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 26 de octubre al 18 de noviembre de 2020

OBJETIVO

En concordancia con el Programa Anual de Auditoría, formulado por la Oficina de Control Interno para la vigencia 2020 y aprobado por el Comité de Coordinación del Sistema de Control Interno, verificar el cumplimiento del procedimiento Backup y Recuperación de la Información, gestionado por la Oficina de Tecnologías de la Información y en el presente informe se relacionan las debilidades encontradas con sus respectivas recomendaciones, para que se formulen acciones que permitan subsanarlas, propiciando un marco de mejoramiento continuo.

ALCANCE

Verificación del procedimiento GIT-P-012 Backup y Recuperación de la Información, gestionado por la Oficina de Tecnologías de la Información, para lo cual se tiene en cuenta lo relacionado con cumplimiento, gestión, diseño y estructuración del procedimiento, controles, seguridad de la información y demás aspectos asociados, respecto a la vigencia 2019 y lo corrido del 2020.

LIMITACIONES AL ALCANCE

Durante la auditoría interna practicada al procedimiento Backup y Recuperación 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

En la presente verificación se utilizaron diferentes técnicas de auditoría para obtener evidencias suficientes, tales como: indagación mediante entrevista, comparación, 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 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), como también la ISO 27001, sus requerimientos, recomendaciones y consideraciones frente a la gestión de la información, procurando por su seguridad, confidencialidad, integridad y disponibilidad.

Luego del análisis realizado a la información recopilada y de la verificación a la gestión del procedimiento, se generan las siguientes observaciones, las cuales están acompañadas de sus respectivas recomendaciones:

Observación 1: Debilidades en los puntos de control del procedimiento GIT-P-012 BACKUP Y RECUPERACIÓN DE LA INFORMACIÓN, teniendo en cuenta que no se contemplan aspectos críticos para su gestión, de acuerdo a los estándares de buenas prácticas, como la ubicación de los backups en un centro de datos externo, soportes de ejecución y pruebas al plan de seguridad de la información, no incluye la dualidad de copias de seguridad, no se encuentra relacionado a un procedimiento de Continuidad del Negocio o de Recuperación de Desastre, no considera el nivel de protección física y ambiental requerido para las cintas de respaldo, controles de acceso a las copias de seguridad, entre otras situaciones.
Área Responsable: Oficina de Tecnologías de la Información

Recomendaciones:

1. Probar regularmente los medios de respaldo, para asegurar que se pueda confiar en ellos para usarlos cuando sea necesaria en caso de emergencia.

2. Identificar la información crítica de la entidad y aplicar controles efectivos garantizando su seguridad e integridad y su pronta recuperación al momento en que sea requerida.

3. Dar a la información de respaldo el nivel de protección física y ambiental apropiado.

4. Almacenar las copias de respaldo en un lugar apartado, a la distancia suficiente como para escapar de cualquier daño por un desastre en el edificio principal.

5. Chequear y probar de manera frecuente los procedimientos de restauración realizados, para asegurar que sean efectivos y que pueden ser completados dentro del tiempo asignado en los procedimientos operacionales para la recuperación.

6. Asegurar las condiciones ambientales y físicas para la ubicación de las copias de respaldo.

7. Aplicar los controles de ingreso apropiados para asegurar que sólo se permita el acceso al Datacenter de personal autorizado.

8. Actualizar el mapa de riesgos del proceso, teniendo en cuenta la validación y fortalecimiento de todos los puntos débiles del procedimiento.

Observación 2: Falencias en el procedimiento GIT-P-012 BACKUP Y RECUPERACIÓN DE LA INFORMACIÓN, en el numeral 2.1 DESCRIPCIÓN DEL PROCEDIMIENTO DE BACKUP Y RESPALDO, en las tareas 4, 14 y 17, toda vez que el soporte definido para estas actividades no es coherente con las mismas, lo cual no permite evaluar su ejecución y efectividad.
Área Responsable: Oficina de Tecnologías de la Información

Esta debilidad se genera, en atención a que la tarea 4 está definida como “Autorización de solicitud”, mientras que el producto de la misma como “Solicitud de copia de seguridad y restauración o Correo electrónico”, lo cual no guarda relación, debiendo ser un formato o soporte donde se evidencie la autorización, por parte del jefe de la Oficina de Tecnologías de la Información, a la solicitud recibida.

Respecto a la tarea 14, el soporte definido para la realización de la actividad no es idóneo, debiendo ser un soporte donde se compruebe que, en la verificación efectuada a la copia de seguridad, la misma cumplía con ciertas características y/ criterios que permitieron determinar su buen estado y que aplica su restauración.

En relación con la tarea 17, para la misma no se registra un soporte que permita evidenciar el resultado de la verificación efectuada sobre la restauración de la copia de seguridad.

Recomendaciones:

1. Analizar el procedimiento GIT-P-012 BACKUP Y RECUPERACIÓN DE LA INFORMACIÓN, realizando las actualizaciones que correspondan e implementando los correctivos necesarios, para asegurar que las tareas guarden relación con los soportes definidos para las mismas, permitiendo evidenciar su cumplimiento y su grado de efectividad.

2. Validar una a una las actividades que se suscriban al procedimiento y determinar aquellas que deben arrojar un producto o soporte.

3. Definir cuáles son los criterios que se deben cumplir para determinar el buen estado de las copias de seguridad.

4. Socializar las actualizaciones que se realicen al procedimiento, entre los actores que guarden relación con el proceso.

Observación 3: Se evidenció que el procedimiento GIT-P-012 BACKUP Y RECUPERACIÓN DE LA INFORMACIÓN, en el numeral 2.2 PROCEDIMIENTO PARA PRUEBA DE RECUPERACIÓN DE BACKUPS, tareas 3 y 4, no tiene definido unos soportes claros e idóneos que den cuenta de su cumplimiento.
Área Responsable: Oficina de Tecnologías de la Información

Para la tarea 3, correspondiente a “Ejecución de procedimiento de restauración”, el soporte es definido como “Manual”, sin dar alguna claridad de las actividades ejecutadas y guardar correlación.

En relación a la tarea 4, no se define un soporte para la verificación realizada por el administrador del sistema, en la cual se compruebe que se efectuaron una serie de pruebas para determinar la realización correcta o no de la restauración.

Recomendaciones:

1. Definir y documentar los criterios que debe cumplir una copia de seguridad para darle visto bueno y certificar que luego de las pruebas practicadas a la misma, la restauración fue realizada de manera correcta.

2. Identificar y definir con claridad, las tareas que se deben ejecutar en este numeral del procedimiento, así mismo los soportes de éstas, conservando la respectiva coherencia e idoneidad entre las actividades y su producto.

3. Organizar y mantener actualizado un repositorio con los soportes de la ejecución de las actividades, que permita en cualquier momento demostrar su ejecución y efectividad.

4. Efectuar socialización de las mejoras implementadas, guardando soportes de su realización.

Observación 4: Incumplimiento del procedimiento GIT-P-012 BACKUP Y RECUPERACIÓN DE LA INFORMACIÓN, en el numeral 2.2 PROCEDIMIENTO PARA PRUEBA DE RECUPERACIÓN DE BACKUP, tareas 3, 4 y 5, en atención a que no se evidenciaron soportes de pruebas de restauración de backups, generándose el riesgo de afectación a la confiablidad, seguridad, integridad y disponibilidad de la información.
Área Responsable: Oficina de Tecnologías de la Información

Recomendaciones:

1. Asegurar que se realice la totalidad de las actividades que se definan en el procedimiento y se conserven los soportes de las mismas, donde se puede evidenciar su cumplimiento.

2. Mantener actualizado el repositorio que se implemente para los soportes de la ejecución de las actividades.

3. Fortalecer los controles definidos para la ejecución de la restauración a los backups realizados.

Observación 5: El procedimiento GIT-P-012 BACKUP Y RECUPERACIÓN DE LA INFORMACIÓN, no presenta un orden coherente, teniendo en cuenta que en el numeral 2.1. DESCRIPCIÓN DEL PROCEDIMIENTO DE BACKUP Y RESPALDO, en la actividad 13, se indica "FIN DEL PROCEDIMIENTO", sin embargo, posteriormente se presentan otras actividades.
Área Responsable: Oficina de Tecnologías de la Información

Recomendaciones:

1. Realizar la actualización del procedimiento, teniendo en cuenta que su diseño y estructuración debe llevar una secuencia lógica de las actividades.

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

3. Efectuar las correspondientes socializaciones del caso.

Observación 6: Existen falencias en el diseño del procedimiento GIT-P-012 BACKUP Y RECUPERACIÓN DE LA INFORMACIÓN, debido a que no se encuentra documentado sobre la Forma 4-600, como lo indica el proceso Control de Documentos de la Oficina Asesora de Planeación, a través del cual se definen los lineamientos para la documentación de los procedimientos; adicionalmente, no contiene diagrama de flujo, no contiene los códigos de las formas y otros procedimientos relacionados; así mismo, el procedimiento guarda relación con el "Formato Pruebas Recuperación de backups", el cual no se encuentra registrado en el numeral 5 "FORMAS".
Área Responsable: Oficina de Tecnologías de la Información

Recomendaciones:

1. Solicitar asesoría a la Oficina Asesora de Planeación, para lo correspondiente a la actualización del procedimiento BACKUP Y RECUPERACIÓN DE LA INFORMACIÓN, conforme a los lineamientos definidos en el proceso Control de Documentos, el cual es gestionado por dicha dependencia.

2. Posterior a la actualización efectuada al procedimiento, realizar la gestión con la Oficina Asesora de Planeación, relacionada con la oficialización del procedimiento a través del sistema de gestión documental de la entidad.

Observación 7: Falta de oficialización de las formas "SOLICITUD DE COPIA DE INFORMACIÓN" y "SOLICITUD DE RESTAURACIÓN DE INFORMACIÓN", relacionadas al procedimiento GIT-P-012 BACKUP Y RECUPERACIÓN DE LA INFORMACIÓN, toda vez que las mismas no se encuentran vinculadas al Sistema de Gestión Documental "Diamante", por consiguiente, no contienen un código asignado.
Área Responsable: Oficina de Tecnologías de la Información

Recomendaciones:

1. Realizar la actualización de las citadas formas y posteriormente su oficialización a través del sistema de gestión documental de la entidad, con la asesoría de la Oficina Asesora de Planeación.

2. Asegurar que todas las formas asociadas al procedimiento queden relacionadas dentro del mismo.

Observación 8: Incumplimiento del numeral 4.9 del "Documento de Especificaciones", el cual está relacionado al procedimiento GIT-P-012 BACKUP Y RECUPERACIÓN DE LA INFORMACIÓN, teniendo en cuenta que no hay soportes de que cada dos (2) meses se realice simulación de recuperación de las copias de seguridad, generando riesgo sobre la seguridad e integridad de la información.
Área Responsable: Oficina de Tecnologías de la Información

Recomendaciones:

1. Implementar puntos de control para asegurar que se ejecute la totalidad de las actividades definidas en el Documento de Especificaciones, que es un insumo del procedimiento BACKUP Y RECUPERACIÓN DE LA INFORMACIÓN.

2. Estimar la opción de incluir el Documento de Especificaciones dentro del mismo procedimiento BACKUP Y RECUPERACIÓN DE LA INFORMACIÓN.

3. Mantener un repositorio organizado con las evidencias de las actividades ejecutadas.

Observación 9: Incumplimiento del numeral 4.11 del "Documento de Especificaciones", el cual está vinculado al procedimiento GIT-P-012 BACKUP Y RECUPERACIÓN DE LA INFORMACIÓN, toda vez que no se conserva la estructura definida para el etiquetado de las cintas de seguridad, conforme a lo señalado en el documento.
Área Responsable: Oficina de Tecnologías de la Información

De acuerdo al "Documento de Especificaciones", todas las copias de seguridad en cinta deben ser etiquetadas con la estructura: tipo de copia (semanal, quincenal, mensual, diaria), nombre de la copia, consecutivo de cintas, Número de slot en Autoloader, Mes y Año; sin embargo, los soportes remitidos no dan cuenta que se realice el etiquetado de las cintas de conformidad con lo suscrito en el documento.

Recomendaciones:

1. Verificar la estructura definida para el etiquetado de las cintas de seguridad y realizar las actualizaciones a que haya lugar, teniendo en cuenta las modificaciones que se realicen al procedimiento.

2. Aplicar controles enfocados en dar cumplimiento a lo definido.

Observación 10: Desactualización del "Documento de Especificaciones" relacionado al procedimiento GIT-P-012 BACKUP Y RECUPERACIÓN DE LA INFORMACIÓN, el cual presenta tareas que no se ejecutan en la actualidad, como el resguardo de las copias de seguridad en el DATACENTER del Laboratorio Nacional de Diagnóstico Veterinario, además de contener logos del ICA y Minagricultura que ya no están vigentes.
Área Responsable: Oficina de Tecnologías de la Información

Recomendaciones:

1. Actualizar el Documento de Especificaciones del procedimiento BACKUP Y RECUPERACIÓN DE LA INFORMACIÓN, en concordancia con los estándares y modelos de buenas prácticas, sus requerimientos y consideraciones, buscando cumplir los objetivos del procedimiento y garantizar la salvaguarda de la información; posteriormente realizar las oficializaciones que apliquen al caso, siguiendo los lineamientos definidos por la Oficina Asesora de Planeación.

2. Validar la opción de incluir las especificaciones y normas para la elaboración de copias de seguridad en servidores (Documento de Especificaciones), dentro de la actualización que se realice al procedimiento BACKUP Y RECUPERACIÓN DE LA INFORMACIÓN.

3. Fortalecer los lineamientos frente a la cadena de custodia del procedimiento, los responsables de la información, los sitios de resguardo, así como las condiciones ambientales y física para su conservación.

Aprobado por:	**Elaborado por:**	**Fecha de Aprobación:**
JUAN FERNANDO PALACIO ORTIZ **Jefe Oficina Control Interno**	Jorge Armando Marimon Acosta **Profesional OCI** ***ORIGINAL FIRMADO*** *(Emergencia sanitaria COVID-19)*	Diciembre 21 de 2020
		FORMA 4-935 Versión 2