





| | | | |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|--------------------------------------|
|  | <p align="center">PROCEDIMIENTOS Versión ISO 9001:2015</p> |  | <p>Código: PR-STIC-25</p> |
| | <p align="center">DIRECCIÓN GENERAL</p> | | <p>Fecha: DIC 20</p> |
| | <p align="center">AUDITORÍA INFORMÁTICA Y DE SEGURIDAD DE LA INFORMACIÓN</p> | | <p>Rev. 03</p> |
| | | | <p>Hoja: 1 de 7</p> |

AUDITORÍA INFORMÁTICA Y DE SEGURIDAD DE LA INFORMACIÓN

| | | | |
|--------|----------------------------------------------------|-------------------------------------------------------------------|-------------------|
| | Elaboró: | Revisó: | Autorizó: |
| Puesto | Jefatura de Departamento de Gestión Estratégica | Subdirección de Tecnologías de la Información y Comunicaciones | Dirección General |
| Firma | | | |

| | | | |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------|------------------------------|
|  | PROCEDIMIENTOS Versión ISO 9001:2015 |  | Código: PR-STIC-25 |
| | DIRECCIÓN GENERAL | | Fecha: DIC 20 |
| | AUDITORÍA INFORMÁTICA Y DE SEGURIDAD DE LA INFORMACIÓN | | Rev. 03 |
| | | | Hoja: 2 de 7 |

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.



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 Auditoría 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 Auditoría 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.

PO1-STIC-PR-25. 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.

PO2-STIC-PR-25. 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. Se aplicarán auditorías de calidad al proceso de cierre del proyecto, revisando el Acta de Aceptación, Acta de Cierre y Lecciones aprendidas.

| | | | |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------|------------------------------|
|  | PROCEDIMIENTOS Versión ISO 9001:2015 |  | Código: PR-STIC-25 |
| | DIRECCIÓN GENERAL | | Fecha: DIC 20 |
| | AUDITORÍA INFORMÁTICA Y DE SEGURIDAD DE LA INFORMACIÓN | | Rev. 03 |
| | | | Hoja: 3 de 7 |

PO3-STIC-PR-25. En el caso de una 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.

PO4-STIC-PR-25. 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

PO5-STIC-PR-25. 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

5. Descripción del procedimiento:



| N° | RESPONSABLE | ACTIVIDAD |
|----|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Coordinador de Auditoría Informática y de Seguridad de la Información | Seleccionar los productos, servicios y soluciones tecnológicas adquiridas o en desarrollo para su verificación. |
| 2 | Coordinador de Auditoría Informática y de Seguridad de la Información | Establecer 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. |
| 3 | Coordinador de Auditoría Informática y de Seguridad de la Información | Identificar y establecer los requerimientos del ambiente en el que se efectuará la verificación. |

| | | | |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------|------------------------------|
|  | PROCEDIMIENTOS Versión ISO 9001:2015 |  | Código: PR-STIC-25 |
| | DIRECCIÓN GENERAL | | Fecha: DIC 20 |
| | AUDITORÍA INFORMÁTICA Y DE SEGURIDAD DE LA INFORMACIÓN | | Rev. 03 |
| | | | Hoja: 4 de 7 |

| | | |
|----|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4 | Coordinador de Auditoría Informática y de Seguridad de la Información | Identifica los recursos disponibles del ambiente de verificación, para su posible reutilización. |
| 5 | Coordinador de Auditoría Informática y de Seguridad de la Información | Integra los datos de los factores críticos anteriores en el Documento de ambiente de verificación. (F03-PR-STIC-25) |
| 6 | Coordinador de Auditoría Informática y de Seguridad de la Información | Identificar las herramientas para la verificación. |
| 7 | Coordinador de Auditoría Informática y de Seguridad de la Información | Elaborar el documento de Auditoría (F02-PR-STIC-25) con base en los factores críticos anteriores. |
| 8 | Coordinador de Auditoría Informática y de Seguridad de la Información | Enviar el documento de Ambiente de Pruebas (F03-PR-STIC-25) y Auditoría (F02-PR-STIC-25) a revisión y autorización por el Jefe del Departamento de Gestión Estratégica |
| 9 | Jefe del Departamento de Gestión Estratégica | Revisar y autorizar los formatos de Ambiente de Pruebas (F-03-PR-STIC-25) y Auditoría (F02-PR-STIC-25) ¿Se autorizan los formatos? Si: Pasar a la actividad 10 No: Realizar las correcciones pertinentes, pasar a la actividad 5. |
| 10 | Auditor de Calidad | Controlar la Calidad (Verificación): Realizar la verificación de los componentes y productos seleccionados y analizar sus resultados |
| 11 | Auditor de Calidad | Identificar y relacionar los componentes y productos intermedios seleccionados para su verificación así como los requerimientos que dichos componentes y productos deben cumplir |

| | | | |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------|------------------------------|
|  | PROCEDIMIENTOS Versión ISO 9001:2015 |  | Código: PR-STIC-25 |
| | DIRECCIÓN GENERAL | | Fecha: DIC 20 |
| | AUDITORÍA INFORMÁTICA Y DE SEGURIDAD DE LA INFORMACIÓN | | Rev. 03 |
| | | | Hoja: 5 de 7 |



| | | |
|----|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12 | Auditor de Calidad | Efectuar las verificaciones de acuerdo al documento Auditoría (F02-PR-STIC-25) |
| 13 | Auditor de Calidad | Documentar la verificación realizada en el formato de Hallazgos y acciones de mejora (F01-PR-STIC-25), para registrar los defectos y Hallazgos encontrados o productos afectados. |
| 14 | Auditor de Calidad | Actualizar el Repositorio de revisiones de calidad |
| 15 | Coordinador de Auditoría Informática y de Seguridad de la Información | Analizar los resultados de las Actividades de verificación |
| 16 | Coordinador de Auditoría Informática y de Seguridad de la Información | Identificar los componentes y productos que no han cumplido con sus requerimientos o cuyos defectos, hallazgos y “no conformidades” persisten. |
| 17 | Coordinador de Auditoría Informática y de Seguridad de la Información | Acordar y documentar las propuestas para resolver los defectos, hallazgos y “no conformidades”, señalando los tiempos de resolución y los responsables en el formato de Hallazgos y acciones de mejora (F01-PR-STIC-25) |
| 18 | Coordinador de Auditoría Informática y de Seguridad de la Información | Analizar los defectos, hallazgos y “no conformidades” para constatar si existen tendencias de calidad que puedan apoyar su resolución |
| 19 | Coordinador de Auditoría Informática y de Seguridad de la Información | Informar a los responsables y demás participantes en el proyecto servicio o solución tecnológica de que se trate, del resultado de dicho análisis |

| | | | |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------|------------------------------|
|  | PROCEDIMIENTOS Versión ISO 9001:2015 |  | Código: PR-STIC-25 |
| | DIRECCIÓN GENERAL | | Fecha: DIC 20 |
| | AUDITORÍA INFORMÁTICA Y DE SEGURIDAD DE LA INFORMACIÓN | | Rev. 03 |
| | | | Hoja: 6 de 7 |

| | | |
|----|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 20 | Jefe del Departamento de Gestión Estratégica | Solicitar a los responsables y demás participantes en el proyecto, servicio y/o solución tecnológica, la presentación de alternativas que permita resolver los defectos, hallazgos o “no conformidades” pendientes de resolución, definir los tiempos de entrega y documentar en Hallazgos y acciones de mejora (F01-PR-STIC-25). |
| 21 | Auditor de Calidad | Verificar que se resuelva cada defecto, hallazgo o “no conformidad” con los responsables y demás participantes en el proyecto, servicio o solución tecnológica de que se trate |
| 22 | Auditor de Calidad | Actualizar, con la información obtenida de la revisión de calidad, el repositorio correspondiente. |
| 23 | Auditor de Calidad | Da seguimiento a los defectos, hallazgos y “no conformidades” hasta su cierre mediante el documento Hallazgos y Acciones de Mejora. ¿Procede? No: Documenta los defectos, hallazgos y “no conformidades” que no fue posible resolver durante la ejecución del proyecto mediante las Lecciones Aprendidas. 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. TERMINA PROCEDIMIENTO |

6. Documentos de referencia:

| DOCUMENTO | CODIGO |
|-----------------------------------------------------------------------|-----------|
| NMX-CC-9001-IMNC-2015 ISO 9001:2015 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 |

| | | | |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------|------------------------------|
|  | PROCEDIMIENTOS Versión ISO 9001:2015 |  | Código: PR-STIC-25 |
| | DIRECCIÓN GENERAL | | Fecha: DIC 20 |
| | AUDITORÍA INFORMÁTICA Y DE SEGURIDAD DE LA INFORMACIÓN | | Rev. 03 |
| | | | Hoja: 7 de 7 |

| REGISTRO | TIEMPO DE CONSERVACIÓN | RESPONSABLE DE CONSERVACIÓN | CODIGO |
|--------------------------------|------------------------|--------------------------------------------------------------------|-----------------|
| Ambiente de Pruebas | 3 años | Coordinador de Auditoría Informática y Seguridad de la Información | F03-PR-STIC-25 |
| Auditoría | 3 años | Coordinador de Auditoría Informática y Seguridad de la Información | F02-PR-STIC-25 |
| Hallazgos y acciones de mejora | 3 años | Coordinador de Auditoría Informática y Seguridad de la Información | F01-PR-STIC-25 |
| Lecciones Aprendidas | 3 años | Encargado de Procesos | F03-PR--STIC-13 |

7. Glosario

1. MAAGTICSI - Manual Administrativo de Aplicación General de Tecnologías de Información y Comunicaciones y Seguridad de la Informo.
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 |
|----------|-----------------------------------------------------------------------|--------|
| 01 | Actualización de la imagen institucional | JUN 15 |
| 02 | Transición del SGC de la Norma ISO 9001:2008 a la Norma ISO 9001:2015 | MAY 18 |
| 03 | Actualización de Imagen Institucional | DIC 20 |
| | | |