1.0 OBJETIVO

Establecer una metodología estándar que garantice el desarrollo y mantenimiento seguro de las aplicaciones del organismo.

2.0 ALCANCE Y CAMPO DE APLICACIÓN

Este procedimiento aplica al desarrollo y mantenimiento de los sistemas informáticos, la infraestructura que utilicen, y las personas que participen del proceso de desarrollo, tanto explicita como implícitamente.

El presente procedimiento solo aplica para proveedores externos.

3.0 REFERENCIAS

Manual de Gestión, 7.1.3 Infraestructura
MG-15 Declaración de Aplicabilidad (SoA)

- A.9.4.5 Control de acceso al código fuente de los programas
- A.12.1.4 Separación de los entornos de desarrollo, prueba y operación
- A.12.6.1 Gestión de vulnerabilidades técnicas
- A.14.1.1 Análisis de Requisitos y Especificación de Seguridad de la Información
- A.14.2.1 Política de Desarrollo Seguro
- A.14.2.2 Procedimiento de Control de Cambios
- A.14.2.5 Principios de Ingeniería de Sistemas Seguros
- A.14.2.6 Entorno de Desarrollo Seguro
- A.14.2.7 Externalización del Desarrollo de Software
- A.14.2.8 Prueba de la Seguridad del Sistema
- A.14.2.9 Pruebas de Aceptación del Sistema
- A.14.3.1 Protección de los Datos de Prueba
- A.18.2.3 Revisión del cumplimiento técnico

4.0 RESPONSABILIDADES

Es responsabilidad de la Subgerente de Informática la elaboración, implantación, modificación, actualización, mantenimiento y difusión del presente procedimiento, así como, verificar y asegurarse de que éste sea seguido. Le corresponde también el resguardar, controlar, consultar y utilizar adecuadamente los Registros de Calidad derivados del presente.

La Dirección General es responsable de asegurar que la Subgerencia de Informática cuente con los recursos necesarios para la ejecución de sus funciones, así como de vigilar que éste cumpla con sus responsabilidades.

La Subgerencia de Informática es responsable también de:

- Asegurar que el organismo, en todas sus áreas, cuente con los sistemas y aplicaciones que le permitan un mejor ambiente de productividad en el ámbito informático.
- Asegurar que los sistemas y aplicaciones en uso en el ambiente de administración, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.
- Realizar pruebas a los sistemas y aplicaciones desarrollados y/o mantenidos por un proveedor, a fin de asegurar que éstos cumplen con las normas de seguridad de la información respectivas, y que los datos de prueba con manejados con la debida seguridad.

Todas las áreas y/o departamentos involucrados en el desarrollo y/o mantenimiento de sistemas y aplicaciones administrativas, son responsables de seguir este procedimiento.

5.0 GENERALIDADES

La planificación y ejecución del desarrollo y mantenimiento de sistemas y aplicaciones (en adelante el software), contempla diversas etapas, en las cuales se garantiza y valida en todo momento la seguridad de la información:

1. Análisis
2. Diseño
3. Desarrollo
4. Pruebas
5. Implementación
6. Liberación

Desde las primeras etapas el organismo y el proveedor consideran los aspectos de seguridad. Comenzando con el análisis, en donde se identifican los requisitos de seguridad que luego el software deberá cumplir, así como la validación a la que deberá ser sometido para tal efecto.

En la etapa de Diseño se delinean los controles necesarios para satisfacer los requisitos identificados.

Durante la etapa de desarrollo el proveedor manipula y programa los controles que soportarán la operación y procesamiento de información, considerando en todo momento la seguridad de la información que éstos deben asegurar.

Para la etapa de pruebas, el proveedor en coordinación con los usuarios finales del software, identificarán y seleccionarán cuidadosamente los datos que serán utilizados para la realización de pruebas y ajustes al software, dichas pruebas deberán contemplar tanto el cumplimiento de los requisitos de seguridad y funcionalidad, como los criterios de aceptación del software.

En la etapa de Implementación se pondrá el software en producción, de manera controlada y supervisada, a fin de asegurar su adecuado funcionamiento. Para el caso de actualizaciones, éstas deberán ser implementadas en horarios de baja o nula producción.

Para la última etapa, de liberación, se documentarán los resultados del software, incluyendo los resultados de las pruebas de aceptación de éste y el visto bueno del área solicitante.

Políticas Generales de Desarrollo

1. El proveedor que realice el desarrollo o mantenimiento deberá sujetarse a los lineamientos de seguridad que se describen en el presente, no obstante, podrá utilizar sus propias metodologías de desarrollo.
2. La Subgerencia de Informática es la única área facultada para determinar si el desarrollo o mantenimiento de software deberá llevarse a cabo por un proveedor externo.
3. Todo software deberá contar con las reglas mínimas de seguridad:
   a) Cuenta de usuario, única y fija, por cada usuario operador o administrador.
   b) Contraseña de usuario segura, que cumpla con las políticas de seguridad relativas a las contraseñas seguras, ya emitidas por el organismo.
   c) Histórico de movimientos controlado por la cuenta de usuario.
   d) Histórico de accesos al software.
   e) Control de operaciones por rol específico
4. Todo desarrollo o mantenimiento de software deberá cumplir las etapas de ingeniería de software definidas y detallas en este procedimiento.
5. Los cambios en el software deberán registrarse y controlarse mediante versiones de la aplicación. Las versiones se incrementarán en un punto cuando los cambios involucren actividades, módulos o procesos nuevos, y una décima de punto para cambios generales.
6. El acceso al código fuente deberá estar restringido al personal definido por la Subgerencia de Informática.

Etapa I: Análisis

- Durante la fase de análisis:

El problema, situación, oportunidad de mejora, actividad y/o proceso identificados, en los cuales se requiere la aplicación de ingeniería de software en el ámbito de un nuevo desarrollo o mantenimiento de software ya en producción. La situación puede derivarse de la supervisión y validación constante del personal de desarrollo sobre las aplicaciones en operaciones y/o los procesos de la organización, o bien, a solicitud expresa de personal de cualquier área.

- Detallar la situación, considerando:
  - Tipo, cantidad y clasificación de la información involucrada
  - Periodos, áreas y personal involucrado
  - Procesos, actividades y tareas implicadas
  - Amplitud, contexto y alcance de la situación
  - Niveles de seguridad requeridos
  - Prioridades

- Los criterios de pruebas y aceptación del software que se utilizarán en las etapas respectivas de prueba y liberación del mismo.
- Requerimientos particulares aplicables respecto de la seguridad de la información.
- Requerimientos de conectividad y/o transferencia de datos.
- Aspectos o estrategias para la seguridad de la información.
- Relación costo-beneficio para la organización.
- Controles que deberán aplicarse durante todo el ciclo de vida del software, según el ámbito de éste.
- Datos de la nueva versión del software.
- Los requerimientos especiales, de existir.
- Los tiempos reales de ejecución.

Etapa II: Diseño

En la segunda etapa:

- Esquemas y parámetros de seguridad para la operación del software.
- Diagramas de flujo, de requerirse, que determinen el flujo y procesamiento adecuado de los datos.
- Pruebas de operación y seguridad que se realizarán al software y/o sus componentes.

Etapa III: Desarrollo

La etapa de Desarrollo no requiere la generación de documentación específica, a menos que haya sido determinado como un requisito en la etapa de análisis.

Etapa IV: Pruebas

Deberán llevarse a cabo dos tipos de pruebas: la primera por parte del personal. El segundo tipo de pruebas deberá ser realizado por el personal involucrado identificado en la etapa de Análisis.

Para ambos tipos de pruebas, el personal podrá utilizar datos ficticios o solicitar a las áreas correspondientes los datos de prueba determinados durante la etapa de Análisis, dichos datos deberán ser entregados vía electrónica.

La protección de los datos de prueba deberá incluir:
- Despersonalización de los datos antes de su uso.
- Eliminar inmediatamente, una vez completadas las pruebas, la información operativa utilizada.

Será requisito documentar:
- El tipo de pruebas realizadas
- Los datos utilizados para ellas, incluyendo su origen
- Los resultados obtenidos y, en su caso, los ajustes realizados
- La aceptación y visto bueno del usuario que realizó las pruebas

Para evitar la pérdida, modificación o uso inadecuado de los datos en el software, se verificará:
- La validación de datos de entrada.
- El procesamiento interno.
- La autenticación de mensajes (interfaces entre sistemas).
- La validación de datos de salida.

Etapa V: Implementación

Concluido el desarrollo o mantenimiento del software, y obtenidos resultados satisfactorios de las pruebas tanto del personal de la Subdirección de Informática como del usuario.

La implementación contemplará tres etapas, cuyos tiempos pueden variar dependiendo el tamaño, complejidad y características específicas del software.

Capacitación.- El personal de producción que utilizará el software o los cambios realizados en éste, deberá ser capacitado y adiestrado para su uso adecuado, para lo cual, el personal de la Subgerencia de Informática deberá apoyarse en el procedimiento de Capacitación.

Durante esta etapa, se deberán entregar las cuentas de usuario, para el caso de nuevos desarrollos.

Instalación.- De tratarse de software de escritorio que requiera estar instalado localmente en el equipo, o bien, archivos ejecutables que deban ser actualizados, se procederá según lo estipulado en el procedimiento de Mantenimiento Correctivo y Preventivo, mediante el cual se controla el software instalado en los equipos.

Apoyo.- El inicio de las operaciones de software nuevo o con nuevas características deberá contar con el apoyo del personal de la Subgerencia de informática, quien deberá asistir al personal de producción hasta que éste lo controle.

Como medida de seguridad, antes de la puesta en producción del software o su nueva versión, deberá realizarse una copia de seguridad tanto de la aplicación como de su base de datos.

Una vez puesto en producción el software, se realizarán verificaciones correspondientes a la seguridad de la aplicación que no interfieran con la producción.

Etapa VI: Liberación

Una vez que el proveedor, determinen que el personal es autosuficiente para operar el software o sus nuevas características, se dará por concluido y liberado el proyecto, documentando la fecha y observaciones que se consideren pertinentes.

Toda la información documentada por el proveedor durante el proceso de desarrollo será entregada al organismo

Ya liberado el software, la Subgerencia de Informática mantendrá el control de la administración de éste, la cual incluye:

- Administración de usuarios
- Administración de la base de datos
- Asignación, cancelación y modificación de roles

Dicha administración se gestionará mediante los procedimientos ya definidos para cada caso y a través de solicitudes generadas mediante el Help Desk.

En ningún caso el administrador del software podrá realizar operaciones ni a través de éste ni de manera directa en la base de datos.

En caso de haber existido una solicitud para el desarrollo o mantenimiento del software, ésta será cerrada mediante los procedimientos ya establecidos, detallando los resultados de la atención de la misma.

Separación de los entornos de desarrollo, prueba y operación

Para lograr una adecuada separación de ambientes se debe:

- Asegurar un mayor control por parte de la supervisión
- Incrementar el control sobre las versiones fuentes de desarrollo o mantenimiento, evitando que varios programadores trabajen simultáneamente sobre el mismo programa, pudiéndose perder lo realizado en ellos.
- Eficiente utilización de los recursos informáticos al evitar la repetición de los archivos y programas.
- Asegurar el acceso autorizado a los programas fuentes para su modificación.

6.0 DIFUSIÓN

• MG-02 ESTRUCTURA ORGANIZACIONAL			
• Dirección General	• Secretaría Particular	• Secretaría Técnica	• Subgerencia de Calidad
• Subgerencia de Planeación y Evaluación	• Subgerencia de Transparencia y Oficialía de Partes	• Subgerencia de Relaciones Publicas	• Contraloría Interna
• Subgerencia de Responsabilidades	• Subgerencia de Control de Obras	• Subgerencia de Auditoria Administrativa Financiera y Administrativa	• Dirección de Administración y Finanzas
• Gerencia de Administración	• Gerencia de Finanzas	• Subgerencia de Recursos Humanos	• Subgerencia de Informática
• Subgerencia de Recursos Materiales	• Subgerencia de Patrimonio	• Subgerencia de Tesorería	• Subgerencia de Contabilidad
• Dirección Jurídica	• Subgerencia de Ejecución Fiscal	• Subgerencia de Penal, Civil, Laboral.	• Subgerencia de lo Contencioso y Procedimientos Administrativos
• Dirección de Comercialización	• Gerencia de Atención a Usuarios	• Gerencia de Inspecciones y Restricciones	• Subgerencia de Altas Padrón y Censo
• Sugerencia de Medidores	• Subgerencia Central	• Subgerencia San Esteban	• Subgerencia San Esteban

• Subgerencia Tecamachalco	• Subgerencia Satélite	• Subgerencia Lomas Verdes	• Subgerencia Echegaray
• Subgerencia San Mateo	• Dirección de Construcción y Operación Hidráulica	• Gerencia de Operación Hidráulica	• Gerencia Técnica
• Subgerencia de Drenaje y Alcantarillado	• Subgerencia de Electromecánica	• Subgerencia de Efluentes y Calidad del Agua	• Subgerencia de Agua Potable
• Subgerencia de Planeación e Integración de Obra	• Subgerencia de Construcción	• Subgerencia de Estudios y Proyectos y Sectorización	• Subgerencia de Bacheo
• Subgerencia de Factibilidades	•	•	•

8.0 REGISTROS DE CALIDAD
Ninguno.

9.0 TABLA DE REVISIONES

TABLA DE REVISIONES	
TÍTULO:	Desarrollo Seguro
CÓDIGO:	PC-14-05
REVISIÓN:	06
CAMBIO / DESCRIPCIÓN:	Se actualiza el nombre del titular de la Dirección de Administración y Finanzas.
FECHA DE ELABORACIÓN:	09 de Noviembre del 2011
FECHA DE REVISIÓN:	02 de Julio del 2021

10.0 AUTORIZACIÓN

ELABORÓ	REVISÓ	AUTORIZÓ
José Luis Ayala López **Unidad de Soporte Informático**	José Antonio Arias Montes **Subgerencia de Informática**	**Armando Rodríguez García** **Dirección de Administración y Finanzas**
NOMBRE Y CARGO		