

INSTITUTO COLOMBIANO AGROPECUARIO ICA		
OFICINA DE CONTROL INTERNO		
PROCEDIMIENTO EVALUACION Y SEGUIMIENTO		
INFORME DE AUDITORIA		
Responsable del proceso: OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN		
Proceso a auditar en:	Oficinas Nacionales <u>X</u> Seccional _____ Oficina Local _____ Otros _____	
Tipo de Informe:	Preliminar ____ Definitivo <u>X</u>	Fecha: Del 21 de octubre al 29 de noviembre de 2019

OBJETIVO

De conformidad con el Programa Anual de Auditoría, formulado por la Oficina de Control Interno para la vigencia 2019 y aprobado por el Comité de Coordinación del Sistema de Control Interno, verificar el cumplimiento del proceso GESTIÓN DEL SERVICIO TIC, gestionado por la Oficina de Tecnologías de la Información y en el presente informe se relacionan las debilidades detectadas con sus respectivas recomendaciones, para que se formulen acciones que permitan subsanarlas, propiciando un marco de mejoramiento continuo.

ALCANCE

Verificación al proceso GESTIÓN DEL SERVICIO TIC de la Oficina de Tecnologías de la Información, con un enfoque al Sistema de Información Epidemiológica y Vigilancia Fitosanitaria - SISFITO, incluyendo de ser necesario a las áreas encargadas de la administración funcional del aplicativo, para lo cual se tuvo en cuenta lo relacionado con controles, seguridad de la información, planes de contingencia, gestión de cambios, gestión del servicio, cumplimiento de procedimientos y demás aspectos gestionados durante la vigencia 2018.

LIMITACIONES AL ALCANCE

Durante la auditoría interna practicada al proceso GESTIÓN DEL SERVICIO TIC, con enfoque al Sistema de Información Epidemiológica y Vigilancia Fitosanitaria - SISFITO, que está en cabeza de la Oficina de Tecnologías de la Información, no se presentaron limitaciones que pudieran comprometer el alcance establecido, el acceso a los registros, personal y bienes relevantes, la programación realizada y/o la ejecución de los procedimientos aplicados para la realización de la auditoría.

DESARROLLO DE LA AUDITORÍA

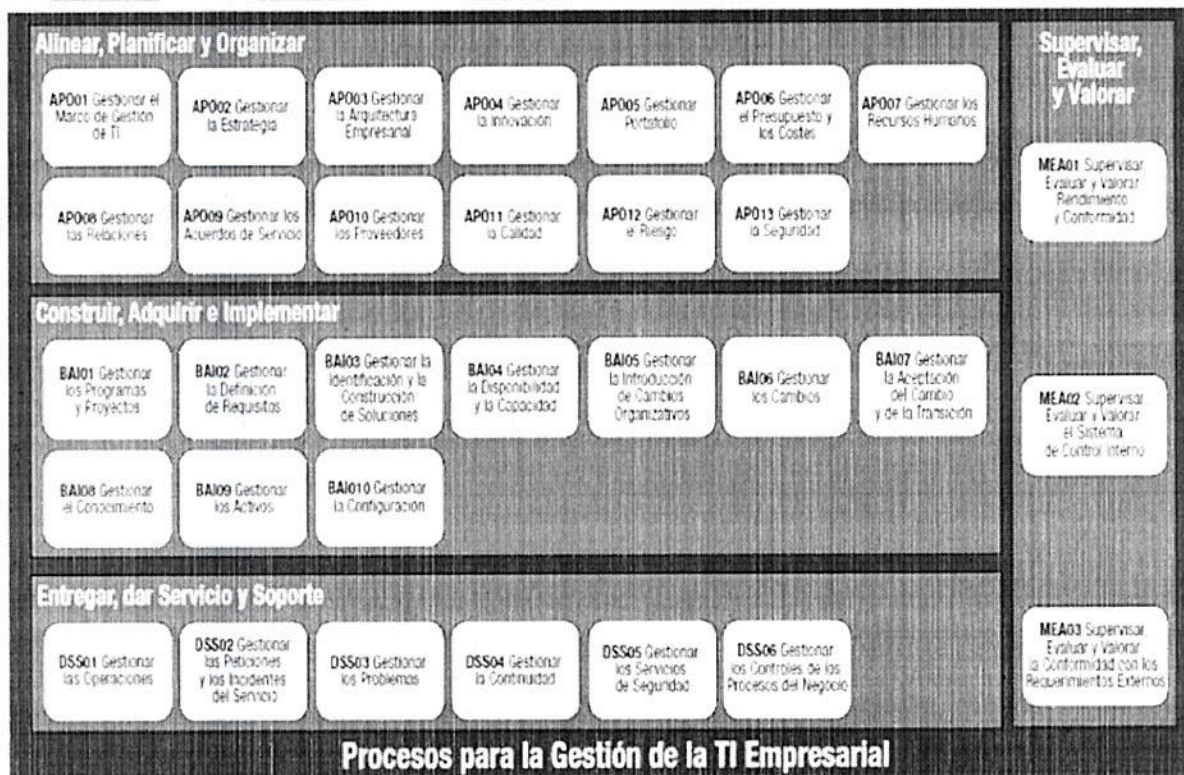
La presente verificación se ha realizado con base en las Normas Internacionales de Auditoría y se utilizaron diferentes técnicas para obtener evidencias suficientes, tales como: indagación, comparación, comprobación, verificación documental, que permitieron obtener y evaluar la evidencia de auditoría, proporcionando una base razonable para la determinación de las debilidades encontradas.

Así mismo, se tomó como lineamiento el marco de referencia de buenas prácticas para el Gobierno y Gestión de las TI, COBIT (Objetivos de Control para Sistemas de Información y Tecnologías Relacionadas - Versión 5), el cual está conformado como se puede apreciar a continuación:

Figura 16—Modelo de Referencia de Procesos de COBIT 5

Procesos de Gobierno de TI Empresarial

Evaluar, Orientar y Supervisar



Fuente: COBIT® 5, Figura 16. © 2012 ISACA®. Todos derechos reservados.

Teniendo en cuenta esta metodología, se realizó indagación a la Oficina de Tecnologías de la Información, área encargada de la administración técnica del SISFITO, donde se solicitó información afín al aplicativo y se practicó una serie de pruebas al mismo, para verificar el diseño, parametrización, controles, seguridad, planes de contingencia y correcta ejecución de sus funcionalidades.

Igualmente, se solicitó información relacionada con el aplicativo a la Dirección Técnica de Sanidad Vegetal, dependencia encargada de la administración funcional de la Unidad Productiva “Ornamentales de Exportación”, presente en el SISFITO.

Luego del análisis realizado a la información recopilada y posterior a las pruebas efectuadas al aplicativo, se generan las siguientes observaciones, las cuales están acompañadas de sus respectivas recomendaciones:

Observación 1: Se evidenció que no se controla la “Fecha Informe” y “Fecha de Visita”, presentes en la unidad productiva “Forestales” del SISFITO, admitiendo registrar una fecha de informe anterior a la fecha de la visita (lo cual no es coherente) y a su vez la generación de trámites con errores.

Área Responsable: Oficina de Tecnologías de la Información

Recomendaciones:

1. Aplicar puntos de control en el sistema, para garantizar que las fechas de programación de las visitas y de los informes, sean idóneas y afines a la realidad.
2. Validar todos los campos de fechas del sistema, implementando las parametrizaciones que se requieran, con el fin de mantener la calidad y veracidad de la información que es ingresada sobre estos.

Observación 2: No se dispone de un mismo protocolo de autenticación para el ingreso de los funcionarios a su equipo y al SISFITO.

Área Responsable: Oficina de Tecnologías de la Información

Esta observación se genera, luego de identificar que los funcionarios del Instituto ingresan a sus equipos de cómputo mediante el directorio activo de la entidad, a través del protocolo de autenticación y de acceso a directorios LDAP, mientras que al SISFITO ingresan por medio de un usuario y contraseña asociados a perfiles, lo cual genera un proceso dispendioso para el usuario, al tener que administrar varias cuentas de ingreso, con el riesgo de su olvido. Adicionalmente, el ingreso de los usuarios al SISFITO normalmente se realiza a través de su cédula, la cual algunos modifican para crear un nuevo perfil en el sistema, generándose en algunos casos un mismo usuario con varias cuentas de ingreso; un ejemplo de esta situación se presenta con el usuario de la funcionaria Ángela Adriana Hidalgo Ocampo, la cual posee varias cuentas de ingreso y varias contraseñas, por cuanto tiene varios perfiles para ejecutar en el aplicativo.

Recomendaciones:

1. Implementar como única vía de autenticación para los usuarios internos del SISFITO, las credenciales de acceso al directorio activo LDAP, con la finalidad que los funcionarios de la entidad administren una sola cuenta de ingreso al equipo y a los aplicativos, fortaleciendo a su vez la seguridad en el proceso de entrada al sistema.
2. Estimar la opción de definir un módulo de administración de usuarios en el aplicativo, que sea gestionado por las áreas encargadas de la dirección funcional del SISFITO, desde el cual se administren y se asignen los roles y perfiles a los usuarios que lo requieran.
3. Socializar a las partes interesadas, los ajustes que se apliquen para la autenticación de los usuarios a través del SISFITO, guardando las respectivas evidencias de su realización.

Observación 3. Se identificó que en la actualidad no se cuenta con un plan de contingencia operativo, para el SISFITO.

Área responsable: Oficina de Tecnologías de la Información

Existe un alto riesgo que al fallar el sistema, se presente la interrupción en los servicios propios del mismo y que las tareas de los usuarios también se vean afectadas; así mismo, la información que se procesa a través del sistema no está suficientemente protegida, coexistiendo con el riesgo de afectar su seguridad e integridad.

Recomendaciones:

1. Definir e implementar un plan de contingencia para el SISFITO, que asegure la normal operatividad del sistema y la realización del conjunto de actividades que se ejecutan a través del mismo, garantizando a su vez la continuidad en el servicio, la oportuna atención a los usuarios y el blindaje de la entidad frente a los sucesos que amenacen la seguridad de la información que es gestionada a través del aplicativo.
2. Realizar todas las pruebas necesarias para verificar la efectividad del plan de contingencia y garantizar que cumpla con los objetivos.
3. Analizar la opción de publicar el plan de contingencia del SISFITO en el gestor documental de la entidad.
4. Realizar las capacitaciones requeridas para el personal de la mesa de ayuda del sistema, así como también a los usuarios del mismo, en relación con el plan de contingencia.

Observación 4: Se evidenció la existencia de campos dentro de algunos formularios del SISFITO, los cuales no están correctamente parametrizados de acuerdo a su tipo, permitiendo ingresar caracteres inválidos, lo que puede generar errores en el guardado de datos y prolongados tiempos de espera al momento de las consultas.

Área Responsable: Oficina de Tecnologías de la Información - Dirección Técnica de Sanidad Vegetal

Ejemplo de esta falencia, se puede apreciar en los campos "Registro ICA" e "Inscripción", los cuales admiten el ingreso y guardado de cualquier tipo de carácter.

Recomendaciones:

1. Realizar una validación general a los campos de los formularios del SISFITO, aplicando una adecuada parametrización sobre los mismos, en la cual se asegure el ingreso de datos acorde al tipo de campos que estén presentes.
2. Validar todos los formularios del sistema junto con sus campos, ya que al verificar los datos de un formulario mientras el usuario lo llena, inmediatamente puede saber si ha cometido algún error, ahorrándole tiempo de espera a una respuesta y evitando al servidor lidiar con entradas incorrectas en el formulario.
3. Socializar con los usuarios del sistema, acerca de las mejoras de validación que se efectúen sobre los diferentes campos de los formularios.

Observación 5: Se evidenciaron debilidades en el SISFITO, al momento del registro de usuarios en la plataforma, toda vez que se generan mensajes alusivos a que la identificación del usuario ya existe o que el correo electrónico ya está registrado, cuando en realidad se está haciendo el proceso de registro por primera vez.

Área responsable: Oficina de Tecnologías de la Información - Dirección Técnica de Sanidad Vegetal

Esta situación se pudo observar al momento de intentar efectuar el registro en la plataforma por primera vez y el sistema generó esta serie de mensajes, indicando que el usuario ya existía, lo cual no era coherente; así mismo, se formuló con base en lo informado por la Dirección Técnica de Sanidad Vegetal, quien señaló que es una debilidad del aplicativo que se presenta repetidamente al momento del registro de los usuarios.

Recomendaciones:

1. Revisar el diseño y configuración de la funcionalidad para el registro de usuarios en el SISFITO, aplicando los ajustes correspondientes, con la finalidad que ésta se ejecute exitosamente.
2. Practicar las pruebas que sean necesarias para certificar que la debilidad ha sido superada, guardando soportes de su realización.

Observación 6: Se evidenció que el SISFITO no dispone de una opción para consultar la trazabilidad de la información, que permita rastrear los cambios que un usuario por error o intencionalmente haya efectuado en el sistema, imposibilitando obtener la información de qué usuario ejecutó alguna modificación y la fecha de realización.

Área responsable: Oficina de Tecnologías de la Información - Dirección Técnica de Sanidad Vegetal

Recomendaciones:

1. Validar de la opción de retirar la acción "Eliminar Predio" del sistema y analizar si es mejor cambiar por una opción que permita su inactivación.
2. De no ser posible el retiro de la acción "Eliminar Predio", implementar en el sistema una opción de consulta, que le permita al usuario hacer seguimiento a los predios,

visualizar su estado, sus documentos y toda la trazabilidad de la información relacionada al mismo, guardando las restricciones de seguridad del caso.

3. Ejecutar las pruebas pertinentes para verificar la efectividad de la mejora realizada, anterior a su aprobación y paso a producción.
4. Incluir en el manual de usuario del aplicativo los ajustes que se implementen, realizando además la divulgación correspondiente a las partes interesadas.

Observación 7: *Se identificó que el SISFITO no tiene comunicación con el aplicativo SISPAF, muy a pesar que manejan información y trámites en común, como es el caso del registro de los predios, lo que puede conllevar a duplicidad de información entre ambos sistemas.*

Área responsable: *Oficina de Tecnologías de la Información - Dirección Técnica de Sanidad Vegetal*

Recomendaciones:

1. Realizar un levantamiento de la información en común entre los aplicativos SISFITO y SISPAF.
2. A través de la realización de dicho estudio, identificar y diseñar el medio adecuado para que exista una comunicación entre ambos sistemas de información y se gestione la misma información en común, evitando con ello la duplicidad de datos.
3. Ejecutar las pruebas que se requieran, validando su correcta ejecución, previo a su implementación.
4. Socializar entre las partes interesadas las nuevas mejoras efectuadas, guardando soportes de su realización.

Observación 8: *Se evidenció que al momento de la generación de algunos reportes del SISFITO, estos se producen con información duplicada, denotando debilidades en su ejecución; en otros casos, se presentan errores al momento de su generación, como es el caso del reporte de Predios y Especies por Empresa Exportadora.*

Área responsable: *Oficina de Tecnologías de la Información*

Recomendaciones:

1. Realizar una verificación de todos los reportes que se generan a través del SISFITO, identificando aquellos que se conciben con información incompleta, duplicada o con alguna otra inconsistencia.
2. Realizar los ajustes que se requieran, asegurando la veracidad y completitud de la información que se produce de los mismos, la cual debe coincidir con la información ingresada al sistema.

Observación 9: *El SISFITO presenta problemas de estabilidad en la última semana de cada trimestre, al parecer por cuanto en este periodo es cuando los asistentes técnicos suben al sistema los reportes de sus actividades, de acuerdo a lo informado por la Dirección Técnica de Sanidad Vegetal.*

Área responsable: *Oficina de Tecnologías de la Información*

La Dirección Técnica de Sanidad Vegetal, que es una de las áreas de la entidad encargada de la administración funcional del sistema, señaló que en dicho periodo se percibe lentitud y caídas del sistema.

Recomendaciones:

1. Efectuar diagnósticos para determinar las causas que pueden estar ocasionando la inestabilidad en el sistema, en los periodos de tiempo señalados.
2. Establecer acciones para evitar que estas causas que originan la inestabilidad en el aplicativo, se sigan presentando y afecten la normal operatividad del SISFITO.

Observación 10: El SISFITO no permite realizar la consulta del estado y comportamiento de las plagas, lo cual constituye una debilidad en el funcionamiento del aplicativo.

Área responsable: Oficina de Tecnologías de la Información

Recomendaciones:

1. Validar la funcionalidad contenida en el sistema, diseñada para estudiar la conducta de las plagas, con el fin de atacar la falencia señalada.
2. Ajustar el aplicativo a través de las acciones a que haya lugar, con el objetivo que éste permita generar la información relacionada a las plagas, de manera oportuna y eficiente.
3. Aplicar pruebas a los ajustes que se implementen sobre la funcionalidad en mención, certificando su normal ejecución.

Observación 11: Se evidenció falencias en la funcionalidad de envío de emails masivos que posee el SISFITO, por cuanto al seleccionar un grupo determinado para enviarle un correo, en el mismo se visualiza la dirección de correo de todas las personas relacionadas, lo que genera que la información sensible (dirección de correo), sea visible para todos los integrantes del grupo, denotando una inadecuada configuración de la funcionalidad.

Área responsable: Oficina de Tecnologías de la Información

Recomendación:

1. Revisar la configuración de la funcionalidad diseñada para el envío de correos masivos a través del SISFITO, ajustando los detalles necesarios para que al momento del envío de un correo masivo, solo sean visualizados los nombres de los integrantes del grupo y no sus direcciones electrónicas u otros datos sensibles.

Observación 12: No es suficiente la infraestructura tecnológica con que se cuenta actualmente, para atender todos los requerimientos técnicos que demanda el SISFITO.

Área responsable: Oficina de Tecnologías de la Información

Recomendaciones:

1. Realizar las gestiones correspondientes ante las directivas de la entidad, para lograr la consecución de los recursos que se requieran para el normal funcionamiento del SISFITO.
2. Fortalecer la infraestructura del SISFITO, con el fin que el sistema cuente con todo lo necesario para satisfacer las necesidades de los usuarios y permita el cumplimiento de los objetivos.

Observación 13: No se tienen suscritos acuerdos de niveles de servicio para el SISFITO, a pesar que el servidor de aplicaciones y de base de datos están ubicados en un Datacenter contratado por el ICA.

Área responsable: Oficina de Tecnologías de la Información

Esta observación se genera, luego de lo informado por parte de la Oficina de Tecnologías de la Información, quien indicó que no se han suscrito Acuerdos de Niveles de Servicio, SLA, relacionados con el funcionamiento del sistema.

Recomendación:

1. Realizar la gestión para la suscripción de los documentos que se requieran, en los cuales se definan los estándares de servicio que el proveedor está obligado a cumplir, los cuales deben asegurar el normal rendimiento del aplicativo.

Observación 14: *No existe un procedimiento de gestión de la continuidad del servicio para los aplicativos de la entidad, entre estos el SISFITO, impidiendo tener un adecuado control de los riesgos que podrían afectar los servicios de TI.*

Área responsable: *Oficina de Tecnologías de la Información*

Recomendación:

1. Definir y documentar una herramienta que asegure una pronta recuperación en los servicios críticos de la entidad, contemplando los elementos a controlar a partir del análisis de los riesgos asociados, definiciones, responsables, etapas, fechas de ejecución, recursos y acciones, que a su vez permitan prevenir o reaccionar oportuna y adecuadamente, ante posibles incidentes que pongan en riesgo la continuidad del servicio.
2. Ejecutar de forma planificada las acciones que sean determinadas, analizando los resultados obtenidos y validando su efectividad.
3. Comunicar las estrategias implementadas, entre los actores relacionados con el aplicativo, guardando evidencia de su realización.

Observación 15: *No se dispone de un procedimiento para controlar la creación, activación e inactivación de usuarios en el SISFITO, que permita gestionar eficientemente la administración de los usuarios en el aplicativo y al cual se le pueda hacer verificación y seguimiento de su efectividad.*

Área responsable: *Oficina de Tecnologías de la Información - Dirección Técnica de Sanidad Vegetal*

Recomendación:

1. Implementar y oficializar un procedimiento, estableciendo las acciones pertinentes que conlleven a realizar las tareas relacionadas con la administración de usuarios en el SISFITO.
2. Socializar el documento que se elabore entre las áreas encargadas de la administración de usuarios en el aplicativo.

Observación 16. *No se tiene implementado un modelo de medición, para evaluar el nivel de satisfacción de los usuarios del SISFITO frente al aplicativo.*

Área responsable: *Oficina de Tecnologías de la Información - Dirección Técnica de Sanidad Vegetal*

Recomendaciones:

1. Diseñar un modelo que posibilite evaluar el nivel de satisfacción de los usuarios frente al sistema, gestionar sus necesidades y requerimientos y que a su vez permita identificar aspectos de mejora para fortalecer los servicios ofrecidos desde el aplicativo.
2. Documentar, oficializar e implementar el modelo que se diseñe.
3. Realizar campañas de socialización entre los usuarios de la aplicación, dando a conocer la importancia de esta nueva herramienta y su diligenciamiento.
4. Establecer políticas o actividades de mejora a partir de los resultados obtenidos, encaminadas hacia el perfeccionamiento del sistema y sus componentes.

Observación 17. Se evidenció que el SISFITO admite la eliminación de usuarios, unidades productivas e informes de monitoreo y con ello la pérdida de información de los trámites relacionados a éstos.

Área responsable: Oficina de Tecnologías de la Información - Dirección Técnica de Sanidad Vegetal

Recomendaciones:

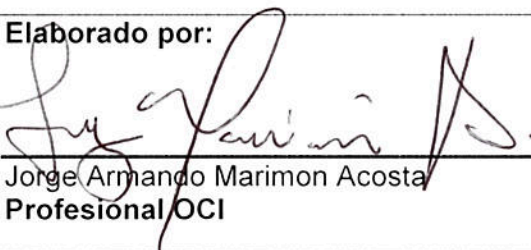
1. Validar la opción de retirar la acción "Eliminar Unidad Productora", manteniendo la opción de inactivación para aquellos casos donde no se deba seleccionar más una unidad Productiva.
2. Analizar la opción de efectuar la misma acción, para el caso de los usuarios del sistema y para los informes de monitoreo.
3. Socializar a las partes interesadas las acciones que se realicen.

Observación 18. Se evidenció un error en la unidad productiva "Forestales" del SISFITO, debido a que al seleccionar la opción "Gráficos", el sistema visualiza el formulario "Seleccione el tipo de Gráfico que desea", el cual contiene duplicado el municipio "BOGOTA D.C.".

Área responsable: Oficina de Tecnologías de la Información

Recomendaciones:

1. Aplicar la debida corrección sobre esta lista desplegable, la cual es visible al seleccionar el nivel "DISTRITO CAPITAL".
2. Validar el resto de listas desplegables contenidas en el aplicativo, con la finalidad de identificar si este tipo de errores se repiten, realizando los ajustes correspondientes.

Aprobado por:  JUAN FERNANDO PALACIO ORTIZ Jefe Oficina Control Interno	Elaborado por:  Jorge Armando Marimon Acosta Profesional OCI	Fecha de Aprobación: 17 de enero de 2020 FORMA 4-935 Versión 2
---	---	--