

|  |
| --- |
|  |
| Instituto Nacional de las Mujeres |
|  |
| ***UNIDAD DE INFORMÁTICA*** |

**Políticas para la Gestión Operativa de Tecnologías de Información**

23 de julio del 2014

Control de versiones del documento

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión #** | **Notas** | **Fecha** | **Desarrolado por** |
| **1.00** | **Versión Inicial** | **8 de agosto del 2011** | **INAMU:**   * **Ingrid Trejos Marin** * **José Pablo Beita Granados**   **Dinámica Consultores:**   * **Freddy Ramírez Mora** |
| **2.00** | **Actualización general** | **18 de enero del 2013** | **INAMU:**   * **Ingrid Trejos Marin**   **Dinámica Consultores:**   * **Sergio De León Treviño** |
| **2.01** | **Actualización punto 1.4 para cumplir con recomendación de la Unidad de Asesoría Legal (Oficio AL-060-13)** | **1 de abril del 2013** | **INAMU:**   * **Ingrid Trejos Marin**   **Dinámica Consultores:**   * **Sergio De León Treviño** |
| **2.02** | **Actualización Comité Tecnologías de Información** | **19 de setiembre del 2013** | **Comité de Tecnologías de Información** |
| **3.0** | **Actualización con base en observaciones del Comité de Tecnologías de Información** | **03 de febrero del 2014** | **Comité de Tecnologías de Información** |
| **4.0** | **Actualización y revisión para presentación a Junta Directiva** | **1 de abril del 2014** | **Ingrid Trejos Marin, Unidad de Informática** |
| **20140723** | **Actualización General** | **Julio del 2014** | **INAMU:**   * **Ingrid Trejos Marin**   **Dinámica Consultores:**   * **Sergio De León Treviño** |
| **20190327** | **Aprobación Política número 21.** | **Marzo 2019** | **Junta Directiva** |

**Aprobación final**

**Aprobado por Junta Directiva en Sesión Ordinaria No. 13-2014 del 2 de febrero del 2014.**

Contenido

[1. Marco General de Cumplimiento 6](#_Toc13585816)

[1.1. Presentación 6](#_Toc13585817)

[1.2. Comisión de Tecnologías de Información 6](#_Toc13585818)

[1.3. Comunicación de las políticas y procedimientos 6](#_Toc13585819)

[1.4. Sanciones por incumplimiento 6](#_Toc13585820)

[1.5. Marco legal y jurídico 7](#_Toc13585821)

[1.6. Glosario de Términos 7](#_Toc13585822)

[1.7. Revisión y actualización de las políticas 7](#_Toc13585823)

[2. Políticas para la gestión de la calidad. 8](#_Toc13585824)

[2.1. Propósito 8](#_Toc13585826)

[2.2. Alcance 8](#_Toc13585827)

[2.3. Declaración de políticas 8](#_Toc13585828)

[2.3.1. Manual de calidad 8](#_Toc13585834)

[2.3.2. Diseño de formatos y formularios 8](#_Toc13585835)

[2.3.3. Aseguramiento de la calidad en los desarrollos 8](#_Toc13585836)

[2.3.4. Evaluaciones de la calidad y seguimiento a sus resultados 8](#_Toc13585837)

[2.3.5. Gestión y cumplimiento de la normativa vigente 9](#_Toc13585838)

[3. Políticas para asegurar la independencia y recurso humano de la función de TI 10](#_Toc13585839)

[3.1. Propósito 10](#_Toc13585841)

[3.2. Alcance 10](#_Toc13585842)

[3.3. Declaración de políticas 10](#_Toc13585843)

[3.3.1. Actualización del manual de puestos 10](#_Toc13585848)

[3.3.2. Actualización de normas, métodos y procedimientos 10](#_Toc13585849)

[3.3.3. Divulgación de los cambios en procedimientos, instructivos, normas, etc. 10](#_Toc13585850)

[3.3.4. Gestión del Recurso Humano 11](#_Toc13585851)

[3.3.5. Plan de rotación de personal 11](#_Toc13585852)

[3.3.6. Plan de capacitación 11](#_Toc13585853)

[4. Políticas para la administración de recursos financieros. 12](#_Toc13585854)

[4.1. Propósito 12](#_Toc13585856)

[4.2. Alcance 12](#_Toc13585857)

[4.3. Declaración de políticas 12](#_Toc13585858)

[4.3.1. Proceso de compra 12](#_Toc13585863)

[4.3.2. Presupuesto para la adquisición de recursos tecnológicos 12](#_Toc13585864)

[4.3.3. Validación, ejecución y seguimiento de contratos y carteles 13](#_Toc13585865)

[4.3.4. Coordinación del proceso presupuestario 13](#_Toc13585866)

[4.3.5. Análisis de costo beneficio de la inversión de TI 13](#_Toc13585867)

[5. Políticas sobre las consideraciones generales de la implementación de TI. 14](#_Toc13585868)

[5.1. Propósito 14](#_Toc13585870)

[5.2. Alcance 14](#_Toc13585871)

[5.3. Declaración de políticas 14](#_Toc13585872)

[5.3.1. Definición de imágenes para equipo de cómputo 14](#_Toc13585877)

[6. Políticas para la implementación de software 15](#_Toc13585878)

[6.1. Propósito 15](#_Toc13585880)

[6.2. Alcance 15](#_Toc13585881)

[6.3. Declaración de políticas 15](#_Toc13585882)

[6.3.1. Administración de cambios 15](#_Toc13585887)

[7. Políticas para la implementación de infraestructura tecnológica 16](#_Toc13585888)

[7.1. Propósito 16](#_Toc13585890)

[7.2. Alcance 16](#_Toc13585891)

[7.3. Declaración de políticas 16](#_Toc13585892)

[7.3.1. Contrato de mantenimiento de recursos críticos 16](#_Toc13585897)

[7.3.2. Diseño y documentación de red (diagramas) 16](#_Toc13585898)

[7.3.3. Seguridad de los equipos de red 16](#_Toc13585899)

[7.3.4. Plan de infraestructura de TI 16](#_Toc13585900)

[7.3.5. Mantenimiento de la infraestructura de TI 17](#_Toc13585901)

[7.3.6. Adquisición de recursos de TI 17](#_Toc13585902)

[8. Políticas para la contratación de terceros para la implementación y mantenimiento de software e infraestructura. 18](#_Toc13585903)

[8.1. Propósito 18](#_Toc13585905)

[8.2. Alcance 18](#_Toc13585906)

[8.3. Declaración de políticas 18](#_Toc13585907)

[8.3.1. Administración de servicios de terceros 18](#_Toc13585912)

[8.3.2. Administración de proveedores 19](#_Toc13585913)

[9. Políticas para la definición y administración de acuerdos de servicio. 20](#_Toc13585914)

[9.1. Propósito 20](#_Toc13585916)

[9.2. Alcance 20](#_Toc13585917)

[9.3. Declaración de políticas 20](#_Toc13585918)

[9.3.1. Catálogo de servicios de TI 20](#_Toc13585923)

[10. Políticas para la administración y operación de la plataforma tecnológica 21](#_Toc13585924)

[10.1. Propósito 21](#_Toc13585926)

[10.2. Alcance 21](#_Toc13585927)

[10.3. Declaración de políticas 21](#_Toc13585928)

[10.3.1. Plan de capacidad y desempeño 21](#_Toc13585933)

[10.3.2. Sustitución de servidores 21](#_Toc13585934)

[10.3.3. Sustitución de equipo de comunicaciones 22](#_Toc13585935)

[10.3.4. Monitoreo de recursos críticos 22](#_Toc13585936)

[10.3.5. Parámetros de rendimiento 22](#_Toc13585937)

[10.3.6. Revisión y reporte de instalación de software no autorizado 22](#_Toc13585938)

[10.3.7. Actualización y verificación de información de configuración 23](#_Toc13585939)

[10.3.8. Solicitudes para la ejecución de procesos 23](#_Toc13585940)

[10.3.9. Copias de archivos entre los ambientes de producción y desarrollo 23](#_Toc13585941)

[11. Políticas para la atención de requerimientos de las personas usuarias de TI 23](#_Toc13585942)

[11.1. Propósito 23](#_Toc13585944)

[11.2. Alcance 23](#_Toc13585945)

[11.3. Declaración de políticas 24](#_Toc13585946)

[11.3.1. Catálogo de servicios de TI 24](#_Toc13585951)

[12. Políticas para la administración de servicios prestados por terceros. 24](#_Toc13585952)

[12.1. Propósito 24](#_Toc13585954)

[12.2. Alcance 24](#_Toc13585955)

[12.3. Declaración de políticas 24](#_Toc13585956)

[12.3.1. Administración de servicios y contratos de servicios de terceros 24](#_Toc13585961)

[12.3.2. Administración de proveedores de TI 24](#_Toc13585962)

[12.3.3. Evaluación y suspensión de proveedores de TI 24](#_Toc13585963)

[13. Políticas para el seguimiento de los procesos de TI. 25](#_Toc13585964)

[13.1. Propósito 25](#_Toc13585966)

[13.2. Alcance 25](#_Toc13585967)

[13.3. Declaración de políticas 25](#_Toc13585968)

[13.3.1. Seguimiento del Plan Operativo 25](#_Toc13585973)

[13.3.2. Mejoramiento continuo 25](#_Toc13585974)

[14. Políticas para la confidencialidad, integridad y disponibilidad de los datos de la plataforma tecnológica. 25](#_Toc13585975)

[14.1. Propósito 25](#_Toc13585977)

[14.2. Alcance 26](#_Toc13585978)

[14.3. Declaración de políticas 26](#_Toc13585979)

[14.3.1. Pertenencia de los datos y equipo de la plataforma tecnológica 26](#_Toc13585985)

[14.3.2. Confidencialidad de los datos y la información 26](#_Toc13585986)

[14.3.3. Resguardo de los datos e información 26](#_Toc13585987)

[14.3.4. Solicitud y salida de información de la Institución 27](#_Toc13585988)

[15. Políticas para el uso de la plataforma tecnológica de la Institución. 27](#_Toc13585989)

[15.1. Propósito 27](#_Toc13585991)

[15.2. Alcance 27](#_Toc13585992)

[15.3. Declaración de políticas 27](#_Toc13585993)

[15.3.1. Uso de los recursos de la plataforma tecnológica 27](#_Toc13585994)

[15.3.1. Asignación y distribución de los equipos de la plataforma tecnológica 28](#_Toc13585995)

[15.3.2. Equipo nuevo en la plataforma tecnológica y equipos de terceros 28](#_Toc13585996)

[15.3.3. Seguimiento de los equipos de la plataforma tecnológica 28](#_Toc13585997)

[15.3.4. Salida del equipo de la plataforma tecnológica de las instalaciones 29](#_Toc13585998)

[15.3.5. Detección de fallas en los equipos de la plataforma tecnológica 29](#_Toc13585999)

[15.3.6. Licenciamiento del software de la plataforma tecnológica 29](#_Toc13586000)

[16. Políticas para la seguridad física de las instalaciones de tecnologías de información. 30](#_Toc13586001)

[16.1. Propósito 30](#_Toc13586003)

[16.2. Alcance 30](#_Toc13586004)

[16.3. Declaración de políticas 30](#_Toc13586005)

[16.3.1. Acceso físico 30](#_Toc13586010)

[16.3.2. Condiciones ambientales 30](#_Toc13586011)

[17. Políticas para la seguridad lógica de la plataforma tecnológica. 31](#_Toc13586012)

[17.1. Propósito 31](#_Toc13586014)

[17.2. Alcance 31](#_Toc13586015)

[17.3. Declaración de políticas 31](#_Toc13586016)

[17.3.1. Solicitud y mantenimiento de los accesos a la plataforma tecnológica 31](#_Toc13586021)

[17.3.2. Control de software no autorizado 32](#_Toc13586022)

[17.3.3. Control de los ataques de virus 32](#_Toc13586023)

[17.3.4. Uso de claves, contraseñas y palabras de paso 33](#_Toc13586024)

[17.3.5. Palabras de paso para equipos principales de la plataforma tecnológica 34](#_Toc13586025)

[17.3.6. Uso de Internet y Correo Electrónico 35](#_Toc13586026)

[18. Políticas para el aseguramiento de la continuidad de las operaciones. 35](#_Toc13586027)

[18.1. Propósito 35](#_Toc13586029)

[18.2. Alcance 35](#_Toc13586030)

[18.3. Declaración de políticas 35](#_Toc13586031)

[18.3.1. Mantenimiento y niveles del servicio de la plataforma tecnológica 35](#_Toc13586036)

[18.3.2. Respaldos y resguardo de información de las bases de datos 36](#_Toc13586037)

[18.3.3. Respaldos de la información de la computación de la persona usuaria final 36](#_Toc13586038)

[18.3.4. Capacidad de la plataforma tecnológica 37](#_Toc13586039)

[18.3.5. Administración de problemas 37](#_Toc13586040)

[18.3.6. Administración de la configuración 37](#_Toc13586041)

[18.3.7. Procesamiento de datos alterno 37](#_Toc13586042)

[19. Políticas para seguimiento y evaluación del control interno en TI. 38](#_Toc13586043)

[19.1. Propósito 38](#_Toc13586045)

[19.2. Alcance 38](#_Toc13586046)

[19.3. Declaración de políticas 38](#_Toc13586047)

[19.3.1. Autoevaluación de la Unidad de Informática 38](#_Toc13586052)

[19.3.2. Monitoreo y evaluación del control interno 38](#_Toc13586053)

[20. Políticas sobre la participación de la Auditoría Interna. 39](#_Toc13586054)

[20.1. Propósito 39](#_Toc13586056)

[20.2. Alcance 39](#_Toc13586057)

[20.3. Declaración de políticas 39](#_Toc13586058)

[20.3.1. Monitoreo y evaluación del control interno 39](#_Toc13586063)

[21. Política para el seguimiento y evaluación del Plan Estratégico de Tecnologías de Información, PETI vigente y las Políticas de Gestión Operativa de Tecnologías de Información. 39](#_Toc13586064)

[21.1. Propósito 39](#_Toc13586065)

[21.2. Alcance 39](#_Toc13586066)

[21.3. Declaración de políticas 39](#_Toc13586067)

[21.3.1. Sobre el seguimiento y evaluación del Plan Estratégico de Tecnologías de Información: 40](#_Toc13586068)

# Marco General de Cumplimiento

## Presentación

El Instituto Nacional de las Mujeres, en adelante “La Institución”, proporcionará a las personas colaboradoras la utilización de las herramientas tecnológicas necesarias para el procesamiento, transmisión y análisis de datos generados a partir de la naturaleza de las operaciones diarias, con el propósito de facilitar las labores que les son asignadas en sus respectivos puestos de trabajo.

La información gestionada por la plataforma tecnológica de la Institución es considerada como un activo de gran valor en su desarrollo y crecimiento, por lo cual es responsabilidad de las personas colaboradoras velar por el adecuado funcionamiento y resguardo de las herramientas implícitas en ésta.

Dentro de este marco, la Institución establece el siguiente conjunto de políticas y procedimientos para la gestión operativa de la Unidad de Informática del INAMU, con el propósito de cumplir con los requerimiento regulatorios a los que la Institución está sujeta.

## Comisión de Tecnologías de Información

La Comisión de Tecnologías de Información de la Institución es el ente recomendativo, con respecto a la planificación, administración y toma de decisiones referente a la plataforma tecnológica, el cual reporta a la Presidencia Ejecutiva. Sus integrantes, funciones y responsabilidades se encuentran integradas en la Circular de conformación de la Comisión de Tecnologías de Información.

## Comunicación de las políticas y procedimientos

Mediante circular Institucional de la Presidencia Ejecutiva, serán difundidas y distribuidas a todas las personas colaboradoras de la Institución.

## Sanciones por incumplimiento

En caso de incumplimiento de las políticas para la gestión y control de tecnología de información de La Institución, por parte de alguna persona colaboradora, la Jefatura respectiva y la Unidad de Informática, serán responsables de realizar la documentación de la situación y presentar las respectivas evidencias ante la Presidencia Ejecutiva de la Institución.

Será responsabilidad de la Presidencia Ejecutiva del INAMU aplicar las respectivas sanciones o descargo de la situación a la persona colaboradora según las consideraciones pertinentes.

## Marco legal y jurídico

El marco legal y jurídico de la Institución son las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE) de la Contraloría General de la República, publicadas en La Gaceta No. 119 del 21 de junio 2007.

## Glosario de Términos

**Plataforma tecnológica:** se refiere al aspecto tecnológico de un sistema de información, incluye el hardware, las bases de datos, el software, las redes y otros dispositivos.

**Respaldos:** Mecanismo de control y resguardo que permite recuperar la información de la Institución ante eventuales fallas en el funcionamiento de los equipos que almacenan la información.

**La Institución:** Instituto Nacional de las Mujeres (INAMU)

**Hardware:** Dispositivos físicos que componen la plataforma tecnológica de la Institución, como por ejemplo: computadoras de escritorio y portátiles, equipos de red, servidores, etc.

**Software:** Programas, aplicaciones, herramientas, sistemas, que permiten a partir del uso del hardware realizar procesos de comunicación, procesamiento de datos, etc.

## Revisión y actualización de las políticas

Las políticas para la gestión operativa de la Unidad de Tecnología de Información del INAMU deberán ser revisadas y actualizadas al menos una vez al año por la Comisión de Tecnologías de Información.

La aprobación de la revisión y actualización de dichas políticas será responsabilidad de la Junta Directiva de La Institución.

Si producto de la revisión de las políticas para la utilización de la plataforma tecnológica de La Institución, se determina que se deben realizar modificaciones se deberá seguir el control de versión siguiente:

* Se asignará el número de versión al documento de acuerdo a la fecha de modificación en el siguiente formato: AAAAMMDD, AAAA: Año (cuatro dígitos), MM: Número de mes (dos dígitos), DD: Día (dos dígitos).

# Políticas para la gestión de la calidad.



## Propósito

Garantizar que la Unidad de Informática esté dando valor a la Institución, mejora continua y transparencia para las personas interesadas.

## Alcance

Los lineamientos mencionados en la presente política aplican a todas las personas colaboradoras de la Institución.

## Declaración de políticas



# Manual de calidad

* Se deberá definir un “Manual de Calidad en TI” donde se definan el marco y los principios de calidad que aseguren que la entrega de servicios de TI se orienten hacia el impulso y la sostenibilidad tecnológica a los servicios porporcionados por las diferentes áreas del INAMU, enfocándose en la satisfacción de las personas usuarias mediante procesos eficientes y control del riesgo.
* Se deberá establecer un plan de trabajo de aseguramiento y verificación de la calidad basado en el Manual de referencia y con enfoque de mejoramiento continuo.

# Diseño de formatos y formularios

* Cualquier formato y/o formulario que se diseñe o actualice para realizar y estandarizar los procedimientos de la Unidad de Informática y sus dependencias deberán estar basados en el Manual de Identidad del Inamu.

# Aseguramiento de la calidad en los desarrollos

* La responsabilidad de definir la calidad de los productos y entregables del proyecto, durante y en la finalización del mismo, corresponderá directamente a la Jefatura de la Unidad de Informática, o en su caso, a la persona responsable del proyecto según su envergadura (Persona administradora de Proyecto o líder técnico), y la Jefatura de la Unidad solicitante del sistema.

# Evaluaciones de la calidad y seguimiento a sus resultados

* Se deben llevar a cabo evaluaciones de calidad de los proyectos y otros servicios brindados por la Unidad de Informática en conjunto con las Unidades a cargo, a fin de verificar el cumplimiento de las funciones, requisitos, procedimientos, metodologías, procesos y estándares establecidos, e informar de los resultados obtenidos de dichas evaluaciones a la Comisión de Tecnologías de Información,así como a la Presidencia Ejecutiva.
* Las no conformidades identificadas durante las evaluaciones de calidad o durante las actividades del día a día deberán ser atendidas de acuerdo con negociación previa en el plazo estipulado para el logro del objetivo de cada actividad.
* Las propuestas de mejora (acciones correctivas y preventivas) señaladas basándose en no conformidades detectadas, deberán de llevarse a cabo obligatoriamente por el personal de la Unidad de Informática en el período de tiempo acordado.
* En caso de existir acciones correctivas y preventivas, se deberá presentar un informe y su estado de atención a la Comisión de Tecnologías de Información para su información, seguimiento e intervención en caso de incumplimiento de las partes responsables.

# Gestión y cumplimiento de la normativa vigente

* Será responsabilidad de la jefatura de la Unidad de Informática:
  + Vigilar que el reglamento, políticas, metodologías y procedimientos aplicables se respeten y lleven a cabo en conformidad
  + Comunicar y escalar las excepciones en los controles establecidos previamente a que los mismos sean aplicados.
  + Revisar y actualizar continuamente las metodologías y procedimientos correspondientes a las actividades técnicas informáticas, al menos cada dos años, o bien cuando se presenten cambios. Estos cambios serán comunicados a la Comisión de Tecnologías de Información, elevados a la Presidencia Ejecutiva y publicadas en el medio adecuado.
* Se debe controlar y mantener la documentación original y actualizada de la normatividad vigente, incluyendo entre otros, el reglamento, políticas, metodologías, procedimientos, estándares de programación y normas de operación de la Unidad de Informática.
* De forma trimestral la Unidad de Informática realizará un reporte informativo al Comisión de Tecnologías de Información sobre los documentos pendientes de actualizar por referentes a la normatividad de tecnologías de información y, entre otros, cambios a sistemas, cambios en la infraestructura tecnológica, solicitud y préstamo de software para su instalación, el cual será enviado a la Comisión de Tecnologías de Información para su cumplimiento inmediato y revisado.

# Políticas para asegurar la independencia y recurso humano de la función de TI



## Propósito

Garantizar la independencia de la Función de TI respecto de las áreas usuarias y que ésta mantenga la coordinación y comunicación con las demás dependencias internas y externas y el uso correcto y eficiente de los recursos de la plataforma tecnológica de la Institución. Asimismo, garantizar la adquisición, mantenimiento y motivación de una fuerza de trabajo para la creación y entrega de servicios de TI para las unidades, facilitando el ambiente de gobierno y control interno.

## Alcance

Los lineamientos mencionados en la presente política aplican a todas las personas colaboradoras de la Institución.

## Declaración de políticas



# Actualización del manual de puestos

* Los perfiles de TI incluidos en el Manual de Puestos Institucional deberán actualizarse al menos una vez cada dos años para lo cual la Unidad de Informática deberá coordinar las acciones requeridas con el Área de Recursos Humanos.

# Actualización de normas, métodos y procedimientos

* Se deberán revisar y actualizar continuamente las normas de operación, metodologías y procedimientos correspondientes a las actividades de la Unidad de Informática, al menos cada dos años, las cuales deberán ser presentadas a la Comisión de Teconologías de Información y posteriormente elevadas a la Presidencia.

# Divulgación de los cambios en procedimientos, instructivos, normas, etc.

* La Unidad de Informática deberá publicar los cambios a métodos, procedimientos, instructivos, normas, documentos, entre otros, relacionados a la gestión de las TI y bajo las recomendaciones de la Comisión de Tecnologías de Información y el aval de la Presidencia Ejecutiva.

# Gestión del Recurso Humano

* La Jefatura de la Unidad de Informática será la persona encargada de autorizar cualquier trámite de nombramientos, ascensos e ingresos relacionados al personal de la Unidad de Informática, con el debido respaldo del Área de Recursos Humanos.
* La Jefatura de la Unidad de Informática será la persona encargada de asegurar la debida segregación de funciones entre el personal de dicha Unidad, a fin de evitar la concentración de funciones, separar funciones incompatibles, y aplicar controles compensatorios en caso necesario, incluyendo la contratación de terceros para prevenir o reducir el riesgo de errores o irregularidades en los procesos y servicios propios de la Unidad de Informática.

# Plan de rotación de personal

* La Jefatura de la Unidad de Informática deberá ser cubierta por una persona colaboradora, y viceversa, de manera temporal al menos anualmente, considerando lo siguiente:
  + Las necesidades propias del área
  + Como una medida de control interno para validar la ejecución de funciones, los procesos y los procedimientos aplicados.
  + Como apoyo a la continuidad de las funciones, para distribución del conocimiento y evitar que el mismo recaiga en una sola persona.
  + Al finalizar la rotación temporal de funciones, los involucrados deben realizar un informe que respalde los puntos anteriores.

# Plan de capacitación

* La Unidad de Informática deberá elaborar, revisar y actualizar al menos una vez por año los planes de capacitación de su personal de acuerdo con los objetivos y metas propuestos. Lo anterior a partir de la evaluación del desempeño que se realiza a nivel Institucional de forma anual y al plan de capacitación presentado de forma anual a la Presidencia Ejecutiva.
* Cualquier requerimiento de capacitación requerirá del visto bueno de la Unidad de Informática.

# Políticas para la administración de recursos financieros.



## Propósito

Fomentar la asociación entre TI y las necesidades Institucionales, facilitar el uso efectivo y eficiente de recursos de TI, y brindar transparencia y responsabilidad dentro del costo total de la propiedad, la materialización de los servicios Institucionales y el seguimiento y control de las inversiones en TI.

## Alcance

Los lineamientos mencionados en la presente política aplican a todas las personas colaboradoras de la Institución.

## Declaración de políticas



# Proceso de compra

* Cualquier compra que requiera efectuar la Unidad de Informática, deberá tramitarse de acuerdo al proceso y las políticas del Área de Proveeduría.
* Antes de concretar cualquier compra, la Unidad de Informática deberá efectuar un análisis de factibilidad y mercado requerido para utilizar/implementar el objeto de la compra, a fin de establecer el plazo contractual adecuado.

# Presupuesto para la adquisición de recursos tecnológicos

* Cualquier trámite que afecte el presupuesto asignado para la adquisición de recursos tecnológicos deberá seguir las políticas y procedimientos vigentes en la Institución.
* Cualquier alta, baja o actualización a los artículos considerados como recursos tecnológicos deberá identificar los beneficios correspondientes, o bien, incluir la justificación adecuada.
* El presupuesto anual de la Unidad de Informática correspondiente a los proyectos y objetivos propuestos y establecidos en el Plan Estratégico de Tecnologías de Información, es autorizado por la Junta Directiva de la Institución.

# Validación, ejecución y seguimiento de contratos y carteles

* La Jefatura de la Unidad de Informática será la responsable de:
  + Definir el objeto de contratación, los requerimientos y la validación de los carteles de contratación en conjunto con las unidades involucradas.
  + Asegurar el cumplimiento de los acuerdos entre las partes involucradas
  + Informar cualquier incumplimiento a la Comisión de Tecnologías de Información a fin de analizar las posibles consecuencias.
  + Definir a la luz de la metodología de administración de proyectos los diferentes roles y responsabilidades de las diferentes personas involucradas en un proyecto.
  + Velar en conjunto con las unidades involucradas, por el cumplimiento de las responsabilidades según se defina en los documentos elaborados.

# Coordinación del proceso presupuestario

* El presupuesto anual de la Unidad de Informática, debe ser definido, coordinado, consolidado, y justificado por la Jefatura de la Unidad de Informática, apoyado con las diferentes áreas financieras involucradas en el proceso presupuestario institucional.
* La persona encargada de la Unidad de Informática estimará el presupuesto requerido para sus planes y actividades regulares enviando dicha estimación en la fecha que en que la unidad encargada del presupuesto institucional así lo solicite.
* El presupuesto de la Unidad de Informática deberá estar alineado al plan estratégico de tecnología de información y al Plan Operativo Institucional.
* La jefatura de la Unidad de Informática deberá poner el presupuesto a consideración y aprobación por parte de la Presidencia Ejecutiva. Una vez aprobado por esta instancia, es elevado a la Unidad de Planificación para su trámite correspondiente.

# Análisis de costo beneficio de la inversión de TI

* La inversión de TI debe ser propuesta por la jefatura de la Unidad de Informática en conjunto con las demás personas interesadas y/o Unidades solicitantes a fin de facilitar la identificación, control de costos y beneficios totales e individuales de cada proyecto del portafolio acordado en el plan estratégico y operativo de TI.

# Políticas sobre las consideraciones generales de la implementación de TI.



## Propósito

Garantizar que exista un soporte tecnológico continuo para las aplicaciones.

## Alcance

Los lineamientos mencionados en la presente política aplican a todas las personas colaboradoras de la Institución.

## Declaración de políticas



# Definición de imágenes para equipo de cómputo

* Las personas colaboradoras de la Unidad de Informática, con base en las necesidades de las áreas de la Institución, definirá y actualizará periódicamente las características de software a instalar en los equipos de persona usuaria final (escritorio, laptops, etc.).
* La Unidad de Informática es la única autorizada para la instalación de las imágenes de software en los equipos utilizados por las personas usuarias finales (equipos de escritorio, laptops, etc.).

# Políticas para la implementación de software



## Propósito

Garantizar que exista un soporte tecnológico continuo para las aplicaciones.

## Alcance

Los lineamientos mencionados en la presente política aplican a todas las personas colaboradoras de la Institución.

## Declaración de políticas



# Administración de cambios

* Los archivos solo podrán ser modificados por un solo colaborador de la Unidad de Informática a la vez.
* Es obligación del personal de la Unidad de Informática el mantener las versiones de los archivos debidamente actualizadas, a fin de garantizar que siempre se trabaje sobre las últimas versiones de los mismos.
* Todos los servidores del ambiente de producción deberán estar actualizados con la última versión de software, paquetes y archivos que hayan pasado por el proceso de pruebas en el ambiente de desarrollo correspondiente.
* Todos los servidores del ambiente de producción deberán organizar sus archivos en dos directorios, con el propósito de facilitar la instalación de aplicaciones:
  + Fuentes: contendrá todos los códigos fuente de las aplicaciones en ejecución.
  + Ejecutables: contendrá los archivos ejecutables de las aplicaciones instaladas.
* Todos los servidores del ambiente de producción tendrán dos tipos de privilegios de acceso, administrados por la Jefatura de la Unidad de Informática:
  + Persona usuaria Administradora: con acceso y control total al ambiente de producción, es decir, para ambos directorios: Fuentes y Ejecutables.
  + Persona usuaria ordinaria: con permisos de lectura y ejecución al directorio de Ejecutables solamente.

# Políticas para la implementación de infraestructura tecnológica



## Propósito

Garantizar que exista un soporte tecnológico continuo para las aplicaciones.

## Alcance

Los lineamientos mencionados en la presente política aplican a todas las personas colaboradoras de la Institución.

## Declaración de políticas



# Contrato de mantenimiento de recursos críticos

* Los recursos críticos que soportan la operación deberán contar con un contrato de mantenimiento que asegure la continuidad de las operaciones u otras alternativas que mitiguen este riesgo, como lo son los Care Pack Services, SMARTnet Services, soporte técnico preventivo, correctivo y evolutivo de los equipos, dispositivos y servidores institucionales.

# Diseño y documentación de red (diagramas)

* La Unidad de Informática será la responsable de diseñar, implementar, mantener y documentar propiamente la(s) red(es) y equipos de comunicaciones, incluyendo entre otros, routers, switches y enlaces de datos. Cualquier cambio a la infraestructura mencionada deberá realizarse por la misma Unidad de Informática de conformidad a los procedimientos de control de cambios.

# Seguridad de los equipos de red

* La Unidad de Informática será la responsable de implementar sistemas de autenticación y autorización para los equipos de comunicaciones que permitan administrar de forma segura los accesos (control de registros, control de personas usuarias, control de perfiles, respaldo, verificación y monitoreo de accesos), incluyendo las medidas necesarias para facilitar la visibilidad y accesos necesarios para las revisiones de estos aspectos por parte de procesos de auditoría interna y externa.

# Plan de infraestructura de TI

* El Plan Estratégico de Tecnologías de Información deberá incluir un apartado para la adquisición, implementación y mantenimiento de la infraestructura tecnológica, que contenga la definición y estándares tecnológicos de infraestructura de TI que deberán seguirse en la Institución y que den el soporte adecuado a las aplicaciones de interés Institucional, considerando la flexibilidad necesaria para prevenir necesidades futuras, costos de transición, riesgos técnicos, requerimientos de control interno/seguridad y el tiempo de vida útil de las inversiones para actualizar la tecnología.

# Mantenimiento de la infraestructura de TI

* La Jefatura de la Unidad de Informática deberá realizar verificaciones de la Infraestructura y equipo de manera semestral.
* La Jefatura de la Unidad de Informática deberá elaborar e implementar un programa de mantenimiento preventivo a la infraestructura y equipos, considerando la disponibilidad de recursos (internos y/o externos) y presupuestales, dando la debida prioridad a los equipos críticos para la Institución, así como a los equipos que requieran atención inmediata de acuerdo a su situación actual.
* Sólo el personal de mantenimiento debidamente autorizado (internos y/o externos) debería realizar reparaciones y mantenimiento de la infraestructura y equipo organizacional, implementando los controles apropiados al equipo cuando éste sea dispuesto para mantenimiento.
* La Unidad de Informática es la responsable de mantener el registro de los mantenimientos preventivos y correctivos realizados por el personal de mantenimiento debidamente autorizado (internos y/o externos), así como el registro de las fallas en los componentes de infraestructura.

# Adquisición de recursos de TI

* La Unidad de Informática en conjunto con la Dirección Administrativa y la Dirección Técnica deberá incluir anualmente, o según el período de la administración pública, en el Plan Operativo Institucional, las necesidades de recursos de TI percibidas y planteadas por las unidades, el cual deberá ser presentado a la Comisión de Tecnologías de Información y posteriormente elevado a la Presidencia Ejecutiva, previamente para su aval e implementación.
* La persona encargada del Plan de Compras deberá verificar que toda solicitud de compra se apegue al estándar establecido en el Plan Estratégico de Tecnologías de Información. En caso de que se requiera realizar alguna compra fuera del mencionado estándar, ésta requerirá de recomendación previa de la Unidad de Informática.
* Para ser considerada, cualquier oferta deberá cumplir con la normativa vigente institucional en esta materia y en caso necesario contar al menos con la siguiente información:

1. Especificaciones técnicas.
2. Condiciones, lugar y plazos de entrega.
3. Experiencia del proveedor (opcional).
4. Condiciones de instalación (opcional).
5. Condiciones del servicio post-venta (opcional).
6. Otras facilidades que el proveedor considere necesario (opcional).

* Las órdenes de compra y contratos de servicio seguirán los lineamientos y procedimientos institucionales establecidos por el INAMU.
* La Unidad de Informática es la responsable de verificar que el equipo informático y/o el software adquiridos cumplan con las especificaciones técnicas informáticas preestablecidas en la orden de compra.

# Políticas para la contratación de terceros para la implementación y mantenimiento de software e infraestructura.



## Propósito

Garantizar que los servicios provistos por terceros cumplan con los requerimientos Institucionales.

## Alcance

Los lineamientos mencionados en la presente política aplican a todas las personas colaboradoras de la Institución.

## Declaración de políticas



# Administración de servicios de terceros

* Cualquier servicio prestado por terceras personas deberá estar definido, documentado y respaldado adecuadamente mediante un contrato de servicio. Por tanto, antes de utilizar a un proveedor externo se deberá verificar que el contrato de servicio respectivo se encuentre vigente, y gestionar las adecuaciones necesarias al mismo para incluir los nuevos servicios, en caso de así requerirlo.

* Se debe mantener documentación formal sobre las relaciones técnicas y organizacionales con proveedores que contemple, entre otros: roles y responsabilidades, metas, entregables esperados y credenciales de los representantes de los proveedores y de las empresas.
* Los contratos deben estar de acuerdo con los estándares institucionales y basados en los requerimientos legales y regulatorios, identificando los riesgos con cada proveedor y la forma de mitigarlos para garantizar que el servicio sea eficiente, efectivo, seguro y asegure la continuidad de operaciones.
* La administración de los riesgos con la contratación de terceros, incluye entre otros, la definición de:
  + Acuerdos de confidencialidad
  + Contratos de garantía
  + Viabilidad de un servicio continuo por parte del proveedor
  + Conformidad con los requerimientos de seguridad
  + Proveedores alternativos (en caso de ser requerido)
  + Penalidades
* El clausulado mínimo de los contratos de servicios de terceros deberían contener, al menos:
  + Alcance del trabajo
  + Servicios/Entregables
  + Riesgos/Supuestos
  + Cronograma
  + Costos
  + Acuerdos de pago
  + Responsabilidades
  + Controles de seguimiento
* La Jefatura de la Unidad de Informática deberá evaluar al menos al final de la contratación mediante el formulario correspondiente, el desempeño de los servicios brindados por terceros, dejando evidencia de sus acciones al respecto y de las acciones correctivas realizadas en su caso.
* La Jefatura de la Unidad de Informática en conjunto con las unidades involucradas, deberá asegurar el cumplimiento de los contratos de servicios de terceros, así como el cumplimiento de las políticas de la Unidad de Informática y del INAMU al respecto.

# Administración de proveedores

* Dentro de las actividades para la administración de proveedores, a cargo del Área de Proveeduría, se deberán considerar al menos:
  + Mantener una base de datos de proveedores y contratos (catálogo de proveedores).
  + Categorizar los proveedores por tipo de servicio brindado
  + Evaluar los riesgos de cada proveedor según su categoría y características propias del mismo.
  + Negociar acuerdos y contratos.
  + Gestionar el rendimiento de los proveedores.
  + Estandarizar contratos, términos y condiciones, disputas, métricas y condiciones de subcontratación, a fin de facilitar la administración de contratos y proveedores.

# Políticas para la definición y administración de acuerdos de servicio.



## Propósito

Garantizar una comunicación efectiva entre la jefatura de Informática y las personas usuarias de la Institución respecto de los servicios requeridos, así como alinear los servicios de TI con los requerimientos del INAMU relacionados.

## Alcance

Los lineamientos mencionados en la presente política aplican a todas las personas colaboradoras de la Institución.

## Declaración de políticas



# Catálogo de servicios de TI

* La Unidad de Informática deberá definir y mantener un catálogo de servicios de TI, a fin de llevar un registro estándar de los servicios que utilizan las personas usuarias de TI. El cumplimiento de los niveles de servicio estará asociado a la definición y seguimiento de indicadores de gestión de los servicios considerados críticos, debiendo éstos ser sujetos de conocimiento, aprobación y gestión de parte de la Junta Directiva.

* El catálogo de servicios de TI deberá identificar los servicios críticos de TI según los requerimientos de las personas usuarias y las capacidades de TI, y deberá definir la administración de los niveles de servicio cubriendo roles, actividades y responsabilidades de las personas usuarias y de los proveedores internos y externos, de acuerdo con la estructura organizacional. Asimismo, deberá considerar, entre otras actividades: la creación de requerimientos de servicio, definiciones de servicio, acuerdos de niveles de servicio (SLA), acuerdos de niveles de operación (OLA), y fuentes de financiamiento.
* Los acuerdos de niveles de servicio deberán considerar, previo acuerdo entre las personas interesadas, entre otros:
  + Compromisos de las personas usuarias
  + Requerimientos de servicio de soporte
  + Métricas cuantitativas y cualitativas sobre el servicio.
  + Arreglos comerciales y de financiamiento
  + Definición de roles y responsabilidades
  + Consideraciones sobre disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte, plan de continuidad, seguridad y restricciones.
* Los acuerdos de niveles de operación deberán definirse como apoyo a los acuerdos de niveles de servicio para explicar la forma en que los servicios serán entregados técnicamente, explicando los procesos en forma técnica y de uso significativo para el proveedor.
* La Jefatura de la Unidad de Informática deberá llevar el control del cumplimiento de los niveles de servicio, a fin de identificar tendencias positivas y negativas sobre el servicio brindado, emprender acciones correctivas en su caso y mantener informados a las personas interesadas del servicio.
* Los acuerdos de niveles de servicio que involucren o dependan de contratos con terceros, deberán actualizarse regularmente dejando evidencia de esto, a fin de asegurar que el servicio siga siendo efectivo y los requerimientos continúen cumpliéndose.

# Políticas para la administración y operación de la plataforma tecnológica



## Propósito

Asegurar que los recursos de información que soportan los requerimientos Institucionales están disponibles de manera continua, facilitar la disponibilidad, minimizar los problemas de producción, resolver los problemas de manera eficiente, mantener la integridad de los datos y reducir los retrasos en el trabajo y los costos operativos de TI.

## Alcance

Los lineamientos mencionados en la presente política aplican a todas las personas colaboradoras de la Institución.

## Declaración de políticas



# Plan de capacidad y desempeño

* La Unidad de Informática deberá contar con un plan anual de capacidad y desempeño, que permita asegurar que la capacidad y el desempeño de la infraestructura de TI esté alineada con el plan estratégico de TI y soporte los objetivos estratégicos de la Institución, este plan será presentado a la Comisión de Tecnologías de Información y posteriormente elevado a Presidencia Ejecutiva.

# Sustitución de servidores

* La Unidad de Informática deberá contar un plan de sustitución de servidores de acuerdo con los resultados obtenidos del monitoreo de su capacidad y desempeño, prevención de obsolescencia y/o saturación y vida útil estimada, a fin de asegurar la entrega adecuada y la continuidad de los servicios.

# Sustitución de equipo de comunicaciones

* La Unidad de Informática deberá contar un plan de sustitución de equipo de comunicaciones de acuerdo con los resultados obtenidos del monitoreo de su capacidad y desempeño, prevención de obsolescencia y/o saturación y vida útil estimada, a fin de asegurar la entrega adecuada y la continuidad de los servicios.

# Monitoreo de recursos críticos

* La Unidad de Informática, a través del personal técnico autorizado (interno y/o externo) deberá monitorear continuamente la cantidad utilizada de recursos de CPU, memoria y almacenamiento en los servidores, bases de datos y equipo de comunicaciones, que soporten la operación y que hayan sido catalogados como críticos, y deberá mantener evidencia de este proceso y los resultados del mismo.

# Parámetros de rendimiento

* Los siguientes son los niveles máximos a alcanzar en la capacidad de la infraestructura para realizar las gestiones adecuadas para corregir, aumentar y/o actualizar los dispositivos involucrados:
  + 1. Servidores: 80% de utilización de CPU, memoria y/o almacenamiento.
    2. Líneas de comunicación: 80% de utilización.
    3. Equipo de comunicación (routers, switches): 70% utilización CPU, 80% utilización memoria
    4. Equipos de uso de Personas usuarias : 90% de utilización de CPU, memoria y/o almacenamiento.
    5. Fuente de poder institucional 90% de utilización.
* Cualquier aumento, actualización y/o sustitución de la infrastructura deberá estar plenamente justificado mediante estudios de capacidad y desempeño que sustenten dicha acción.

# Revisión y reporte de instalación de software no autorizado

* La Unidad de Informática contará con herramientas de monitoreo que le permitirán percibir la instalación de software no autorizado en el equipo tecnológico de la Institución, y generará un reporte para la Jefatura respectiva con los hallazgos encontrados. Una vez que se cuente con la autorización de la Jefatura respectiva se gestionará la eliminación del software indebido.

# Actualización y verificación de información de configuración

* La Unidad de Informática, a través del personal técnico autorizado (interno y/o externo) deberá verificar, respaldar y en su caso actualizar, al menos cada tres meses, la información de la configuración y las líneas base, la cual incluye la SAN-INAMU.

# Solicitudes para la ejecución de procesos

* Cualquier proceso que se ejecute en los servidores centrales productivos deberá contar con la respectiva solicitud de ejecución de parte de un área usuaria, o bien, formar parte de la calendarización de procesos habituales.
* Esta política no aplica en la actualidad al INAMU, se mantiene para posible implementación futura.

# Copias de archivos entre los ambientes de producción y desarrollo

* Siempre deberá existir la debida autorización por parte de la persona responsable de la unidad usuaria para realizar copias de archivos de datos productivos hacia el ambiente de pruebas y/o desarrollo.
* Nunca se podrán instalar en el ambiente productivo copias de archivos de datos de los ambientes de pruebas y/o desarrollo, esto no incluye los archivos de códigos fuente y/o ejecutables, los cuales requieren ser trasladados del ambiente de desarrollo – integración al ambiente de producción.

# Políticas para la atención de requerimientos de las personas usuarias de TI



## Propósito

Garantizar una comunicación efectiva entre la unidad de tecnologías de información y las personas usuarias, de los servicios requeridos, así como alinear los servicios de TI con los requerimientos Institucionales relacionados.

## Alcance

Los lineamientos mencionados en la presente política aplican a todas las personas colaboradoras de la Institución.

## Declaración de políticas



# Catálogo de servicios de TI

* Referirse a la Política 9.3.1

# Políticas para la administración de servicios prestados por terceros.



## Propósito

Garantizar que los servicios provistos por terceros cumplan con los requerimientos Institucionales.

## Alcance

Los lineamientos mencionados en la presente política aplican a todas las personas colaboradoras de la Institución.

## Declaración de políticas



# Administración de servicios y contratos de servicios de terceros

* Referirse a la Política 8.3.1

# Administración de proveedores de TI

* Referirse a la Política 8.3.2

# Evaluación y suspensión de proveedores de TI

* La Unidad de Informática en conjunto con el área de Proveeduría, deberá contar con un proceso de evaluación del desempeño de proveedores de TI, al finalizar la contratación, el cual debe darse a conocer a los proveedores a través del expediente a fin de que utilicen los resultados de la evaluación para mejorar los servicios brindados por ellos, o bien, como instrumento preventivo de posibles problemas y sus consecuencias. En caso necesario, se podrá requerir el apoyo del área de Asesoría Legal. El proceso podrá contar, con algunos de los siguientes aspectos:
  + Indicadores clave de desempeño (KPIs) definidos
  + Indicadores clave de metas (KGIs) definidos
  + Documentación de las evaluaciones, manteniendo un historial de las mismas.
  + Análisis de resultados a fin de detectar faltas en el cumplimiento de contratos y acuerdos de niveles de servicio.
  + Dependiendo de la calificación se procederá según la normativa vigente de incumplimientos.
  + En caso de presentarse alguna anomalía en el servicio recibió de proveedores, las áreas usuarias de la Institución deberán comunicarlo a la Unidad de Informática para tomar las acciones respectivas.

# Políticas para el seguimiento de los procesos de TI.



## Propósito

Garantizar que las cosas correctas se hagan y que estén de acuerdo con el conjunto de direcciones y políticas.

## Alcance

Los lineamientos mencionados en la presente política aplican a todas las personas colaboradoras de la Institución.

## Declaración de políticas



# Seguimiento del Plan Operativo

* La Jefatura de la Unidad de Informática deberá presentar a la Comisión de Tecnologías de Información un informe sobre el seguimiento del Plan operativo, indicando las tareas culminadas, en proceso y pendientes de realizar para cada uno de los procesos definidos en dicho plan.

# Mejoramiento continuo

* La Jefatura de la Unidad de Informática deberá asegurarse que se adopte una filosofía de mejoramiento continuo para todas las tareas realizadas en dicha unidad, revisando y actualizando cuando corresponda los procesos y procedimientos en práctica.

# Políticas para la confidencialidad, integridad y disponibilidad de los datos de la plataforma tecnológica.



## Propósito

Garantizar la confidencialidad, protección, resguardo y disponibilidad de los datos procesados y de la plataforma tecnológica de la Institución.

## Alcance

Los lineamientos mencionados en la presente política aplican a los todas las personas colaboradoras de la Institución.

## Declaración de políticas



## Pertenencia de los datos y equipo de la plataforma tecnológica

* En lo que respecta a la pertenencia de los datos y equipo de la plataforma tecnológica, las personas colaboradoras del INAMU se regirán por lo establecido en el Reglamento de Administración de Activos Institucional, enfatizando los siguientes puntos:
* La Institución asignará a sus personas colaboradoras las herramientas necesarias para el procesamiento y comunicación de datos en la plataforma tecnológica, con el propósito de facilitar el desempeño y cumplimiento de las labores establecidas.
* Tanto las herramientas suministradas como los datos administrados por estas herramientas son propiedad de la Institución, por lo que no deberán ser utilizadas para fines personales o distintos a las actividades propias de cada persona colaboradora.

## Confidencialidad de los datos y la información

* Toda información referente a los datos provenientes de la naturaleza de las operaciones de La Institución, deben ser considerados como confidenciales, por lo cual se considerará como una falta grave el divulgar, compartir o copiar dicha información sin el consentimiento previo.

## Resguardo de los datos e información

* Toda información considerada confidencial que se encuentre en poder de las personas colaboradoras, producto de las labores que le son asignadas, ya sea en medios de almacenamiento digitales o físicos, deberá mantenerse debidamente resguardada y fuera del alcance de terceros.
* Una vez finalizadas las labores diarias, es responsabilidad de cada persona colaboradora ordenar su lugar de trabajo, de tal forma que la información confidencial utilizada en sus labores se encuentre debidamente protegida.
* En caso de reubicaciones físicas de la persona colaboradora en el lugar de trabajo, éste será el responsable de transportar los datos e información en su poder, tomando las previsiones necesarias que garanticen la confidencialidad y disponibilidad de la información.

## Solicitud y salida de información de la Institución

* En caso extraordinario que se requiera solicitar, respaldar, copiar o trasladar fuera de las instalaciones de la Institución información considerada como confidencial, se requerirá completar el formulario de Servicio Técnico disponible en el portal web de la Institución, el cual deberá ser impreso y autorizado mediante firma de la Jefatura correspondiente, previo al envío del mismo a la Unidad de Informática.

# Políticas para el uso de la plataforma tecnológica de la Institución.



## Propósito

Garantizar el uso correcto y eficiente de los recursos de la plataforma tecnológica de la Institución.

## Alcance

Los lineamientos mencionados en la presente política aplican a los todas las personas colaboradoras de la Institución.

## Declaración de políticas

## Uso de los recursos de la plataforma tecnológica

* Es responsabilidad de todas las personas colaboradoras de la Institución velar por el uso adecuado y eficiente de los recursos de la plataforma tecnológica, por lo cual se considerarán como faltas graves las acciones siguientes:

1. Utilización de los recursos de la plataforma tecnológica en fines distintos a los que fueron asignados originalmente como por ejemplo: juegos, pasatiempos, etc.
2. Instalación, desinstalación, o reparación de software en la plataforma tecnológica por personas colaboradoras no facultados por la Institución para dichas labores.
3. Ensamblaje, desensamblaje o reparación de hardware en la plataforma tecnológica por personas colaboradoras no facultados por la Institución para dichas labores.
4. Poner en peligro de daño los equipos de la plataforma tecnológica por condiciones inadecuadas de limpieza o ingesta de bebidas o alimentos.
5. Colocación de objetos cercanos a los equipos de la plataforma tecnológica que puedan alterar o dañar su correcto funcionamiento como por ejemplo: imanes, plantas, objetos pesados, contenedores de líquidos u otros objetos que lo pongan en riesgo.
6. Negligencia por parte de las personas colaboradoras en el uso de la plataforma tecnológica en lo que respecta a condiciones de protección ambiental de los equipos como por ejemplo: polvo, agua, rayos, fuego, entre otros.

# Asignación y distribución de los equipos de la plataforma tecnológica

* La Institución proveerá a sus personas colaboradoras de los equipos de hardware y herramientas de software necesarias para el desarrollo de sus labores, de acuerdo al Reglamento de Administración de Activos del INAMU.
* Para la asignación de los equipos y su respectiva configuración el superior jerárquico de cada persona colaboradora deberá realizar una solicitud en donde se detallen las funciones a realizar con el equipo de cómputo, a fin de que la Unidad de Informática establezca las características técnicas informáticas que deberá cumplir el equipo solicitado. Este equipo deberá cumplir con los lineamientos y políticas para la Gestión Operativa de TI, principalmente con la 5.3.1 Definición de Imágenes de Equipos de Cómputo, 7.3.4. Plan de Infraestructura de TI, y 7.3.6 Adquisición de Recursos de TI. Ver formulario de servicio técnico del Portal web.

# Equipo nuevo en la plataforma tecnológica y equipos de terceros

* Cualquier equipo nuevo en la plataforma tecnológica de la Institución deberá ser sujeto a un proceso de revisión por parte de las personas colaboradoras de la Unidad de Informática previo al momento de instalación en el ambiente de producción.
* Es responsabilidad de las personas colaboradoras de la Unidad de Informática autorizar la instalación de los equipos nuevos al ambiente de producción de la Institución.
* En caso de requerir la instalación de equipos de terceros en la plataforma tecnológica de la Institución, la Unidad de Informática deberá realizar el proceso manual de evaluación del equipo y la respectiva autorización.

# Seguimiento de los equipos de la plataforma tecnológica

* El encargado de activos fijos de la Institución será la persona responsable de contar con un inventario detallado y actualizado de los equipos de la plataforma tecnológica asignados a las personas colaboradoras y departamentos en general.
* Es responsabilidad de la Unidad de Informática contar con un inventario de características técnicas de los equipos principales de la plataforma tecnológica.
* En caso de traslado de equipo de la plataforma tecnológica se requerirá la respectiva boleta por parte del responsable del envío del equipo según corresponda:
  + Boleta de autorización de salida de activos para reparación
  + Formulario de servicio técnico de la Unidad de Informática
  + Boleta de traslado de activos y equipos de oficina
  + Boleta de devolución de activos a bodega.

# Salida del equipo de la plataforma tecnológica de las instalaciones

* Se considera como falta grave la salida de equipo de la plataforma tecnológica de la Institución sin una autorización formal y por escrito del superior jerárquico a la persona colaboradora que realizará la acción.

# Detección de fallas en los equipos de la plataforma tecnológica

* Cada persona colaboradora será responsable de la correcta utilización del equipo de la plataforma tecnológica que se le asigne por parte de la Institución, así como de velar por el correcto funcionamiento de los equipos de uso compartido de la plataforma tecnológica como por ejemplo: impresoras, escáner, etc.
* Es responsabilidad de todas las personas colaboradoras de la Institución reportar de forma inmediata cualquier situación de error o falla en los equipos de la plataforma tecnológica a los superiores inmediatos y a las personas colaboradoras de la Unidad de Informática a través del formulario de servicio técnico disponible en el Portal WEB con base en la circular 106-2010 del 6 de agosto del 2010.

# Licenciamiento del software de la plataforma tecnológica

* En la plataforma tecnológica de la Institución se instalará únicamente software debidamente registrado y autorizado para uso del INAMU conforme a la adquisición y distribución a cargo de la Unidad de Informática.
* Se considerarán como falta grave la instalación y uso de software que no se encuentre debidamente registrados a nombre de la Institución.
* En caso de recibir software de prueba, éste deberá ser instalado y desinstalado por la personal de la Unidad de Informática de la Institución, según las reglas establecidas por los respectivos proveedores.
* Es responsabilidad de la Unidad de Informática, mantener un control detallado y actualizado de las licencias de software de La Institución.

# Políticas para la seguridad física de las instalaciones de tecnologías de información.



## Propósito

Delimitar los mecanismos de control que regulen el acceso físico y las condiciones ambientales de los recintos que albergan los equipos principales de la plataforma tecnológica de la Institución

## Alcance

Los lineamientos mencionados en la presente política aplican a los todas las personas colaboradoras de la Institución.

## Declaración de políticas



# Acceso físico

* El acceso físico de las personas colaboradoras al Centro de Datos del INAMU, en donde se ubican los equipos principales de la plataforma tecnológica de La Institución, será exclusivo para las personas autorizadas.
* Las personas autorizadas para ingresar al Centro de Datos del INAMU son las relacionadas con la Unidad de Informática, terceros autorizados y/o contratados por dicha Unidad para realizar cualquier servicio relacionado a los equipos principales y personal de limpieza de forma controlada.
* La Unidad de Informática deberá llevar una bitácora de registro de accesos de personal ajeno a dicha Unidad al Centro de Datos del INAMU. Ver Bitácora de Accesos al Centro de Datos.

# Condiciones ambientales

* La Institución velará por las condiciones ambientales del Centro de Datos del INAMU, para lo cual mantendrá controles estrictos en lo que respecta a:
  1. Mecanismos que garanticen la restricción de acceso a personas no autorizadas.
  2. Equipos de aire acondicionado que controlen la temperatura de los equipos.
  3. Instalaciones eléctricas adecuadas para garantizar el suministro de energía de manera confiable.
  4. Mecanismos que permitan la extinción de fuego.
  5. Equipos de iluminación adecuada en caso de ausencia de energía.
  6. Equipos alternos de suministro de energía.
  7. Labores diarias de limpieza .

# Políticas para la seguridad lógica de la plataforma tecnológica.



## Propósito

Mantener la estabilidad, seguridad, confianza, continuidad y privacidad en la plataforma tecnológica de la Institución, mediante el control de los accesos lógicos de las personas usuarias.

## Alcance

Los lineamientos mencionados en la presente política aplican a todas las personas colaboradoras de la Institución.

## Declaración de políticas



# Solicitud y mantenimiento de los accesos a la plataforma tecnológica

* La Institución le brindará a sus personas colaboradoras los accesos lógicos a la plataforma tecnológica de forma consistente con las labores que le son asignadas.
* Se deberá definir para cada una de las personas colaboradoras de la Institución el perfil de acceso a la plataforma tecnológica y las herramientas necesarias a utilizar en sus gestiones diarias. Ésta labor es responsabilidad del Superior Jerárquico de cada persona colaboradora. Para atender estas solicitudes se debe utilizar el formulario de Servicio Técnico definido por la Unidad de Informática.
* En caso de que una persona colaboradora requiera modificar el perfil de accesos que le fue asignado originalmente o presente modificaciones en las herramientas que utiliza en sus gestiones diarias, se deberá de redefinir el perfil por parte del Superior Jerárquico a la mayor brevedad posible. Para atender estas solicitudes se debe utilizar el formulario de servicio técnico definido por la Unidad de Informática.
* En caso de que las condiciones laborales de algún persona colaboradora cambien, como por ejemplo por situaciones de: traslados, renuncias, despidos, etc., es responsabilidad del Área de Recursos Humanos comunicar dicha situación de forma inmediata a la Unidad de Informática, para la respectiva cancelación en los accesos lógicos de la persona colaboradora. Para atender estas solicitudes se debe enviar un correo eletrónico a la Jefatura de la Unidad de Informática.
* En caso de que las condiciones laborales sean contrataciones por servicios, es responsabilidad del Superior Jerárquico solicitar el perfil de acceso a la Unidad de Informática, así como comunicar a ésta última cualquier cambio en dicho perfil o finalización de las labores contratadas.
* Se prohíbe el uso de persona usuarias genéricos para acceder a la plataforma tecnológica de la Institución. Esta situación no aplica para la red wifi-INAMU la cual es de acceso público con restricciones y se encuentra aislada lógicamente de la red principal del INAMU.
* Las personas usuarias de la plataforma tecnológica de la Institución serán identificadas mediante la primera letra del nombre y el primer apellido completo. En caso de encontrar coincidencia en persona usuarias se utilizarán las letras subsecuentes del nombre hasta lograr la diferenciación.

# Control de software no autorizado

* Se considera como falta grave la copia, instalación y utilización de software no autorizado por la Institución en los equipos de la plataforma tecnológica.

# Control de los ataques de virus

* La Institución contará con software de control antivirus en la plataforma tecnológica, el cual deberá ser instalado y programado por el Unidad de Informática, de tal forma que se garantice la protección constante contra ataques de cualquier tipo de “software malicioso”.
* Las actualizaciones de las herramientas de control de software antivirus, deberán estar programadas de tal forma que las actualizaciones e instalación de “parches” requeridos, se realicen de forma automática y con una periodicidad diaria.
* Es responsabilidad de la Unidad de Informática realizar las instalaciones, configuraciones y demás procedimientos necesarios, que garanticen la correcta actualización de las herramientas de protección contra software antivirus de la Institución.
* Es responsabilidad de la Unidad de Informática mantener controles estrictos referentes a:
  1. Instalación, configuración y actualización del software antivirus.
  2. Seguimiento de los sitios visitados por parte de las personas colaboradoras en Internet.
  3. Negación de la navegación de equipos de la plataforma tecnológica sin el correcto funcionamiento del software antivirus.
  4. Monitoreo, limpieza y corrección de equipos infectados con virus en la plataforma tecnológica.
  5. Análisis de las bitácoras de eventos y fallas atendidas en la plataforma tecnológica.
* Es responsabilidad de las personas colaboradoras, informar de forma inmediata al superior jerárquico y a la Unidad de Informática cualquier tipo de comportamiento “extraño” o sospechoso, o cualquier duda con respecto a la infección de virus de algún equipo de la plataforma tecnológica de la Institución.
* Se considerará como falta grave la negligencia por parte de las personas colaboradoras , con respecto a la desactualización de las herramientas de control contra ataque de “software malicioso”.

# Uso de claves, contraseñas y palabras de paso

* Las claves de acceso, contraseñas y palabras de paso en general, son únicas para cada persona colaboradora de la Institución.
* Las personas colaboradoras no deberán anotar sus palabras clave en sitios de fácil acceso por terceros, de preferencia dichas claves deberán ser memorizadas por las personas colaboradoras respectivos.
* Cada persona colaboradora es responsable por las acciones que se ejecuten bajo su identificación personal, por lo cual se considerará como falta grave el compartir o revelar sus palabras de paso a cualquier persona interna y/o externa a la Institución.
* Cada una de las personas colaboradoras de la Institución deberá ser asociado a un rol o perfil tanto a nivel de los sistemas de información como de las redes de comunicación de la Institución.
* Los roles o perfiles tanto a nivel de los sistemas de información como de las redes de comunicación de la Institución, estarán sujetos a diferentes permisos y privilegios dentro de la plataforma tecnológica.
* La asignación de los roles y perfiles a las personas colaboradoras de la Institución deberán estar en función con las labores que le son asignadas a cada persona colaboradora, previa solicitud del Superior Jerárquico de dicho persona colaboradora.
* Las claves de acceso, contraseñas y palabras de paso en general, serán asignadas a las personas colaboradoras por parte de la Unidad de Informática , previa solicitud del Área de Recursos Humanos, o bien del superior jerárquico de la persona colaboradora en caso de contratación externas.
* Las palabras claves utilizadas en la plataforma tecnológica de la Institución son exclusivas para dicho uso, por lo cual no deberán ser utilizadas como palabras de paso para acceder a otras aplicaciones externas como por ejemplo: correos gratis en Internet, chats, entre otros.
* Será responsabilidad de la Unidad de Informática configurar los equipos de la plataforma tecnológica de la Institución de tal forma que se garanticen los controles siguientes:

* 1. Los equipos de la plataforma tecnológica deben de bloquearse ante una inactividad de 20 minutos.
  2. En caso de que una persona colaboradora no identifique correctamente durante tres intentos el acceso a la plataforma tecnológica, la cuenta de la persona colaboradora será bloqueada, hasta determinar la causa de los fallos.
* Cuando una persona colaboradora de la Institución deba retirarse de su lugar de trabajo deberá bloquear o cerrar la sesión de trabajo en su estación, de tal forma que pueda ser utilizado nuevamente, hasta la previa validación del persona usuaria responsable con la inclusión de su respectiva palabra de paso. Al finalizar el día laboral, la persona persona colaboradoraa deberá dejar apagado el equipo de cómputo a su cargo.
* En caso de que la persona colaboradora sospeche que la confidencialidad de sus palabras claves se encuentre vulnerable, deberá de comunicarlo de forma inmediata al superior jerárquico y al Unidad de Informática con el propósito de realizar el respectivo cambio de palabra de paso.
* Para la selección de palabras de paso se deberán seguir las siguientes indicaciones:
  1. Tamaño mínimo de 8 caracteres.
  2. La composición de la clave debe de contener: letras mayúsculas, minúsculas y números.
  3. La composición de la clave no debe contener caracteres especiales.
  4. No se permiten claves en blanco ni nombres o palabras fácilmente identificables.
* Las palabras clave deberán de ser cambiadas por las personas colaboradoras , con un periodo máximo de 42 días.

# Palabras de paso para equipos principales de la plataforma tecnológica

* Los nombres preestablecidos por los sistemas operativos, motores de bases de datos y demás componentes de la plataforma tecnológica como por ejemplo: “administrador” y “admin.”, deberán ser renombrados y mantener debidamente documentados.
* Las claves de acceso, contraseñas y palabras de paso en general, de los equipos principales de la plataforma tecnológica de La Institución deberán de estar sujetas a los controles siguientes:
  1. Tamaño mínimo de 10 caracteres.
  2. La composición de la clave debe de contener: letras mayúsculas, minúsculas y números.
  3. No se permiten claves en blanco ni nombres o palabras fácilmente identificables.
  4. Se deben de mantener debidamente documentadas y con mecanismos de protección adecuados, preferentemente en una ubicación externa a las instalaciones de La Institución.

# Uso de Internet y Correo Electrónico

En lo que respecta al uso de Internet y Correo Electrónico, las personas colaboradoras del INAMU se regirán por un Reglamento para el uso del correo electrónico e Internet Institucional.

# Políticas para el aseguramiento de la continuidad de las operaciones.



## Propósito

Mantener la disponibilidad de la plataforma tecnológica de La Institución, así como el establecimiento de las condiciones que aseguren la continuidad de las operaciones de la Institución, indistintamente de la materialización de potenciales riesgos tecnológicos que la afecten.

## Alcance

Los lineamientos mencionados en la presente política aplican a los todas las personas colaboradoras de la Institución.

## Declaración de políticas



# Mantenimiento y niveles del servicio de la plataforma tecnológica

* La responsabilidad por garantizar la continuidad de las operaciones de la Institución será de todas las personas usuarias de la plataforma tecnológica.
* Ante la presencia de un evento extraordinario de índole tecnológico, que impida a una persona usuaria la utilización de los equipos que le fueron asignados, éste deberá comunicarlo a su superior jerárquico y la Unidad de Informática mediante el formulario de servicio técnico, con el fin de diagnosticar el origen de la falla y su respectiva medida de corrección.
* La Unidad de Informática será responsable de realizar las siguientes actividades:

1. Mantener un inventario técnico detallado y actualizado del equipo de la plataforma tecnológica (System Center – Configuration Manager).
2. Mantener una ficha técnica de los equipos que conforman la plataforma tecnológica.
3. Realizar la respectiva planificación con las personas usuarias de la plataforma tecnológica, para la ejecución formal de mantenimientos preventivos de los equipos de la plataforma tecnológica de la Institución.
4. Atención inicial al llamado de las personas usuarias de la plataforma tecnológica, mediante el Formulario de Servicio Técnico, ante problemas referentes a: correo electrónico, uso de Internet, comunicación de datos en las redes internas y uso de los sistemas de información.

# 

# Respaldos y resguardo de información de las bases de datos

* La Unidad de Informática será responsable de realizar de forma diaria, el respaldo de las bases de datos de La Institución mediante la SAN-INAMU y dispositivos de almacenamiento.
* En el caso de la solicitud de un respaldo por parte de una persona colaboradora de la Institución se utilizará el Formulario de Servicio Técnico.
* La Institución proporcionará tanto lugares internos como externos a las oficinas principales de la Institución para el respectivo almacenamiento de los dispositivos físicos utilizados para realizar los respaldos.
* Los lugares de almacenamiento para los dispositivos físicos de respaldo, deben tener las condiciones necesarias con respecto a la seguridad y condiciones ambientales que permitan asegurar la adecuada disponibilidad de los datos almacenados.
* En el proceso de respaldo de las bases de datos de la Institución, se deberá mantener controles con el fin de verificar las situaciones siguientes:
  1. Uso adecuado de las herramientas de software y hardware utilizadas para realizar los respaldos.
  2. Verificación de la correcta ejecución de los respaldos por parte de las herramientas de software y hardware utilizadas.
  3. Periodicidad de ejecución del proceso de respaldo.
  4. Identificación clara de los datos a respaldar en los medios físicos.
  5. Administración adecuada de los medios físicos para realizar los respaldos.
  6. Levantado de los datos respaldados para garantizar la calidad del respaldo realizado.
  7. Traslados de las copias de seguridad físicas a los respectivos lugares de almacenamiento.
  8. Medios alternos para la recuperación de los datos almacenados en los respaldos.
  9. Mecanismos para la incorporación de los datos respaldados en el ambiente de producción de la plataforma tecnológica.
  10. Verificación de la capacidad de almacenamiento de los medios de respaldo.

# Respaldos de la información de la computación de la persona usuaria final

* La Unidad de Informática proporcionará a las personas colaboradoras de la Institución, las condiciones necesarias para el respaldo de los datos del persona usuaria final que se encuentre directamente relacionados con sus labores. Para esto destinará una carpeta exclusiva para cada persona usuaria en uno de los servidores destinados para esta función.
* La(s) persona(s) usuaria(s) identificada(s) como responsable(s) de ejecutar los respaldos de cada Unidad, deberá incluir la información en la carpeta designada para tal fin por la Unidad de Informática, siendo su responsabilidad la administración y el contenido de la misma. La carga de los datos a respaldar por parte de la persona usuaria responsable deberá realizarse de manera diaria.
* Será responsabilidad de cada persona colaboradora realizar las gestiones respectivas ante el superior jerárquico y el Unidad de Informática para la ejecución del proceso de respaldo de datos y posteriores recuperaciones.

# Capacidad de la plataforma tecnológica

* La Unidad de Informática deberá de mantener controles estrictos con respecto a la capacidad de procesamiento de todos los equipos de plataforma tecnológica de la Institución.
* La Unidad de Informática deberá de realizar procesos de monitoreo periódicos para evaluar lo siguiente:

1. Tiempos de respuesta de los sistemas de información
2. Niveles de utilización de la plataforma tecnológica
3. Disponibilidad de los recursos de los servidores principales de la Institución.
4. Tiempos de transmisión en las redes de comunicación.
5. Cambios importantes sufridos por la plataforma tecnológica.

# Administración de problemas

* La Unidad de Informática deberá presentar al menos de forma semestral a la Comisión de Tecnologías de Información un informe referente a los principales problemas identificados en la plataforma tecnológica de La Institución.

# Administración de la configuración

* La Unidad de Informática deberá mantener formalmente documentados, los parámetros de configuración para mantener el adecuado funcionamiento de la plataforma tecnológica de La Institución tanto a nivel de software como de hardware.

# Procesamiento de datos alterno

* La Institución deberá de planificar en el mediano – largo plazo la posibilidad de mantener contratos de procesamiento alterno de datos con el fin de garantizar la continuidad de las operaciones, ante un evento que imposibilite continuar utilizando la plataforma tecnológica disponible de la Institución.
* Dentro de este contexto será necesario realizar los esfuerzos necesarios que permitan a la Institución lo siguiente:
  + Coordinar con las personas colaboradoras desginadas, la incorporación de los datos respaldados y las condiciones de comunicación necesarias para restablecer las operaciones de la Institución.
  + Realizar al menos una vez por semestre la ejecución del plan para operar con el sitio de procesamiento alterno de datos. Para lo cual la Unidad de Informática será la responsable de coordinar las diferentes actividades a ejecutar.
  + En los contratos de procesamiento alterno con el proveedor, la Institución debe garantizar lo siguiente:

1. Clausulas de confidencialidad de la información.
2. Tiempos de respuesta a la atención de fallas.
3. Cantidad de espacio requerido.
4. Condiciones propias de configuración de los equipos, sistemas operativos, motores de bases de datos, sistemas de información, etc.
5. Niveles mínimos de servicio.
6. Tiempo de prestación de los servicios.

# Políticas para seguimiento y evaluación del control interno en TI.



## Propósito

Proporcionar seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las leyes y regulaciones aplicables.

## Alcance

Los lineamientos mencionados en la presente política aplican a todas las personas colaboradoras de la Institución.

## Declaración de políticas



# Autoevaluación de la Unidad de Informática

* Cada año, la Unidad de Informática deberá realizar un proceso de autoevaluación del Plan Estretégico de Tecnologías de Información a fin de cumplir con los requerimientos normativos y regulatorios. Lo anterior a la luz de lo establecido formalmente por la Unidad de Planificación del INAMU.

# Monitoreo y evaluación del control interno

* Además de las autoevaluaciones, se deberán llevar a cabo revisiones periódicas para verificar el procesamiento de la información dentro de la Unidad de Informática, pudiendo realizarse mediante auditores internos o externos.

* La Unidad de Informática será la responsable de revisar y analizar cualquier informe emitido por terceros sobre la situación de la Unidad, y definirá y desarrollará las acciones correspondientes, que serán elevadas a la Comisión de Tecnologías de Información.

* La Jefatura de la Unidad de Informática será la responsable de evaluar la necesidad de implementar acciones correctivas para asegurar que se corrija cualquier incumplimiento y/o situación negativa detectada por las revisiones periódicas.

# Políticas sobre la participación de la Auditoría Interna.



## Propósito

Proporcionar seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las leyes y regulaciones aplicables.

## Alcance

Los lineamientos mencionados en la presente política aplican a todas las personas colaboradoras de la Institución.

## Declaración de políticas



# Monitoreo y evaluación del control interno

Ver Política 14.3.2.

# Política para el seguimiento y evaluación del Plan Estratégico de Tecnologías de Información, PETI vigente y las Políticas de Gestión Operativa de Tecnologías de Información.

# Propósito

Garantizar el fortalecimiento del seguimiento al PETI vigente y a las Políticas de gestión operativa de Tecnologías de Información.

# Alcance

Los lineamientos mencionados en la presente política aplican a todas las personas colaboradoras de la Institución.

# Declaración de políticas

# Sobre el seguimiento y evaluación del Plan Estratégico de Tecnologías de Información:

* Se establece que la responsabilidad de efectuar la valoración del cumplimiento de la política de TI es la Unidad de Planificación del INAMU en coordinación con la misma Unidad de Informática.
* Los mecanismos empleados para verificar el cumplimiento de la política de TI son varios, a saber:

**a. Aval de vinculación entre el Plan Estratégico de Tecnologías de Información PETI y, el Plan Estratégico Institucional** **PEI INAMU**. Este análisis de vinculación lo resolverá la UPI conforme el PETI y PEI vigentes en la institución y su aval es determinante para la puesta en ejecución o no del PETl, ya que el mismo debe formar parte del PEI de cara al fortalecimiento institucional.

**b. Seguimiento al cumplimiento del PETI**: En este sentido, la UPI dará seguimiento trimestral al PETI por medio de los indicadores, metas y escalas de desempeño de los proyectos del PETI que han sido incluidos en el Plan operativo institucional (POI) cada año y que cuenten con asignación de recursos humanos, financieros y materiales.

* **Evaluación externa del PETI:** Se establecerá una evaluación trianual del PETI (cuya gestión será realizada por la Unidad de Planificación, y la Comisión de Tecnologías de Información fungirá como gestor de la Evaluación. El informe final y las recomendaciones deberán ser del conocimiento y aprobación de la Junta Directiva. Las recomendaciones aprobadas se tomarán como insumos para la confección del PETI para el siguiente período.
* **Uso de las recomendaciones evaluativas y planes remediales.** El Establecimiento de los planes de acción y medidas correctivas en caso de incumplimientos encontrados, o bien, recomendaciones de mejora se incluirán en el PETI y POI inmediato siguiente, como parte de sus planes de operación, y éstos serán sometidos al seguimiento trimestral ya indicado en el inciso b).

**21.3.2 Sobre el seguimiento de las Políticas de Gestión Operativa de Tecnologías de Información:**

* La Unidad de Planificación Institucional UPI, dará seguimiento a los planes de acción de mejoras derivados de los incumplimientos a las políticas de gestión operativa de las tecnologías de información, cada tres meses. Sí y solo sí, estas acciones hayan sido incluidas como parte del POI de la Unidad de Informática, ya sea como una modificación programática, o en el POI del año siguiente y para su cumplimiento en el corto plazo. Esta proyección de acciones de mejora deberá contar con el presupuesto y/o recursos requeridos institucionalmente y fijará metas específicas para analizar su cumplimiento. Deberá emitir informe para la Comisión Institucional de Tecnologías de Información.
* Mediante circular de la Presidencia Ejecutiva se informará a todas las dependencias cualquier modificación de estas políticas, que permita a las personas funcionarias conocer las Políticas de Gestión Operativa de Tecnologías de Información, cada vez que haya cambios.
* Es obligatorio que el personal del INAMU curse y certifique que ha participado en el curso virtual sobre Políticas de Gestión Operativa de TI desarrollado por la Unidad de Informática mediante la plataforma Virtual Aprende Conmigo, la cual debe estar permanentemente habilitada. La CAAD es la instancia de certificar dicho curso.