INSTITUTO COLOMBIANO AGROPECUARIO - ICA
OFICINA CONTROL INTERNO
PROCEDIMIENTO EVALUACION Y SEGUIMIENTO
PLAN DE MEJORAMIENTO AUDITORIA OFICINA CONTROL INTERNO

Responsable del Proceso: **Oficina de Tecnologías de la Información**

Fecha de Visita: **27 de mayo al 12 de junio** **Año:** **2019**

DESCRIPCION OBSERVACIÓN	DESCRIPCION RECOMENDACIÓN	AREA RESPONSABLE	ACCION DE MEJORAMIENTO	RESPONSABLES	FECHAS DE CUMPLIMIENTO		SEGUIMIENTO ÁREA RESPONSABLE			SEGUIMIENTO OCI		
					FECHA INICIO	FECHA TERMINACIÓN	DESCRIPCION DEL AVANCE	EVIDENCIA	PORCENTAJE DE CUMPLIMIENTO	PORCENTAJE DE CUMPLIMIENTO	ESTADO	OBSERVACIÓN
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.	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.	Oficina de Tecnologías de la Información	Realizar la actualización del Procedimiento de Incidente de Seguridad	Adriana Florez Martinez	16-sep.-19	18-oct.-19						
			Publicar el Procedimiento de Incidentes de Seguridad en el Aplicativo Diamante.	OTI	19-oct.-19	31-oct.-19						
	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.		Definir un repositorio donde se evidencie la gestión de los Incidentes de Seguridad de la Información reportados, de igual forma dentro del procedimiento se indicará está ubicación.	Adriana Florez Martinez	16-sep.-19	18-oct.-19						
	3. Diligenciar debidamente las formas relacionadas con el procedimiento.		Diligenciar el formato de Incidente de Seguridad de la Información.	OTI	16-sep.-19	31-dic.-19						
Observación 2: Existe debilidad en los controles implementados en la entidad,	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.		Actualizar las Politicas de Seguridad y Privacidad de la Información, frente a la instalación de software no licenciado en los equipos de la Entidad.	Adriana Florez Martinez	16-sep.-19	21-oct.-19						
	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.		Solicitar informe mensual de los equipos de la Entidad frente al software instalado.	Danny Peter Gutierrez Beltran	30-sep.-19	31-dic.-19						

DESCRIPCION OBSERVACIÓN	DESCRIPCION RECOMENDACIÓN	AREA RESPONSABLE	ACCION DE MEJORAMIENTO	RESPONSABLES	FECHAS DE CUMPLIMIENTO		SEGUIMIENTO ÁREA RESPONSABLE			SEGUIMIENTO OCI		
					FECHA INICIO	FECHA TERMINACIÓN	DESCRIPCION DEL AVANCE	EVIDENCIA	PORCENTAJE DE CUMPLIMIENTO	PORCENTAJE DE CUMPLIMIENTO	ESTADO	OBSERVACIÓN
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.	3. Socializar las mejoras efectuadas, entre los funcionarios y contratistas del instituto, generando conciencia de la responsabilidad y el quehacer de cada uno.	Oficina de Tecnologías de la Información	Socializar en la intranet y por correo de ICA-COMUNICA el cambio de las Politicas de Seguridad y Privacidad de la Información de la Entidad, cuando sea aprobada por el Comité Institucional de Gestión y Desempeño en el mes de Noviembre de 2019.	Adriana Florez Martinez	1-nov.-19	2-dic.-19						
			Generar SISAD para todos los Procesos donde se informe que no se puede habilitar permisos a software no licienciado en la Entidad.	Carlos Alberto Pinto	13-sep.-19	20-sep.-19						
	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.		Socializar al interior de la OTI lo referente a derechos de autor en aras de minimizar Riesgos.	Adriana Florez Martinez	1-oct.-19	31-dic.-19						
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.	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.	Oficina de Tecnologías de la Información	Realizar la actualización del Procedimiento de Incidente de Seguridad	Adriana Florez Martinez	16-sep.-19	18-oct.-19						
	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”.											

DESCRIPCION OBSERVACIÓN	DESCRIPCION RECOMENDACIÓN	AREA RESPONSABLE	ACCION DE MEJORAMIENTO	RESPONSABLES	FECHAS DE CUMPLIMIENTO		SEGUIMIENTO ÁREA RESPONSABLE			SEGUIMIENTO OCI		
					FECHA INICIO	FECHA TERMINACIÓN	DESCRIPCION DEL AVANCE	EVIDENCIA	PORCENTAJE DE CUMPLIMIENTO	PORCENTAJE DE CUMPLIMIENTO	ESTADO	OBSERVACIÓN
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.	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.	Oficina de Tecnologías de la Información	Definir un Plan de Recuperación de Desastres (DRP) en la Oficina de Tecnólogia de Información.	OTI	1-oct.-19	31-dic.-20						
	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.		Definir en el Mapa de Riesgos de SGSI los riesgos que se generen por no contar con un DRP.	Adriana Florez Martinez	1-oct.-19	31-dic.-20						
	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.	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.	Oficina de Tecnologías de la Información	Realizar la actualización del Procedimiento de Incidente de Seguridad	Adriana Florez Martinez	16-sep.-19	18-oct.-19						
	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.		Publicar el Procedimiento de Incidentes de Seguridad en el Aplicativo Diamante.	OTI	19-oct.-19	31-oct.-19						
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.	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.	Oficina de Tecnologías de la Información	Realizar la actualización del Procedimiento de Incidente de Seguridad	Adriana Florez Martinez	16-sep.-19	18-oct.-19						
	2. Publicar en el sistema de gestión documental de la entidad, los ajustes realizados sobre el procedimiento, guardando evidencia de su cumplimiento.		Publicar el Procedimiento de Incidentes de Seguridad en el Aplicativo Diamante.	OTI	19-oct.-19	31-oct.-19						

DESCRIPCION OBSERVACIÓN	DESCRIPCION RECOMENDACIÓN	AREA RESPONSABLE	ACCION DE MEJORAMIENTO	RESPONSABLES	FECHAS DE CUMPLIMIENTO		SEGUIMIENTO ÁREA RESPONSABLE			SEGUIMIENTO OCI		
					FECHA INICIO	FECHA TERMINACIÓN	DESCRIPCION DEL AVANCE	EVIDENCIA	PORCENTAJE DE CUMPLIMIENTO	PORCENTAJE DE CUMPLIMIENTO	ESTADO	OBSERVACIÓN
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.	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.	Oficina de Tecnologías de la Información	Actualizar los ANS en la herramenta Discovery de Mesa de Ayuda de acuerdo al Catalogo de Servicio de TI y suprimir nombres propios.	Danny Peter Gutierrez Beltran	16-sep.-19	31-dic.-19						
	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.		El catalogo de Servicio de TI se publica en el aplicativo DIAMANTE.	Gustavo Orozco	11-sep.-19	31-dic.-19						
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 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.	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.	Oficina de Tecnologías de la Información	Realizar la actualización del Procedimiento de Incidente de Seguridad	Adriana Florez Martinez	16-sep.-19	18-oct.-19						
	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.		El catalogo de Servicio de TI se publica en el aplicativo DIAMANTE.	Gustavo Orozco	11-sep.-19	31-dic.-19						
	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.		Definir un repositorio donde se evidencie la gestión de los Incidentes de Seguridad de la Información reportados, de igual forma dentro del procedimiento se indicará está ubicación.	Adriana Florez Martinez	16-sep.-19	18-oct.-19						
	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.		Realizar capacitación a Mesa de Ayufda frente a los cambios de los Incidentes de Seguridad.	Adriana Florez Martinez	19-oct.-19	31-dic.-19						
Observación 9: Se encuentran “rotos” los enlaces (links) inmersos en el procedimiento GIT-SOP-P-002 Gestión de Incidentes de Seguridad de la Información.	1. Actualizar el procedimiento Gestión de Incidentes de Seguridad, asegurando que los enlaces insertados al mismo se ejecuten correctamente y despliegen los documentos que correspondan.	Oficina de Tecnologías de la Información	Realizar la actualización del Procedimiento de Incidente de Seguridad	Adriana Florez Martinez	16-sep.-19	18-oct.-19						
	2. Realizar la publicación de las actualizaciones efectuadas, en el sistema de gestión documental del Instituto y guardar evidencia de ello.		Publicar el Procedimiento de Incidentes de Seguridad en el Aplicativo Diamante.	OTI	19-oct.-19	31-oct.-19						
Observación 10: Dentro del procedimiento GIT-SOP-P-002 Gestión de Incidentes de Seguridad de la Información, no se hace	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.		Realizar la actualización del Procedimiento de Incidente de Seguridad	Adriana Florez Martinez	16-sep.-19	18-oct.-19						

DESCRIPCION OBSERVACIÓN	DESCRIPCION RECOMENDACIÓN	AREA RESPONSABLE	ACCION DE MEJORAMIENTO	RESPONSABLES	FECHAS DE CUMPLIMIENTO		SEGUIMIENTO ÁREA RESPONSABLE			SEGUIMIENTO OCI		
					FECHA INICIO	FECHA TERMINACIÓN	DESCRIPCION DEL AVANCE	EVIDENCIA	PORCENTAJE DE CUMPLIMIENTO	PORCENTAJE DE CUMPLIMIENTO	ESTADO	OBSERVACIÓN
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.	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.	Oficina de Tecnologías de la Información	Realizar capacitación a Mesa de Ayuda frente a los cambios de los Incidentes de Seguridad.	Adriana Florez Martinez	19-oct.-19	31-dic.-19						
	3. Realizar la publicación de las actualizaciones efectuadas, en el sistema de gestión documental del Instituto y guardar evidencia de ello.		Publicar el Procedimiento de Incidentes de Seguridad en el Aplicativo Diamante.	OTI	19-oct.-19	31-oct.-19						
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.	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.	Oficina de Tecnologías de la Información	Realizar la actualización del Procedimiento de Incidente de Seguridad	Adriana Florez Martinez	16-sep.-19	18-oct.-19						
	2. Diseñar y mantener actualizada una base de datos, que contenga la gestión dada a los incidentes de seguridad acontecidos.		Definir un repositorio donde se evidencie la gestión de los Incidentes de Seguridad de la Información reportados, de igual forma dentro del procedimiento se indicará está ubicación.	Adriana Florez Martinez	16-sep.-19	18-oct.-19						
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.	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.	Oficina de Tecnologías de la Información	Realizar la actualización del Procedimiento de Incidente de Seguridad	Adriana Florez Martinez	16-sep.-19	18-oct.-19						
	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.		Diligenciar el formato de Incidente de Seguridad de la Información.	OTI	16-sep.-19	31-dic.-19						
	1. Adelantar una efectiva organización de los registros de incidentes que se presentan en la entidad, guardando los respectivos soportes de su gestión.		Realizar la actualización del Procedimiento de Incidente de Seguridad	Adriana Florez Martinez	16-sep.-19	18-oct.-19						

DESCRIPCION OBSERVACIÓN	DESCRIPCION RECOMENDACIÓN	AREA RESPONSABLE	ACCION DE MEJORAMIENTO	RESPONSABLES	FECHAS DE CUMPLIMIENTO		SEGUIMIENTO ÁREA RESPONSABLE			SEGUIMIENTO OCI		
					FECHA INICIO	FECHA TERMINACIÓN	DESCRIPCION DEL AVANCE	EVIDENCIA	PORCENTAJE DE CUMPLIMIENTO	PORCENTAJE DE CUMPLIMIENTO	ESTADO	OBSERVACIÓN
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.	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.	Oficina de Tecnologías de la Información	Definir un repositorio donde se evidencie la gestión de los Incidentes de Seguridad de la Información reportados, de igual forma dentro del procedimiento se indicará está ubicación.	Adriana Florez Martinez	16-sep.-19	18-oct.-19						
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.	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.	Oficina de Tecnologías de la Información	Realizar un inventario de las aplicaciones del ICA para identificar cuales tienen el certificado de seguridad protocolo HTTPS.	OTI	16-oct.-19	31-dic.-19						
										FORMA: 4-510 VERSIÓN 3		