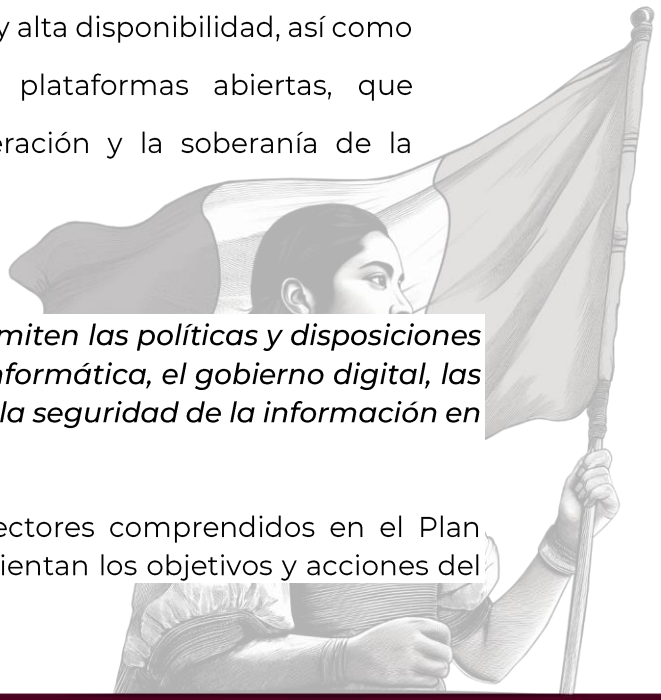
POLÍTICAS PARA EL DESARROLLO DE SISTEMAS INFORMÁTICOS

INTRODUCCIÓN

La necesidad de dotar a las áreas del INAH, las herramientas tecnológicas adecuadas para coadyuvar a realizar sus funciones, implica constantemente la creación de sistemas informáticos, que permitan optimizar eficientemente la operación.

Dentro de las funciones de la Dirección de Procesos y Servicios Informáticos se encuentran:

- Desarrollar, documentar e implementar los sistemas informáticos, con el objetivo de optimizar la operación institucional.
- Formular, presentar para aprobación y aplicar proyectos, políticas y lineamientos para homogeneizar las plataformas y estándares de la infraestructura de tecnologías y los sistemas de información en el INAH.
- Supervisar la correcta implementación de bases de datos institucionales que garanticen su adecuada operación y resguardo mediante mecanismos de seguridad y alta disponibilidad, así como favorecer y privilegiar el uso de plataformas abiertas, que garanticen la autonomía en la operación y la soberanía de la información institucional.



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

Que la honradez y honestidad son principios rectores comprendidos en el Plan Nacional de Desarrollo 2019-2024, mismos que orientan los objetivos y acciones del

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

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

OBJETIVO

Establecer criterios que permitan crear, actualizar, administrar y homologar los desarrollos Web del Instituto, con el objetivo de construir sistemas de alta calidad, basados en un modelo de arquitectura de software que genere aplicaciones reutilizables e interoperables entre las áreas del Instituto, privilegiando el uso de lenguajes de programación y las plataformas de desarrollo basadas en software libre y estándares abiertos.

POLÍTICAS

- Definir los lineamientos y objetivos para la elaboración de desarrollos informáticos web del Instituto, establecer un ámbito de referencia general en el cual se garantice que los desarrollos informáticos coadyuven en las tareas sustantivas del instituto, y que permitan una adecuada interacción entre las áreas, así como a satisfacer las necesidades del manejo de la información, con la creación y el diseño de una base de datos que permita integrar y consolidar un banco institucional de sistemas en un futuro.

- Los desarrollos de sistemas hechos por las áreas internas del instituto o por algún desarrollador externo, deberá cumplir con las normas, establecidas por la Coordinación Nacional de Desarrollo

Institucional, y deberá estar avalada por la DPSI, requisito indispensable para la liberación de un sistema.

- Todos los sistemas y sus componentes desarrollados por las áreas del Instituto o proveedores externos, serán propiedad del INAH, por los que podrán ser utilizados por las diferentes áreas del instituto si así se requiriera.

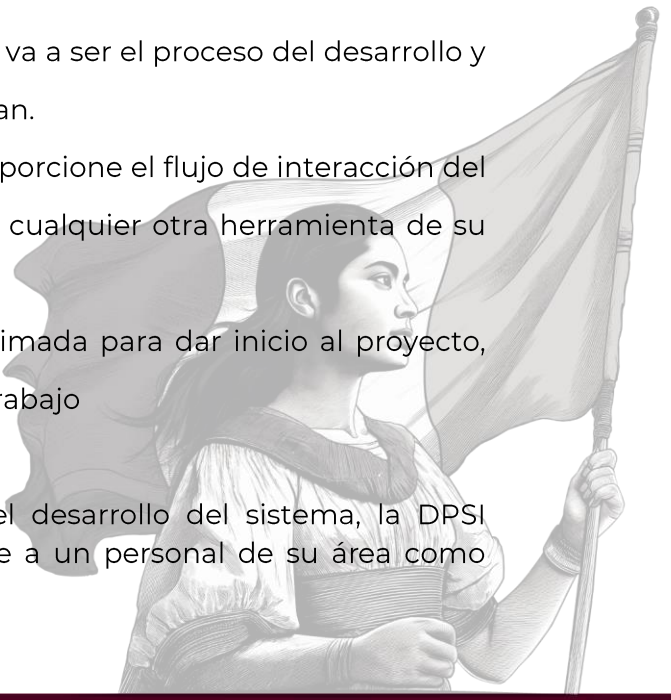
NORMAS GENERALES

Los desarrollos de sistemas realizados por las áreas del Instituto o por proveedores externos, deberán apegarse a los lineamientos y estándares definidos por la CNDI.

1. Para que la DPSI realice un sistema informático, el área requirente lo deberá solicitar formalmente a la CNDI mediante un oficio. Una vez recibido, se verificará la viabilidad del desarrollo y el tiempo, si el desarrollo es viable, la DPSI se pondrá en contacto con el área para fijar una mesa de trabajo, en la que se abordarán los siguientes temas.

    a. El área expondrá a grandes rasgos sus necesidades y el flujo que pretende llevar el sistema.
    b. La DPSI explicará al área cual va a ser el proceso del desarrollo y las tecnologías que se ocuparan.
    c. Se le solicitará al área que proporcione el flujo de interacción del sistema (Word, PowerPoint o cualquier otra herramienta de su preferencia).
    d. Se le otorga una fecha aproximada para dar inicio al proyecto, dependiendo de la carga de trabajo

2. Una vez que se defina el inicio del desarrollo del sistema, la DPSI solicitará al área requirente, nombre a un personal de su área como



enlace, el cual debe de tener toda la facultad para tomar decisiones con respecto a las necesidades del sistema.

3. Se firmará un formato de apertura del sistema, con el cual se da por iniciado el desarrollo del sistema.

4. El área de sistemas de la DPSI, realizará una maquetación como propuesta del sistema para presentarla al área requirente.

    a. Se le notificará por correo electrónico al enlace, para validar la maquetación.

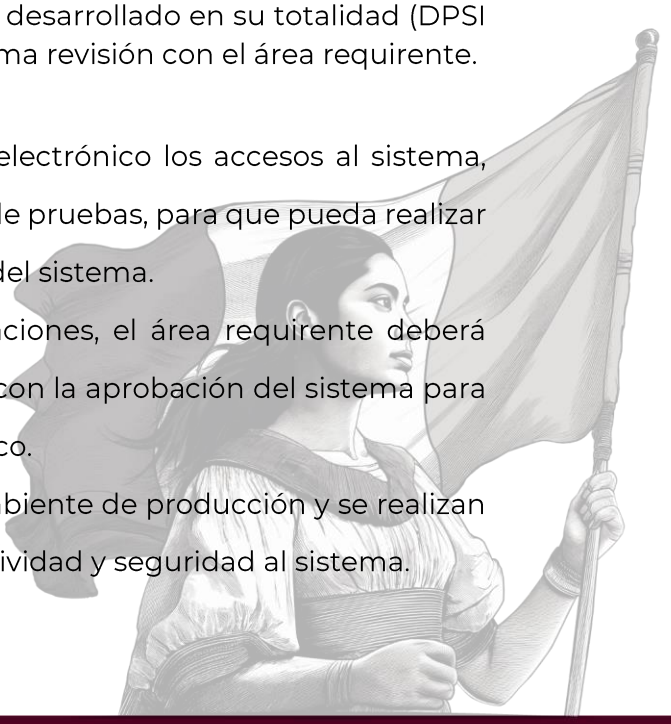
    b. Si todo es correcto se presenta un plan de trabajo, o en caso contrario se realizarán las adecuaciones necesarias y se volverá a presentar.

5. Una vez que la maquetación es aprobada por el área requirente y elaborados los planes de trabajo, se comienza con el desarrollo.

6. Semanal o quincenal se realizarán revisiones del progreso que se tiene en el sistema con en el enlace hasta la conclusión del mismo.

7. Una vez que el sistema se encuentre desarrollado en su totalidad (DPSI y administrador) se realizará una última revisión con el área requirente.

    a. Se le envía al enlace, correo electrónico los accesos al sistema, que se alojará en un servidor de pruebas, para que pueda realizar todas las pruebas necesarias del sistema.
    b. En caso de no tener observaciones, el área requirente deberá enviar por correo electrónico con la aprobación del sistema para colocarlo en un servidor público.
    c. El sistema se coloca en un ambiente de producción y se realizan las últimas pruebas de conectividad y seguridad al sistema.



d. Una vez y puesto en producción se le coloca un certificado de seguridad.
e. Se le entrega al área requirente un formato para firma, el cual indica que el sistema se encuentra operando y define quien es el encargado de administrar los contenidos del sistema.
f. Se le entrega por correo electrónico al enlace, usuario y contraseña, para tener acceso total al sistema.

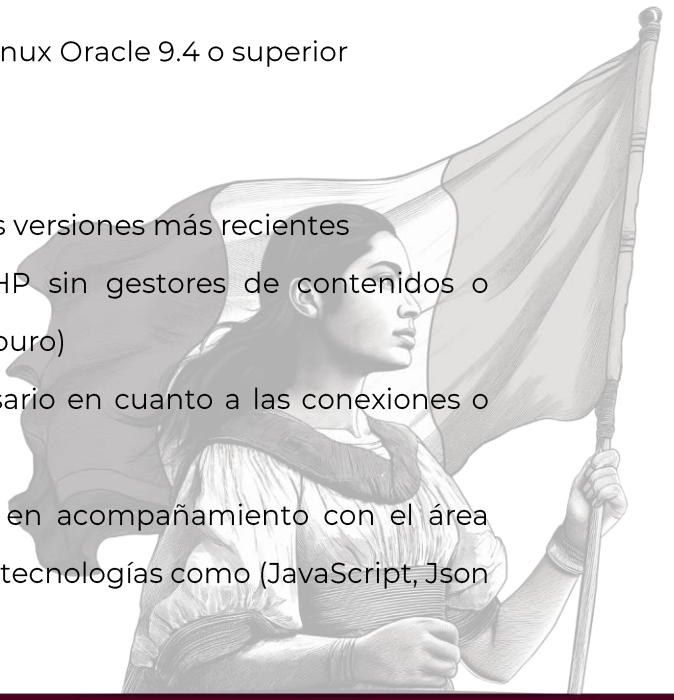
8. Se da por concluido el desarrollo y la implementación del sistema, por parte de la Dirección de Procesos y Servicios Informáticos

DESARROLLO DE SISTEMAS POR TERCEROS O ÁREAS DEL INAH

1. Notificar formalmente con un oficio a la CNDI, que el área desarrollará un sistema o pretende contratar a un tercero para su desarrollo.

2. La CNDI responderá, indicando la siguiente normatividad a la que deberá apegarse.

a. Desarrollar en un ambiente Linux Oracle 9.4 o superior
b. Apache 2.4 o superior
c. PHP 8.0 o superior
d. Base de datos MariaDB en sus versiones más recientes
e. Código fuente hecho en PHP sin gestores de contenidos o FrameWorks (Código fuente puro)
f. Solo ocupar PHP en lo necesario en cuanto a las conexiones o consultas de la base de datos.
g. El desarrollo debe realizarse en acompañamiento con el área requirente del INAH, y utilizar tecnologías como (JavaScript, Json



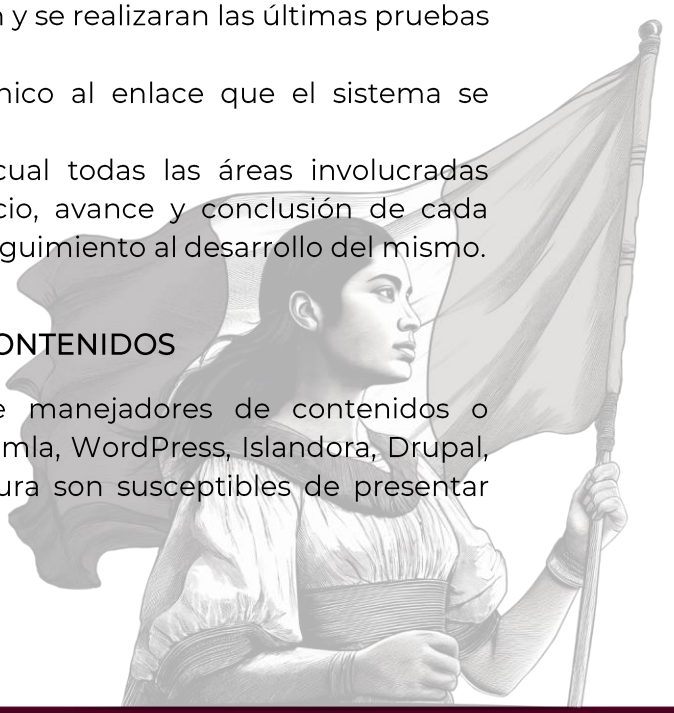
o Ajax)

h. Para los estilos o animación de las páginas utilizar limpio CSS o Boostrap
i. Las variables que se ejecutan en la URL del sitio deberán de ser encriptadas en base64
j. Las contraseñas para acceder el administrador del sitio deben de ser encriptadas en md5
k. Los archivos no deben de superar los 20 megas y deben de ser renombrados con una serie de números o TIMESTAMP (que es la codificación de la fecha en números)
l. Una vez que el sistema cumpla con los requisitos se colocará en un servidor de prueba para que la DPSI realizar las pruebas de seguridad
m. En caso de que se encuentren errores se notificara vía correo electrónico al enlace para su corrección

3. En caso de que el sistema funcione adecuadamente se le solicitara vía correo electrónico el nombre de la URL para el sitio.
4. Se colocará el sistema en producción y se realizaran las últimas pruebas de seguridad del sistema.
5. Se le notificara por correo electrónico al enlace que el sistema se encuentra publicado.
6. Se emitirá documentación en el cual todas las áreas involucradas firmaran de mutuo acuerdo el inicio, avance y conclusión de cada proyecto, esto con el fin de dar un seguimiento al desarrollo del mismo.

IMPLEMENTACIÓN DE UN MANEJADOR DE CONTENIDOS

1. No se recomienda que se utilice manejadores de contenidos o FrameWorks como por ejemplo Joomla, WordPress, Islandora, Drupal, Moodle, etc. Ya que por su estructura son susceptibles de presentar problemas de seguridad.



2. En el caso de que opte por utilizar este tipo de tecnologías se les recomienda:

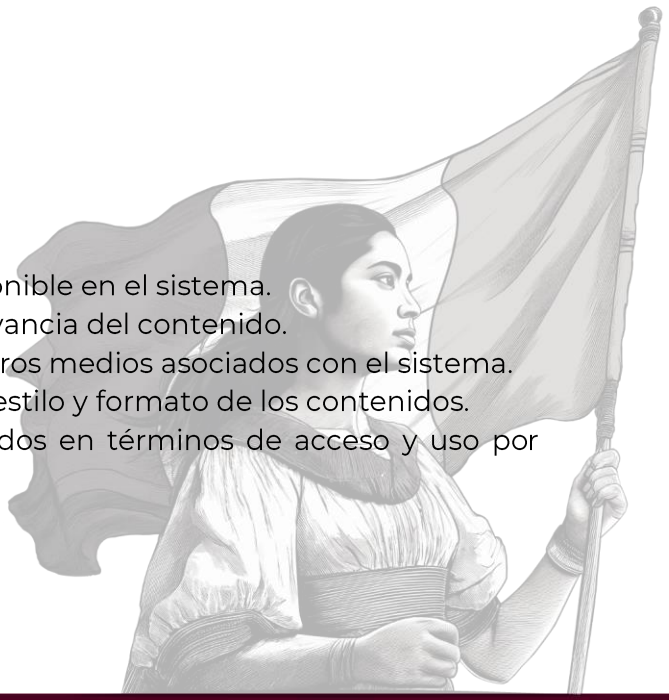
    a. Utilizar las tecnologías más actualizas
    b. Informar a la DPSI que se utilizara estas tecnologías por oficio
    c. Se tendrá que proporcionar a la DPSI manual de instalación, base de datos, código fuente última versión del manejador de contenidos, manual de operación y demás documentación según sea requerida.
    d. La DPSI realizará las pruebas de seguridad requeridas
    e. En caso de no cumplir con dichas medidas de seguridad no se le dará alojamiento en el servidor institucional
    f. En caso de que el sistema cumpla con los requerimientos de seguridad necesarios, por correo electrónico se le solicitara URL del sitio
    g. Una vez publicado el sitio web el área de informática no se hará responsable de la actualización, respaldo y/o mantenimiento del mismo.

Responsabilidades de las Áreas Requirente

Administrar Contenidos

- Actualizar y modificar la información disponible en el sistema.
- Revisar periódicamente la precisión y relevancia del contenido.
- Cargar y gestionar archivos, imágenes y otros medios asociados con el sistema.
- Asegurar la coherencia y consistencia del estilo y formato de los contenidos.
- Monitorear el desempeño de los contenidos en términos de acceso y uso por parte de los usuarios.

Mejoras del Sistema



- Identificar y documentar áreas de mejora o nuevas funcionalidades que pueden incrementar la eficiencia o usabilidad del sistema.
- Coordinar con el equipo técnico para implementar las mejoras propuestas.
- Realizar pruebas de las mejoras implementadas para asegurar que funcionen correctamente.
- Recopilar retroalimentación de los usuarios para ajustar y perfeccionar las mejoras.
- Actualizar la documentación técnica y de usuario para reflejar las nuevas características del sistema.

Ciclo de vida de una página web o sistema

1. Planeación o Identificación de Necesidades

    - **Objetivo:** Definir los problemas o necesidades que el sistema debe resolver.
    - Actividades:
        - Análisis de viabilidad (técnica y operativa)
        - Identificación de objetivos y metas

2. Análisis de Requisitos

    - **Objetivo:** Especificar de manera detallada qué debe hacer el sistema.
    - Actividades:
        - Recopilación de requisitos funcionales y no funcionales
        - Documentación y validación de requisitos con los usuarios
        - Creación de un modelo conceptual del sistema

3. Diseño del Sistema

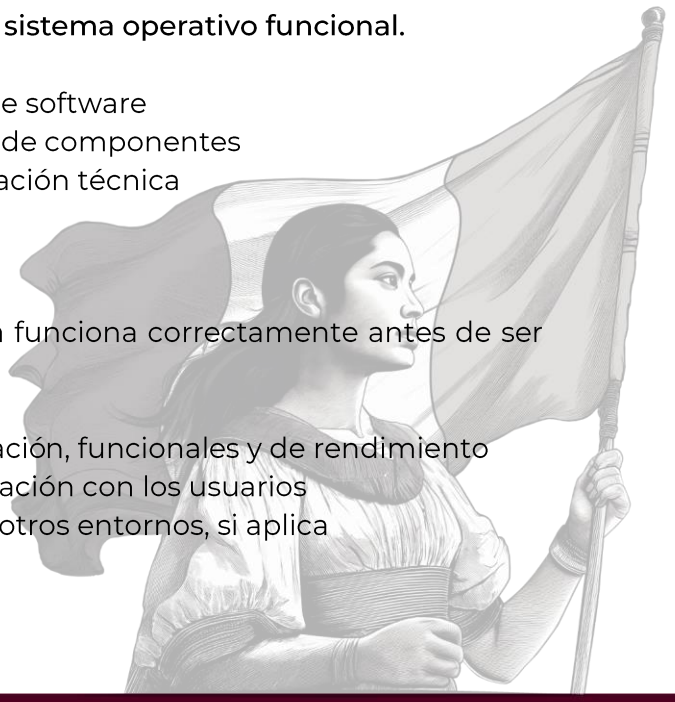
    - **Objetivo:** Establecer cómo funcionará el sistema para cumplir con los requisitos.
    - Actividades:
        - Diseño de la arquitectura del sistema
        - Definición de la base de datos, interfaces y componentes

4. Desarrollo o Construcción

    - **Objetivo: Convertir el diseño en un sistema operativo funcional.**
    - Actividades:
        - Programación o desarrollo de software
        - Configuración e integración de componentes
        - Generación de la documentación técnica

5. Pruebas e Integración

    - **Objetivo:** Garantizar que el sistema funciona correctamente antes de ser desplegado.
    - Actividades:
        - Pruebas unitarias, de integración, funcionales y de rendimiento
        - Corrección de errores y validación con los usuarios
        - Integración del sistema con otros entornos, si aplica



Implementación

- **Objetivo:** Poner el sistema en operación en el entorno real.
- Actividades:
  - Instalación del sistema
  - Capacitación de usuarios
  - Transferencia de datos, si es necesario
  - Soporte inicial para asegurar el funcionamiento correcto

6. Operación y Mantenimiento

- **Objetivo:** Asegurar el funcionamiento continuo y eficiente del sistema.
- Actividades:
  - Monitoreo del desempeño
  - Resolución de problemas y corrección de errores
  - Actualizaciones y mejoras
  - Soporte técnico y mantenimiento preventivo

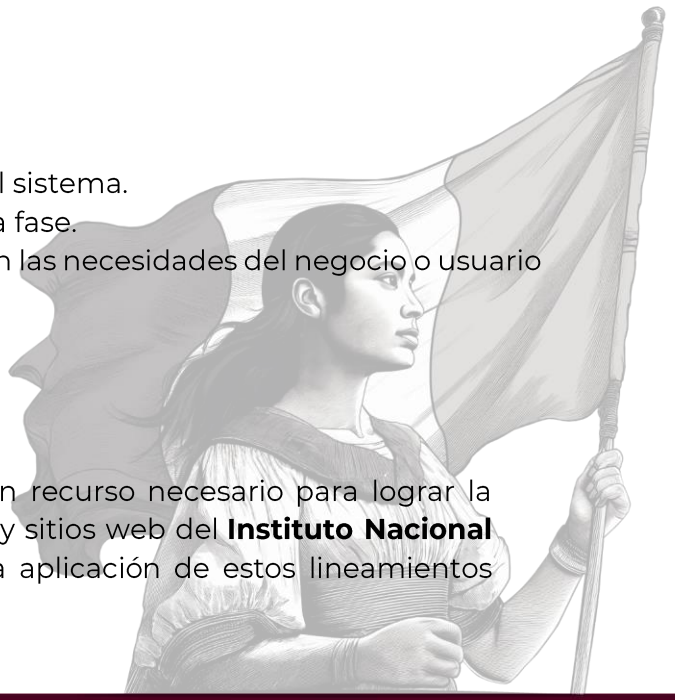
7. Retiro o Desmantelamiento

- **Objetivo:** Retirar el sistema cuando ya no sea útil o haya sido reemplazado.
- Actividades:
  - Planificación del retiro
  - Migración de datos o transición a un nuevo sistema
  - Desmantelamiento de la infraestructura asociada
  - Evaluación final y cierre del proyecto

Importancia del Ciclo de Vida del Sistema

El ciclo de vida ayuda a:

- Garantizar la calidad y eficiencia del sistema.
- Identificar y mitigar riesgos en cada fase.
- Asegurar que el sistema cumpla con las necesidades del negocio o usuario final.



Sitios y sistemas con grafica base

La **Gráfica Base del Gobierno de México** es un recurso necesario para lograr la uniformidad visual y estructural en los sistemas y sitios web del **Instituto Nacional de Antropología e Historia (INAH)**. La correcta aplicación de estos lineamientos

garantiza que todas las publicaciones digitales reflejen una identidad coherente y alineada con los valores gubernamentales.

Requerimientos para los sistemas y sitios web del INAH

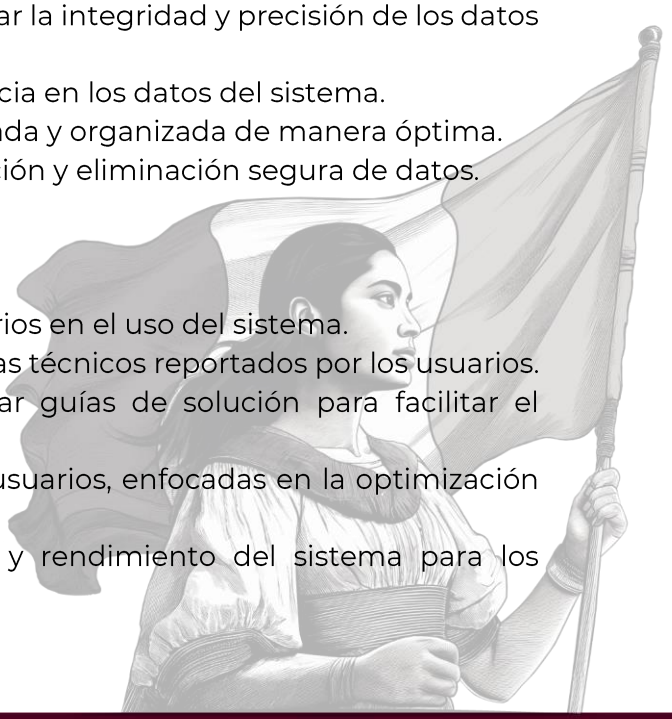
1. **Aplicación de la identidad gráfica**:
   - Todos los sistemas y sitios web deben emplear los elementos visuales oficiales: logotipos, tipografía y paleta de colores institucionales.
   - El Escudo Nacional y demás elementos gráficos deben integrarse conforme a las directrices establecidas en el Manual de Identidad Institucional.
2. **Estructuración de contenidos**:
   - La información debe organizarse de manera lógica y jerárquica, facilitando la navegación y búsqueda de contenidos por parte de los usuarios.
   - Los formatos y plantillas digitales deben adaptarse a los lineamientos de claridad y accesibilidad.
3. **Comunicación eficiente**:
   - Los mensajes publicados deben ser claros y directos, utilizando un lenguaje comprensible para todo tipo de audiencia.
   - Se debe priorizar la publicación de información relevante y actualizada.

Depuración de Información

- Revisar y eliminar información obsoleta o incorrecta del sistema.
- Implementar procedimientos para asegurar la integridad y precisión de los datos almacenados.
- Realizar análisis de consistencia y coherencia en los datos del sistema.
- Asegurar que la información esté actualizada y organizada de manera óptima.
- Establecer y aplicar políticas para la retención y eliminación segura de datos.

Soporte a Usuarios del Sistema

- Proporcionar asistencia técnica a los usuarios en el uso del sistema.
- Responder a consultas y resolver problemas técnicos reportados por los usuarios.
- Documentar incidencias comunes y crear guías de solución para facilitar el soporte.
- Realizar capacitaciones o tutoriales para usuarios, enfocadas en la optimización del uso del sistema.
- Monitorear y asegurar la disponibilidad y rendimiento del sistema para los usuarios.



Respaldo de Información

- Configurar y programar copias de seguridad automáticas de la información crítica del sistema.
- Verificar periódicamente que las copias de seguridad se estén realizando correctamente.
- Almacenar las copias de seguridad en ubicaciones seguras y accesibles en caso de recuperación de datos.
- Realizar pruebas de restauración de datos para asegurar la integridad de las copias de seguridad.
- Documentar los procedimientos de respaldo y recuperación para referencia futura.

Gestión de usuarios (Altas y bajas)

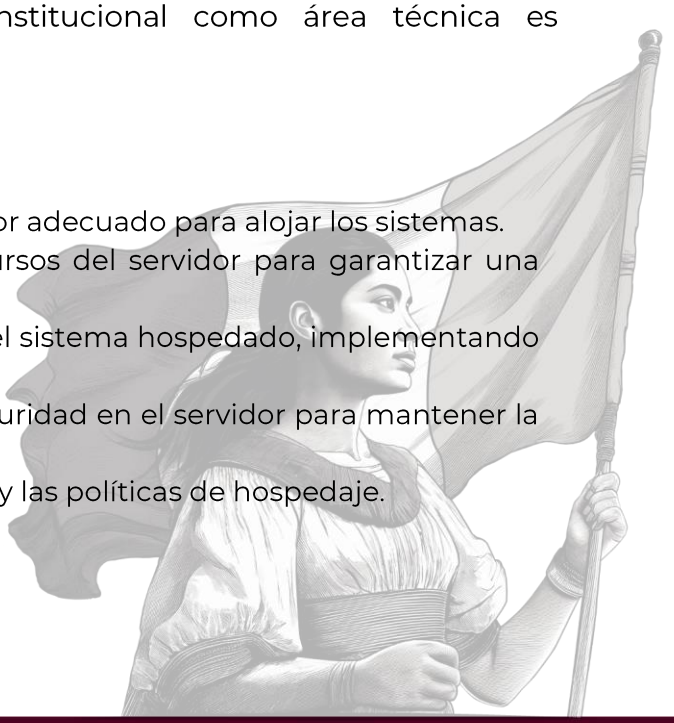
- Crear y configurar cuentas de usuario, asignando los permisos y roles adecuados según las necesidades.
- Actualizar los permisos y accesos de usuarios existentes conforme a cambios en sus responsabilidades.
- Desactivar o eliminar cuentas de usuario que ya no requieren acceso al sistema.
- Monitorear y auditar el uso de las cuentas de usuario para asegurar el cumplimiento de las políticas de seguridad.
- Mantener un registro actualizado de todas las cuentas de usuario activas e inactivas en el sistema.

La Coordinación Nacional de Desarrollo Institucional como área técnica es responsable de:

Hospedaje de sistemas

- Proveer y configurar un entorno de servidor adecuado para alojar los sistemas.
- Monitorizar el rendimiento y uso de recursos del servidor para garantizar una operación óptima.
- Asegurar la disponibilidad y estabilidad del sistema hospedado, implementando medidas de redundancia.
- Realizar actualizaciones de software y seguridad en el servidor para mantener la integridad del sistema.
- Documentar la configuración del servidor y las políticas de hospedaje.

Servicio de energía con respaldo UPS



- Instalar y mantener Unidades de Respaldo de Energía (UPS) para asegurar la continuidad eléctrica en caso de fallas.
- Realizar pruebas periódicas de los sistemas UPS para verificar su funcionalidad.
- Monitorear el estado de carga y vida útil de las baterías UPS, reemplazándolas cuando sea necesario.

Aire acondicionado de precisión

- Instalar sistemas de aire acondicionado diseñados para mantener la temperatura y humedad adecuadas en la sala de servidores.
- Monitorizar constantemente la temperatura y humedad para prevenir sobrecalentamientos o daños a los equipos.
- Realizar mantenimiento preventivo regular a los sistemas de aire acondicionado para asegurar su eficiencia.

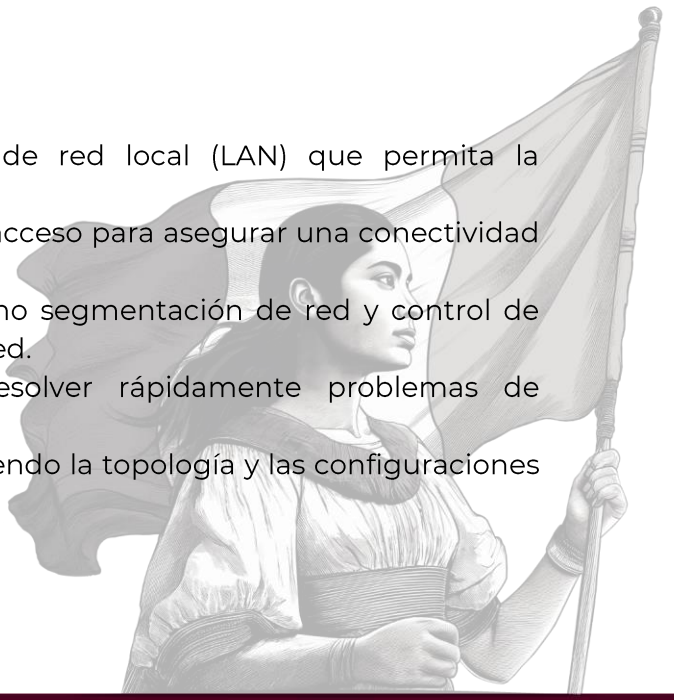
Salida a Internet

- Configurar y mantener las conexiones de red necesarias para asegurar una salida a internet estable y segura.
- Monitorear la disponibilidad y velocidad de la conexión a internet para asegurar un rendimiento óptimo.
- Implementar medidas de seguridad como firewalls y filtros para proteger la red del Instituto.
- Establecer redundancias o rutas alternativas de conexión para evitar interrupciones en el servicio.
- Documentar la configuración de la red y los procedimientos de mantenimiento.

Red LAN

- Diseñar y mantener la infraestructura de red local (LAN) que permita la interconexión eficiente de los sistemas.
- Configurar switches, routers y puntos de acceso para asegurar una conectividad óptima entre los dispositivos.
- Implementar medidas de seguridad, como segmentación de red y control de acceso, para proteger la integridad de la red.
- Monitorear la red para detectar y resolver rápidamente problemas de conectividad o rendimiento.
- Documentar el esquema de la red, incluyendo la topología y las configuraciones de los dispositivos.

Certificados de Seguridad



- Generar y gestionar certificados SSL/TLS para asegurar las comunicaciones entre los sistemas y los usuarios.
- Configurar los servidores y aplicaciones para utilizar los certificados de seguridad correctamente.
- Monitorear la vigencia de los certificados y renovar antes de su vencimiento para evitar interrupciones.
- Realizar auditorías periódicas para asegurar que los certificados están implementados adecuadamente.

VPN (si se requiere)

- Configurar y mantener una red privada virtual (VPN) para permitir el acceso seguro y remoto a los sistemas institucionales.
- Implementar políticas de acceso que definan quién y cómo puede conectarse a través de la VPN.
- Monitorizar las conexiones VPN para asegurar que se cumplan con los estándares de seguridad y rendimiento.
- Proporcionar soporte técnico a los usuarios para la configuración y uso de la VPN.
- Documentar la configuración y políticas de uso de la VPN.

Mantenimiento a la infraestructura

- Realizar inspecciones regulares y mantenimiento preventivo de todos los equipos y sistemas de infraestructura.
- Llevar a cabo actualizaciones de hardware y software según sea necesario para asegurar la compatibilidad y seguridad.
- Implementar planes de contingencia para el reemplazo rápido de componentes críticos en caso de falla.
- Documentar los procedimientos de mantenimiento y las intervenciones realizadas en la infraestructura.