# AUDITORÍA INFORMÁTICA Y DE SEGURIDAD DE LA INFORMACIÓN

| | Elaboró: | Revisó: | Autorizó: |
|---|---|---|---|
| Puesto | Jefe de Departamento de Gestión Estratégica | Subdirección de Tecnologías de la Información y Comunicaciones | Subdirección de Tecnologias de la Información y Comunicaciones |
| Firma | | | |

## 1. Propósito

Verificar mediante revisiones de calidad, que los productos, servicios, procesos y soluciones tecnológicas adquiridas o en desarrollo que integran el MAAGTICSI, cumplan con los requerimientos definidos.

## 2. Alcance

Aplica al Departamento de Gestión Estratégica y a los departamentos involucrados con los productos, servicios, procesos y soluciones tecnológicas adquiridas o en desarrollo que integran el MAAGTICSI ra.

## 3. Responsabilidades

- **Subdirector de Tecnologías de la Información y Comunicaciones:** Facilitar los recursos humanos y gestionar los recursos financieros que permitan llevar a cabo las actividades programadas de revisiones de calidad.

- **Jefe de Departamento de Gestión Estratégica:** Identificar las principales iniciativas para la evaluación de la operación y cumplimiento de los objetivos plasmados para la Auditoría Informática y de Seguridad, así como concentrar los resultados obtenidos de las revisiones de calidad y generar los reportes correspondientes para la STIC.

- **Coordinador de Auditoria Informática y Seguridad de la Información:** Coordinar las revisiones de calidad, verificar y validar que los componentes, productos, servicios y/o soluciones tecnológicas adquiridas o en desarrollo, cumplan con los requerimientos definidos. Coordinar, y reportar el seguimiento del proceso de calidad al Jefe del Departamento de Gestión Estratégica.

- **Auditor de calidad, Auditor de Seguridad:** Aplicar las revisiones de calidad a componentes, productos, servicio y/o soluciones tecnológicas para verificar el cumplimiento de los requerimientos definidos e identificar los defectos, hallazgos y “no conformidades”. Documentar los resultados de las auditorías en el Reporte de revisión, reportar los resultados al Coordinador de Auditoria Informática y Seguridad de la Información, cotejar los requerimientos definidos de los componentes, productos, servicios y/o soluciones tecnológicas con la documentación generada durante el cumplimiento de las actividades programadas, así como dar seguimiento a los hallazgos y “no conformidades” hasta el cierre de la revisión.

## 4. Políticas de operación y normas.

- El Responsable de revisiones de calidad deberá someter a cualquier solución tecnológica de TIC que se contrate, así como en aquellos casos en que se integren o adicionen componentes de software, sistemas o aplicativos a una solución tecnológica o servicio de TIC ya existente, a las siguientes pruebas: unitarias, integrales de funcionalidad, estrés, volumen, aceptación del Usuario y de seguridad, con la finalidad de comprobar la calidad de la solución tecnológica de TIC, y para comprobar que la funcionalidad de la solución o servicio existente se mantiene inalterada y que la

relativa al componente integrado o adicionado es consistente con la de la solución o servicio de que se trate.

- El Responsable de calidad de productos, servicios y soluciones tecnológicas de TIC, deberá continuar el seguimiento de los defectos, hallazgos y "no conformidades" detectados en cada proceso, que se encuentren pendientes de resolución.
- En el caso de una auditoría a proyecto se realizará una revisión de calidad a los documentos de Acta Constitutiva, Alcance de Proyectos y Planeación del Proyecto y se verificará que contengan el plan de calidad descrito correctamente. Se aplicarán auditorias de calidad a las pruebas de verificación y validación descrita en el Plan de Proyecto, verificando la existencia y correcto llenado de los productos involucrados así como de que las pruebas se lleven a cabo conforme a lo establecido en el ambiente de pruebas, listas de verificación y plan de calidad. Se aplicará auditorias de calidad al proceso de cierre del proyecto, revisando el Acta de Aceptación, Acta de Cierre, Cuestionario de retroalimentación y lecciones aprendidas.
- En el caso de una auditoría de calidad a los procesos se revisarán los documentos de descripción de las metodologías, con el objeto de verificar la existencia de las metas y objetivos de calidad de los procesos así como los criterios de aceptación de sus productos. Se realizarán auditorías de calidad al Plan de Evaluación de Procesos y se aplicarán auditorias de calidad a los proyectos de mejora, de acuerdo a lo establecido en la regla de proceso Proyectos.
- En el caso de una auditoría de calidad a contrataciones de servicios de proveedores se realizarán revisiones de calidad a las propuestas de anexo técnico, cuyo contenido deberá integrar los criterios de calidad, aceptación y niveles de servicio esperados. Se aplicarán auditorias de calidad a los estudios de mercado con el objeto de evitar incongruencias entre documentos.
- En el caso de auditoría de calidad a las actividades de proveedor, se realizarán las revisiones a las listas de verificación de compromisos contractuales, a los informes de avance de proyecto, además se seleccionará una muestra de las actividades que lleva a cabo el proveedor y se efectuará una auditoria de calidad.
- En el caso de una auditoría a Servicios, se realizarán las revisiones a los niveles de servicio, con el objeto de comparar los niveles de servicio comprometidos con los reportados y verificar la información contenida en los reportes de revisión y monitoreo de servicios. Además se realizarán auditorias de calidad al Programa de Mejora de Servicios y a los Proyectos de Mejora.
- En caso de auditoría a la Seguridad de la Información se llevarán a cabo las revisiones de calidad al documento de SGSI con el objeto de verificar la información contenida, la correcta descripción de los controles y la ejecución del programa de implantación. Además, se realizarán auditorias de calidad a cada uno de los controles definidos en el SGSI, asegurando que cada uno se haya implantado de acuerdo a lo establecido en el SGSI. Además se aplicarán auditorias de calidad al proceso de mejora del SGSI cuyo fin es verificar los informes de evaluación, los documentos de mejora y su programa de evaluación.
- En lo que refiere a la nomenclatura el número de cada auditoria deberá contener número identificador que se compone de cuatro secciones:
  1. La primera refleja tipo de proyecto (de acuerdo a la nomenclatura establecida en el portafolio de proyectos);
  2. La segunda el número de proyecto (establecido en el portafolio de proyectos).
  3. La tercera tipo y número de auditoría.
  4. La cuarta el año de ejecución.

  (Ejemplo PO-01-AI01/2013 donde:
    - PO indica que es un proyecto de operación
    - 01 Indica el número de proyecto

- AI01 indica auditoria informática número 1
- 2013 indica el año de ejecución).

**5. Descripción del procedimiento:**

| N° | RESPONSABLE | ACTIVIDAD |
|---|---|---|
| 1 | **Coordinador de Auditoría Informática y de Seguridad de la Información** | **Planea la Calidad (Verificación):**<br>Selecciona los productos, servicios y soluciones tecnológicas adquiridas o en desarrollo para su verificación.<br><br>Establece los criterios de verificación a productos, servicios y soluciones tecnológicas, referentes a revisión, inspección y prueba interna, así como registra dichos criterios como activos de este proceso.<br><br>Identifica y establece los requerimientos del ambiente en el que se efectuará la verificación.<br><br>Identifica los recursos disponibles del ambiente de verificación, para su posible reutilización.<br><br>Integra los datos de los factores críticos anteriores en el Documento de ambiente de verificación.<br><br>Identifica las herramientas para la verificación.<br><br>Elabora el programa con base en los factores críticos anteriores. |

| | | |
|---|---|---|
| **2** | **Auditor de Calidad** | **Controla la Calidad (Verificación):**<br>Realiza la verificación de los componentes y productos seleccionados y analiza sus resultados.<br><br>Identifica y relaciona los componentes y productos intermedios seleccionados para su verificación, así como los requerimientos que dichos componentes y productos deben cumplir.<br><br>Prepara el ambiente, elabora las Listas de verificación y efectúa las verificaciones de acuerdo al programa de calidad.<br><br>Registra y analiza los resultados de las actividades en verificación.<br><br>Define las acciones a implementar como resultado de la verificación a los componentes o productos intermedios, y da seguimiento hasta el cierre de los hallazgos identificados.<br><br>Documenta la verificación realizada en los documentos de Auditoria y Hallazgos, destacando los defectos y hallazgos encontrados, así como los componentes o productos afectados.<br><br>Se asegura de que se actualice el Repositorio de revisiones de calidad. |
| **3** | **Responsable de la Calidad** | **Controla la Calidad (Verificación):**<br>Presencia la realización de revisiones sobre los componentes y productos seleccionados, por parte de los diversos involucrados que realicen actividades similares, para la identificación de defectos en una etapa temprana.<br><br>Presencia las pruebas de funcionalidad de productos, servicios y/o soluciones tecnológicas con el propósito de identificar los defectos y hallazgos encontrados en los componentes y productos afectados, y documenta las revisiones realizadas en el Reporte de revisión correspondiente.<br><br>Se asegura de que en las pruebas efectuadas hayan cumplido los acuerdos previstos en las Listas de Verificación, de acuerdo con el Documento de planeación de calidad.<br>¿Procede?<br>No: Solicita nuevamente la ejecución de las pruebas.<br>Si: Se asegura que se almacene la información obtenida en el Repositorio. |

| | | |
|---|---|---|
| **4** | **Coordinador de Auditoría Informática y de Seguridad de la Información** | **Controla la Calidad (Verificación):**<br>Analiza los resultados de las actividades de verificación.<br><br>Define la forma y términos para la aceptabilidad de los componentes y productos verificados.<br><br>Identifica, con base en el factor crítico anterior, los componentes y productos que no han cumplido con sus requerimientos o cuyos defectos, hallazgos y "no conformidades" persisten.<br><br>Analiza los resultados de la verificación, para constatar la validez de los datos utilizados en los casos en que se detectaron defectos, hallazgos y "no conformidades".<br><br>Registra los resultados del análisis efectuado en el Documento Auditoria.<br><br>Documenta las propuestas para resolver los defectos, hallazgos y "no conformidades", señalando los tiempos de resolución y los responsables. |
| **5** | **Auditor de Calidad** | **Asegura la Calidad (Verificación):**<br>Asegura, con la intervención de los responsables y demás participantes en el proyecto de la solución tecnológica, la resolución de los defectos, hallazgos y "no conformidades" detectados.<br><br>Resuelve cada defecto, hallazgo o "no conformidad" con los responsables y demás participantes en el proyecto, servicio o solución tecnológica de que se trate. |
| **6** | **Coordinador de Auditoría Informática y de Seguridad de la Información** | Analiza los defectos, hallazgos y "no conformidades" para constatar si existen tendencias de calidad que puedan apoyar su resolución.<br><br>Informa a los responsables y demás participantes en el proyecto servicio o solución tecnológica de que se trate, del resultado de dicho análisis.<br><br>Solicita a los responsables y demás participantes en el proyecto, servicio y/o solución tecnológica de que se trate, la presentación de alternativas que permitan resolver los defectos, hallazgos o "no conformidades" pendientes de resolución y documenta en Lecciones Aprendidas. |

| | | |
|---|---|---|
| **7** | **Auditor de Calidad** | Actualiza, con la información obtenida de la revisión de calidad, el repositorio correspondiente.<br><br>Da seguimiento a los defectos, hallazgos y "no conformidades" hasta su cierre mediante el documento Hallazgos y Acciones de Mejora.<br>¿Procede?<br>No: Documenta los defectos, hallazgos y "no conformidades" que no fue posible resolver durante la ejecución del proyecto mediante las Lecciones Aprendidas.<br>Si: Realiza revisiones, al menos una vez al año, sobre los defectos, hallazgos y "no conformidades" detectados en los diversos proyectos, servicios y/o soluciones tecnológicas, con motivo de la ejecución de las actividades de este proceso, con la finalidad de apoyar la mejora continua de dicho proceso.<br><br>**TERMINA PROCEDIMIENTO** |

## 6. Documentos de referencia:

| DOCUMENTO | CODIGO |
|---|---|
| NMX-CC-9001-IMNC-2008 ISO 9001:2008 Sistemas de Gestión de la Calidad | N/A |
| Manual de Gestión de la Calidad | MGC-DG-01 |
| Control de Documentos y Registros | PR-SGC-01 |

| REGISTRO | TIEMPO DE CONSERVACIÓN | RESPONSABLE DE CONSERVACIÓN | CODIGO |
|---|---|---|---|
| Metodología de Auditoría Informática y Seguridad de la Información | Sin fecha límite | Coordinador de Auditoría Informática y Seguridad de la Información | INRSTIC_PROY_ MAAGTICSIAUDI_ Descripción Proceso (OSGP-A8-F2)_VB2_VER 5.4 (2) |
| Ambiente de Pruebas | 2 años | Coordinador de Auditoría Informática y Seguridad de la Información | INR-STIC-FO_ATE2013-01A_Ambiente_de_pruebas_ver-val_V0.1 |
| Auditoría | 2 años | Coordinador de Auditoría Informática y Seguridad de la Información | INR-MAAGTIC-SDI_Auditoria_Procesos_Ejecutados (ATC_A14-F3)V1 |
| Hallazgos y acciones de mejora | 2 años | Coordinador de Auditoría Informática y Seguridad de la Información | N/A |

## 7. Glosario

1. MAAGTICSI - Manual Administrativo de Aplicación General de Tecnologías de Información y Comunicaciones y Seguridad de la Inform.

2. MAUDI – Metodología de Auditoría Informática y Seguridad de la Información.

3. Ambiente de Pruebas – Formato donde se establecen las necesidades de ambiente que se requiere para realizar la verificación-validación requerida sobre componentes de proyectos, procesos o servicios**.**

## 8. Control de cambios

| Revisión | Descripción del cambio | Fecha |
|---|---|---|
| 00 | Inicio en el Sistema de Gestión de la Calidad | Julio 2013 |
| 01 | Actualización de la imagen institucional | JUN 15 |
| | | |