con la Coordinación de Informática la cual analizará la viabilidad de los cambios solicitados.

14. Queda estrictamente prohibido compartir una carpeta con derecho a todos. El área de informática puede cambiar permisos de recursos compartidos por los usuarios si detecta que éstos no cumplen con las mejores prácticas definidas en los lineamientos internos de seguridad.

15. Reproducir música de cualquier formato que no esté ubicada en el disco duro de la PC del usuario o en CD. No se permite la reproducción de archivos de música si éstos están ubicados en un recurso compartido de la red privada del IEM o en cualquier URL de Internet (aplicable para los usuarios que hacen uso del servicio de Internet).

16. Descargar archivos de música desde Internet.

6.4.1 Excepciones

Para propósitos de mantenimiento de la red y de seguridad algunos empleados del IEM, pueden estar exentos de seguir algunas de las restricciones anteriores, debido a las responsabilidades de su cargo o a eventos programados. Estas excepciones deben ser solicitadas a la Coordinación de Informática anexando la justificación respectiva vía correo electrónico al correo sistemas@iem.org.mx.

6.5. Políticas de contraseñas

1. Todos los usuarios internos de IEM requieren de un nombre de usuario y una contraseña para utilizar el equipo de cómputo que tiene asignado y servicios de red como correo electrónico, impresión, archivos compartidos, Intranet, Internet etc. Su solicitud deberá de realizarse tal y como lo establece el procedimiento "Gestión de cuentas en la Red IEM".
2. Las contraseñas de los usuarios deben cumplir con ciertos requerimientos de seguridad los cuales definirá la Coordinación de Informática con el objetivo de evitar que los usuarios elijan contraseñas débiles. Las contraseñas son

personales y conocidas únicamente por el propio usuario el cual será responsable de toda la actividad que se realice con ella.

3. Por seguridad las contraseñas se cambian cada cierto tiempo por el propio usuario.

4. La Coordinación de Informática se reserva el derecho de restablecer en cualquier momento la contraseña de cualquiera de los usuarios del IEM, con previo aviso para no afectar de ninguna manera la continuidad de su trabajo, si se detecta que ha sido comprometida.

5. Todas las computadoras de escritorio y portátiles deben tener configurados un protector de pantalla con clave y el cual se activará si el equipo se deja desatendido después de 15 minutos sin tener actividad.

6. Los equipos de cómputo portátiles y los que no se encuentran dentro de oficinas con acceso controlado, deben contar con una contraseña adicional en el momento del encendido del equipo.

7. Los sistemas internos cuentan con su propia contraseña independiente de la utilizada para iniciar sesión en la red institucional.

8. Los usuarios y contraseñas de los equipos localizados en las Órganos Desconcentrados son responsabilidad de la Coordinación de Informática y sólo ésta tiene la autoridad para realizar cambios de configuración a dichos equipos a petición de la Dirección Ejecutiva de Organización Electoral mediante el formato establecido en el procedimiento para la "Gestión de la Infraestructura de Tecnologías de Información y Comunicaciones".

9. Las cuentas de correo electrónico y la contraseña de éstas para personal de los Órganos Desconcentrados del IEM, son asignadas por la Coordinación de Informática.

10. Todas las computadoras de escritorio y portátiles en Órganos Desconcentrados del IEM deben tener configurados un protector de pantalla

con clave y con un tiempo de espera de un máximo de 15 minutos cuando el equipo esté desatendido.

11. Se prohíbe a los usuarios revelar su contraseña a personal no autorizado o permitir su uso a terceros para actividades ajenas al IEM. La prohibición incluye familiares y cualquier otra persona que habite en la residencia del funcionario, cuando la conexión a la red IEM se realice desde el hogar.

12. Anotar la contraseña en Post-It o cualquier otro medio físico y tenerla a la vista de todos en su lugar de trabajo. Se recomienda que la contraseña sea aprendida de memoria y no anotarla en ningún medio físico como libretas, cuadernos etc.

6.6. Políticas de Respuesta a Incidentes

Propósito

Establecer un conjunto de directrices que permitan a la Coordinación de Informática del IEM responder de manera eficiente, coordinada y sistemática a incidentes de seguridad que puedan comprometer la confidencialidad, integridad o disponibilidad de los sistemas y datos institucionales, asegurando la continuidad de las operaciones y el cumplimiento normativo.

Alcance

Estas políticas aplican a todos los sistemas, redes, aplicaciones y datos gestionados por la Coordinación de Informática, así como a los empleados, contratistas y proveedores que interactúan con dichos recursos.

Incidentes cubiertos:

- Ciberataques (phishing, ransomware, denegación de servicio).
- Brechas de datos.
- Fallos críticos de infraestructura.

- Abusos de privilegios de acceso.
- Uso indebido de sistemas por personal interno o externo.

Definiciones

Incidente de seguridad: Evento que compromete o pone en riesgo los sistemas, redes o datos del IEM.

Evento sospechoso: Actividad no habitual que puede escalar a incidente (por ejemplo, intentos de acceso no autorizado).

Equipo de Respuesta a Incidentes (ERI): Grupo designado dentro de la Coordinación de Informática responsable de gestionar los incidentes.

Roles y Responsabilidades

- Equipo de Respuesta a Incidentes (ERI):
- Detectar, analizar y gestionar los incidentes.
- Implementar medidas correctivas y preventivas.
- Notificar a las partes interesadas y a las autoridades regulatorias cuando sea necesario.

Coordinador de Informática:

- Supervisar la implementación de estas políticas.
- Aprobar planes de acción ante incidentes mayores.
- Usuarios finales (personal del IEM):
- Reportar cualquier evento sospechoso al ERI de forma inmediata.
- Cooperar en las investigaciones proporcionando información relevante.

Proceso de Respuesta a Incidentes

A. Detección y Notificación

- Identificar incidentes a través de sistemas de monitoreo, auditorías o reportes de usuarios.

- Registrar el incidente en el sistema de seguimiento interno.
- Notificar al Coordinador de Informática y, si aplica, a las autoridades internas del IEM.

B. Clasificación y Priorización

- Evaluar el impacto según los siguientes niveles:
- Crítico: Afecta operaciones esenciales del IEM (por ejemplo, sistemas de votación).
- Alto: Compromete información sensible o varios sistemas.
- Medio: Impacta procesos no esenciales.
- Bajo: Incidentes menores que no comprometen la operación.
- Asignar recursos en función de la severidad del incidente.

C. Contención

- Implementar medidas inmediatas para limitar el impacto (desconexión de sistemas comprometidos, bloqueo de accesos no autorizados).
- Documentar las acciones tomadas durante esta etapa.

D. Erradicación

- Identificar y eliminar la causa raíz del incidente (por ejemplo, malware, configuraciones erróneas).
- Actualizar software, parches y configuraciones según sea necesario.

E. Recuperación

- Restaurar sistemas, servicios y datos afectados asegurando su integridad.
- Monitorear los sistemas para prevenir recurrencias.

F. Revisión Post-Incidente

- Generar un informe que documente el incidente, su impacto, las acciones tomadas y las lecciones aprendidas.
- Actualizar las políticas y medidas preventivas con base en los hallazgos.

Herramientas y Recursos

- Soluciones de monitoreo de seguridad (SIEM).
- Sistemas de respaldo y recuperación de datos.
- Planes de escalamiento internos y comunicación con proveedores de TI.

Cumplimiento y Auditoría

- Garantizar que las acciones estén alineadas con normativas nacionales e internacionales aplicables (por ejemplo, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados).
- Realizar auditorías periódicas para evaluar la efectividad de las políticas.

Entrenamiento y Simulaciones

- Capacitar a todo el personal del IEM en el reconocimiento y reporte de incidentes.
- Realizar simulacros anuales de respuesta a incidentes para evaluar la preparación y ajustar los procedimientos.

Actualización de la Política

- Estas políticas deberán revisarse y actualizarse anualmente o tras la ocurrencia de un incidente significativo.

6.7. Normas de Desarrollo de Software

Propósito

Establecer un conjunto de normas para garantizar que el desarrollo de software realizado o gestionado por la Coordinación de Informática del IEM sea de alta calidad, seguro, eficiente y conforme a las necesidades del Instituto, respetando las normativas aplicables y asegurando la confiabilidad de los sistemas institucionales.

Alcance

Estas normas aplican a todos los proyectos de desarrollo de software realizados por la Coordinación de Informática, así como a los sistemas adquiridos o desarrollados por terceros bajo supervisión del IEM.

Principios Generales

1. Calidad: Todo el software debe cumplir con los estándares de calidad definidos por el IEM, alineándose con las mejores prácticas de la industria.
2. Seguridad: Garantizar que el desarrollo incorpore prácticas seguras para prevenir vulnerabilidades.
3. Escalabilidad y Mantenimiento: Diseñar software fácil de escalar, mantener y actualizar.
4. Cumplimiento Normativo: Asegurar que los sistemas cumplan con las leyes y regulaciones aplicables, como la Ley General de Protección de Datos Personales.
5. Documentación: Todo el código y los procesos deben estar debidamente documentados.

Normas de Desarrollo

A. Planeación del Proyecto

1. Análisis de Requerimientos:
   - Realizar un análisis detallado de las necesidades del usuario final.
   - Documentar los requerimientos funcionales y no funcionales en un formato estándar.
2. Gestión de Proyectos:
   - Utilizar metodologías de desarrollo establecidas (Agile, Scrum, Cascada, según aplique).

- Definir cronogramas claros y establecer puntos de control (hitos).

B. Diseño del Software

1. Implementar principios de diseño modular, favoreciendo la reutilización de componentes.
2. Usar patrones de diseño cuando sea adecuado para garantizar soluciones robustas y flexibles.
3. Garantizar la compatibilidad con las plataformas tecnológicas utilizadas por el IEM.

C. Desarrollo

1. Normas de Codificación:
   - Utilizar convenciones de codificación estandarizadas (nomenclatura, formato, comentarios).
   - Escribir código legible y mantenible.
2. Gestión de Versiones:
   - Usar sistemas de control de versiones como Git para gestionar el ciclo de vida del código.
   - Documentar los cambios realizados en cada versión (historial de commits).
3. Prácticas de Seguridad:
   - Validar y sanitizar entradas del usuario para prevenir ataques como inyección de SQL o cross-site scripting (XSS).
   - Implementar cifrado para datos sensibles en reposo y en tránsito.
   - Realizar pruebas de seguridad regulares durante el ciclo de desarrollo.

D. Pruebas

1. Tipos de Pruebas:
   - Unitarias: Verificar la funcionalidad de componentes individuales.

- Integración: Asegurar que los módulos interactúan correctamente.
- Funcionales: Validar que el sistema cumple con los requerimientos establecidos.
- Pruebas de carga y estrés: Evaluar el rendimiento bajo diferentes condiciones.

2. Automatización:
   - Usar herramientas de automatización para realizar pruebas repetitivas.
   - Registrar los resultados de las pruebas y abordar los defectos identificados.

E. Implementación y Despliegue

1. Entornos:
   - Mantener entornos separados para desarrollo, pruebas y producción.
   - Validar el correcto funcionamiento en un entorno de pruebas antes del despliegue en producción.
2. Plan de Despliegue:
   - Definir un plan de despliegue detallado que incluya respaldos previos y medidas de contingencia.
   - Notificar a los usuarios sobre los cambios programados y proporcionar instrucciones claras.

F. Mantenimiento y Soporte

1. Establecer un plan de mantenimiento preventivo y correctivo.
2. Responder a incidencias en tiempo y forma conforme a los acuerdos de nivel de servicio (SLA).
3. Actualizar el software regularmente para incluir mejoras y parches de seguridad.

Herramientas Recomendadas

- Gestión de proyectos: Jira, Trello o herramientas similares.
- Control de versiones: GitHub, GitLab o Bitbucket.
- Pruebas automatizadas: Selenium, JUnit, o equivalentes según el lenguaje.
- Monitoreo y análisis: Nagios, Splunk, o sistemas similares.

Documentación

- Manual Técnico: Describir la arquitectura del software, diagramas y detalles de implementación.
- Manual de Usuario: Proporcionar guías claras para los usuarios finales.
- Historial de Cambios: Mantener un registro actualizado de modificaciones en el sistema.

Cumplimiento y Auditoría

- Realizar revisiones periódicas del código y auditorías de cumplimiento normativo.
- Involucrar a equipos externos cuando sea necesario para verificar la calidad y seguridad del software.

8. Actualización de las Normas

- Estas normas deben revisarse y actualizarse anualmente o cuando surjan nuevas tecnologías, regulaciones o necesidades específicas.

6.8. Normas de Administración de Redes

Propósito

Establecer las directrices para la administración, mantenimiento y seguridad de las redes del IEM, con el objetivo de garantizar su disponibilidad, confiabilidad, desempeño y protección frente a amenazas, asegurando el soporte adecuado a las operaciones institucionales.

Alcance

Estas normas aplican a toda la infraestructura de redes del IEM, incluidas redes cableadas, inalámbricas, equipos de red (switches, routers, firewalls, etc.), servidores, y cualquier dispositivo conectado que sea administrado por la Coordinación de Informática.

Principios Generales

1. Seguridad: Proteger las redes contra accesos no autorizados y ciberataques.
2. Disponibilidad: Garantizar que las redes estén operativas de manera continua y eficiente.
3. Monitoreo: Supervisar el desempeño y detectar anomalías en tiempo real.
4. Documentación: Mantener un registro detallado de la infraestructura de red, configuraciones y cambios realizados.

Normas de Administración de Redes

A. Diseño y Configuración

1. Topología:
   - Diseñar la red con una topología escalable y redundante que permita la continuidad operativa.
   - Separar las redes internas en segmentos lógicos mediante VLANs para mayor seguridad y eficiencia.

2. Configuración de Equipos:
   - Usar configuraciones estándar y seguras para todos los dispositivos de red.

- Deshabilitar servicios y puertos innecesarios para reducir vectores de ataque.
- Establecer contraseñas seguras y únicas para cada dispositivo.

3. Acceso a la Red:
   - Implementar políticas de control de acceso basadas en roles (RBAC).
   - Usar sistemas de autenticación robusta (como RADIUS o 802.1X) para el acceso a redes cableadas e inalámbricas.

B. Seguridad de la Red

1. Cortafuegos y Filtros:
   - Configurar firewalls para restringir el tráfico no autorizado entre segmentos de red.
   - Implementar listas de control de acceso (ACLs) para filtrar el tráfico entrante y saliente.

2. Protección contra Amenazas:
   - Implementar sistemas de detección y prevención de intrusos (IDS/IPS).
   - Monitorear en tiempo real para identificar y responder a actividades sospechosas.

3. Actualizaciones:
   - Actualizar regularmente el firmware y los sistemas operativos de los dispositivos de red.
   - Aplicar parches de seguridad de manera oportuna.

4. Cifrado de Comunicaciones:
   - Usar protocolos seguros (como TLS, IPsec o WPA3) para proteger los datos en tránsito.

C. Monitoreo y Auditoría

1. Monitoreo Continuo:
   - Usar herramientas de monitoreo (como Nagios, Zabbix o SolarWinds) para supervisar el desempeño de la red.
   - Configurar alertas para notificar sobre fallos, congestión o actividades inusuales.

2. Auditorías:
   - Realizar auditorías periódicas de la configuración y seguridad de la red.
   - Revisar los registros de eventos (logs) de dispositivos de red y sistemas.

D. Mantenimiento

1. Preventivo:
   - Programar mantenimientos regulares para verificar el estado de los dispositivos y actualizar configuraciones.
   - Realizar pruebas de rendimiento para garantizar el correcto funcionamiento de la red.

2. Correctivo:
   - Establecer procedimientos para responder rápidamente a fallos en la red.
   - Documentar todas las acciones correctivas realizadas.

E. Gestión de Usuarios y Dispositivos

1. Acceso de Usuarios:
   - Proporcionar acceso a la red únicamente a personal autorizado.
   - Usar políticas de expiración de contraseñas y autenticación multifactor para los usuarios administrativos.

2. Dispositivos Conectados:
   - Registrar todos los dispositivos conectados a la red (dirección MAC, IP, propietario).
   - Desconectar cualquier dispositivo no autorizado o que represente un riesgo de seguridad.

Documentación

1. Inventario: Mantener un registro actualizado de los equipos de red, direcciones IP, contraseñas administrativas y configuraciones.
2. Mapeo de Red: Crear y mantener diagramas actualizados de la topología de la red.
3. Cambios: Registrar todas las modificaciones realizadas en la configuración o infraestructura de la red.

6. Respuesta a Incidentes de Red
    1. Detección: Supervisar constantemente la red para identificar incidentes como caídas, accesos no autorizados o ataques cibernéticos.
    2. Respuesta: Implementar las medidas de contención, análisis y recuperación detalladas en las Políticas de Respuesta a Incidentes del IEM.
    3. Reporte: Notificar de manera inmediata al Coordinador de Informática sobre incidentes críticos.

7. Entrenamiento y Capacitación
    - Capacitar al personal de la Coordinación de Informática en administración, configuración y seguridad de redes.
    - Mantenerse actualizado sobre las mejores prácticas y nuevas tecnologías.

8. Actualización de las Normas
    - Estas normas deberán revisarse anualmente o cuando se realicen cambios significativos en la infraestructura o tecnologías empleadas.

6.9. Normas de Respaldo y Recuperación de Datos

Propósito

Establecer las normas para realizar respaldos y garantizar la recuperación eficiente y segura de los datos críticos del IEM, minimizando el impacto de incidentes como fallos técnicos, ciberataques o desastres naturales, y asegurando la continuidad operativa y el cumplimiento normativo.

Alcance

Estas normas aplican a todos los sistemas, bases de datos, aplicaciones y servicios gestionados por la Coordinación de Informática del IEM, así como a los dispositivos de almacenamiento y procesos relacionados con los respaldos y la recuperación.

Principios Generales

1. Seguridad: Garantizar la protección de los datos respaldados frente a accesos no autorizados.
2. Disponibilidad: Asegurar que los respaldos estén accesibles para su recuperación en caso de necesidad.
3. Integridad: Verificar que los datos respaldados sean completos y estén libres de corrupción.
4. Cumplimiento Normativo: Asegurarse de que los procesos cumplan con las leyes aplicables, como la Ley General de Protección de Datos Personales.

4. Normas de Respaldo

A. Planificación de Respaldos

1. Identificación de Datos Críticos:
   - Definir los datos, sistemas y aplicaciones que deben incluirse en los respaldos, priorizando aquellos esenciales para la operación del IEM.

2. Frecuencia de Respaldos:
   - Diaria: Datos de uso crítico y sistemas esenciales.
   - Semanal: Bases de datos completas y configuraciones de sistemas.
   - Mensual: Respaldos completos archivados para fines históricos.

3. Tipos de Respaldo:
   - Completo: Copia de todos los datos seleccionados.
   - Incremental: Copia de los datos modificados desde el último respaldo.
   - Diferencial: Copia de los datos modificados desde el último respaldo completo.

B. Procedimientos de Respaldo

1. Automatización:

- Usar herramientas de respaldo automatizado para garantizar la consistencia y puntualidad de los respaldos.

2. Verificación:
   - Realizar pruebas regulares para verificar que los respaldos sean válidos y restaurables.

3. Encriptación:
   - Encriptar los datos respaldados para protegerlos contra accesos no autorizados, tanto en tránsito como en almacenamiento.

4. Ubicación:
   - Mantener copias de seguridad en al menos dos ubicaciones:
     - On-site: Para recuperaciones rápidas.
     - Off-site: En un sitio remoto seguro, para casos de desastres en las instalaciones principales.

C. Retención de Respaldos

1. Políticas de Retención:
   - Respaldos diarios: Conservar por un período de 15 días.
   - Respaldos semanales: Conservar por un período de 3 meses.
   - Respaldos mensuales: Conservar por un período de 1 año.

2. Eliminación Segura:
   - Asegurar la destrucción segura de respaldos obsoletos para proteger la confidencialidad de los datos.

Normas de Recuperación

A. Planificación de la Recuperación

1. Identificación de Escenarios:
   - Fallos menores (archivo eliminado, sistema comprometido).
   - Fallos mayores (pérdida de múltiples sistemas o datos críticos).

- Desastres (incendios, inundaciones u otros eventos catastróficos).

2. Prioridad en la Recuperación:
   - Restaurar primero los sistemas críticos para la operación del IEM.

B. Procedimientos de Recuperación

1. Evaluación del Incidente:
   - Determinar el alcance del daño y las causas para seleccionar la estrategia de recuperación adecuada.

2. Restauración:
   - Usar las herramientas y copias de respaldo correspondientes para restaurar los datos y sistemas afectados.
   - Validar la integridad de los datos después de la restauración.

3. Documentación:
   - Registrar todos los pasos realizados durante el proceso de recuperación.

C. Pruebas de Recuperación

1. Pruebas Regulares:
   - Realizar simulacros de recuperación al menos dos veces al año para evaluar la efectividad de los procedimientos.

2. Revisión Post-Prueba:
   - Documentar los resultados de las pruebas y realizar ajustes en los planes según sea necesario.

Herramientas y Tecnologías Recomendadas

- Software de respaldo y recuperación como Veeam, Acronis o similares.
- Almacenamiento en la nube seguro para copias off-site.
- Soluciones de almacenamiento en red (NAS) para respaldos locales.

Seguridad de Respaldos

1. Acceso Restringido:
   - Limitar el acceso a los respaldos al personal autorizado.

2. Registros de Actividad:
   - Mantener bitácoras detalladas de las actividades relacionadas con respaldos y recuperaciones.

3. Auditorías:
   - Realizar auditorías periódicas para garantizar el cumplimiento de estas normas.

Documentación

1. Política de Respaldo: Detallar los procedimientos, horarios y sistemas involucrados en los respaldos.

2. Plan de Recuperación: Especificar los pasos para restaurar sistemas y datos críticos.

3. Historial de Respaldos y Recuperaciones: Mantener un registro actualizado de todos los respaldos realizados y recuperaciones efectuadas.

Actualización de las Normas

Estas normas deberán revisarse y actualizarse anualmente o cuando se implementen nuevas tecnologías o cambios en los sistemas del IEM.

7. Procedimientos de Gestión

Actualmente solo se cuenta con dos procedimientos aprobados, el primero mediante acuerdo del Consejo General número IEM-CG-34-2022, mediante el cual

fueron aprobados los Lineamientos para la Publicación y Gestión de Contenidos WEB y el segundo mediante acuerdo IEM-CG-50-2022, a través del cual se aprueba el Lineamiento para el correcto uso del Correo Electrónico Institucional.

7.1. Procedimiento de Publicación y Gestión de Contenidos WEB

El portal de Internet del Instituto es el instrumento electrónico de acceso público, a través del cual el Instituto comparte con la ciudadanía y público en general, información pública relevante.

Los objetivos del portal de Internet son los siguientes:

a) Ser un medio de acceso eficaz para facilitar a la ciudadanía la información que requiere para ejercer en plenitud sus derechos político-electorales, así como de los mecanismos de participación ciudadana

b) Constituirse en un instrumento tecnológico eficiente para la ejecución y gestión de los programas institucionales de las áreas del Instituto que requieren de una comunicación efectiva con los diversos tipos de público a los que sirve, a fin de garantizar una óptima experiencia de usuario.

c) Ser un instrumento de notificaciones de sentencias, acuerdos e información que emita el Consejo General de este Instituto por medio de un Estrado Electrónico permanente en el sitio de internet.

d) Ser un instrumento para la rendición de cuentas del Instituto, al permitir el acceso público a la información que describe las actividades, explica las decisiones de sus órganos y da cuenta del uso de los recursos públicos que le han sido asignados, así como para el cumplimiento de las obligaciones legales y políticas de transparencia y acceso a la información pública de la autoridad electoral, incluida la divulgación de información de interés público.

e) Ser un medio de acceso para que la ciudadanía y público en general, puedan disponer de información pública relevante, tanto del Instituto, como de los partidos políticos, candidaturas independientes, agrupaciones políticas, entre otros.

f) Ser un medio que coadyuve en la difusión de las políticas de comunicación social del Instituto.

g) Ser un sitio accesible para las personas con discapacidad visual y auditiva; además sus contenidos se deberán exponer en las principales lenguas indígenas del Estado.

La dirección electrónica del portal electrónico del Instituto es www.iem.org.mx, Los sitios complementarios corresponden a todas las páginas web bajo el dominio iem.org.mx, que se desarrollen para la clasificación de información específica; por ejemplo, los micrositios de los procesos electorales locales, o los sistemas de información institucional.

El portal electrónico institucional y las páginas electrónicas complementarias deberán construirse atendiendo las recomendaciones que se establecen en los presentes Lineamientos, procurando una actualización constante con la finalidad de incorporar las mejoras necesarias, de acuerdo con el avance en materia de tecnologías de información y comunicaciones.

El mapa oficial del portal de Internet se compondrá por lo menos, de los segmentos o apartados siguientes:

I. Información General del Instituto

II. Estructura Orgánica

III. Estrados Electrónicos

IV. Partidos Políticos

V. Marco Legal

VI. Archivo con la documentación oficial para consulta

VII. Procesos Electorales

VIII. Publicaciones

IX. Transparencia

X. Redes Sociales

XI. Actividades del Instituto

Además, se deberán resaltar espacios informativos para temas especializados en Asuntos Indígenas, Derechos Humanos, Equidad de Género, Educación Cívica y Participación Ciudadana, Transparencia Proactiva, Migrantes, Violencia Política contra las mujeres en Razón de Género, diversidad sexual, entre otros.

La administración técnica del portal de Internet corresponde exclusivamente a la Coordinación de Informática.

Serán usuarios autorizados para la publicación de Contenido en el portal de Internet, la Secretaría Ejecutiva para la publicación de la documentación oficial del Consejo General y de la Junta Estatal Ejecutiva; la Coordinación de Comunicación Social, lo relativo a los segmentos de Noticias, Galería Institucional y Redes Sociales, Publicaciones (libros, revistas, cuadernillos, convocatorias, guías, manuales y otros); y a la Coordinación de Transparencia todo lo relativo al cumplimiento de las obligaciones que en dicha materia tiene el Instituto.

Para la publicación, modificación o retiro de Contenido del Portal de Internet, con excepción de los segmentos señalados en el artículo anterior, que se regirán por las disposiciones que emitan los titulares de las áreas mencionadas, se deberá seguir el procedimiento a continuación.

Toda la información que deba publicarse para cumplir con las obligaciones que impone la Ley de Transparencia, deberá cumplir con los términos, plazos y procedimientos que al efecto establece el Reglamento de Transparencia y Acceso a la Información del Instituto y demás normativa interna de la materia.

El Contenido que se publique en el Portal de Internet deberá cumplir con las características y criterios siguientes:

I. Características del Contenido del Portal de Internet:

a. Formatos abiertos (Información Proactiva). Estar disponible con el conjunto de características técnicas y de presentación que corresponden a la estructura lógica usada para almacenar datos en un archivo digital, cuyas especificaciones técnicas están disponibles públicamente, que no supongan una dificultad de acceso y que su aplicación y reproducción no esté condicionada a contraprestación alguna.

b. Disponibilidad. Debe estar disponible para cualquier persona, sin discriminación alguna o necesidad de registro, para lo cual la Coordinación de Informática, se encargará de realizar el trámite conducente para que los datos del contenido sean accesibles para las personas con discapacidad Visual y auditiva, y que los mismos se expongan en las principales lenguas indígenas del Estado.

c. Accesibilidad: Tendrá como finalidad que personas con algún tipo de discapacidad puedan percibir, entender, navegar, interactuar y hacer uso del portal de internet, contando con los elementos de Accesibilidad.

II. Criterios de contenido:

a. a Legalidad. La obligación normativa de publicar la información en el portal del Instituto será criterio determinante para las decisiones editoriales de publicación.

b. Prioridad de la publicación. La Coordinación de Informática, Comunicación Social y Transparencia, así como la Secretaría Ejecutiva, dependiendo del tipo de información de que se trate y de conformidad a cada una con sus atribuciones establecidas en los presentes Lineamientos, serán las instancias ante las que deberá justificarse el valor editorial del contenido que se desea publicar.

c. Confiabilidad y verificabilidad. El Contenido debe ser fidedigno, proporcionando elementos y/o datos que permitan identificar su origen, fecha de generación, de emisión, registro de actualizaciones y difusión de la misma, a fin de que sea posible comprobar la veracidad de la información.

d. Comprensibilidad. Debe estar estructurado de forma clara, precisa y sencilla, con un lenguaje simple que facilite la comprensión de la ciudadanía y público en general.

e. Oportunidad Deberá publicarse a tiempo, de tal manera que sea posible preservar su valor y sea útil para la toma de decisiones de los usuarios.

f. Viabilidad Técnica. Deberá ajustarse a las especificaciones técnicas que determine la Coordinación de Informática.

g. Mayor interés de la ciudadanía. Para la publicación de contenido, se tomarán en cuenta los datos que acrediten el grado de interés de la ciudadanía y público en general.

Para el seguimiento de las actividades de publicación web se creará un Grupo de Trabajo que estará conformado por la Presidencia del Instituto quien lo encabezará, una Consejería Electoral, así como por la Secretaría Ejecutiva, y las Coordinaciones de Informática, Comunicación Social y Transparencia y Acceso a la Información.

El Grupo de Trabajo se reunirá bimestralmente para revisar que el diseño y el contenido publicado cumpla con lo establecido en los presentes Lineamientos, previa convocatoria hecha por la Presidencia del Instituto.

Las áreas responsables ingresarán su solicitud de publicación a la Coordinación de Informática, a través del correo oficial, al menos con tres días de anticipación a la fecha en que requieran la publicación.

En aquellos casos en los que el Contenido que se pretenda publicar requiera de diseño gráfico, las áreas responsables deberán remitirlo previamente a la Persona Técnico de Diseño adscrito a la Coordinación de Comunicación Social, a efecto de que éste, realice las gestiones necesarias a efecto de pro\leer de conformidad.

En el caso de publicaciones urgentes en proceso electoral, vinculadas con el cumplimiento de sentencias, u otras que se justifiquen, su publicación deberá ser inmediata.

En el caso de publicaciones de documentación para las sesiones de Comisiones y Comités del Consejo General, así como la información de difusión, el plazo de presentación de la solicitud será con veinticuatro horas de anticipación.

Los tipos de solicitudes que podrán ingresar son los siguientes:

a. Actualización de contenido o información que ya se encuentra publicada en el portal de Internet del Instituto y que, por razón de su Vigencia, debe ser actualizada.
b. Corrección de contenido, información o secciones en las que existe algún error.

c. Creación de apartados y difusión. Estas solicitudes son aplicables para la generación apartados a incorporar dentro de las secciones ya existentes y previamente aprobadas por la Coordinación de Informática; pueden solicitarse siempre y cuando se respete la estructura del mapa de sitio.

d. Publicación. Contenido o documentos nuevos que no han sido publicados con anterioridad, pero que ya cuentan con un apartado específico dentro del portal de Internet.

e. Retiro, baja o eliminación de información por haber cumplido su vigencia, uso o utilidad, o bien porque normativamente es necesario retirarla, tomando en consideración los plazos establecidos en el Reglamento de Transparencia y Acceso a la Información Pública del Instituto. Las áreas responsables deberán conservar el respaldo de la información a retirar del portal de Internet.

Las solicitudes deberán contener, al menos los siguientes datos:

I. Nombre del titular del área que solicita la publicación o retiro de contenido.

II. Tipo de solicitud que realiza.

III. Archivo, formato, texto o diseño del contenido que se pretende publicar, actualizar o corregir, el cual deberá ser de fácil acceso.

IV. Indicar las razones o preceptos legales por la que se solicita su publicación o retiro.

V. Precisar el segmento o sección del Portal de Internet donde se solicita la publicación.

VI. Señalar la vigencia de su difusión de conformidad a lo establecido en el Reglamento de Transparencia y Acceso a la Información Pública del Instituto y demás normativa aplicable de la materia.

VII. La manifestación expresa de que el contenido que se solicita publicar se ajusta a las disposiciones aplicables en materia de transparencia y protección de datos personales.

VIII. Los contenidos ya deberán venir con el nombre que se subirán al sitio web, el cual deberá cumplir con lo establecido en el Anexo que contendrá las claves de información.

IX. Descripción de la publicación.

X. Al menos 10 palabras claves que hagan referencia al contenido de la publicación.

Una vez recibida la solicitud, la Persona técnica de publicación digital y la Coordinación de Informática, contarán con un plazo no mayor de dos días hábiles para revisar de forma simultánea, que la información a publicar se ajuste a los criterios establecidos en los presentes Lineamientos.

El plazo indicado podrá ser ampliado de manera excepcional por una sola vez, hasta por un periodo que no exceda de dos días, lo que deberán hacer del conocimiento del área responsable a través del correo electrónico oficial.

En caso de que se advierta el incumplimiento de algún criterio, dentro del plazo de verificación de la solicitud, deberá realizarse la observación correspondiente, a fin de que se atiendan las mismas, bajo el apercibimiento que, de no cumplir, la solicitud será improcedente y tratándose de Contenidos que por disposición legal tengan que ser publicados, se dará vista al órgano de control interno, a fin de que determine lo que en derecho corresponda. Las observaciones que se realicen en ningún caso podrán versar sobre la sustancia del contenido.

Las observaciones fundadas y motivadas que, en su caso emita la Coordinación de Informática, deberán ser remitidas por correo electrónico oficial al área solicitante, dentro del plazo de revisión.

Las áreas responsables contarán con un día hábil a partir de la recepción de las observaciones, para su atención.

La emisión de observaciones interrumpe el plazo de inicio del procedimiento, por lo que se tomará en consideración la fecha en que se reciba el desahogo correspondiente.

En caso de no haber observaciones o habiendo sido desahogadas las mismas, la Persona técnica de publicación digital contará con día hábil para otorgar el visto bueno y remitir la solicitud validada a la Coordinación de Informática.

Las solicitudes que sean realizadas por instituciones, organismos o en colaboración con alguna otra instancia, el área correspondiente deberá validar el contenido de la información, posteriormente se sujetará al procedimiento descrito en este manual.

La Coordinación de Informática, una vez recibida la solicitud validada por la Persona técnica de publicación digital dentro del día hábil siguiente publicará los Contenidos, salvo que por la dificultad y requerimientos técnicos que implique la solicitud, sea necesario ampliarlo, situación que se deberá hacer del conocimiento del área solicitante por correo electrónico oficial, indicando la fecha de publicación.

Una vez publicado el Contenido, la Coordinación de Informática deberá enviar el aviso correspondiente al área solicitante, a fin de que verifique y valide la atención a la solicitud. Si hubiera observaciones deberán ser remitidas por correo electrónico oficial, mismas que se deberán atender a más tardar al día siguiente.

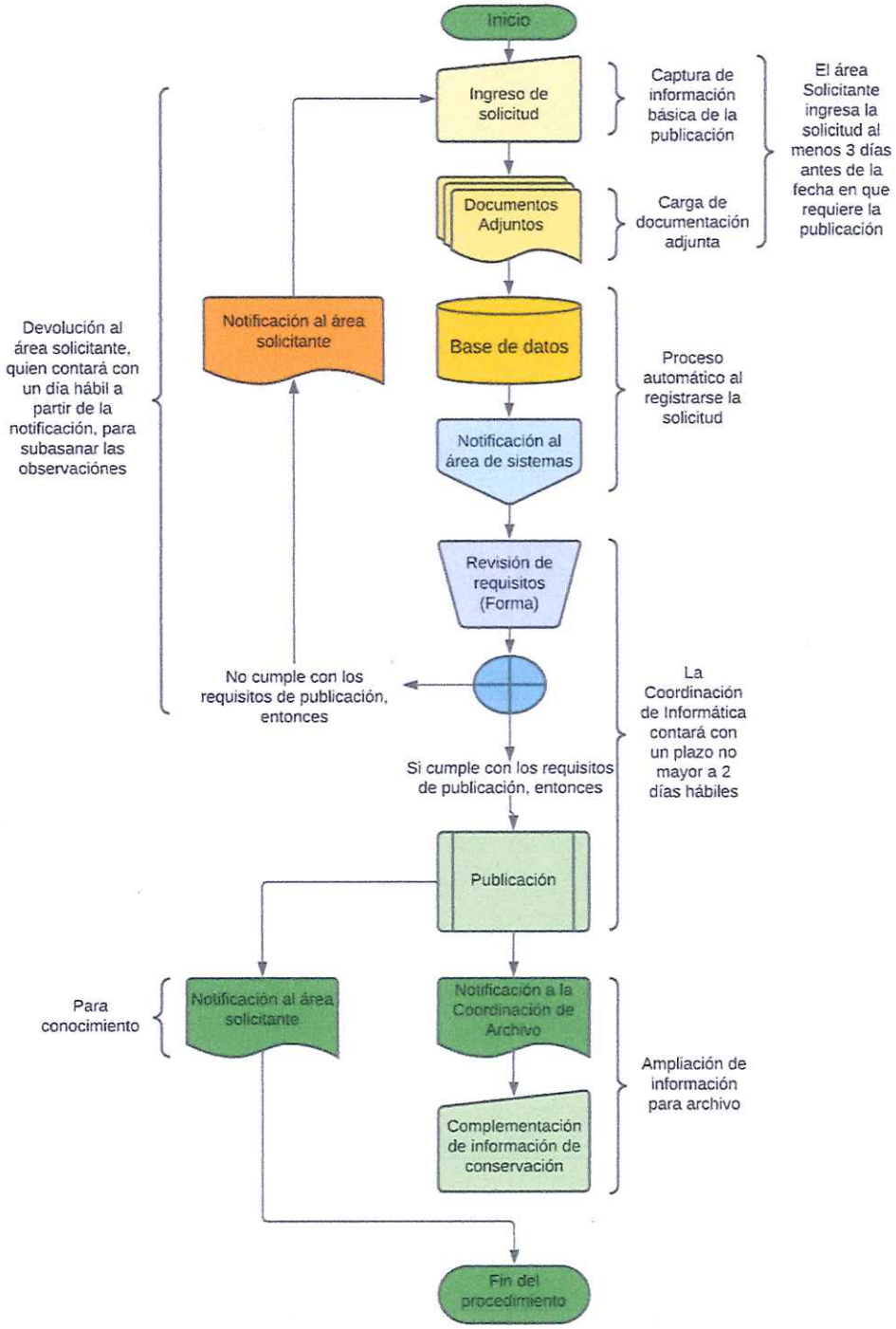
De igual forma notificará a la Coordinación de Archivo del Instituto, a efecto de que dicha área establezca la temporalidad que dicha publicación deberá conservarse de acuerdo con la vigencia documental que se establezca en el Catálogo de Disposición Documental en términos de lo establecido en el Reglamento de Archivos de este Instituto.

Tratándose de solicitudes urgentes derivadas de causas no previsibles o imputables al Área Responsable o por mandato expreso de autoridad y de resultar materialmente posible, deberá darse tratamiento prioritario a las mismas y recortarse los plazos señalados en el procedimiento de publicación establecido en los presentes Lineamientos.

Una vez hecha la publicación, esta no podrá ser reubicada en las secciones y apartados de los portales, salvo manifestación expresa del área que generó la información.

7.1.1 Flujograma del Procedimiento de Publicación y Gestión de Contenidos WEB

Diagrama del flujo de información del sistema de publicación WEB



7.2. Procedimiento de Solicitud de Creación, Modificación y Baja de Cuenta de Correo Institucional.

El correo electrónico institucional es una herramienta de comunicación e intercambio de información oficial entre las áreas internas del Instituto, así como a las distintas instituciones externas con las que el Instituto tiene relación, por lo que, queda estrictamente prohibido su uso para fines personales.

El sistema de correo electrónico es parte integral de los sistemas de información, por lo que, el único dueño de las cuentas, contraseñas, mensajes y contenidos es el Instituto, quien también es responsable de proteger la información sensible que en su caso llegare a haber.

Para la redacción del texto del correo, se deberá seguir la misma formalidad usualmente utilizada para la redacción de un oficio tradicional, como lo es el título de a quién va dirigido el documento, contenido del documento y el nombre de quien envía, con formato simple, evitando el uso generalizado de letras mayúsculas, además de tabuladores, debido a que, en ciertos usuarios de correo puede introducir caracteres no válidos.

Además de la redacción del texto de los correos, se deberán adjuntar a los mismos la documentación soporte para minimizar en la medida de lo posible la remisión de dichos documentos de manera impresa, para con ello lograr uno de los objetivos de estos Lineamientos que es el de optimizar los recursos e insumos tales como hojas de papel y consumibles de impresión.

En caso de que los usuarios tengan problemas técnicos al momento de adjuntar dicha documentación, podrán solicitar el apoyo y asesoría del personal de la Coordinación de Informática.

Para contribuir a una estandarización en la nomenclatura de los documentos adjuntos, se recomienda lo siguiente:

a. Utilizar sólo mayúsculas en el nombre del archivo.

b. El nombre del archivo deberá contener, de preferencia, guiones bajos para separación de los elementos que contenga.

c. De preferencia, el nombre del archivo deberá tener relación concisa con el asunto del correo electrónico emitido.

Los usuarios deberán contar con una firma preconfigurada para su uso

en la redacción del correo electrónico, que será elaborada por la persona encargada del área técnica de diseño de la Coordinación de Comunicación Social, misma que deberá contener al menos la siguiente estructura:

Nombre Completo – Cargo

Área de Adscripción

Correo Electrónico | Teléfono conmutador y extensión (en su caso).

IEM Instituto Electoral de Michoacán

Bruselas 118, Colonia Villa Universidad. (Domicilio de oficina alterna en su caso)

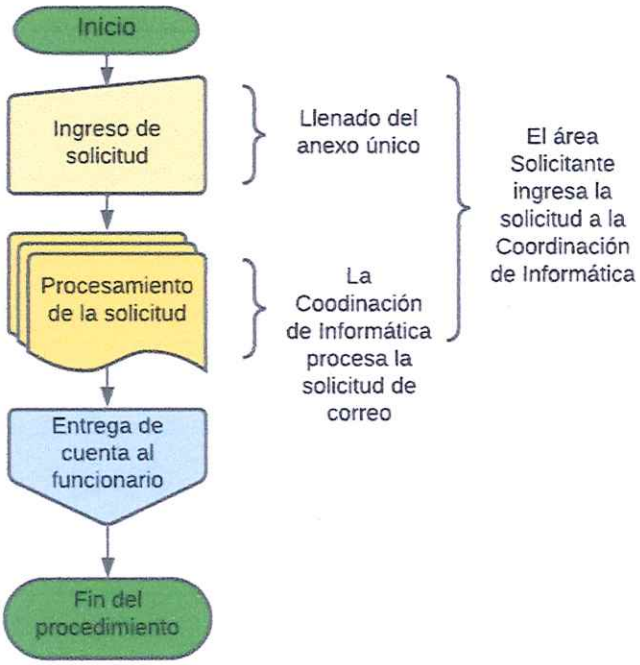
Morelia, Michoacán,58060

www.iem.org.mx

Para la generación de trámite de cuenta de correo, ya sea alta, modificación o baja de cuenta institucional, bastará con la notificación a la Coordinación de Informática a través del Anexo único establecido en los Lineamientos para el correcto uso del Correo Electrónico Institucional, el cual estará suscrito por el Titular del área solicitante, el Titular de la cuenta solicitada, y el Vo.Bo. de la Coordinación de Informática.

7.2.1 Flujograma del Procedimiento para la solicitud de creación, modificación o baja de cuentas de correo institucionales

Diagrama de flujo del Procedimiento para la solicitud de creación, modificación o baja de cuentas de correo institucionales



8. Anexos

ANEXO ÚNICO

Formato para la creación, modificación, suspensión y/o cancelación de cuentas de correo electrónico del Instituto Electoral de Michoacán por parte de la Coordinación de Informática

Datos Generales		
Área de Adscripción:		
Nombre del Titular de la Cuenta:		
Puesto:		
Tipo de Solicitud:		
	Creación de Cuenta	Cancelación de Cuenta
Nombre de quien realiza la solicitud:		
Nombre de usuario:		
Contraseña*:		

La persona titular de la cuenta de correo electrónico institucional se compromete a utilizar la misma de conformidad a lo establecido en los Lineamientos para el Correcto Uso del Correo Electrónico del Instituto Electoral de Michoacán, como medio de comunicación oficial por lo que, queda estrictamente prohibido su uso para fines personales, reconociendo que la información contenida en el mismo es propiedad exclusiva del Instituto, por lo que, manifiesta desde este momento su consentimiento para que una vez concluida la relación laboral con el mismo, la Coordinación de Informática proceda a elaborar el respaldo de dicha información y a la cancelación de la misma, con la debida protección de datos personales que pudieran encontrarse en el mismo.

Titular del área solicitante	Titular de la cuenta	Vo.Bo. Coordinación de Informática
Nombre y Firma	Nombre y Firma	Nombre y Firma

*La contraseña proporcionada deberá ser cambiada por las y los usuarios titulares de las cuentas.

8.1. Glosario de Términos

I. Contraseña: Conjunto de letras y números que se encuentran asociados a una cuenta de usuario para poder acceder a determinada aplicación y/o servicio.

II. Código de Conducta: Código de Conducta de las Personas Servidoras Públicas del Instituto Electoral de Michoacán.

III. Código de Ética: Código de Ética de las Personas Servidoras Públicas del Instituto Electoral de Michoacán.

IV. Correo Electrónico Institucional: Es el servicio de mensajería del Instituto que permite el intercambio de documentos electrónicos utilizando como medio de transporte la intranet o el internet, que administra la Coordinación de Informática a través de cuentas de correo electrónico.

V. Coordinación de Informática: La Coordinación de Informática del Instituto Electoral de Michoacán.

VI. Datos sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

VII. Información confidencial: Se considera información confidencial la que contiene datos personales concernientes a una persona identificada o identificable.

VIII. Instituto: El Instituto Electoral de Michoacán.

IX. Lineamientos: Los Lineamientos para el correcto uso del correo electrónico del Instituto Electoral de Michoacán.

X. Phishing: Término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza (suplantación de identidad de tercero

de confianza), para manipularla y hacer que realice acciones que no debería realizar (por ejemplo, revelar información confidencial o hacer click en un enlace).

XI. Secretaría Ejecutiva: Secretaría Ejecutiva del Instituto Electoral de Michoacán.

XII. Servidores Públicos: Las trabajadoras y los trabajadores que prestan un servicio físico, intelectual, técnico o administrativo subordinado al Instituto Electoral de Michoacán.

XIII. Spyware: Software diseñado para recopilar datos de un ordenador u otro dispositivo y reenviarlos a un tercero sin el conocimiento o consentimiento del usuario.

XIV. Usuario: Las y los servidores públicos que tiene asignada una cuenta de correo electrónico institucional.

XV. URL. Acrónimo del inglés Uniform Resource Locator (localizador de recursos uniforme), es como comúnmente se conoce a una dirección web, en referencia a un recurso web que especifica su ubicación en una red informática y un mecanismo para la recuperación de esta misma.

XVI. Virus: Es un tipo de programa o código malicioso escrito para modificar el funcionamiento de un equipo.