INSTITUTO COLOMBIANO AGROPECUARIO ICA		
OFICINA DE CONTROL INTERNO		
PROCEDIMIENTO EVALUACIÓN Y SEGUIMIENTO		
INFORME DE AUDITORÍA		
Responsable del proceso: OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN		
Proceso a auditar en:	Oficinas Nacionales __X__ Seccional _____ Oficina Local _____ Otros _____	
Tipo de Informe:	Preliminar ___ Definitivo X	**Fecha**: Del 27 de mayo al 12 de junio de 2019

INTRODUCCIÓN

En concordancia con el Programa Anual de Auditoría, aprobado para la vigencia 2019, se adelantó verificación al procedimiento Gestión de Incidentes de Seguridad de la Información, adelantado por la Oficina de Tecnologías de la Información y en el presente informe se relacionan las debilidades encontradas y las recomendaciones respectivas, con el fin de que se emprendan las acciones que permitan superar éstas y se propicien procesos de mejoramiento continuo.

OBJETIVO

A través de la actividad independiente de aseguramiento y asesoría, verificar y realizar seguimiento al cumplimiento de la normatividad vigente, procesos, aspectos técnicos e implementación de controles, para efectos de informar a la Gerencia General, los resultados de esta actividad.

ALCANCE

Verificar el procedimiento Gestión de Incidentes de Seguridad de la Información, desarrollado por la Oficina de Tecnologías de la Información, para lo cual se tiene en cuenta lo relacionado con controles, seguridad de la información, planes de contingencia, gestión del procedimiento y demás aspectos desarrollados durante la vigencia 2018 y lo corrido del 2019.

LIMITACIÓN AL ALCANCE DE LA AUDITORÍA

Se presentó limitación al alcance de la auditoría, toda vez que solicitada la información relacionada con los incidentes de seguridad de la información, presentados durante la vigencia 2018, la Oficina de Tecnologías de la Información no suministró la información completa, entregando una base de datos, la cual contiene únicamente los casos registrados en los meses de enero y febrero de 2018; por otro lado, tampoco se suministró la documentación relacionada con los soportes de la gestión efectuada frente a dichos incidentes.

Debido a lo anterior, no fue posible seleccionar una muestra de auditoría para evaluar la debida aplicación del procedimiento GIT-SOP-P-002 Gestión de Incidentes de Seguridad de la Información.

El campo es de todos Minagricultura

DESARROLLO DE LA AUDITORÍA

Para la realización de esta actividad, se tuvieron en cuenta las normas internacionales de auditoría, mediante la utilización de diferentes métodos y aplicación de técnicas, tales como; indagación mediante entrevista, comprobación y verificación documental, que permitieron obtener y evaluar la evidencia de auditoría, proporcionando una base razonable para la determinación de las debilidades encontradas.

De igual manera, se tuvo en cuenta la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información, del MinTIC, la cual acoge los lineamientos recomendados por la Norma ISO / IEC 27001 (Gestión de la Seguridad de la Información).

Luego del análisis realizado a la información que se pudo obtener y de la verificación a la gestión del procedimiento, se generan las observaciones y recomendaciones que se plasman a continuación:

Observación 1: Se evidenció incumplimiento del procedimiento GIT-SOP-P-002 Gestión de Incidentes de Seguridad de la Información, en razón a que la Oficina de Tecnologías de la Información, no presenta una adecuada organización de la documentación y soportes de los incidentes de seguridad de la información, acontecidos y gestionados en la entidad; de igual manera, no se ejecuta la totalidad de las tareas definidas en el procedimiento, debido a que no se demostró el diligenciamiento de las formas: "Formato de Registro de Incidentes de Seguridad" y "Formato de Recolección de Evidencia y Entrega"; además, no se gestionan todos los roles definidos en el procedimiento, no se realiza la correspondiente clasificación de los incidentes, entre otras situaciones, lo que denota falencias en la realización de su gestión.
Área Responsable: Oficina de Tecnologías de la Información

Recomendaciones:

1. Analizar el procedimiento "Gestión de Incidentes de Seguridad de la Información", realizando las actualizaciones que correspondan, diseñando e implementando los controles necesarios para asegurar que se dé un estricto cumplimiento al mismo y que el producto de su gestión, redunde en la eficiencia frente a la salvaguarda de la información de la entidad.

2. Adelantar una adecuada organización de los soportes de las acciones ejecutadas, frente a los incidentes de seguridad de la información acaecidos en la entidad, permitiendo la verificación de los mismos, la efectividad de la gestión realizada y teniendo una referencia de su tratamiento para futuros casos similares.

3. Diligenciar debidamente las formas relacionadas con el procedimiento.

Observación 2: Existe debilidad en los controles implementados en la entidad, para minimizar los incidentes de seguridad de la información, evidenciado con la presencia de casos donde algunos equipos de cómputo, se encontraban sin software licenciado y conteniendo antivirus sin los respectivos parches de seguridad actualizados, generándose el riesgo de infección a causa de virus informáticos, ataques a la red de la entidad, exposición a sanciones por causas legales y amenazándose la disponibilidad, la integridad y la confidencialidad de la información del Instituto.
Área Responsable: Oficina de Tecnologías de la Información

Ejemplo de esta debilidad se logró advertir en el caso: 78723, Archivo de correo electrónico: "No.2-RE Solicitud Envío Equipo Primavera Vichada", donde se presentó esta serie de sucesos que afectan la seguridad de la información.

Recomendaciones:

El campo es de todos
Minagricultura

1. Fortalecer los controles y políticas definidas por la entidad, frente a la instalación de aplicativos sin el licenciamiento apropiado, antivirus y demás estrategias, las cuales están orientadas a reducir el riesgo de impacto de incidentes de seguridad de la información.

2. Monitorear y verificar frecuentemente los elementos de control implementados, con el fin de detectar oportunamente un posible incidente de seguridad de la información y darle un adecuado tratamiento, en concordancia con el procedimiento definido para su gestión.

3. Socializar las mejoras efectuadas, entre los funcionarios y contratistas del instituto, generando conciencia de la responsabilidad y el quehacer de cada uno.

4. Analizar entre los funcionarios y contratistas de la Oficina de Tecnologías de la Información, la normatividad expedida sobre derechos de autor y el uso de software no licenciado, con el fin de realizar socialización al ICA, en aras de minimizar estos riesgos informáticos.

Observación 3: Actualmente no se gestionan los roles Gestor de Incidentes de Seguridad de la información (GI) y Líder de Seguridad de la Información (LSI), los cuales se encuentran enmarcados dentro del procedimiento GIT-SOP-P-002 Gestión de Incidentes de Seguridad de la Información.
Área Responsable: Oficina de Tecnologías de la Información

Recomendaciones:

1. Gestionar la ubicación de personal calificado, que se encargue de la ejecución de todos los roles inmersos en el procedimiento "Gestión de Incidentes de Seguridad de la Información", con el fin de cubrir en su totalidad todos los aspectos relacionados al mismo.

2. Definir personal idóneo para la gestión de los roles Gestor de Incidentes de Seguridad de la información (GI) y Líder de Seguridad de la Información (LSI), procurando mantener la operación, la continuidad y la disponibilidad del servicio, apoyado en la correcta ejecución del procedimiento "Gestión de Incidentes de Seguridad de la Información".

Observación 4: No se cuenta con un procedimiento para gestionar los Servicios de TI y asegurar la continuidad de los servicios críticos de la entidad.
Área Responsable: Oficina de Tecnologías de la Información

Teniendo presente lo anterior, se genera un alto riesgo que cualquier interrupción imprevista y grave, sea por virus, ataques de denegación de servicios, etc., tenga grandes consecuencias en el desarrollo de las funciones propias del Instituto y afecte la seguridad e integridad de la información.

Recomendaciones:

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 adecuadamente, ante posibles incidentes de seguridad que pongan en riesgo la continuidad del servicio y la disponibilidad de la información.

2. Ejecutar de forma planificada las acciones que sean determinadas, analizando los resultados obtenidos y validando su efectividad.

3. Incluir en el mapa de riesgos de la entidad, lo relacionado con esta observación, teniendo presente su valoración, controles y seguimientos.

El campo es de todos Minagricultura

4. Publicar en el sistema de gestión documental de la entidad, las estrategias implementadas, guardando evidencia de su realización.

Observación 5: No se encuentran definidos los tiempos de atención y respuesta a los incidentes, dentro del procedimiento GIT-SOP-P-002 Gestión de Incidentes de Seguridad de la Información, lo que impide medir la efectividad del tratamiento dado a estos, la oportunidad en su atención y la gestión en general de la Oficina de Tecnologías de la Información.
Área Responsable: Oficina de Tecnologías de la Información

Recomendaciones:

1. Actualizar el procedimiento GIT-SOP-P-002 - Gestión de Incidentes de Seguridad de la Información, estableciendo la prioridad respectiva acorde al incidente, y con base a la misma, definir los tiempos máximos de atención y respuesta para su solución; así mismo se deben definir los soportes necesarios para evaluar su gestión.

2. Diseñar e implementar puntos de control, enfocados al cumplimiento de los tiempos de atención y respuesta que se definan en el procedimiento.

3. Publicar en el sistema de gestión documental de la entidad, los ajustes efectuados sobre el procedimiento, guardando evidencia de su realización.

Observación 6: No se define dentro del procedimiento GIT-SOP-P-002 Gestión de Incidentes de Seguridad de la Información, soporte para la acción N° 16.3: "Notificar al Líder u Oficial de seguridad de la Información del Cierre del Incidente", por lo que no es claro el medio mediante el cual se ejecuta dicha acción y el producto de su realización.
Área Responsable: Oficina de Tecnologías de la Información

Recomendaciones:

1. Precisar el producto o soporte resultante de la realización de todas las tareas definidas dentro del procedimiento, efectuando las actualizaciones que correspondan sobre el mismo, permitiendo a su vez medir la efectividad de su gestión.

2. Publicar en el sistema de gestión documental de la entidad, los ajustes realizados sobre el procedimiento, guardando evidencia de su cumplimiento.

Observación 7: Se evidenció la desactualización de los Acuerdos de Niveles de Servicio (SLA), suscritos por la mesa de ayuda de la Oficina de Tecnologías de la Información, respecto a la atención de incidentes de seguridad, ya que se tiene como responsable de algunas tareas, a personas que se encuentran retiradas de la entidad.
Área Responsable: Oficina de Tecnologías de la Información

Recomendaciones:

1. Documentar los Acuerdos de Niveles de Servicio (SLA), suscritos por la mesa de ayuda de la Oficina de Tecnologías de la Información, aplicando las actualizaciones que sean necesarias.

2. Publicar en el sistema de gestión documental de la entidad los Acuerdos de Niveles de Servicios que se suscriban, guardando evidencia de su divulgación.

Observación 8: Se evidenció el diligenciamiento inconsistente del formato "INFORME CASOS SEGURIDAD_DISCOVERY-2018", ya que existen casos donde no se registró información relevante, como tipo de incidente, incidentes que se encuentran en

El campo es de todos
Minagricultura

estado "Asignado", es decir, que aún no se han cerrado; se ingresan Tipos de Incidentes diferentes a los que están definidos en el procedimiento GIT-SOP-P-002 Gestión de Incidentes de Seguridad de la Información, entre otras inconsistencias.
Área Responsable: Oficina de Tecnologías de la Información

Recomendaciones:

1. Diligenciar el formato diseñado para el registro de los incidentes de seguridad, dando cumplimiento a lo determinado en el procedimiento Gestión de Incidentes de Seguridad de la Información y a los tipos de incidente de seguridad que se definan.

2. Atender de manera oportuna los incidentes de seguridad de la información que se presenten, teniendo en cuenta los tiempos de atención y respuesta estipulados.

3. Mantener una adecuada organización de los respectivos soportes que se generen, producto de las acciones realizadas en desarrollo de la atención a los incidentes de seguridad presentados.

4. Realizar capacitaciones a los actores relacionados con el procedimiento Gestión de Incidentes de Seguridad de la Información, en procura del debido diligenciamiento del formato "INFORME CASOS SEGURIDAD_DISCOVERY-2018", guardando los respectivos soportes de la ejecución de la actividad.

Observación 9: Se encuentran "rotos" los enlaces (links) inmersos en el procedimiento GIT-SOP-P-002 Gestión de Incidentes de Seguridad de la Información.
Área Responsable: Oficina de Tecnologías de la Información

Esta observación se presenta luego de advertir que los links "Diagrama de Flujo", "Ilustración No. 1 - Diagrama de flujo del procedimiento", "Formato de Registro de Incidentes de Seguridad" y "Formato de recolección de evidencia y entrega", no tienen funcionalidad al dar clic sobre ellos.

Recomendaciones:

1. Actualizar el procedimiento Gestión de Incidentes de Seguridad, asegurando que los enlaces insertados al mismo se ejecuten correctamente y desplieguen los documentos que correspondan.

2. Realizar la publicación de las actualizaciones efectuadas, en el sistema de gestión documental del Instituto y guardar evidencia de ello.

Observación 10: Dentro del procedimiento GIT-SOP-P-002 Gestión de Incidentes de Seguridad de la Información, no se hace referencia al diligenciamiento del numeral 9 (ANEXOS QUE SOPORTAN EL INCIDENTE), el cual está presente en el documento "Formato de Registro de Incidentes de Seguridad", por lo que no es claro quién realiza su gestión y cuál es el resultado de la misma.
Área Responsable: Oficina de Tecnologías de la Información

Recomendaciones:

1. Realizar las actualizaciones que correspondan sobre el procedimiento Gestión de Incidentes de Seguridad, teniendo en cuenta que se haga claridad frente al diligenciamiento de todos los documentos anexos al mismo.

2. Efectuar capacitaciones a los actores relacionados con el procedimiento Gestión de Incidentes de Seguridad de la Información, en procura del debido diligenciamiento de las formas anexas al mismo, guardando los respectivos soportes de la ejecución de la actividad.

El campo es de todos
Minagricultura

3. Realizar la publicación de las actualizaciones efectuadas, en el sistema de gestión documental del Instituto y guardar evidencia de ello.

Observación 11: No se evidencian planes de acción con tareas correctivas, respecto a los incidentes de seguridad de la información relacionados y gestionados por la Oficina de Tecnologías de la Información, durante la vigencia 2018, con la finalidad de evitar su ocurrencia en posteriores ocasiones.
Área Responsable: Oficina de Tecnologías de la Información
Recomendación:

1. Incluir en el procedimiento documentado, el deber de formular el respectivo plan de mejoramiento para los incidentes de seguridad de la información, conteniendo acciones preventivas, correctivas y de optimización, orientadas a evitar que estas situaciones se vuelvan a presentar; así mismo, se recomienda dejar evidencia que soporte la ejecución del plan.

2. Diseñar y mantener actualizada una base de datos, que contenga la gestión dada a los incidentes de seguridad acontecidos.

Observación 12: Se presenta falta de oportunidad en la atención de algunos casos relacionados con incidentes de seguridad de la información, los cuales son reportados a través del aplicativo de Mesa de Ayuda, lo que puede generar que se materialicen riesgos que impacten la confidencialidad, disponibilidad e integridad de la información.
Área Responsable: Oficina de Tecnologías de la Información

Recomendaciones:

1. Realizar una adecuada clasificación a los incidentes de seguridad que se presenten, con base en la actualización que se efectúe sobre el procedimiento Gestión de Incidentes de Seguridad de la Información, y de acuerdo a la prioridad asignada al incidente, atenderlo de forma oportuna, evitando su impacto y su afectación; igualmente guardar los soportes necesarios para evaluar su gestión.

2. Aplicar puntos de control, enfocados al cumplimiento de los tiempos de atención y respuesta que se definan en el procedimiento.

3. Registrar el incidente en el "Formato de Registro de Incidentes de Seguridad", definido por la Oficina de Tecnologías de la Información, diligenciando adecuadamente la información relevante al caso y poder obtener la trazabilidad del mismo.

Observación 13: No está completa la información reportada por la Oficina de Tecnologías de la Información, relacionada con los incidentes de seguridad de la información, acontecidos durante la vigencia 2018.
Área Responsable: Oficina de Tecnologías de la Información

Esta observación se genera, a partir de la limitación presentada en desarrollo de la auditoría, en razón a que la Oficina de Tecnologías de la Información, informó que solo tiene la información relacionada con los casos presentados en los meses de enero y febrero de 2018 y no la de todos los meses de dicha vigencia, lo que genera incertidumbre sobre la certeza de la completitud de casos sucedidos, de la gestión realizada por la dependencia a los mismos y de la afectación causada sobre la información de la entidad.

Recomendaciones:

1. Adelantar una efectiva organización de los registros de incidentes que se presentan en la entidad, guardando los respectivos soportes de su gestión.

El campo es de todos
Minagricultura

2. Aplicar los controles necesarios en la Oficina de Tecnologías de la Información, encaminados al cumplimiento del procedimiento Gestión de Incidentes de Seguridad de la Información y todos los aspectos derivados del mismo, entre ellos el del inventario de los incidentes.

3. Dar aplicabilidad y cumplimiento a lo dispuesto en la política de gestión documental del ICA, con el fin de asegurar la información en su contenido e integridad.

Observación 14: Se evidenció que el Instituto aún no ha implementado el protocolo HTTPS (HyperText Transfer Protocol Secure), en la totalidad de los aplicativos que dispone para la gestión de la información, afectándose la integridad y privacidad de la información de la entidad.
Área Responsable: Oficina de Tecnologías de la Información

Esta observación se origina luego de advertir que los aplicativos "Forestales" y "Sigma", se encuentran ejecutándose en producción sobre el protocolo HTTP, con lo cual está presente el riesgo que la información de la entidad, la cual es gestionada en dichos aplicativos, sea accedida por terceras personas no autorizadas.

Recomendaciones:

1. Dotar de mayor seguridad a los sistemas de información de la entidad, implantando certificados de seguridad a través del protocolo HTTPS, resguardando a su vez la seguridad de la información.

2. Realizar las pruebas y configuraciones que sean necesarias, con la finalidad de asegurar que los aplicativos se ejecuten normalmente, posterior a la implementación del protocolo de seguridad HTTPS.

Aprobado por:	**Elaborado por:**	**Fecha de Aprobación:**
JUAN FERNANDO PALACIO ORTIZ **Jefe Oficina Control Interno**	Jorge Armando Marimon Acosta **Profesional OCI**	Agosto 22 de 2019
		FORMA 4-935
		Versión 1.1

El campo es de todos
Minagricultura