FECHA DE EMISIÓN DEL INFORME: 30-06-2023

ASPECTO EVALUABLE

Sistema de Gestión de Seguridad de la Información - SGSI en el MADR a los Procesos de Gestión y Gobierno de Tecnología de la Información -TI y Gestión de Servicios Tic.

LÍDER DE PROCESO / JEFE(S) DEPENDENCIA(S)

Oficina de Tecnologías de la Información y las Comunicaciones.

OBJETIVO DE LA AUDITORÍA

Evaluar el "Sistema de Gestión de Seguridad de la Información - SGSI" en el MADR.

OBJETIVOS ESPECÍFICOS

1. Evaluar la política "*Política de Seguridad y Privacidad de la Información*" publicada en el Sistema Integrado de Gestión el 30102020 Versión 3.

2. Evaluar el cumplimiento del documento denominado "*Políticas Específicas de Seguridad de la Información*" publicada en el Sistema Integrado de Gestión el 30102020 Versión 3

3. Evaluar el cumplimiento del Procedimiento "*Gestión de Incidentes de Seguridad de la Información*" publicado en el SIG el 20112020 Versión 1.

4. Visita a Dependencia con Áreas Seguras.

5. Evaluar los Indicadores de SGSI de los procesos de Gestión y Gobierno de la Información - TI y Gestión de Servicios Tics.

6. Evaluar los Riesgos y Controles asociados a los Activos de Información "*Matriz_Instrumentos_de_Gestión_de_Información_Publica*" publicada.

7. Evaluar la ejecución presupuestal asignada al SGSI.

8. Evaluar los riesgos del SGSI y controles los procesos de Gestión y Gobierno de la Información - TI y Gestión de Servicios Tics.

ALCANCE DE LA AUDITORÍA

Se enfocará en las operaciones realizadas entre el 1 de noviembre de 2022 y el 30 de abril de 2023 del Sistema de Seguridad de la Información - SGSI incluyendo las políticas "P*olítica de Seguridad y Privacidad de la Información*" y "*Políticas Específicas de Seguridad de la Información*"; los procedimientos: "*Gestión de Incidentes de Seguridad de la Información*" y "*Acceso a Áreas Seguras de Almacenamiento de Información*", publicados en el Sistema Integrado de Gestión, tomando como criterio de auditoria la regulación externa e interna sobre el particular que delimitan su funcionamiento y ejecución del Sistema de Seguridad de la Información - SGSI.

CRITERIOS DE LA AUDITORÍA

- Ley 87 del 29 de noviembre 1993; "*Por lo cual se definen las normas básicas para el ejercicio del Control Interno en las entidades y organismos del estado y se dictan otras disposiciones". Artículo 12 ítem i. "Evaluar y verificar la aplicación de los mecanismos de participación ciudadana, que, en desarrollo del mandato constitucional y legal, diseñe la entidad correspondiente"*
- Ley 1712 de 2014; "Por *la cual se crea la Ley de Transparencia y del Derecho de Acceso a la información Pública Nacional y se dictan otras disposiciones". Artículo 76 ítem h.*
- Documentación interna (procesos, procedimiento, políticas, directrices, etc.) de los Procesos de Gestión y Gobierno de Tecnología de la Información -TI y Gestión de Servicios Tics.
- Normativa
- Mapa de Riesgos Asociados a los Activos de Información (Sistema de Información TIC).
- Mapa de riesgos de los Procesos
- Norma ISO 27001:2013 y Anexo A
- Modelo de Seguridad y Privacidad de la Información de MINTIC
- Convenios y contratos suscritos

DESARROLLO DE LA AUDITORÍA

Oficina de Control Interno en cumplimiento de la Ley 87 de 1993 en su rol de seguimiento, verificación y control a los procesos del Ministerio de Agricultura y Desarrollo Rural y según lo establecido en el plan anual de auditoría de la vigencia 2023, realiza el presente informe cuyo objeto principal es verificar el cumplimiento de los requisitos y normativa que regula el Sistema de Seguridad de la Información - SGSI, con el fin de proporcionar observaciones, recomendaciones y determinar oportunidades de mejora, encaminadas al mejoramiento continuo del SGSI.

1. Normatividad que rige para el Sistema de Seguridad de la Información - SGSI

A continuación, se describe la normatividad que rige el Sistema de Gestión de Seguridad de la Información – SGSI, para el proceso de Gestión y Gobierno de Tecnologías de la Información – TI, la cual se relaciona a continuación:

1.1 Leyes

Se consultaron las Leyes publicados en la página web de la entidad relacionadas con seguridad de la información, encontrando lo siguiente:

Macroproceso	Proceso	Tipo	Origen	Fecha emisión	Nombre documento o norma
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Ley	Externa	29/07/2021	2108 de 2021
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Ley	Externa	24/07/2018	1928 de 2018
Procesos Estratégicos	Direccionamiento Estratégico Institucional	Ley	Externa	6/03/2014	1712 DE 2014
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Ley	Externa	17/10/2012	1581 DE 2012
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Ley	Externa	5/01/2009	1273 DE 2009
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Ley	Externa	31/12/2008	1266 DE 2008
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Ley	Externa	5/02/1993	44 DE 1993
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Ley	Externa	28/01/1982	23 DE 1982

Tabla 1 – Información extraída publicada en la página WEB de la entidad – Normograma Proceso de Gestión y Gobierno de Tecnologías de la información -TI

1.2 Decretos

Se consultaron los Decretos publicados en la página web, con los siguientes resultados:

Macroproceso	Proceso	Tipo	Origen	Fecha emisión	Nombre documento o norma
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Decreto	Externa	16/05/2022	767 de 2022
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Decreto	Externa	8/03/2022	338 DE 2022
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Decreto	Externa	24/01/2022	088 de 2022
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Decreto	Externa	24/09/2020	1287 de 2020
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Decreto	Externa	2/05/2020	620 DE 2020
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Decreto	Externa	26/05/2015	1078 de 2015
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Decreto	Externa	12/12/2014	2573 DE 2014
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Decreto	Externa	27/06/2013	1377 DE 2013

Macroproceso	Proceso	Tipo	Origen	Fecha emisión	Nombre documento o norma
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Decreto	Externa	14/12/2012	2609 de 2012
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Decreto	Externa	2/11/2006	3851 de 2006

Tabla 2 – Información extraída publicada en la página WEB de la entidad – Normograma Proceso de Gestión y Gobierno de Tecnologías de la información -TI

1.3 Resoluciones

Se consultaron las Resoluciones publicados en la página web, con los siguientes resultados:

Macroproceso	Proceso	Tipo	Origen	Fecha emisión	Nombre documento o norma
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Resolución	Interna	27/07/2022	230 de 2022
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Resolución	Externa	11/03/2022	746 de 2022
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Resolución	Externa	10/03/2021	500 de 2021
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Resolución	Externa	24/08/2020	01519 de 2020
Procesos Estratégicos	Direccionamiento Estratégico Institucional	Resolución	Interna	30/04/2018	00198 de 2018
Procesos Estratégicos	Administración del Sistema Integrado de Gestión	Resolución	Interna	14/09/2017	000297 de 2017
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Resolución	Interna	26/07/2017	00233 de 2017
Procesos Estratégicos	Direccionamiento Estratégico Institucional	Resolución	Interna	11/04/2014	000204 de 2014

Tabla 3 – Información extraída publicada en la página WEB de la entidad – Normograma Proceso de Gestión y Gobierno de Tecnologías de la información -TI

1.4 CONPES

Se consultaron los CONPES publicados en la página web, con los siguientes resultados:

Macroproceso	Proceso	Tipo	Origen	Fecha emisión	Nombre documento o norma
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	CONPES	Externa	1/07/2020	3995 de 2020
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	CONPES	Externa	11/04/2016	3854 de 2016

Tabla 4 – Información extraída publicada en la página WEB de la entidad – Normograma Proceso de Gestión y Gobierno de Tecnologías de la información -TI

1.5 Directivas

Se consultaron las Directivas Publicadas en la página web con los siguientes resultados:

Macroproceso	Proceso	Tipo	Origen	Fecha emisión	Nombre documento o norma
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Directiva	Externa	24/02/2022	02 de 2022
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Directiva	Externa	15/03/2021	03 de 2021
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Directiva	Externa	14/05/2019	006 de 2019
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Directiva	Externa	12/02/2002	2 de 2002

Tabla 5 – Información extraída publicada en la página WEB de la entidad – Normograma Proceso de Gestión y Gobierno de Tecnologías de la información -TI

1.6 Circulares

Se consultaron las Circulares publicadas en la página web con los siguientes resultados:

Macroproceso	Proceso	Tipo	Origen	Fecha emisión	Nombre documento o norma
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Circular	Externa	22/09/2021	018 de 2021

Tabla 6 – Información extraída publicada en la página WEB de la entidad – Normograma Proceso de Gestión y Gobierno de Tecnologías de la información -TI.

1.7 Guías

Se consultó las guías publicadas en la página web con los siguientes resultados:

Macroproceso	Proceso	Tipo	Origen	Fecha emisión	Nombre documento o norma
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Guía	Externa	31/10/2019	Guías del Marco de Referencia de Arquitectura Empresarial
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Guía	Externa	1/10/2019	G.ES.06 Guía Cómo Estructurar el Plan Estratégico de Tecnologías de la Información - PETI

Tabla 7 – Información extraída publicada en la página WEB de la entidad – Normograma Proceso de Gestión y Gobierno de Tecnologías de la información -TI

1.8 Otros Documentos

Se consultó otros documentos publicados en la página web, con los siguientes resultados:

Macroproceso	Proceso	Tipo	Origen	Fecha emisión	Nombre documento o norma
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Otros documentos	Externa	31/10/2019	MGGTI.G.GEN.01 – Documento Maestro del Modelo de Gestión y Gobierno de TI
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Otros documentos	Externa	31/10/2019	Modelos del Marco de Referencia de Arquitectura Empresarial
Procesos Estratégicos	Gestión y Gobierno de Tecnologías de la Información-TI	Otros documentos	Externa	11/03/2016	Modelo de Seguridad y Privacidad de la Información

Tabla 8 – Información extraída publicada en la página WEB de la entidad – Normograma Proceso de Gestión y Gobierno de Tecnologías de la información -TI

2. Contexto

Para el Desarrollo del Sistema de Gestión de la Seguridad de la información la entidad cuenta con los siguientes elementos:

1. Talento Humano - funcionarios de Planta:

Nombre	Función Principal
Adriana María Jaramillo Pinzón	Jefe de la Oficina de Tecnologías de la Información – Orientación en la Política de Seguridad de la Información Digital.
Raúl Alberto Avellaneda Flórez	Profesional OTIC
John Edilson Patiño Tenorio	Coordinador Grupo
Genny Alexandra Sanabria Cardenas	Reporte de Información incluido el tema de seguridad de la información

Tabla 9 – Elaboración Equipo Auditor con la Información suministrada por la Oficina de Tecnologías de la Información.

2. Plan Estratégico de Tecnologías de la Información – PETI Institucional. 2020-2023

   Actualmente se encuentra publicado en el Sistema Integrado de Gestión la Versión 5 del PETI publicado el 11 de mayo de 2022; en el alcance se encuentra el tema de seguridad de la Información, en el numeral 8.5 de Infraestructura tecnología y de seguridad y privacidad de la información, contiene el estado actual de lo asociado a la seguridad en los siguientes términos: "*Respecto a Seguridad y Privacidad de la Información, en el Ministerio de Agricultura se han implementado medidas de seguridad informática y seguridad organizacional que propenden por la protección de los activos de información institucionales. Sin embargo, es necesario dar continuidad a la estrategia de seguridad y privacidad de la información, a través de la actualización del Sistema de Gestión de Seguridad de la Información y la creación de una cultura organizacional*".

   Así mismo en los objetivos estratégicos de TI por dominios, se encuentra el objetivo: *"Fortalecer la gestión de servicios tecnológicos y de seguridad de la información"*, con propósitos de política de gobierno digital en proceso interno seguros y eficientes, con situación deseada de Seguridad de la Información fortalecida.

   Igualmente, para su desarrollo, presenta un proyecto denominado: "*Fortalecimiento de la implementación del Sistema de Gestión de Seguridad de la Información*", que presenta una proyección de recurso financieros de $3.145.804.395 para un periodo de ejecución de 48 meses; para las vigencias 2022 contó con una proyección de $704.975.250 y 2023 con: $2.033.072.000.

3. Proyecto de Inversión denominado: *"Fortalecimiento de la Gestión de Tecnologías de la Información - TI en el Ministerio de Agricultura y Desarrollo Rural en Función de*

la Transformación Digital del Sector Agropecuario"

En el proyecto de inversión para la vigencia 2022, se encuentra el objetivo: "… *específico 4: Fortalecer la gestión de servicios tecnológicos y de seguridad de la información*". Para el tema de seguridad se hace referencia a la actividad "… *2: Evaluar, planificar, implementar y realizar seguimiento a la estrategia de seguridad de la información institucional*", con un costo equivalente a la proyección de PETI, es decir, $704.975.250.

El proyecto de Inversión presenta la siguiente cadena de valor para el año 2022:

CADENA DE VALOR							
Nombre del proyecto	Fortalecimiento de la Gestión de Tecnologías de la Información - TI en el Ministerio de Agricultura y Desarrollo Rural en función de la transformación digital del sector agropecuario.						
Código del proyecto	2019011000108						
Objetivo general proyecto	Fortalecer la Gestión de Tecnologías de Información -TI en el Ministerio de Agricultura y Desarrollo Rural en función de la transformación digital del sector agropecuario.						
Objetivo específico	**Producto**	**Unidad de medida**	**Indicador**	**Meta horizonte**	**Actividad**	**Año 2022**	
						Costo	**Producto**
1. Fortalecer la alineación estratégica y el gobierno de TI entre entidades del sector.	1.1. Documento para la planeación estratégica en TI.	Documento	3	2022	1.1.1. Gestionar la planeación estratégica de Tecnologías de la Información y las Comunicaciones - PETI sectorial e institucional.	$ 325.284.900	**$ 559.834.900**
					1.1.2. Gestionar la política de TI a nivel institucional y sectorial.	$ 193.300.000	
					1.1.3. Elaborar el capítulo de Tecnologías de la Información para el Plan Estratégico Institucional 2023 - 2026.	$ -	
					1.1.4. Implementar y realizar el seguimiento del Plan de Comunicaciones de la Estrategia de TI.	$ 41.250.000	
	Costo total producto					**$ 559.834.900**	
2. Gestionar la política de información conforme a las necesidades del sector agropecuario.	2.1. Documentos normativos.	Documento	3	2022	2.1.1. Gestionar la política de información sectorial e institucional incorporando el ciclo de vida de los componentes de información.	$ 45.775.600	**$ 149.942.000**
					2.1.2. Mejorar la gestión de la información en función del esquema de gobierno definido y en armonía con el Marco de Referencia de Arquitectura TI.	$ 45.775.600	
					2.1.3. Implementar y realizar seguimiento del Plan de Calidad de la información en función del marco de referencia de TI.	$ 58.390.800	
	Costo total producto					**$ 149.942.000**	
3. Fomentar la articulación entre los sistemas de información del sector.	3.1. Documentos de lineamientos técnicos.	Documento	3	2022	3.1.1. Gestionar los sistemas de información con apoyo de las metodologías y arquitecturas adecuadas para su construcción o evolución.	$ 1.217.700.000	**$ 1.324.299.400**
					3.1.2. Elaborar y actualizar el catálogo de sistemas de información sectorial e institucional.	$ 74.027.800	
					3.1.3. Tramitar la transferencia de los derechos patrimoniales sobre los sistemas de información o desarrollos al que haya lugar.	$ 32.571.600	
	Costo total producto					**$ 1.324.299.400**	

CADENA DE VALOR							
Nombre del proyecto	Fortalecimiento de la Gestión de Tecnologías de la Información - TI en el Ministerio de Agricultura y Desarrollo Rural en función de la transformación digital del sector agropecuario.						
Código del proyecto	2019011000108						
Objetivo general proyecto	Fortalecer la Gestión de Tecnologías de Información -TI en el Ministerio de Agricultura y Desarrollo Rural en función de la transformación digital del sector agropecuario.						
Objetivo específico	**Producto**	**Unidad de medida**	**Indicador**	**Meta horizonte**	**Actividad**	**Año 2022**	
						Costo	**Producto**
4. Fortalecer la gestión de servicios tecnológicos y de seguridad de la información.	4.1. Servicios tecnológicos.	Porcentaje disponibilidad Plataforma Tecnológica	95%	2022	4.1.1. Asegurar la disponibilidad de los servicios de TI incluidos en el portafolio de servicios TI, los cuales son soportados por infraestructura tecnológica tanto de software como de hardware, así como la instalación, adecuación y mejoramiento de redes de conectividad y comunicación a nivel institucional.	$ 7.162.822.450	**$ 7.867.797.700**
					4.1.2. Evaluar, planificar, implementar y realizar seguimiento a la estrategia de seguridad de la información institucional.	$ 704.975.250	
	Costo total producto					**$ 7.867.797.700**	
5. Promover el uso y apropiación de las iniciativas de TI.	5.1. Documentos de planeación.	Documento	4	2022	5.1.1. Caracterizar y priorizar los grupos de interés involucrados en iniciativas de TI como insumo para determinar la gestión del cambio necesaria.	$ 41.250.000	**$ 398.126.000**
					5.1.2. Formular y actualizar la estrategia de uso y apropiación a partir de la caracterización de los grupos de interés.	$ 198.438.000	
					5.1.3. Implementar la estrategia de uso y apropiación que permita realizar una gestión del cambio.	$ 90.000.000	
					5.1.4. Realizar el seguimiento periódico a la percepción del impacto del uso y apropiación de TI.	$ 68.438.000	
	Costo total producto					**$ 398.126.000**	
Costo total proyecto						**$**	**10.300.000.000,00**

Tabla 10 – Información Suministrada por la Oficina de Tecnologías de la Información del Proyecto de Inversión para la vigencia 2022.

Como se puede observar en la tabla No. 10, en el objetivo 4, se encuentra actividad relacionada con la seguridad de la Información: *"4.1.2. Evaluar, planificar, implementar y realizar seguimiento a la estrategia de seguridad de la información institucional",* que cuenta para el año 2022, una asignación presupuestal de $704.975.250, para el Sistema de Gestión de Seguridad de la información.

Para el desarrollo de la actividad de seguridad de la información, se realizaron los siguientes contratos y/o convenios:

No. Contrato /Convenio	Ejecutor	Objeto
20220551	UT Soft IG 3	Orden de Compra: El suministro de páginas web, servidores (hosting), computación en la nube (cloud computing), se encuentran exceptuados del impuesto sobre las ventas – IVA, lo cual aplica para los para los servicios de software de Nube (Licencias de Office365 y Power BI Pro).

No. Contrato /Convenio	Ejecutor	Objeto
20220575	Cirion Technologies Colombia S.A.S	Orden de Compra: 93874 - Contratar los servicios de custodia de cintas de copias de respaldo, al amparo del Acuerdo Marco de Precios vigente
20220598	Id Logics Ltda.	Renovación del derecho de acceso y uso de la plataforma Intélisis: suscripción activa en modalidad SaaS del software Intelisis módulos PDCA e ISO27001:2013
20220684	Adsum Soluciones Tecnológicas S.A.S	Adquisición, Instalación, Configuración y Puesta en Funcionamiento de una Solución Tecnológica que Permita Gestionar el Proceso de Copias de Respaldo Institucional.

Tabla 11 – Construcción del Equipo Auditor con la Información Suministra por la Oficina de Tecnologías de la Información.

Igualmente se suscribieron Contratos de Prestación de servicios de acuerdo con la siguiente relación:

No. Contrato	Nombre	Objeto
20220187	Rubén Darío Peña Sierra	Prestar servicios profesionales para la ejecución de actividades inherentes a los dominios de Arquitectura de Infraestructura Tecnológica y Arquitectura de Seguridad, de conformidad con el Modelo de Arquitectura Empresarial.
20220300	Ana Cecilia Cundumi Morales	Prestar servicios de apoyo a la gestión para dar continuidad con la implementación de la estrategia de seguridad de la información y los procesos del dominio de Infraestructura Tecnológica del Ministerio de Agricultura y Desarrollo Rural.

Tabla 12 – Construcción del Equipo Auditor con la Información Suministra por la Oficina de Tecnologías de la Información.

Nota: De acuerdo con la minuta del contrato 20220187 a nombre de Rubén Darío Peña, presenta una actividad como es: *"Liderar desde el rol de oficial de seguridad de la información, el mantenimiento y actualización del Sistema de Gestión de Seguridad de la Información de conformidad con el Marco de Arquitectura Empresarial".*

Para la vigencia 2023, se cuenta con la siguiente Cadena de Valor:

CADENA DE VALOR							
Nombre del proyecto	Fortalecimiento de la Gestión de Tecnologías de la Información - TI en el Ministerio de Agricultura y Desarrollo Rural en función de la transformación digital del sector agropecuario.						
Código del proyecto	2019011000108						
Objetivo general proyecto	Fortalecer la Gestión de Tecnologías de Información -TI en el Ministerio de Agricultura y Desarrollo Rural en función de la transformación digital del sector agropecuario.						
Objetivo específico	**Producto**	**Unidad de medida**	**Indicador**	**Meta horizonte**	**Actividad**	**Año 2023**	
						Costo	**Producto**
1. Fortalecer la alineación estratégica y el gobierno de TI entre entidades del sector.	1.1. Documento para la planeación estratégica en TI.	Documento	4	2023	1.1.1. Gestionar la planeación estratégica de Tecnologías de la Información y las Comunicaciones - PETI sectorial e institucional.	$ 156.220.313,00	**$ 436.330.126,00**
					1.1.2. Gestionar la política de TI a nivel institucional y sectorial.	$ 173.880.000,00	
					1.1.3. Elaborar el capítulo de Tecnologías de la Información para el Plan Estratégico Institucional 2023 - 2026.	$ 56.239.313,00	
					1.1.4. Implementar y realizar el seguimiento del Plan de Comunicaciones de la Estrategia de TI.	$ 49.990.500,00	
	Costo total producto					**$ 436.330.126**	

CADENA DE VALOR							
Nombre del proyecto	Fortalecimiento de la Gestión de Tecnologías de la Información - TI en el Ministerio de Agricultura y Desarrollo Rural en función de la transformación digital del sector agropecuario.						
Código del proyecto	2019011000108						
Objetivo general proyecto	Fortalecer la Gestión de Tecnologías de Información -TI en el Ministerio de Agricultura y Desarrollo Rural en función de la transformación digital del sector agropecuario.						
Objetivo específico	**Producto**	**Unidad de medida**	**Indicador**	**Meta horizonte**	**Actividad**	**Año 2023**	
						Costo	**Producto**
2. Gestionar la política de información conforme a las necesidades del sector agropecuario.	2.1. Documentos normativos.	Documento	3	2023	2.1.1. Gestionar la política de información sectorial e institucional incorporando el ciclo de vida de los componentes de información.	$ 108.675.000,00	**$ 2.103.329.150,00**
					2.1.2. Mejorar la gestión de la información en función del esquema de gobierno definido y en armonía con el Marco de Referencia de Arquitectura TI.	$ 1.932.806.000,00	
					2.1.3. Implementar y realizar seguimiento del Plan de Calidad de la información en función del marco de referencia de TI.	$ 61.848.150,00	
	Costo total producto					**$ 2.103.329.150**	
3. Fomentar la articulación entre los sistemas de información del sector.	3.1. Documentos de lineamientos técnicos.	Documento	3	2023	3.1.1. Gestionar los sistemas de información con apoyo de las metodologías y arquitecturas adecuadas para su construcción o evolución.	$ 1.712.202.500,00	**$ 1.897.553.750,00**
					3.1.2. Elaborar y actualizar el catálogo de sistemas de información sectorial e institucional.	$ 96.600.000,00	
					3.1.3. Tramitar la transferencia de los derechos patrimoniales sobre los sistemas de información o desarrollos al que haya lugar.	$ 88.751.250,00	
	Costo total producto					**$ 1.897.553.750**	
4. Fortalecer la gestión de servicios tecnológicos y de seguridad de la información.	4.1. Servicios tecnológicos.	Porcentaje disponibilidad Plataforma Tecnológica	95%	2023	4.1.1. Asegurar la disponibilidad de los servicios de TI incluidos en el portafolio de servicios TI, los cuales son soportados por infraestructura tecnológica tanto de software como de hardware, así como la instalación, adecuación y mejoramiento de redes de conectividad y comunicación a nivel institucional.	$ 7.820.975.974,00	**$ 10.172.888.474,00**
					4.1.2. Evaluar, planificar, implementar y realizar seguimiento a la estrategia de seguridad de la información institucional.	$ 2.351.912.500,00	
	Costo total producto					**$ 10.172.888.474**	
5. Promover el uso y apropiación de las iniciativas de TI.	5.1. Documentos de planeación.	Documento	4	2023	5.1.1. Caracterizar y priorizar los grupos de interés involucrados en iniciativas de TI como insumo para determinar la gestión del cambio necesaria.	$ 49.990.500,00	**$ 389.898.500,00**
					5.1.2. Formular y actualizar la estrategia de uso y apropiación a partir de la caracterización de los grupos de interés.	$ 229.908.000,00	
					5.1.3. Implementar la estrategia de uso y apropiación que permita realizar una gestión del cambio.	$ 80.000.000,00	
					5.1.4. Realizar el seguimiento periódico a la percepción del impacto del uso y apropiación de TI.	$ 30.000.000,00	
	Costo total producto					**$ 389.898.500**	
Costo total proyecto						**$**	**15.000.000.000,00**

Tabla 13 – Información Suministrada por la Oficina de Tecnologías de la información - Proyecto de Inversión para la vigencia 2023

Como observa en la anterior tabla No. 13, en el objetivo 4, se encuentra actividad relacionada con la seguridad de la Información: "*4.1.2. Evaluar, planificar, implementar y realizar seguimiento a la estrategia de seguridad de la*

información institucional", que cuenta para el año 2023, una asignación presupuestal de $ 2.351.912.500, para el Sistema de Gestión de Seguridad de la información.

De acuerdo con la información suministrada por la Oficina de Tecnologías de la Información y las comunicaciones para la actividad "*4.1.2. Evaluar, planificar, implementar y realizar seguimiento a la estrategia de seguridad de la información institucional*", están en el proceso de generar los respectivos contratos para dar continuidad al Sistema de Gestión de Seguridad de la Información.

3. Evaluar el Sistema de Gestión de Seguridad de la Información - SGSI

Para la evaluación del Sistema de Seguridad de la Información se tuvieron en cuenta los siguientes objetivos:

3.1. Evaluar la política "Política de Seguridad y Privacidad de la Información" publicada en el Sistema Integrado de Gestión el 30/10/2020 Versión 3.

Para evaluar este ítem, se tuvo en cuenta los lineamientos generales descritos en el documento maestro de Modelo de Seguridad y Privacidad de la Información de Mintic, el cual se detalla a continuación:

1. Diagnóstico

06. Diagnóstico			Evaluación OCI	
Propósito	Lineamiento	Salida	Observación	Cumple
Identificar el nivel de madurez de seguridad y privacidad de la información se encuentra la entidad, como punto de partida para la implementación del MSPI.	Identificar a través de la herramienta de autodiagnóstico (Análisis GAP) el estado actual de la entidad respecto a la Seguridad y privacidad de la Información.	Documento con el resultado de la herramienta de autodiagnóstico, identificando la brecha en la implementación del MSPI en toda la entidad, y sus acciones de mejora.	En archivo Excel "DIAGNOSTICO-MSPI-2022_Pestaña 1", presenta el Diagnostico, con fecha del 31/12/2022; al realizar la comparación con el archivo Excel "20220310-DIAGNOSTICO-MSPI-2022-I", de fecha 12052022, es idéntico. Pero se cuenta con el respectivo diagnóstico, con resultados reportados del 97%.	Si

Tabla 14 – Elaboración equipo Auditor tomando como base el documento maestro de Modelo de Seguridad de la Información.

2. Planificación

7.1 Contexto				
7.1.1 Comprensión de la organización y de su contexto			Evaluación OCI	
Propósito	Lineamiento	Salida	Observación	Cumple
Conocer en detalle las características de la entidad y su entorno con el fin de implementar el Modelo de Seguridad y Privacidad adaptado a las condiciones específicas de cada entidad.	Determinar los elementos externos e internos que son relevantes con las actividades que realiza la entidad en el desarrollo de su misión y que podrían influir en las capacidades para lograr los objetivos del modelo, alineado con los objetivos estratégicos de la entidad.	Documentos obligatorios: Contexto de la entidad (Política de Planeación Institucional).	El contexto de la entidad se realiza una descripción breve en los documentos estratégico: "Mapa de Procesos", codificación DE-DEI-07; Versión 8 del 6 de octubre de 2022 y "Misión y Visión", codificación DE-DEI-01; Versión 4 del 13 de octubre de 2021; Pero como tal no se encuentra un documento publicado en el SIG. Se solicitó información a la Oficina Asesora de Planeación y Prospectiva a través de correo del 25 de mayo de 2023. Como respuesta, mediate correo del 26052023 presenta la siguiente información: "...relacionada con los Documentos Obligatorios que tengan el contexto de la entidad (Política de Planeación Institucional)", me permito informarles, que, desde la OAPP, se elaborado unos documentos que actualmente están en la página web, en el Plan Estratégico Sectorial e Institucional, los cuales pueden consultar en el siguiente enlace, los cuales contienen el contexto interno y externo de la entidad". Al revisar los documentos, no existe un apartado exclusivo para el tema del contexto, pero en el documento se pude inferir que contiene la información solicitada, para lo cual se considera un cumplimiento porcentual del 25% Se recomienda que para el contexto Institucional se elabore un documento estratégico que se publique en el SIG, donde recoja el contexto interno como externo de la entidad de acuerdo con los lineamientos de MIPG - "Analizar el contexto interno y externo de la entidad para la identificación de los riesgos y sus posibles causas, así como retos, tendencias y oportunidades de mejora e innovación en la gestión".	25%
7.1.2 Necesidades y expectativas de los interesados			Evaluación OCI	
Propósito	Lineamiento	Salida	Observación	Cumple
Conocer las expectativas que se tiene respecto a la implementación del modelo de seguridad y privacidad de la información, para asegurar que el modelo garantizará su cumplimiento.	Se deben determinar las partes interesadas internas o externas y personas, entidades u organizaciones que pueden influir directamente en la seguridad y privacidad de la información de la entidad o que puedan verse afectados en caso de que estas se vean comprometidas. Adicionalmente se deberán determinar las necesidades y/o expectativas (intereses) relacionados con la seguridad y privacidad de la información. Las partes interesadas deberán incluir los requisitos legales, reglamentarios y contractuales.	Documentos obligatorios: Partes interesadas. (Política de Planeación Institucional).	Revisadas las publicaciones en el SIG, no se encuentra documentación estratégica relacionada con las partes Interesadas. Se solicitó información a la Oficina Asesora de Planeación y Prospectiva a través de correo del 25 de mayo de 2023. No se respondió la respectiva solicitud de información; se evidencia una parcialidad, que en términos de evaluación correspondería a un 25%	25%
7.1.3 Definición del alcance del MSPI			Evaluación OCI	
Propósito	Lineamiento	Salida	Observación	Cumple
Identificar qué información (generada o utilizada en los procesos de la entidad) será protegida mediante la adopción del MSPI.	Determinando los límites y la aplicabilidad del MSPI en el marco del modelo de operación por proceso de la entidad. Determinando a que procesos y recursos tecnológicos se realizará la implementación del MSPI.	Alcance del MSPI, (Este alcance puede estar integrado al Manual del Sistema Integrado de Gestión, o en el documento del Modelo de Planeación y Gestión).	El Alcance del MSPI se encuentra definido en el documento estratégico "DE-GGGT-03 Política de Seguridad y Privacidad de la Información" Versión 3 publicada en el SIG el 31-08-2020. En: Cobertura: "Esta política aplica a los procesos del Ministerio de Agricultura (estratégicos, evaluación y control, misionales y de apoyo), lo cual se ve reflejado en las matrices de riesgos institucionales y son desarrollados directamente en el Sistema de Gestión de Seguridad de la Información".	Si

Tabla 15 – Elaboración equipo Auditor tomando como base el documento maestro de Modelo de Seguridad de la Información.

El equipo auditor evaluó la información suministrada por la Oficina de Planeación y Prospectiva, evidenciando información con respecto al contexto de la entidad y de las partes interesadas. Sin embargo, se recomienda

establecer una oportunidad de mejora, para que los documentos del contexto y de las partes interesadas formen parte del Sistema Integrado de Gestión de la entidad con respecto a la Planeación Institucional de la entidad.

7.2 Liderazgo				
7.2.1 Liderazgo y Compromiso			Evaluación OCI	
Propósito	Lineamiento	Salida	Observación	Cumple
Garantizar el liderazgo y el compromiso del comité institucional de gestión y desempeño o quien haga sus veces para conseguir los objetivos definidos para la implementación del MSPI.	La entidad debe incluir dentro del comité institucional de gestión y desempeño o quien haga sus veces, las funciones relacionadas con seguridad y privacidad de la información, adoptando, implementando, manteniendo y mejorando continuamente el MSPI, por medio de un acto administrativo. Con el propósito de garantizar el éxito de su implementación, que permita dar cumplimiento entre otras, a las siguientes acciones: • Establecer y publicar la adopción de la política general, los objetivos y las políticas específicas de seguridad y privacidad de la información. • Garantizar la adopción de los requisitos del MSPI en los procesos de la entidad, • Comunicar en la entidad la importancia del MSPI. • Planear y disponer de los recursos necesarios (presupuesto, personal, tiempo etc.) para la adopción del MSPI. • Asegurar que el MSPI consiga los resultados previstos. • Realizar revisiones periódicas de la adopción del MSPI (al menos dos veces por año y en las que el Nominador deberá estar presente).	Evidencia en el acto administrativo que soporta la conformación del comité de gestión y desempeño o quien haga sus veces, señalando las funciones de seguridad y privacidad de la información.	La resolución 198 de 30 de abril de 2018, "por medio de la cual se adopta el MIPG, y se conforman los Comités Institucional y Sectorial de Gestión y Desempeño", en el literal f) del artículo 10 - "Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia en seguridad digital de la información". Para el equipo auditor es conveniente que la entidad evalué, la función o actividad mencionada, con el fin de incluir, la información que no es digital en el marco del MSPI y la ISO 27001:2013. y Roles y Responsabilidades del MSPI. Mediante resolución 297 de 2017, en su artículo 18 determina que: "**Funciones del Oficial de Seguridad de la Información**: Corresponde al Oficial de Seguridad de la información desarrollar las siguientes funciones:"…. El equipo auditor recomienda la actualización de la resolución, teniendo en cuenta los lineamientos actuales de MINTIC y la normativa vigente. Adicionalmente, el artículo 17, "Designación del Rol de Oficial de Seguridad de la Información. El jefe de la Oficina de las Tecnologías de Información y Comunicaciones del MADR, designará un funcionario de su dependencia para que ejerza el rol de Oficial de Seguridad de la Información ….". Se recomienda atende los lineamientos de Mintic, "si el cargo no existe en la entidad deberá ser delegado por acto administrativo y deberá depender de un área estratégica que no sea la Oficina o Dirección de Tecnología (se recomienda el despacho de nominador), de igual manera la persona designada deberá ser incluida como miembro del comité de gestión institucional con voz y voto y en el comité de control interno con voz". (Documento Maestro MSPI, página 28) y Roles y Responsabilidades del MSPI.	Sí
7.2.2 Política de seguridad y privacidad de la información			Evaluación OCI	
Propósito	Lineamiento	Salida	Observación	Cumple
Orientar y apoyar por parte de la alta dirección de la entidad a través del comité de gestión institucional, la gestión de la seguridad de la información de acuerdo con la misión de la entidad, normatividad y reglamentación pertinente.	Se debe establecer en la política de seguridad y privacidad de la información, que establezca el enfoque de la entidad, para ello debe tener en cuenta: • Misión de la entidad • Normatividad vigente la cual se debe contar para el funcionamiento de la entidad • Establecer compromiso del cumplimiento de los requisitos relacionados con la seguridad y privacidad de la información, así como también el de la mejora continua una vez el MSPI sea adoptado • Estar alineada con el contexto de la entidad, así como la identificación de las áreas que hacen parte de la implementación de seguridad de la información. • Se deben asignar los roles y responsabilidades que se identifiquen. • Ser incluidos y aprobados los temas de seguridad de la información y seguridad digital en el comité gestión y desempeño institucional, modificando el acto administrativo de conformación de este, aprobado por el mismo comité y expedido por el nominador o máxima autoridad de la entidad. • Ser comunicada al interior de la entidad y a los interesados que aplique.	Acto administrativo con la adopción de la Política de seguridad y privacidad de la información.	Actualmente la entidad cuenta con la política. Denominada: "DE-GGT-03 - Política de Seguridad y Privacidad de la información", versión 3 publicada en el SIG el 31 de agosto de 2020. Dicha política, es aprobada por el Comité Institucional de Gestión y Desempeño mediante acta No. 2 del 16 de julio de 2020, en Proposiciones y varios "...votaron positivamente las dos propuestas (implementación del protocolo IPV6 y aprobación de la Política de Seguridad y Privacidad de la Información)".	Sí

7.2 Liderazgo				
7.2.1 Liderazgo y Compromiso			Evaluación OCI	
Propósito	Lineamiento	Salida	Observación	Cumple
	La política establece la base respecto al comportamiento de personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad.			
7.2.3 Roles y responsabilidades				
Propósito	Lineamiento	Salida	Observación	Cumple
Hay que asegurar que los funcionarios de la entidad conozcan qué se espera de ellos, cuál es su impacto en la seguridad de la información y de qué manera contribuyen con la adopción del MSPI.	Articular con las áreas o dependencias de la entidad, los roles y responsabilidades necesarios para la adopción del MSPI, el monitoreo del desempeño y el reporte y seguimiento ante el comité institucional de gestión y desempeño, para que sean aprobados y comunicados dentro de la entidad. Se debe delegar a un responsable de la seguridad y privacidad de la información y el equipo humano necesario para coordinar la implementación del MSPI; si el cargo no existe en la entidad deberá ser delegado por acto administrativo y deberá depender de un área estratégica que no sea la Oficina o Dirección de Tecnología (se recomienda el despacho de nominador), de igual manera la persona designada deberá ser incluida como miembro del comité de gestión institucional con voz y voto y en el comité de control interno con voz.	Roles y responsabilidades	Para el tema de Roles y Responsabilidades, se cuenta con los siguientes documentos: La resolución 198 de 30 de abril de 2018, "por medio de la cual se adopta el MIPG, y se conforman los Comités Institucional y Sectorial de Gestión y Desempeño", en el artículo 9 determina que: "Objeto y conformación del Comité Institucional de Gestión y Desempeño del MADR. El Comité Institucional de Gestión y Desempeño del MADR será la instancia encargada de dirigir la implementación y la evaluación del MIPG en el MADR. Estará conformado por los siguientes funcionarios del MADR: ...". Resolución 297 de 2017, en su artículo 18 determina que: "Funciones del Oficial de Seguridad de la Información: Corresponde al Oficial de Seguridad de la información desarrollar las siguientes funciones: "... El equipo auditor recomienda la actualización de la resolución, teniendo en cuenta los lineamientos actuales de MINTIC y la normativa vigente. Documento estratégico "DE-GGT-04 - Políticas específicas de Seguridad de la Información" Versión 3 publicada en el SIG, 30-10-2020, contiene apartado denominado "Roles y Responsabilidades para la Seguridad de la Información (ISO/IEC 27002:2013, numeral 6.1.1), pero es una descripción muy generalizada, por tal razón se recomienda evaluar y tener en cuenta los lineamientos establecidos en el documento Maestro MSPI en Roles y Responsabilidades.	Parcial

Tabla 16 – Elaboración equipo Auditor tomando como base el documento maestro de Modelo de Seguridad de la Información.

El equipo auditor realizó evaluación la información suministrada por la Oficina de Tecnologías de la Información, relacionada con los roles y responsabilidades y evidenció un cumplimiento parcial, de acuerdo con los lineamientos establecidos en el documento maestro MSPI - Roles y Responsabilidad. Entre ellos la creación del Comité de Seguridad y privacidad de la información, dependiente del Comité Institucional de Gestión y Desempeño Institucional (este comité es opcional, pero al interior de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC, existe un comité o grupo que se encarga de mitigar el riesgo, que se encuentra dirigido a la información digital y cuyo objeto sería que se definiera para toda el SGSI), de la falta de la definición de los roles de la Oficina Asesora Jurídica, del Grupo de Gestión Documental y de los demás que requiera el SGSI, en el caso del Oficial de Seguridad (lineamiento es no pertenecer a la OTIC), la resolución sea encaminada a todo el SGSI y no solo al tema de seguridad de la información digital (como actualmente está planteado), por las anteriores razones, se presenta una No Conformidad.

7.3 Planificación				
7.3.1 Identificación de activos de información e infraestructura critica			Evaluación OCI	
Propósito	Lineamiento	Salida	Observación	Cumple
Estructurar una metodología que permita identificar y clasificar los	Las entidades deben definir y aplicar un proceso de identificación y clasificación de la información, que permita: • Determinar o identificar qué activos de información van a hacer parte del	Procedimiento de inventario y clasificación de la información. (Anexo 1. Guía para la Gestión y Clasificación de Activos de Información)	Se cuenta con la política a través del documento estratégico "DE-GGT-04 - Políticas específicas de Seguridad de la Información" Versión 3 publicada en el SIG, 30-10-2020, contiene apartado denominado: "5.1.6 - Gestión de Activos (ISO/IEC 27002:2013 Numeral (8)). Pero como tal no es un procedimiento de inventario y tampoco es metodológico;	Sí

7.3 Planificación				
7.3.1 Identificación de activos de información e infraestructura critica			Evaluación OCI	
Propósito	Lineamiento	Salida	Observación	Cumple
activos de información	Inventario, que aportan valor agregado al proceso y por tanto necesitan ser protegidos de potenciales riesgos. • Clasificar los activos de información de acuerdo a los tres principios de seguridad de la información, integridad, confidencialidad y disponibilidad para garantizar que la información recibe los niveles de protección adecuados. • Actualizar el inventario y la clasificación de los activos por los propietarios y custodios de los activos de forma periódica o toda vez que exista un cambio en el proceso.	Documento metodológico de inventario y clasificación de la información.	La entidad cuenta con el procedimiento "PR-ALI-26 - Esquema de publicación de Información Pública", versión 2 publicada en el SIG 15-10-2021; donde se determina el procedimiento para la identificación y clasificación de la información; en el mencionado procedimiento se asocia el formato - F01-PR-ALI-26 "Instrumentos de Gestión de Información Pública" Versión 1 publicada en el SIG 15102021. Actualmente se encuentra publicada el mencionado formato diligenciado en la página web de la entidad (Documento metodológico de inventario y clasificación de la información); con fecha de actualización del 23-06-2021 y fecha de publicación de la última versión 08-02-2022. En el procedimiento no determina la periodicidad de la actualización de la identificación y clasificación de la información de acuerdo con los lineamientos del MSPI "Actualizar el inventario y la clasificación de los activos por los propietarios y custodia de los activos de forma periódica o toda vez que exista un cambio en el proceso", presentado una No conformidad. Adicionalmente se recomienda la revisión del procedimiento en cuanto a las definiciones.	
7.3.2 Valoración de los riesgos de seguridad de la información			Evaluación OCI	
Propósito	Lineamiento	Salida	Observación	Cumple
Estructurar una metodología que permita gestionar los riesgos de seguridad y privacidad de la información.	Las entidades deben definir y aplicar un proceso de valoración de riesgos de la seguridad y privacidad de la información, que permita: • Identificar los riesgos que causen la perdida de confidencialidad, integridad, disponibilidad, privacidad de la información, así como la continuidad de la operación de la entidad dentro del alcance del MSPI. • Identificar los dueños de los riesgos. • Definir criterios para valorar las consecuencias de la materialización de los riesgos, y la probabilidad de su ocurrencia. • Determinar el apetito de riesgos definido por la entidad • Establecer criterios de aceptación de los riesgos. • Aplicar el proceso de valoración del riesgo que permita determinar los riesgos asociados a la perdida de confidencialidad, integridad y disponibilidad de la información que se encuentre dentro del alcance. • Determinar los niveles de riesgo. • Realizar la comparación entre los resultados del análisis y los criterios de los riesgos establecidos en este mismo numeral. • Priorización de los riesgos analizados para su tratamiento. Se debe asegurar que las valoraciones repetidas de los riesgos de seguridad y privacidad de la información produzcan resultados consistentes, válidos y comparables.	Procedimiento y metodología de gestión de riesgos institucional incluyendo el capítulo de seguridad y privacidad de la información aprobado por el comité de coordinación de control interno. (Anexo 1. Guía para la gestión de riesgos de seguridad digital)	La entidad cuenta con el documento estratégico denominado "DE-DEI-05 -Política de Administración del Riesgo" Versión 12, Publicada en el SIG el 27-05-2022; Previa aprobación por el Comité de Coordinación de Control Interno, mediante el acta No. 1 del 27 de mayo de 2022, "...la secretaria técnica sometió a consideración por parte de los Integrantes del Comité la nueva política de Administración del riesgo, la cual fue aprobada por unanimidad". La mencionada política, en el apartado 5.8, trata el tema de los Riesgos de Seguridad de la Información: "Para la identificación de los riesgos de Seguridad de la Información, se debe tener en cuenta la Política de Seguridad y Privacidad de la Información (DE-GGT-03), del MADR, que propende por preservar las características de confidencialidad, integridad y disponibilidad de los activos de información que hacen parte de cada uno de los procesos institucionales" y describe el proceder. Se informa del formato F01-PR-SIG-05, donde se realiza la metodología para su desarrollo. Adicionalmente, se cuenta con el procedimiento "PR-SIG-05 - Gestión del Riesgo" Versión 14, publicada en el SIG EL 21-07-2021, en el cual se determina que "La Oficina de Tics, registra los riesgos de seguridad y toda la información de análisis en el aplicativo establecido para tal fin, coordinando todo el proceso de identificación de los activos de información con los responsables de los procesos y establece las valoraciones con los mismos. Así mismo establece los planes de gestión de riesgos a los cuales tenga lugar y realiza los seguimientos a los mismos. La información del aplicativo se traslada al formato "Mapa de Riesgos (F01-PR-SIG-05)" y se publica en la página WEB, de acuerdo con las orientaciones del Grupo Administración del SIG".	Sí
7.3.3 Plan de tratamiento de los riesgos de seguridad de la información			Evaluación OCI	
Propósito	Lineamiento	Salida	Observación	Cumple
Estructurar una metodología que permita definir las acciones que debe seguir la entidad para poder gestionar los riesgos de seguridad y	La entidad debe definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información, que permita: • Seleccionar las opciones (controles) pertinentes y apropiadas para el tratamiento de riesgos. • Elaborar una declaración de	Plan de tratamiento de riesgos, aprobado por los dueños de los riesgos y el comité institucional de gestión y desempeño (Decreto 612 de 2018 Publicación antes de 31 de enero de cada vigencia). Declaración de aplicabilidad,	Se cuenta con el Plan de Tratamiento del Riesgo para los años 2022 y 2023. Para el año 2023, se encuentra aprobado por el Comité Institucional de Gestión y Desempeño en la sesión del 30 de enero de 2023. No se evidencia aprobación por parte de los dueños de los procesos.	Sí

7.3 Planificación				
7.3.1 Identificación de activos de información e infraestructura critica			Evaluación OCI	
Propósito	Lineamiento	Salida	Observación	Cumple
privacidad de la información	aplicabilidad que contenga: los controles necesarios, su estado de implementación y la justificación de posible exclusión. • Definir un plan de tratamiento de riesgos que contenga, fechas y responsables con el objetivo de realizar trazabilidad. • Los dueños de los riesgos deben realizar la aprobación formal del plan de tratamiento de riesgos y esta aceptación debe llevarse a la revisión por dirección en el Comité Institucional y de Desempeño, o quien haga sus veces.	aceptada y aprobadas en el comité de gestión institucional.		

Tabla 17 – Elaboración equipo Auditor tomando como base el documento maestro de Modelo de Seguridad de la Información.

El equipo auditor realizó evaluación a la información suministrada por la Oficina de Tecnologías de la Información, relacionada con el Plan de Tratamiento del Riesgo, el cual, hace referencia para los años 2021 y 2022.

Para el año 2023 se cuenta con el respectivo Plan de Tratamiento del Riesgo para la vigencia, el cual se encuentra aprobado por el Comité de Gestión y Desempeño en la sesión del 30 de enero de 2023. Se encuentra conforme. Se recomienda a la Oficina de Tecnologías de la información y las Comunicaciones revisar dicho plan en estructura con el fin de tratar los riesgos de los activos de información actualmente publicados y que se aprobado por los dueños de los activos de información.

Adicionalmente revisando procedimiento "PR-ALI-26 - Esquema de publicación de Información Pública", versión 2, no determina la periodicidad de la actualización de la identificación y clasificación de la información de acuerdo con los lineamientos del MSPI "*Actualizar el inventario y la clasificación de los activos por los propietarios y custodia de los activos de forma periódica o toda vez que exista un cambio en el proceso*", presentado una No Conformidad. Adicionalmente se recomienda la revisión del procedimiento en cuanto a las definiciones.

7.4 Soporte				
7.4.1 Recursos			Evaluación OCI	
Propósito	Lineamiento	Salida	Observación	Cumple
Determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del MSPI.	La entidad debe determinar y proporcionar los recursos necesarios para adoptar el MSPI, teniendo en cuenta que es un proceso transversal de la entidad, se requiere que se disponga de los recursos financieros, humanos (dedicación de horas/hombre) de sus colaboradores y en general cualquier recurso que permita la adopción, implementación, mantenimiento y mejora continua del MSPI.	Incluir dentro de los proyectos de inversión de la entidad aquellas actividades relacionadas con la adopción de MSPI de acuerdo con el alcance establecido.	Actualmente cuenta con el proyecto "Fortalecimiento de la Gestión de Tecnologías de la Información - TI en el Ministerio de Agricultura y Desarrollo Rural en función de la transformación digital del sector agropecuario", el cual tiene un objetivo relacionado: "Fortalecer la gestión de servicios tecnológicos y de seguridad de la información". Asociado a la Actividad: "Evaluar, planificar, implementar y realizar seguimiento a la estrategia de seguridad de la información institucional"; Para el año 2023 cuenta con un presupuesto de $2.351.912.500; Este tema de amplia en el ítem 3.7. Evaluar la ejecución presupuestal asignada al SGSI.	Sí
7.4.2 Competencia, toma de conciencia y comunicación			Evaluación OCI	
Propósito	Lineamiento	Salida	Observación	Cumple

7.4 Soporte				
7.4.1 Recursos			Evaluación OCI	
Propósito	Lineamiento	Salida	Observación	Cumple
Garantizar una correcta comunicación, sensibilización y concientización con respecto a la seguridad y privacidad de la información, en la que todos sus funcionarios estén al tanto de la política de seguridad y privacidad, cuál es su rol en el cumplimiento del MSPI, beneficios y consecuencias de no poner en práctica las reglas definidas en el modelo (desde el punto de vista de seguridad y privacidad de la información).	La entidad debe definir un plan de comunicación, capacitación, sensibilización y concientización para: • Asegurar que las personas cuenten con los conocimientos, educación y formación o experiencia adecuada para la implementación y gestión del modelo de seguridad y privacidad de la información. • Involucrar al 100% de los funcionarios de la entidad en la implementación y gestión del MSPI. • Concientizar a los funcionarios y partes interesadas en la importancia de la protección de la información. • Identificar las necesidades de comunicaciones internas y externas relacionadas con la seguridad y privacidad de la información. Se deberá definir qué será comunicado, cuándo, a quién, quién debe comunicar y finalmente definir los procesos para lograrlo.	Plan de cambio, cultura, apropiación, capacitación y sensibilización de Seguridad y Privacidad de la Información y seguridad digital. Este se puede incluir en el Plan Institucional de Capacitaciones - PIC. Plan de comunicaciones del modelo de seguridad y privacidad de la información.	Revisadas las publicaciones del PIC para el año 2022 y 2023, no hace referencia al Plan de cambio, cultura, apropiación, capacitación y sensibilización de seguridad y Privacidad de la Información. Se solicitud información a la OTIC, se presenta plan de sensibilización y comunicación en materia de seguridad de la información, "Aplica para las vigencias 2021 y 2022"; se revisaron algunas evidencias.	No

Tabla 18 – Elaboración equipo Auditor tomando como base el documento maestro de Modelo de Seguridad de la Información.

El equipo auditor realizó evaluación a la información suministrada por la Oficina de Tecnologías de la Información, relacionada con el Plan de Cambio, cultura, apropiación, capacitación y sensibilización de seguridad y Privacidad de la Información y seguridad digital, el cual, hace referencia para los años 2021 y 2022, para el año 2023 no cuenta con la respectiva información. Adicionalmente se revisó el PIC, y no se encuentra información al respecto; presentando una No Conformidad. La dependencia manifiesta que no cuenta con todos los profesionales requeridos para el cumplimiento del mencionado plan.

Para finalizar, el proceso de Gestión y Gobierno de TI identificó para el desarrollo de la política los siguientes riesgos:

1. "P*osibilidad de afectación reputacional por no tener en cuenta los lineamientos de MInTic en materia de TI, para la orientación en la formulación de estrategias, instrumentos y herramientas, debido al desconocimiento de la normatividad y lineamientos existentes*".

El proceso estableció el siguiente control: "*El jefe de la Oficina de Tecnologías de Información y las Comunicaciones y los profesionales asignados deben revisar periódicamente las políticas y los cambios en la normatividad vigente de manera que se puedan incorporar los lineamientos necesarios para el mejoramiento del proceso*".

A través del correo del 21 de junio de 2023, la Oficina de Tecnologías de la Información y las comunicaciones nos informa: "*Se realizó la actualización del normograma para la vigencia 2022. Para la vigencia 2023 se están revisando las últimas publicaciones de Mintic, tarea con base en la cual se realizará la actualización del*

normograma en el segundo semestre de la presente vigencia"; que corresponde a el control cuando se presenta una desviación: "*Los funcionarios y/o contratistas de la oficina TIC, informarán sobre las novedades en materia de normatividad de TI para actualizar el normograma, cuando se requiera*".

El equipo auditor procedió a revisar las respectivas evidencias reportas en el mencionado correo, las cuales se relaciona con la Directiva presidencial 02 de 2022 y correos solicitando la actualización del normograma, la cual, se encuentra conforme.

Igualmente, se procede a realizar su evaluación, y de acuerdo con el desarrollo de este ítem se presenta tres (3) no conformidades que afectan el cumplimiento de los lineamientos de Mintic y la normativa, razón por la cual, se establece materialización del riesgo evaluado. Se recomienda a la Oficina de Tecnologías de la Información y las Comunicaciones evaluación del control establecido y establecer las tareas pertinentes con el fin de evitar la materialización del riesgo.

2. Riesgo: "*Posibilidad de afectación reputacional por falta de interés en la aplicación de las políticas de TI. por parte de los servidores Públicos de la Entidad; debido a la resistencia al cambio*" y se estableció el siguiente control "*El jefe de la Oficina de Tecnologías de Información y las Comunicaciones y los profesionales asignados deben realizar campañas de Sensibilización al interior de la Entidad*".

El equipo auditor revisó las respectivas evidencias soportadas en el correo mencionado con anterioridad donde nos informa: "*Para la vigencia 2022 se llevaron a cabo diversas sensibilizaciones. Para la vigencia 2023 y con el apoyo del oficial de seguridad, se tiene contemplado realizar las sensibilizaciones correspondientes en el segundo semestre*", se presenta evidencias de las sensibilizaciones a través de cuatro archivos en Excel con la asistencia a las reuniones virtuales realizadas por la dependencia con el fin de mitigar el riesgo, el cual, se encuentra conforme.

En conclusión: El equipo auditor realizó la respectiva evaluación, encontrando que se está cumpliendo con los lineamientos de la política de gestión de seguridad de la información con las siguientes excepciones:

1. En relación con los roles y responsables se evidenció un cumplimiento parcial, de acuerdo con los lineamientos establecidos en el documento maestro MSPI - Roles y Responsabilidad. Entre ellos falta la creación del Comité de Seguridad y privacidad de la información, dependiente del Comité Institucional de Gestión y Desempeño Institucional (este comité es opcional, pero al interior de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC, existe un comité o grupo que se encarga de mitigar el riesgo, dirigido a la seguridad de la información digital, cuyo objeto sería que se definiera para todo el SGSI) , de la falta de la definición de los roles de la Oficina Asesora Jurídica, del Grupo de

Gestión Documental y de los demás que requiera el SGSI, en el caso del Oficial de Seguridad, el lineamiento es, que no pertenezca a la OTIC, por las anteriores razones, se presenta una No Conformidad

2. El procedimiento "*PR-ALI-26 - Esquema de publicación de Información Pública*", versión 2, no determina la periodicidad de la actualización de la identificación y clasificación de la información de acuerdo con los lineamientos del MSPI "*Actualizar el inventario y la clasificación de los activos por los propietarios y custodia de los activos de forma periódica o toda vez que exista un cambio en el proceso*", conllevando a una No conformidad.

3. Plan de Cambio, cultura, apropiación, capacitación y sensibilización de seguridad y Privacidad de la Información y seguridad digital, para la vigencia 2023 no cuenta con la respectiva información. Adicionalmente se revisó el PIC, y no contempla actividades asociadas con el tema de Seguridad, presentando una No Conformidad.

De la misma manera, esta Oficina evidenció una posible materialización del riesgo "*Posibilidad de afectación reputacional por no tener en cuenta los lineamientos de MinTic en materia de TI, para la orientación en la formulación de estrategias, instrumentos y herramientas, debido al desconocimiento de la normatividad y lineamientos existentes*", de acuerdo con el desarrollo de este ítem, para lo cual se recomienda a la Oficina de Tecnologías de la Información y las Comunicaciones tomar las respetivas acciones al respecto.

Adicionalmente se presentan la siguiente oportunidad para el Sistema de Gestión de Seguridad de la Información en el MADR - Con respecto al contexto y las partes interesadas de la entidad, evidencia el cumplimiento de estos factores. Sin embargo, se recomienda establecedor una oportunidad de mejora, para que los documentos del contexto y de las partes interesadas formen parte del Sistema Integrado de Gestión de la entidad con respecto a la Planeación Institucional de la entidad y sea un instrumento de planeación para el Sistema de Gestión de la Seguridad de la Información y otros procesos.

3.2. Evaluar el cumplimiento del documento denominado "Políticas Específicas de Seguridad de la Información" publicada en el Sistema Integrado de Gestión el 30102020 Versión 3.

Para el Desarrollo de estas Políticas se tomas algunos numerales, los cuales de describen a continuación:

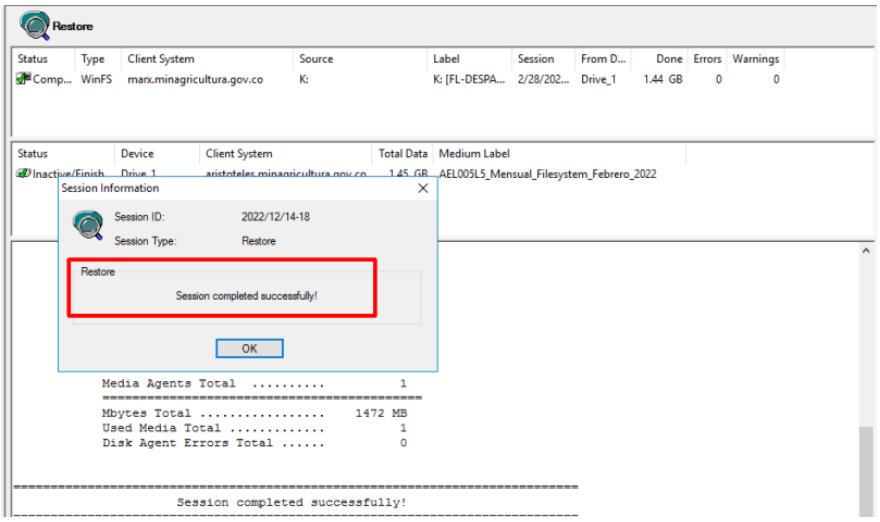
POLÍTICA DE RESPALDO DE INFORMACIÓN:

De acuerdo con las Políticas Específicas de Seguridad y Privacidad de la Información, se debe contar con políticas de respaldo de la información de acuerdo con el ISO/IEC 2700:2013 en su numeral 12.3.1, por lo que la Oficina de las TIC, genera un Documento estratégico llamado Política Técnica de Tic para el Ministerio de Agricultura y Desarrollo Rural.

En este documento está incluido en el numeral 7 capítulo cuarto, copias de respaldo – Backups que tiene inmerso la frecuencia con que se realizan y el tiempo de retención de los medios de almacenamiento que pueden ser virtuales o en cintas.

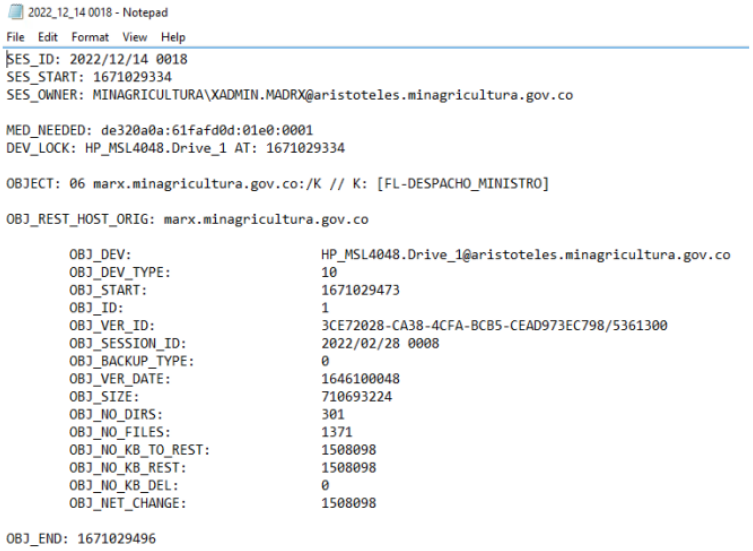
Se evidencia que se realizan las copias de respaldo en el tiempo estipulado en la política, así como la generación del registro de log.

De la mima manera se evidencia que se realiza una prueba de restauración del JOB – Mensual_Servidor_Marx_K_O.TIC, tomando la carpeta 2022_12_14 0018 como referencia a restaurar.

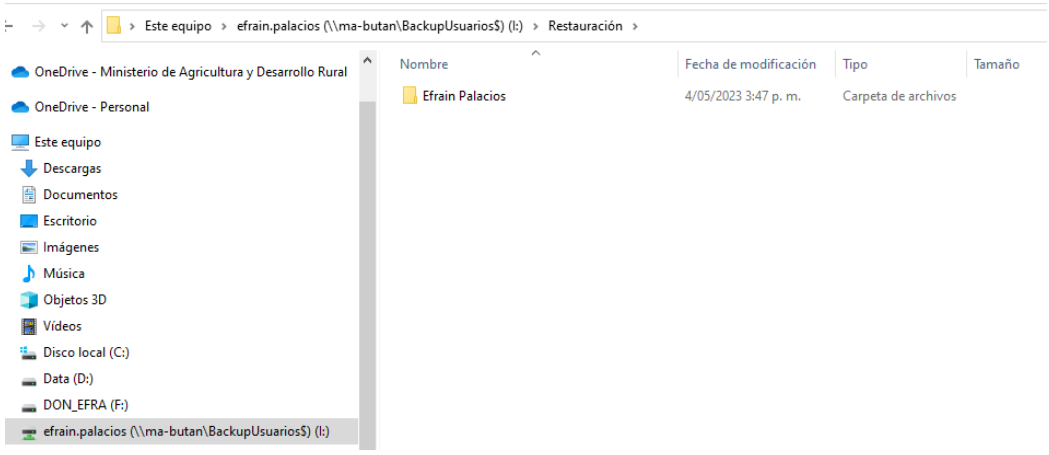


Se evidencia que una vez se elige el archivo a restaurar, se selecciona la carpeta donde se realizará la actividad de restauración, observando que en la carpeta antes seleccionada se restaura el archivo de forma satisfactoria.

A continuación, se presenta el log de restauración del archivo seleccionado.



Así mismo, como prueba para verificar que se cumple con la Política, se solicita la restauración de una carpeta de la OCI, evidenciando que se encuentra la información que se había modificado, así como se observa en la siguiente imagen.



Se evidencia que, para el cuarto trimestre del 2022, se contaba con un proveedor encargado de la custodia de las cintas la cual se realizó bajo la Orden de Compra 93874 celebrando el contrato 20220525 con fecha de finalización el 31 de diciembre del 2022. No obstante, a la fecha de la auditoría no se cuenta con un proveedor para la ejecución de esta actividad, por lo que es necesario realizar la contratación de un proveedor, a fin de dar cumplimiento con la Política Específica de Seguridad y Privacidad de la Información.

NC. Incumplimiento a la Política Específica de Seguridad y Privacidad de la Información, dado que no se cuenta con elementos necesarios para la realización

de copias de respaldo, corriendo el riesgo de perder información y no poderla recuperar.

EVALUACIÓN OFICINA DE CONTROL INTERNO

Se solicita al proceso remitir el contrato que menciona en las observaciones, evidenciando que, si bien se adquirió la solución de Nutanix que realiza las copias de respaldo, esto se encuentra dentro del Ministerio y el objetivo es que estén fuera del edificio por cualquier desastre que pueda ocurrir. Dado lo anterior la NC se mantiene.

ACCESOS Y SERVICIOS

Con respecto al capítulo dos “Seguridad de la Política Específica de Seguridad y Privacidad de la Información en el literal C. Accesos y Servicios, respecto al tema de la cancelación de las cuentas de usuario y el bloqueo de los accesos a la red de la Entidad, se realizan pruebas de verificación de usuarios retirados a fin de verificar el estado en el directorio activo del Ministerio.

Los funcionarios seleccionados se muestran en la siguiente tabla:

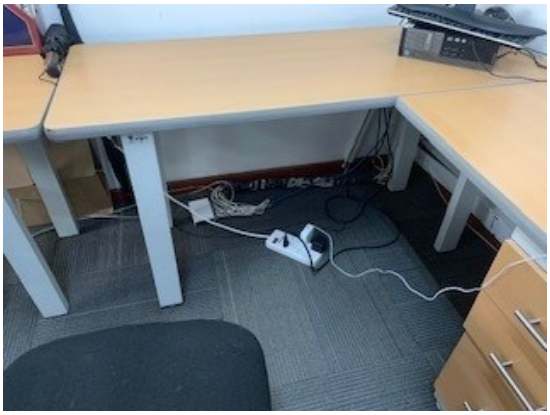
Margarita Maria Palacio Jaramillo	Maria Fernanda Cepeda Gomez
Angela María Pantoja Morales	Yudy Estella Pulgarín Marín
Guillermo Elías González Ganem	Sonia Amada Gutierrez Rivero
Ángel Antonio Tapia Ariza	Diana Rocío Parra Oviedo
German Parra Bustamante	Catalina Franco Gomez
Laura Julieth Saavedra Rueda	Claudia Marcela García Santos
Lury Arantxa Cardenas del Benazir Cardenas Bejarano	Cesar David Muñoz Lombana
Meyler Alfonso Cabrera González	Sara María Campos Infante
José David Velásquez Rodríguez	Maria del Pilar Ruiz Molina
Lorena Constanza Gómez Ramírez	

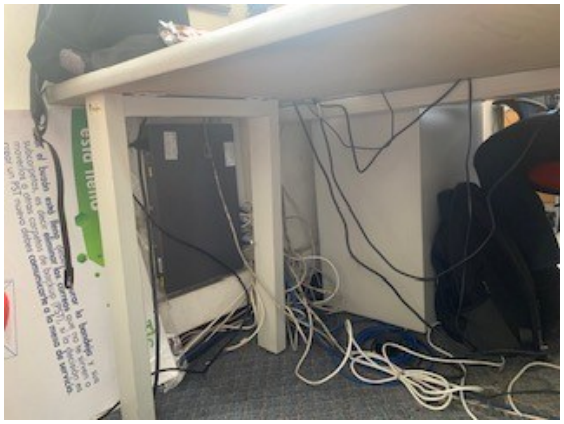
Una vez realizada la verificación en el directorio activo de los usuarios anteriormente seleccionados, se evidencia que todos se encuentran cancelados, cumpliendo así con la Política mencionada anteriormente.

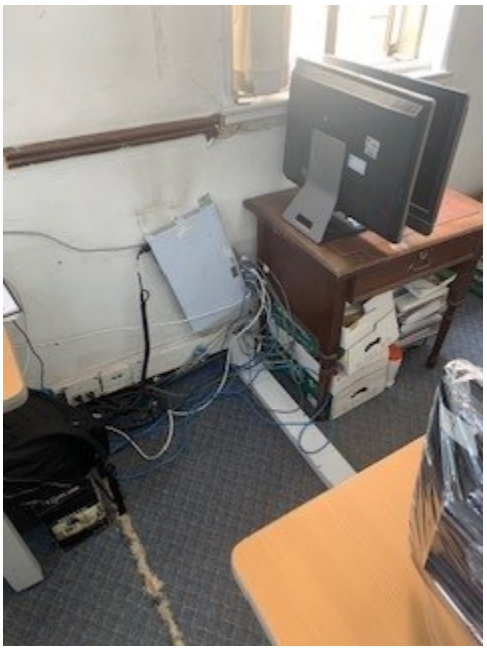
SEGURIDAD EN LAS COMUNICACIONES

En cuanto a la Política de Seguridad en las Comunicaciones de las Políticas Específicas de Seguridad y Privacidad de la Información, cuyo objetivo es prevenir en gran medida que los equipos se vean expuestos a riesgos y carezcan de programas específicos para combatirlos como es el caso de los antivirus o los parches, se puede evidenciar que existen equipos en diferentes áreas del Ministerio fuera del cuarto técnico, elementos que corren el riesgo de daño dado que se encuentran en sitios cerca a los usuarios.

Lo anteriormente mencionado se puede evidenciar en las siguientes imágenes:







NC. Se incumple con la Políticas Específicas de Seguridad y Privacidad de la Información toda vez que se evidencian elementos tecnológicos (switches) que se encuentran ubicados fuera del rack, corriendo el riesgo de dañarse por algún golpe de los usuarios.

EVALUACIÓN OFICINA DE CONTROL INTERNO

Revisado lo descrito por el proceso, se observa que aún no se cuentan con un plan para la ubicación de los switches, por lo que la No Conformidad se mantiene.

De igual manera se evidencia que se encuentran elementos que no pertenecen al cuarto técnico que pueden afectar la temperatura de este, así como el cableado que se encuentra desordenado, teniendo la posibilidad que, en algún momento de brindar soporte en la revisión de cualquier punto, puede desconectarse y sacar de la red de un usuario, tal como se observa en las siguientes imágenes.

En la visita realizada en la sede Mezanine se observa que en el cuarto técnico se encuentran elementos que no corresponden a temas tecnológicos; así mismo se cuenta con un sistema de aire acondicionado que no está funcionando y que puede ayudar a mantener el ambiente adecuado para que no se sobrecaliente el cuarto técnico. Lo anterior se puede observar en las siguientes imágenes:

NC. Se incumple con la Políticas Específicas de Seguridad y Privacidad de la Información dado que, en los cuartos técnicos se evidencian elementos que no pertenecen a Tecnología, generando riesgos que puedan dañar el cableado instalado en los racks.

EVALUACIÓN OFICINA DE CONTROL INTERNO

Revisado lo descrito por la Oficina de TIC, se indica que, si bien los cuartos técnicos los administra el Grupo de Servicios Administrativos, es función de la OTIC velar porque los cuartos estén adecuados para el buen funcionamiento de los racks y así evitar que se corra el riesgo de algún daño, por lo que la No Conformidad se mantiene.

CABLEADO ESTRUCTURADO

En la misma visita a los cuartos técnicos se evidencia que el cableado no se encuentra ordenado, elemento que puede afectar a los usuarios conectados por lo que se recomienda tomar acciones urgentes que subsanen las actividades de la correcta instalación del cableado estructurado del Ministerio. Lo descrito se observa en las siguientes imágenes:

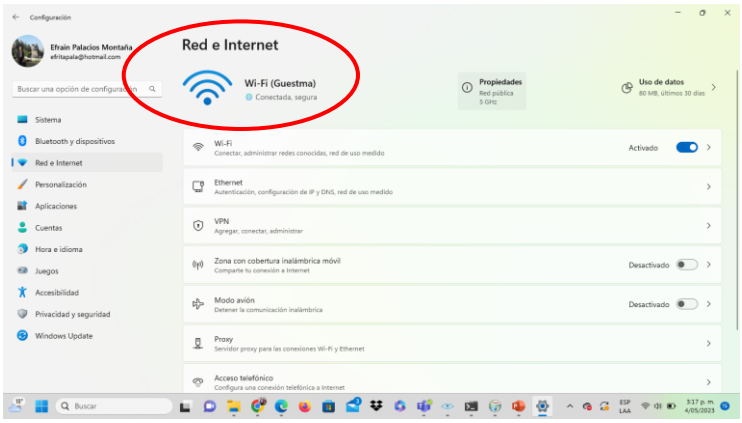
POLÍTICA DE USO DE DISPOSITIVOS MÓVILES

De acuerdo con las Políticas Específicas de Seguridad y Privacidad de la Información, en su numeral 5.1.3 Política de Uso de Dispositivos Móviles cuyo objetivo es Garantizar la seguridad, administración, transmisión o almacenamiento de los activos de información institucionales desde dispositivos móviles, y el uso de estos dentro de MinAgricultura, se realizan pruebas de conexión por medio de un computador portátil externo, es decir que no se encuentra dentro del inventario del

Ministerio conectándose por medio de la red WIFI y por cable UTP, en la red de Bancol, Pedro A. López y Mezanine.

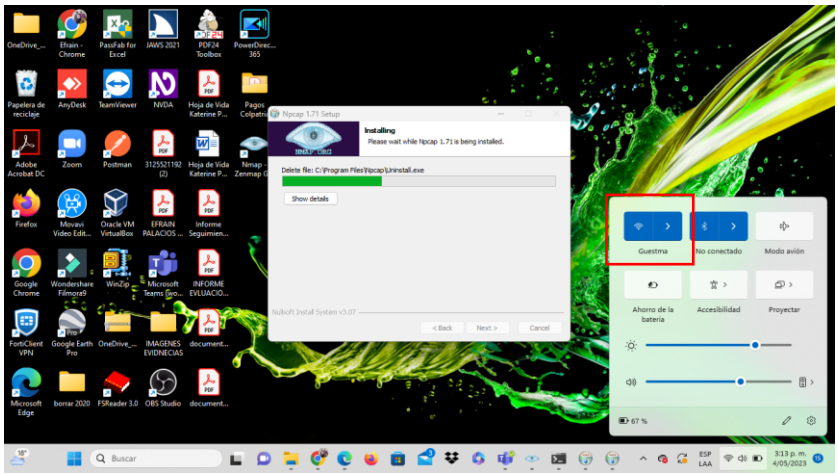
Se inician las pruebas en el Edificio Bancol encontrando la siguiente información:

Para la red wifi, al intentar conectarse solicita conexión obligatoria a las redes disponibles (guestma y Madr_Funcionarios) mediante un usuario y contraseña, observando que la seguridad se encuentra habilitada en el switch de Bancol; en caso de no conectarse, no permite el acceso a ninguna parte del Ministerio.

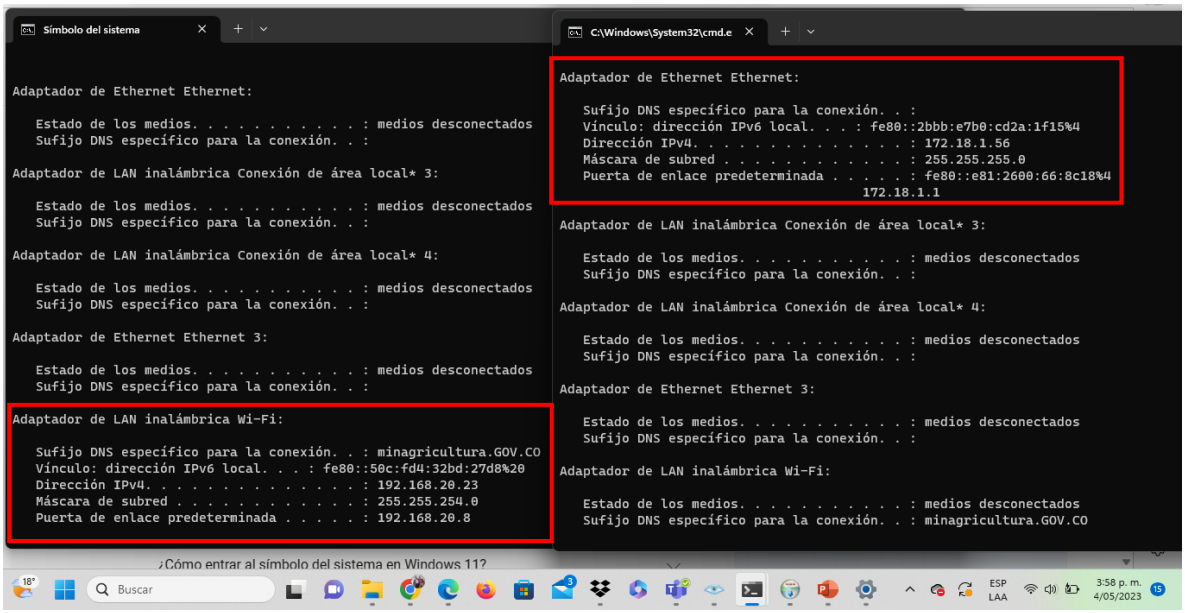


Sin embargo, cuando está conectado a esta red, se permite descargar programas e instalarlos sin necesidad de usuario o contraseña de un administrador. Si bien es cierto que es un computador externo y puede instalar cualquier software bajo su responsabilidad, así mismo se puede instalar un programa que tenga virus o si es con más experiencia, obtener un código malicioso que pueda vulnerar la red del MADR.

Lo anteriormente expuesto se puede observar en la siguiente imagen:

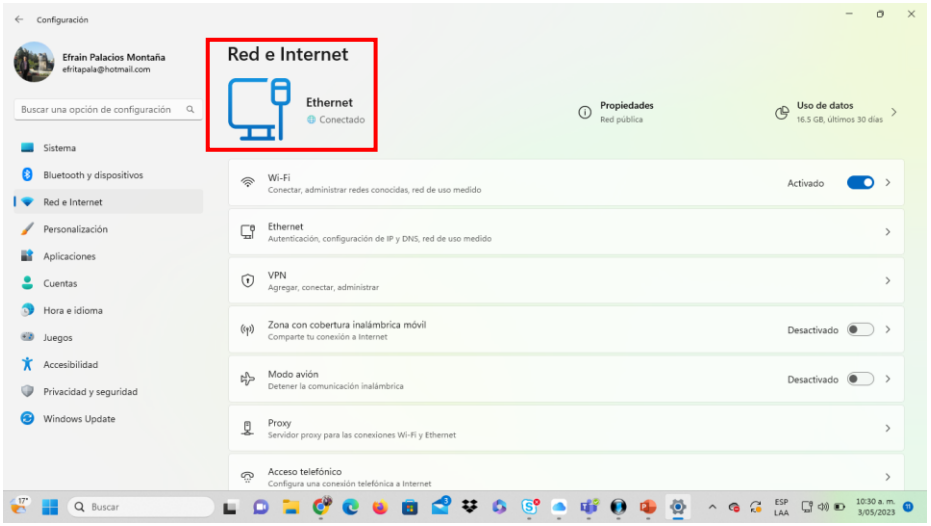


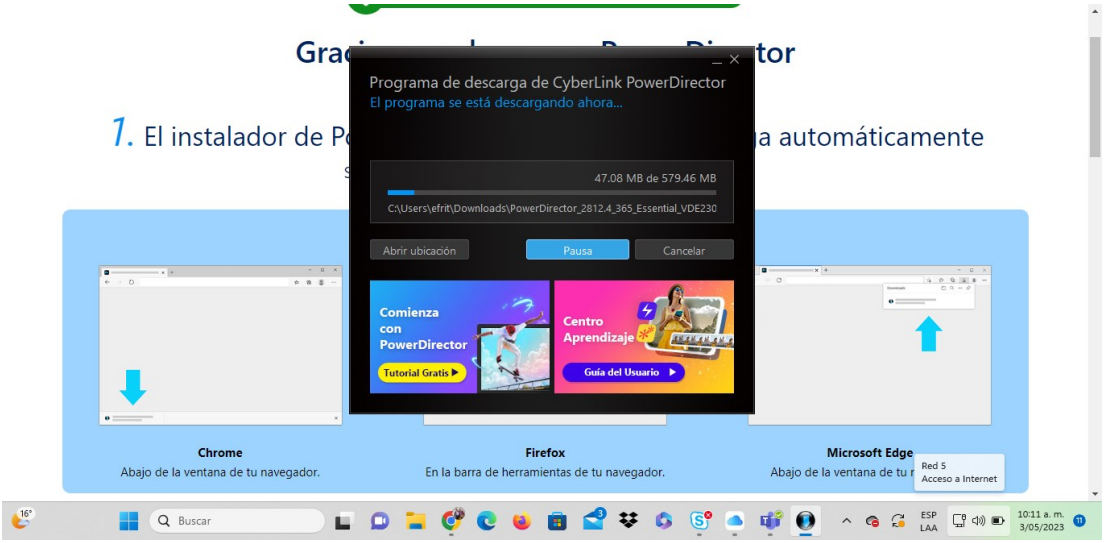
De igual manera se observa que al conectarse por red WIFI por medio del computador externo, se muestra el Sufijo DNS específico para la conexión “minagricultura.gov.co” mientras que por conexión con cable UTP, este no lo muestra, lo anterior se observa en la siguiente imagen:



Esta conexión por cable, no se registra vínculo al dominio del Ministerio por lo que cualquier intruso puede ingresar y realizar maniobras indebidas.

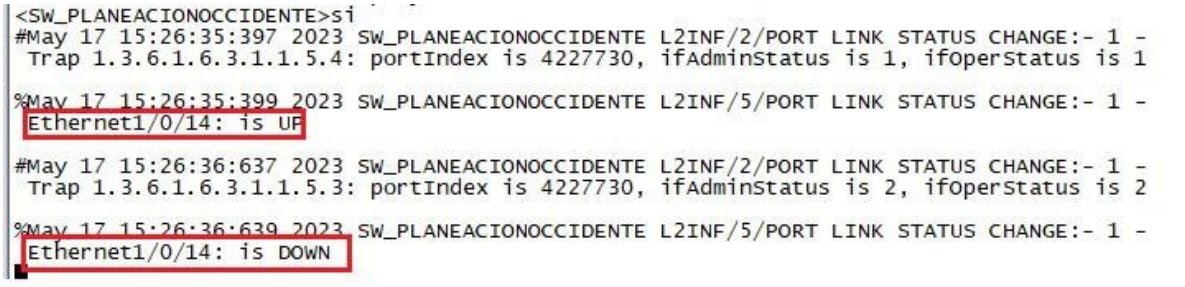
Así como ocurre en la conexión por wifi, por medio del cable UTP se pueden descargar e instalar programas que pueden contener software malicioso.

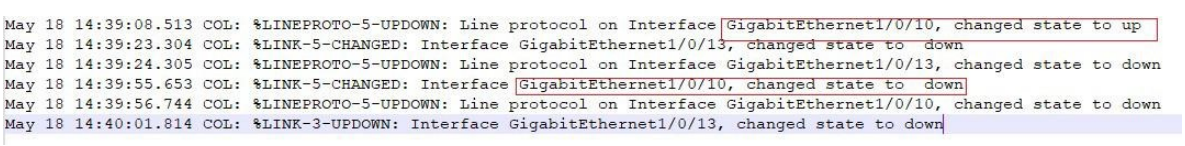




Se recomienda configurar la red del Edificio Bancol en los términos que establece el Ministerio de las TIC y la Política Específica de Seguridad y Privacidad de la Información del Ministerio en el numeral 5.1.3. POLÍTICA DE USO DE DISPOSITIVOS MÓVILES, dado que al conectar el cable UTP a un portátil externo, no ingresa al Dominio del MADR.

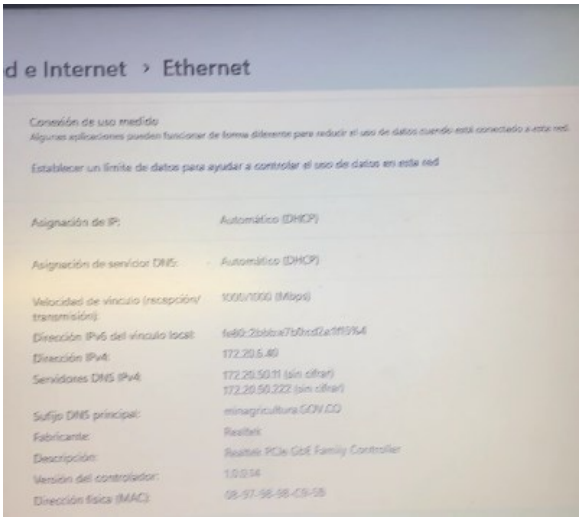
De igual forma se realizan pruebas de las conexiones en el Edificio Pedro A. López en la Oficina de Planeación, Sala de Asesores y Asuntos Internacionales, observando que en algunas oportunidades se bloqueaban automáticamente los puntos de red y en otras ingresaba al Dominio de Minagricultura.gov.co





```
%Apr  2 03:51:03:569 2000 ASUNTOS_INTERNACIONALES L2INF/5/PORT LINK STATUS CHANGE:- 1 -
 Ethernet1/0/18: is UP

<ASUNTOS_INTERNACIONALES>
<ASUNTOS_INTERNACIONALES>
#Apr  2 03:51:33:629 2000 ASUNTOS_INTERNACIONALES L2INF/2/PORT LINK STATUS CHANGE:- 1 -
 Trap 1.3.6.1.6.3.1.1.5.3: portIndex is 4227762, ifAdminStatus is 2, ifOperStatus is 2

%Apr  2 03:51:33:631 2000 ASUNTOS_INTERNACIONALES L2INF/5/PORT LINK STATUS CHANGE:- 1 -
 Ethernet1/0/18: is DOWN

#Apr  2 03:52:00:034 2000 ASUNTOS_INTERNACIONALES L2INF/2/PORT LINK STATUS CHANGE:- 1 -
 Trap 1.3.6.1.6.3.1.1.5.4: portIndex is 4227762, ifAdminStatus is 1, ifOperStatus is 1

%Apr  2 03:52:00:037 2000 ASUNTOS_INTERNACIONALES L2INF/5/PORT LINK STATUS CHANGE:- 1 -
 Ethernet1/0/18: is UP
```

Sin embargo, se realizan pruebas por cable UTP y por WIFI en otras áreas evidenciando que las conexiones, aunque no se bloquean, son seguras, dado que el servidor DNS es minagricultura.gov.co. Esto se observa en la siguiente imagen:



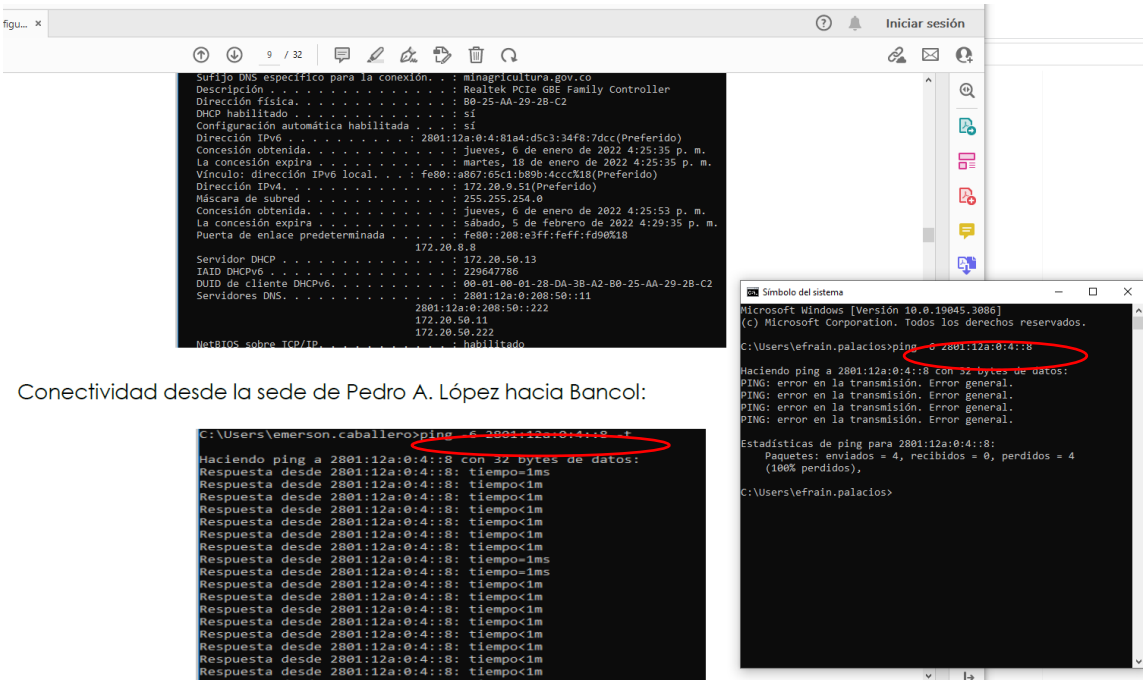
Para la realización de transición de los servicios de TI para los protocolos IPV4 a IPV6 en el MinAgricultura celebró el contrató No. 20190514 con el proveedor REDNEET S.A.S por valor de $379.300.000, cuyo objetivo es "*Realizar las fases para la transición de servicios de TI, del protocolo IPV4 a IPV6 en el Ministerio de Agricultura y Desarrollo Rural"*.

A fin de verificar el cumplimiento del contrato, el equipo auditor revisó las obligaciones específicas del proveedor encontrando que se cumplió con lo establecido en dicho contrato.

El contrato presenta una prórroga en diciembre del 2019 cuya fecha de terminación va hasta el 19 de febrero del 2020 dado que el Registro de Direcciones de Internet

de América Latina y Caribe - LACNIC, entidad proveedora de los protocolos IP, se demora en la solicitud de asignación al Ministerio de esta información. Sin embargo, se realiza la liquidación del contrato el 6 de junio del 2022 por medio del memorando 2022-190-15113-3, tiempo que está fuera de los términos de cuatro (4) meses para dar por terminado un contrato según la cláusula Decima Novena: liquidación.

En cuanto a la transición de IPV4 a la IPV6, de acuerdo con la información suministrada por la OTIC, se realiza una prueba de conectividad a la dirección “2801:12a:0:4::8”, la cual se encuentra dentro del informe y como resultado se observa que es diferente al ejercicio realizado, tal como se observa en la siguiente imagen.

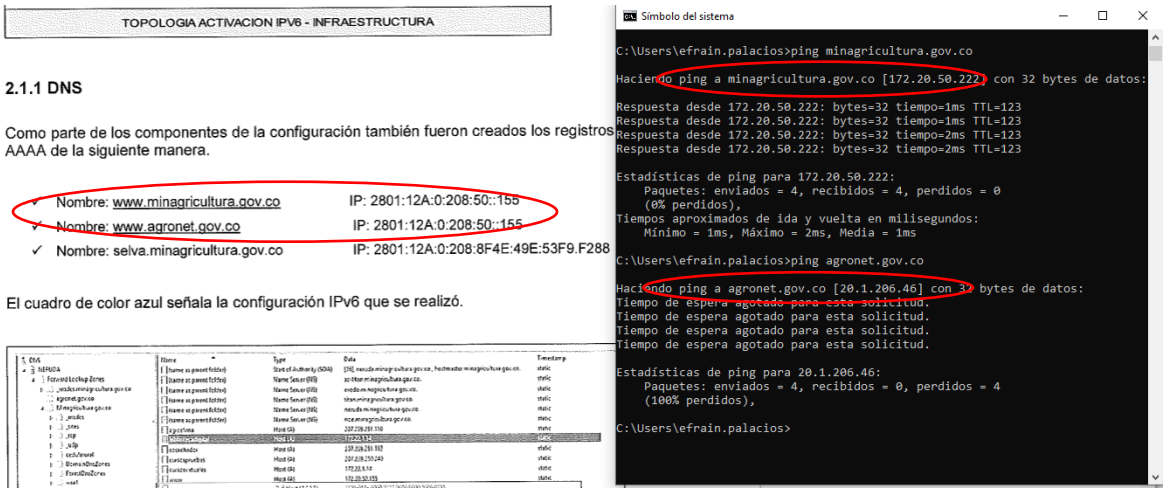


Conectividad desde la sede de Pedro A. López hacia Bancol:

Así mismo se realiza una prueba de conectividad teniendo en cuenta el informe No. 10 del proveedor RedNeet al servidor Neruda, observando que, en el informe suministrado, la respuesta se encuentra diferente a la prueba de conectividad realizada, tal como se observa en la siguiente imagen.

De acuerdo con la imagen anterior, se observa que en el informe presentado por el proveedor el resultado a la conectividad Neruda muestra una dirección IPV6 2801:12:0:208:50::11 mientras que, en la prueba realizada durante la auditoría, la dirección que muestra IPV4 172.20.50.11.

De igual manera se realiza prueba de conectividad presentado en el informe No. 11 del proveedor RedNeet a las direcciones minagricultura.gov.co y agronet.govo.co, obteniendo como resultado la siguiente imagen:



Considerando lo anteriormente presentado, se observa que persiste la diferencia de resultados entre el informe y la prueba realizada, concluyendo que, pese a que se entregó el informe final del contrato, la conectividad de IPV6 se encuentra deshabilitada.

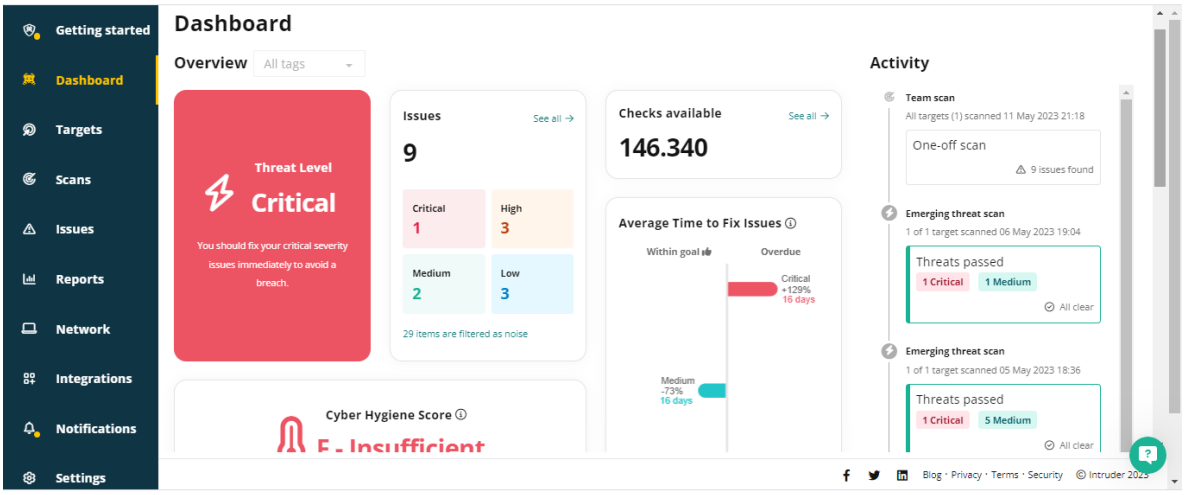
De acuerdo con la información suministrada mediante reunión realizada por teams, el especialista en redes y el profesional de la Oficina de las TIC, indican que el uso de la IPV6 tiene un licenciamiento que se paga anualmente a LACNIC, proveedor de las asignaciones de las direcciones IP para el MADR, sin embargo, se solicitó la desactivación de los recursos de IPV6 toda vez que no se iba a realizar nuevamente el contrato hasta nueva orden. Para el año 2023 ya se está realizando la gestión para la ejecución del contrato para la actualización de esta licencia con la misma entidad.

Es importante tener en cuenta la continuidad del licenciamiento de las asignaciones de las IP, dado que al no tenerla se puede estar pendiendo el rango de asignación y habría que realizar un nuevo contrato para la gestión de la nueva asignación, Tl como lo hizo RedNeet.

Por último y no menos importante, en la carpeta del contrato 20190514 celebrado entre RedNeet S.A.S y el MADR, no se evidencia el certificado de cumplimiento, así como el acta de liquidación firmado entre las partes que celebraron el mencionado contrato. Así mismo se solicitó la liquidación del contrato el 6 de junio del 2022, evidenciando que se demoró más de un año para esta actividad. Por lo que se recomienda tener en cuenta los tiempos establecidos en el contrato en la Cláusula Decima Novena: Liquidación, para la terminación de los contratos.

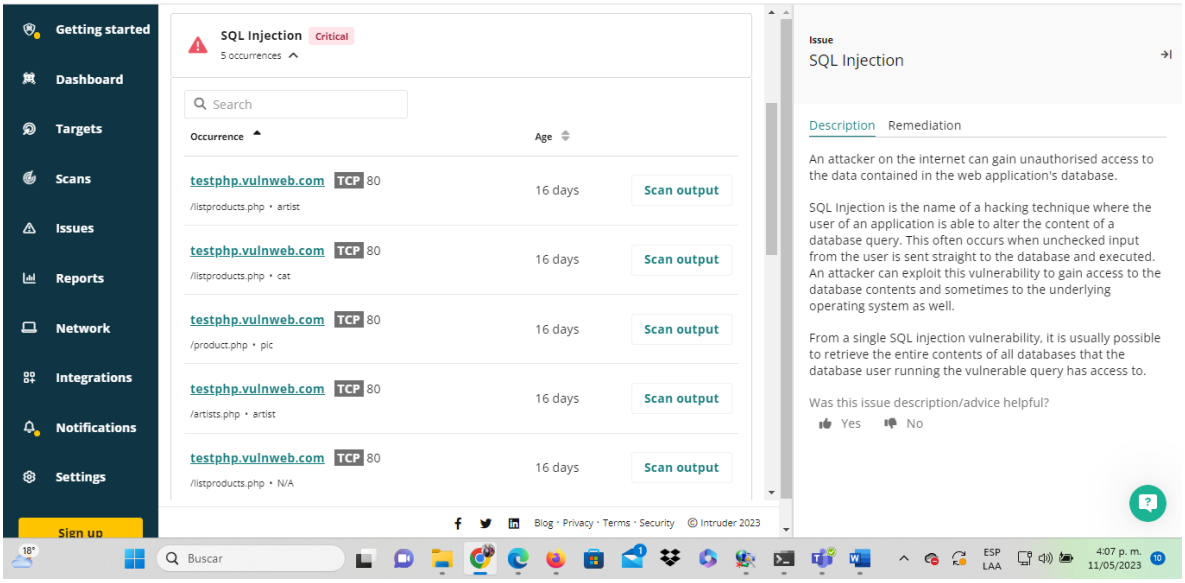
Por otro lado, a fin de verificar la vulnerabilidad de la red del MinAgricultura, se utiliza una herramienta llamada INTRUDER, que es un escáner que verifica la red encontrando posibles espacios abiertos donde se pueda ser peligroso para la entidad, en el caso en que algún intruso quiera ingresar a los servidores del Ministerio.

Se utiliza esta herramienta realizando una búsqueda a la página web del Ministerio, observando como resultado, la siguiente información:



Como se puede observar en la imagen anterior, son 9 sucesos que ocurrieron, distribuidos en, uno crítico, 3 altos, 2 medianos y 3 bajos.

A continuación, se describe el suceso con estado crítico, el cual cuenta con 5 ocurrencias.



Con el uso de la herramienta NetScanTools, se generaron varios informes con los mismos tipos de conexión (UTP y WIFI) desde el edificio Bancol, generando un ping a la dirección 172.18.1.56 el cual recorre todas las direcciones por donde pasa esta dirección, evidenciando que en Bancol, tiene ventanas abiertas, tal como se muestra en la siguiente imagen:

IPv4 Address	MAC Address	I/F Manufacturer	Hostname	Notes or Comments
172.18.1.1	00-00-5E-00-01-01	ICANN, IANA Department	?	
172.18.1.2	28-94-0F-80-14-C1	Cisco Systems, Inc	?	
172.18.1.3	E4-F0-04-5B-24-84	Dell Inc.	?	
172.18.1.5	64-9E-F3-B3-58-2B	Cisco Systems, Inc	?	
172.18.1.6	00-90-8F-36-71-9A	AUDIO CODES LTD.	?	
172.18.1.7	00-0B-AB-F3-20-D4	Advantech Technology (CHINA) Co., Ltd.	Salomon	
172.18.1.11	C0-18-50-48-26-28	Quanta Computer Inc.	PT32687GAC	
172.18.1.12	C8-CB-B8-25-65-F2	Hewlett Packard	P26082-SB	
172.18.1.13	C8-1F-66-B6-DE-C9	Dell Inc.	P27814SB	
172.18.1.14	00-04-F2-9A-4C-CA	Polycom	?	
172.18.1.15	00-04-F2-9A-4D-6E	Polycom	?	
172.18.1.16	C8-CB-B8-24-EE-5D	Hewlett Packard	P25886-SB	
172.18.1.17	00-04-F2-95-9B-F2	Polycom	?	
172.18.1.18	00-04-F2-96-3D-BC	Polycom	?	
172.18.1.21	00-04-F2-96-F0-B6	Polycom	?	
172.18.1.22	00-04-F2-97-23-CD	Polycom	?	

Al realizar la prueba con la misma herramienta a camponet.gov.co y minagricultura.gov.co, se evidencia que se muestra la misma información que con la dirección IP anterior.

No obstante, en el edificio Pedro A. López, esta información ya no se observa, dado que ingresa al dominio minagricultura.gov.co. Esto se puede evidenciar en la siguiente imagen.

IP Address	MAC Address	I/F Manufacturer	Hostname	B31	B16	B8	GRP	M0	M1	M3	Analysis

Notes for this Automated Set of Tests:

No notes found for this test.

Analizada esta información, se evidencia que concuerda con lo anteriormente mencionado y es que parte de la red de Bancol no está protegida dado que no ingresa al dominio minagricultura.gov.co.

En el caso que se requieran los informes de las herramientas, estos se encuentran en la carpeta de la Oficina de Control Interno a disposición de todos.

En Conclusión, de acuerdo con los resultados de la evaluación, el Sistema de Gestión de Seguridad de la Información cuenta con la seguridad necesaria para mantener al MinAgricultura, libre de vulnerabilidades y protección ante intrusos que deseen ingresar a realizar actividades que afecten su información.

3.3. Evaluar el cumplimiento del Procedimiento "Gestión de Incidentes de Seguridad de la Información" publicado en el SIG el 20112020 Versión 1

El equipo auditor procedió a revisar el procedimiento, para ello realizó visita a los responsables de la gestión de los incidentes de seguridad; solicitó la base completa de incidentes, para su valoración, pero la Oficina de Tecnologías de la Información y las Comunicaciones omitió esta solicitud y solo envió los incidentes de seguridad relacionados con “Reportar Spam”, el cual contiene 54 requerimientos, los cuales se encuentran cerrados.

En cuanto al evaluación de cumplimiento del procedimiento se describe a continuación:

No	Actividad	Evaluación OCI	Cumple
1	Detecte y reporte cuando este es evidenciado a través de las diferentes alertas y/o medios de comunicación que posea el Ministerio el potencial evento y/o incidente de seguridad de la información de seguridad. Nota. Algunos ejemplos de alertas y/o medios son: alertas de las plataformas de TIC, caídas del sistema, reportes de usuario, registros de las herramientas administrativas, consolas de antivirus, comunicaciones anónimas, redes sociales, Mesa de servicio, ciudadanía, entre otros.	A través del reporte suministrado por la Oficina de Tecnologías de la Información y las Comunicaciones, se evidencia los diferentes canales utilizados.	Sí
2	Registre la situación de seguridad de la información en la herramienta de gestión, documentando los datos solicitados en el mismo, tales como: línea cronológica, activo de información involucrado o afectado, identificación de las fuentes de información, entre otros.	A través del reporte suministrado por la Oficina de Tecnologías de la Información y las Comunicaciones, se evidencia los registros realizados	Sí
3	Clasificar la situación de seguridad de la información (evento o incidente) si se trata de un incidente se debe registrar el impacto sobre los activos de información. Todo ello se debe documentar en el registro de la herramienta de gestión. Si se clasifica como un incidente de seguridad de la información, este deberá ser remitido al Oficial de Seguridad de la Información del Ministerio de Agricultura y Desarrollo Rural, quien activará al ERISI. Ir al paso 4. © Si se clasifica como un evento de seguridad de la información, este deberá ser finalizado. Ir al paso 10.	A través del reporte suministrado por la Oficina de Tecnologías de la Información y las Comunicaciones, se evidencia la clasificación del incidente y el servicio que afecta. Desde noviembre -diciembre de 2022 y enero-abril de 2023, se encuentran 271 registrados de los incidentes; de los cuales al realizar el filtro por "P-CE-F-Reportar Spam" de la columna "Modelo", cuenta con 29 registros con el nuevo operador.	Sí
4	Realizar un plan de acción que le permita definir las actividades que se deben ejecutar con ocasión de la administración del Incidente de Seguridad. Para ello, determine los lugares a intervenir frente al recaudo de las evidencias, las acciones de contención, erradicación y recuperación, frente a los servicios y/o plataformas afectadas por la incidencia. Nota. Dentro de la planeación para la atención del incidente de seguridad, se debe tener en cuenta los tiempos, así como aquellas necesidades de recursos logísticos, humanos, áreas interesadas, entre otros aspectos.	Los eventos del reporte suministrado por la Oficina de Tecnologías de la información pertenecen a Incidente de Seguridad de la Información, razón por la cual, requiere Plan de Acción como salida. De acuerdo con la información suministrada por la Oficina de Tecnologías de la Información y las Comunicaciones, no existe como tal un Plan, existen correos con la solución del incidente. A través de correos electrónicos del 16 de junio de 2023, se enviaron las respectivas evidencias, en las cuales, se evidencia las acciones realizadas por la dependencia. Se presenta conformidad. Se recomienda evaluar o definir, qué es: "Plan de Acción", en el procedimiento.	Parcial
5	Recolectar las evidencias de los activos de MinAgricultura que con ocasión del incidente de seguridad se ven afectados. Para ello, se aplicarán los lineamientos propios de Cadena de Custodia e Informática Forense, preservando, ante todo, el valor probatorio de las pruebas que se recolecten. ©	De acuerdo con la información suministrada por la Oficina de Tecnologías de la Información y las Comunicaciones, los incidentes presentados en su evaluación realizada, no es necesario activar el ERISI, sino todo se realizado a través del Oficial de Seguridad y la persona que atiende actualmente el tema de seguridad. A través de correos electrónicos del 16 de junio de 2023, se enviaron los respectivos soportes, en las cuales, se evidencia las acciones realizadas por la dependencia. Se presenta conformidad.	Sí
6	Realizar una contención del incidente evitando cualquier tipo de propagación que pueda seguir afectando los activos de información del MinAgricultura. ©	A través del reporte suministrado por la Oficina de Tecnologías de la Información y las Comunicaciones, se evidencia la gestión realiza ante el evento. "Contención: Acciones necesarias para garantizar el control del incidente mientras se realiza un análisis más detallado y se definen las acciones necesarias para remediar el incidente"	Sí
7	Eliminar cualquier causa raíz que pudiera existir con ocasión de la incidencia presentada. Elaborar un plan de remediación, con la finalidad de poder cerrar las vulnerabilidades detectadas.	A través del reporte suministrado por la Oficina de Tecnologías de la Información y las Comunicaciones, se evidencia la gestión realiza ante el evento.	Sí

No	Actividad	Evaluación OCI	Cumple
8	Evaluar la necesidad de notificar y denunciar a los entes de control según sea el caso, las disposiciones establecidas frente a la ocurrencia de los incidentes de seguridad y su impacto dentro de MinAgricultura.	De acuerdo con la información suministrada por la Oficina de Tecnologías de la Información y las Comunicaciones, los incidentes presentados en su evaluación realizada, no es necesario la notificación y denuncia ante los entes de control.	Sí
9	Realizar un registro detallado de toda gestión de incidentes de seguridad, con el fin de poder desarrollar acciones correctivas para posteriores eventos o incidentes. Nota: Las acciones correctivas se adelantan aplicando el "Procedimiento acciones preventivas, correctivas y de mejora (PR-SIG-06)."	A través del reporte suministrado por la Oficina de Tecnologías de la Información y las Comunicaciones, se evidencia el registro en la Herramienta de Gestión. Por incidentes de seguridad de la información no se encuentra Solicitud de Acciones Preventivas, Correctivas o de Mejora.	Sí
10	Notificar al que reportó la situación de seguridad y cerrar el evento o incidente de Seguridad de la Información actualizando en la mesa de ayuda el estado del incidente.	A través del reporte suministrado por la Oficina de Tecnologías de la Información y las Comunicaciones, el equipo auditor revisó algunos casos y evidencia que se realizó la notificación al que reportó el evento de seguridad.	Sí

Tabla 19 – Elaboración equipo Auditor tomando como base el procedimiento de Gestión de Incidentes de Seguridad de la Información".

La Oficina de Tecnologías de la Información y las Comunicaciones, tiene identificado el siguiente riesgo, con respecto a la disponibilidad de la información digital en el MADR:

"*Posibilidad de afectación reputacional por la indisponibilidad de los servicios de TI requeridos por los usuarios institucionales para el desarrollo de actividades que aportan en el cumplimiento de la misionalidad institucional, debido a la deficiencia en la administración de la infraestructura tecnológica que soporta los servicios de TI institucionales*"; con los siguientes controles:

1. "*Los profesionales designados, deberán velar por el monitoreo periódico a los Servicios de Tecnología de la Información-TI, con el fin, de prestar los servicios tecnológicos de forma permanente*".
2. "*Los profesionales designados, deben garantizar la ejecución de los mantenimientos preventivos de conformidad en lo establecido en el procedimiento Mantenimiento Preventivo Infraestructura Tecnológica*".
3. "*El jefe de la Oficina de Tecnologías de la Información y las comunicaciones y los profesionales designados, deben velar por el correcto reporte a través de las herramientas de gestión de los Acuerdos de Niveles de Servicio–ANS, configurados de conformidad con el Catálogo de Servicios de Tecnologías de la Información-TI*".

El equipo auditor procedió a evaluar los controles. A través del correo del 21 de junio de 2023, la Oficina de Tecnologías de la Información y las comunicaciones nos informa para cada uno de los controles:

1. "*Se lleva a cabo el monitoreo desde la Herramienta SiteCope la cual es administrada por la Mesa de Servicios en el marco de sus obligaciones*".

   Se procedió a revisar las respectivas evidencias para los meses de noviembre-diciembre de 2022: en octubre acuerdo con la información suministrada por la dependencia un promedio del 99.80%, noviembre del 99.92% y diciembre del

98.90%, de todos los servicios.

Para el año 2023, en enero y febrero con un promedio de todos los servicios 99.4%, marzo 99,2, abril 99% y mayo 99.3%. Para el equipo auditor esta conforme, la dependencia está llevando a cabo el control del monitoreo periodo.

2. "*Se lleva a cabo los mantenimientos preventivos programados para la vigencia 2022 por parte de la Mesa de Servicio. Para la vigencia 2023 se tienen programados los mantenimientos preventivos para el segundo semestre de 2023, los cuales se tiene estipulado iniciar en el mes de julio*".

   Se procedió a revisar los respectivos soportes remitidos por la dependencia, se encuentra archivo Excel con el seguimiento realizado y el respectivo cronograma de mantenimientos de los equipos. Para el equipo auditor se cumplió con la actividad de mantenimiento preventivo.

3. "*En el marco del contrato vigente con la Mesa de Servicios, se cuenta con los Acuerdos de Niveles de Servicio para la vigencia 2022 – 2023*".

   La Oficina de Tecnologías de la información y las Comunicaciones, presentó los respectivos soportes relacionados con el cumpliendo de los acuerdos de Nivel para los años 2022 y 2023; las evidencias se relacionan con el monitoreo de los servicios, la Información se encuentra conforme.

En Conclusión, de acuerdo con los resultados de la evaluación, la Oficina de Tecnologías de la Información y las Comunicaciones está cumpliendo con el procedimiento "*Gestión de Incidentes de Seguridad de la Información*".

Igualmente, el riesgo "*Posibilidad de afectación reputacional por la indisponibilidad de los servicios de TI requeridos por los usuarios institucionales para el desarrollo de actividades que aportan en el cumplimiento de la misionalidad institucional, debido a la deficiencia en la administración de la infraestructura tecnológica que soporta los servicios de TI institucionales"*, se evaluaron dos controles establecidos por la dependencia para mitigar el riesgo, los cuales se están cumpliendo.

Por último, se recomienda revisar el procedimiento y determinar a que hace referencia en la actividad 4 el producto de "Plan de Acción", o realizar su respectiva definición.

3.4. Visita a dependencia con Áreas Seguras.

El equipo auditor procedió a realiza visita a la dependencia de Gestión Documental – Archivo del Mezanine ubicado en la carrera 10 No 16-92. El 29 de mayo de 2023, con el fin de verificar los riesgos a los cuales está sometido la información que se

encuentra almacenada en dicha área del Grupo de Gestión Documental y Biblioteca de la entidad.

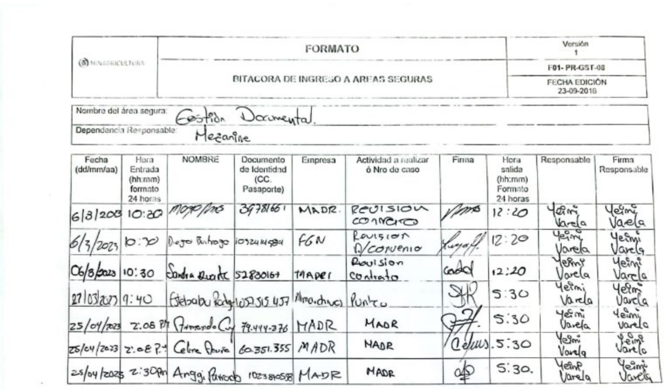
De acuerdo con el documento estratégico: "*DE-ALI-05- Política Institucional de Gestión Documental*", hace referencia a: "*El uso y acceso a los documentos se regirá por lo establecido en la Matriz de información Clasificada y Reservada, la matriz de clasificación de activos de información, estos definidos con código en F01-PR-ALI-26 Instrumentos de Gestión de Información Pública del MinAgricultura*" versión 1 del 20092022, razón por la cual, se procedió a revisar la matriz de Información Clasificada y Reservada unificada publicada en la página web de la entidad con el fin de verificar los riesgos a los cuales está sometida la información almacena en el archivo central.

Al realizar la consulta por la columna "*1. Proceso o Dependencia*" al Grupo de Gestión Documental", no se encontró activo de información asociado al archivo central e histórico de la entidad (se encuentran activos en "*Disponible Archivo de gestión*" desde el año 2013) y del archivo digital (cintas digitales), razón por la cual, no tiene identificado los riesgos asociados a los activos de información del archivo central, presentando una No conformidad en la Identificación de los activos de Informe conforme a lo dispuesto por el artículo 13 de la ley 1712 de 2014 "*Todo sujeto obligado deberá crear y mantener actualizado el Registro de Activos de Información haciendo un listado de: a) Todas las categorías de información publicada por el sujeto obligado; b) Todo registro publicado; c) Todo registro disponible para ser solicitado por el público*".

Sin embargo, la información documenta se encuentra sometida a riesgos de Acceso Indebido al área segura de almacenamiento de la información documentadas, para lo cual el equipo auditor procedió a verificar que el área contenga distintivos, la cual, presenta la siguiente información gráfica:

Gráfico 1 – Fotografía tomada en sitio - Visita.

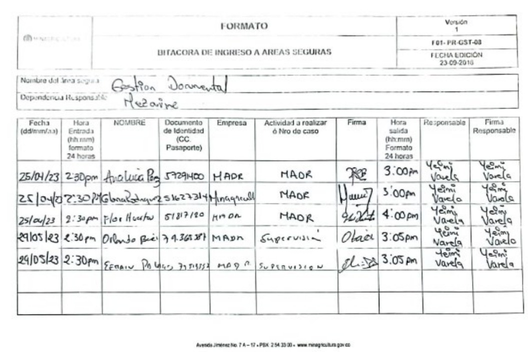
Igualmente, se realizó verificación con respecto al cumplimiento del procedimiento: "*PR–GST–08 - Acceso a Áreas Seguras de Almacenamiento de Información*", se evidenció el registro del ingreso al área, a través del formato "F01-PR-GST-08 - Bitácora de Ingreso a Áreas Seguras", versión 1 con lo muestra la siguiente gráfica:



MINAGRICULTURA	FORMATO	Versión 1
	BITACORA DE INGRESO A AREAS SEGURAS	F01- PR-GST-08
		FECHA EDICIÓN 23-09-2016

Nombre del área segura: Gestión Documental.
Dependencia Responsable: Mezanine

Fecha (dd/mm/aa)	Hora Entrada (hh:mm) formato 24 horas	NOMBRE	Documento de Identidad (CC. Pasaporte)	Empresa	Actividad a realizar ó Nro de caso	Firma	Hora salida (hh:mm) Formato 24 horas	Responsable	Firma Responsable
6/3/2023	10:20	[illegible]	39781661	MADR.	Revision convenio	[illegible]	12:20	Yeimi Varela	Yeimi Varela
6/3/2023	10:30	Diego Buitrago	1032414584	FGN	Revision A/convenio	[illegible]	12:20	Yeimi Varela	Yeimi Varela
06/3/2023	10:30	Sandra Duarte	52830167	TMAPEI	Revision contrato	[illegible]	12:20	Yeimi Varela	Yeimi Varela
27/03/2023	9:40	Esteban Rodg	1052.515.457	Almarchivos	Punteo	[illegible]	5:30	Yeimi Varela	Yeimi Varela
25/04/2023	2:08 PM	Armando Cruz	79.444.376	MADR	MADR	[illegible]	5:30	Yeimi Varela	Yeimi Varela
25/04/2023	2:08 PM	Celina Acuña	60.351.355	MADR	MADR	[illegible]	5:30	Yeimi Varela	Yeimi Varela
25/04/2023	2:30pm	Anggi Parrado	1023840558	MADR	MADR	[illegible]	5:30.	Yeimi Varela	Yeimi Varela



MINAGRICULTURA	FORMATO	Versión 1
	BITACORA DE INGRESO A AREAS SEGURAS	F01- PR-GST-08
		FECHA EDICIÓN 23-09-2016

Nombre del área segura: Gestion Documental
Dependencia Responsable: Mezanine

Fecha (dd/mm/aa)	Hora Entrada (hh:mm) formato 24 horas	NOMBRE	Documento de Identidad (CC. Pasaporte)	Empresa	Actividad a realizar ó Nro de caso	Firma	Hora salida (hh:mm) Formato 24 horas	Responsable	Firma Responsable
25/04/23	2:30pm	Analucia Paz	5729400	MADR	MADR	[illegible]	3:00pm	Yeimi Varela	Yeimi Varela
25/04/23	2:30PM	Gloria Rodriguez	51627314	Minagricultura	MADR	[illegible]	3:00pm	Yeimi Varela	Yeimi Varela
25/04/23	2:30pm	Flor Huerta	51817120	MADR	MADR	[illegible]	4:00pm	Yeimi Varela	Yeimi Varela
29/05/23	2:30pm	Orlando [illegible]	79.363.387	MADR	Supervisión	[illegible]	3:05pm	Yeimi Varela	Yeimi Varela
29/05/23	2:30pm	[illegible]	[illegible]	MADR	Supervision	[illegible]	3:05pm	Yeimi Varela	Yeimi Varela

Avenida Jiménez No. 7 A – 17 • PBX: 254 33 00 • www.minagricultura.gov.co

Gráfico 2 – Fotografía tomada en sitio – Visita a la Bitácora de Ingreso a Áreas Seguras.

Al contrastar la versión del formato actualmente publicada en el Sistema Integrado de Gestión – SIG con la información suministrada por la dependencia, no corresponde a la última versión, se encuentra publicada la versión 2 del mencionado formato y se utilizó la versión1, razón por la cual se recomienda la utilización de la última versión publicada en el SIG.

Por otro lado, los registros documentales también están sometida a los riesgos biológicos. La entidad cuenta con el procedimiento "*PR-ALI-20 – Planeación Documental*" versión 3 del 15072021, el cual determina "*Programa Monitoreo de condiciones Ambientales se implementará en el Formato Monitoreo de condiciones Ambientales F08-PR-ALI-20; el cual tiene como fin "Llevar control de las condiciones ambientales dentro de los depósitos""*, para ello cuenta en el área visita con dos equipos de control ambiental, con las placas de inventario: 32601 y 32602; mediante correo del 13062023 del Grupo de Gestión Documental nos informa que: "*se adjunta archivo comprimido reporte de Dataloggers del mes de noviembre y diciembre del 2022 hasta abril 2023 de los dos equipos para el monitoreo de las condiciones ambientales*", los cuales el equipó auditor procedió a verificar y cuenta con el reporte del control de la temperatura. Con respecto al formato, en el mencionado correo, también informan "*Se remiten los formatos diligenciados de noviembre a diciembre del 2022, para el reporte de enero a abril del 2023 es necesario aclara que el grupo de gestión documental no cuenta con el perfil de microbiólogo y/o conservador para realizar las lecturas respectivas y registrar los datos de análisis conforme a los resultados, sin embargo, la administración ya aprobó la contratación del mismo y realizaremos los respectivos reportes para el segundo trimestre*". Se procedió a revisar los mencionados archivos y cuenta con el respectivo análisis.

Así mismo, se puede presentar el riesgo de Integridad, disponibilidad y

confidencialidad de los archivos documentales, la entidad cuenta con el procedimiento "*PR-ALI-07-Organización, Transferencia, Consulta y Préstamo de Documentos*" versión 14 del 29092022, en donde se hace referencia al procedimiento de: "*6.3 – Consulta y Préstamo de Expedientes*", mediante correo del 13062023, el Grupo de Gestión Documental informa que: "*Como evidencia de la atención del servicio de atención de consulta, es necesario dar claridad que la mayoría de las consultas se dan respuesta con el expediente digital, por lo tanto, el préstamo en físico es mínimo*". En la visita realizada y de acuerdo con la información suministrada por la responsable del área visitada, actualmente y desde la pandemia, no se realiza el préstamo de la documentación física, se procede a digitalizar la información y se envía mediante correo institucional al interesado, esto con el fin, mantener la integridad, disponibilidad de los documentos y de acuerdo con la Matriz de Información clasificada y Reservada la confidencialidad de la información, el equipo auditor procedió verificar la información reportada y es conforme.

En Conclusión, de acuerdo con los resultados de la evaluación, el Grupo de Gestión documental y Biblioteca y el área visitada cumple con los requerimientos de disponibilidad, integridad y seguridad de la información. Sin embargo, No tiene identificado los activos de información relacionados con archivo central e histórico y del archivo digital (cintas digitales), en la herramienta dispuesta (Matriz de Instrumentos de Gestión de Información Pública, publicada en la web de la entidad), presentando una No conformidad en la Identificación de los activos de Informe conforme a lo dispuesto por el artículo 13 de la ley 1712 de 2014 "*Todo sujeto obligado deberá crear y mantener actualizado el Registro de Activos de Información haciendo un listado de: a) Todas las categorías de información publicada por el sujeto obligado; b) Todo registro publicado; c) Todo registro disponible para ser solicitado por el público*"; al no presentar Activo de Información relacionado no se tiene la identificación documental del riesgo y los controles asociados.

Adicionalmente, se recomienda a la administración establecer una oportunidad de mejora estructurando un procedimiento para la creación de áreas seguras, los mecanismos para la identificación del área, sus condiciones de seguridad y controles ambientales.

3.5. Evaluar los Indicadores de SGSI de los procesos de Gestión y Gobierno de la Información – TI y Gestión de Servicios Tics.

De acuerdo con la caracterización, de los procesos de Gestión y Gobierno de Tecnologías de la Información y las Comunicaciones y Servicios TIC cuenta con cuatro indicadores relacionados con seguridad de la Información:

NOMBRE	OBJETIVO	RELACIÓN MATEMÁTICA	FRECUENCIA DE MEDICIÓN	TIPO DE INDICADOR
Eficacia de cumplimiento del PETI Institucional	Medir el avance en la implementación del plan estratégico de tecnologías de la información institucional.	Porcentaje total ejecutado anual / Porcentaje total programado anual * 100	Semestral	Eficacia
Eficacia en la implementación de controles del sistema de gestión de seguridad de la información.	De controles del sistema de gestión de seguridad de la información de acuerdo con la declaratoria de aplicabilidad	Número de controles implementados / Número de controles contenidos en la declaratoria de aplicabilidad del SGSI * 100	Anual	Eficacia
Efectividad de los controles implementados del SGSI	Medir la eficiencia y efectividad de os controles implementados en el SGSI	Número de incidentes de seguridad de la información atendidos satisfactoriamente / Número de incidentes de seguridad de la información reportados * 100	Anual	Efectividad
Eficacia en la atención de incidentes al centro de servicios (TEAM)	Medir la capacidad de respuesta a los incidentes atendidos	Incidentes resueltos / Total incidentes recibidos * 100	Trimestral	Eficacia

Tabla 20 – Información extraída de la Caracterizaciones de los Proceso de Gestión y Gobierno de TI y Servicios TICS

Para la evaluación se consultó la publicación actual en la página web de la entidad, la cual se encuentra publicada con corte al cuarto trimestre de 2022, con los siguientes resultados:

Nombre	Objetivo	Frecuencia de Medición	Meta	Meta Cumplida	Información IV Trimestre de 2022
Eficacia de cumplimiento del PETI Institucional	Medir el avance en la implementación del plan estratégico de tecnologías de la información institucional	Semestral		97%	Se realiza el seguimiento físico y presupuestal de los proyectos del Plan Estratégico de Tecnologías de la Información (PETI).
Eficacia en la implementación de controles del sistema de gestión de seguridad de la información.	De controles del sistema de gestión de seguridad de la información de acuerdo con la declaratoria de aplicabilidad	Anual		99%	Se dio continuidad a las actividades de implementación de controles del SGSI
Efectividad de los controles implementados del SGSI	Medir la eficiencia y efectividad de os controles implementados en el SGSI	Anual		96%	Los incidentes de seguridad reportados fueron atendidos a través de la mesa de servicios con atención por parte del Oficial de Seguridad de la Entidad
Eficacia en la atención de incidentes al centro de servicios (TEAM)	Medir la capacidad de respuesta a los incidentes atendidos	Trimestral		100%	Total, Incidentes Recibidos: 138 Incidentes atendidos: 138 En el cuarto trimestre del año se registraron 138 incidentes para todas las líneas de servicio, los cuales en su totalidad se atendieron dentro del tiempo estipulado y a satisfacción de usuario final

Tabla 21 Complementada por equipo auditor con la Información del Reporte Publicado en la WEB con corte al IV Trimestre de 2022.

El equipo Auditor procedió a revisar la información suministrada por la Oficina de Tecnologías de la información para el indicador: “Eficacia en la atención de incidentes”, cuya medición es trimestral; se realizó consulta al archivo Excel enviado por la dependencia para el último trimestre de 2022; contiene 86 registros de los 138 reportados. Los 86 registros corresponden al operador actual de la mesa de servicios, reporta desde el 18 de noviembre de 2022.

Así mismo, se revisó los informes de la mesa de servicios, correspondiente al mes de noviembre, que hace referencia al periodo 13-30 de noviembre de 2022 reporta 23 incidentes y en informe de diciembre 63 casos, para un total de 86 registros.

En relación con los demás indicadores para la vigencia 2022, las evidencias suministradas por la Oficina de Tecnologías para el indicador “PETI”, no corresponde a evidencia de avances, “Controles con declaratoria de aplicabilidad,

la información suministrada no corresponde a avance del indicador y "Medir la eficacia", se comparten las mismas evidencias del anterior indicador, razón por la cual, hecho por el cual, no fue posible evaluar su cumplimiento.

Igualmente se encuentra publicada la información con corte al primer trimestre de 2023, con la siguiente información para todos los tres primeros indicadores "*Aún no se ha tenido información del primer trimestre respecto a este indicador*", pero la medición es Semestral y Anual, está conforme; para el último indicador se hace referencia a la siguiente información: "T*otal, Incidentes Recibidos: 145; Incidentes atendidos: 138. En el primer trimestre del año se registraron 145 incidentes para todas las líneas de servicio, de los cuales 138 fueron atendidos a satisfacción del usuario final*". Con un reporte del 95%. El equipo auditor procedió a revisar las respectivas evidencias enviadas por la Oficina de Tecnologías de la Información y las Comunicaciones, presentando coincidencia con la información reportada, con categoría de incident 142 y Support Catalog 3. Con respecto a los incidentes de seguridad corresponde a 17 registros para el primer trimestre de 2023.

En conclusión, la Oficina de Tecnología de la Información y las Comunicaciones, no presentó las evidencias de cumplimiento en su totalidad para la vigencia de 2022, razón por la cual, no se evaluó su cumplimiento. Con respecto al año 2023, el equipo auditor evidenció su cumplimiento a través de los archivos suministrados del indicador trimestral.

3.6. Evaluar los Riesgos y Controles asociados a los Activos de Información "Matriz_Instrumentos_de_Gestión_de_Información_Publica" publicada.

El equipo auditor procedió a consultar la matriz de Instrumentos de Información Pública que se encuentra publicado en la página web del Ministerio de Agricultura y Desarrollo Rural en la siguiente ruta:

https://www.minagricultura.gov.co/Paginas/Transparencia/Instrumentos-de-Gestion-de-Informacion-Publica.aspx; 7.1.d. Matriz Unificada Instrumentos de Gestión de Información Pública.

La matriz cuenta con 225 activos de Información identificados por la entidad, el equipo auditor revisó la mencionada matriz y para su evaluación realizó una reclasificación global con los siguientes resultados:

Concepto	Activos Identificados	Concepto	Activos Identificados
Acciones Constitucionales	1	Informes	43
Actas	11	Instrumentos	39
Actos Administrativos	5	Inventarios	6

Concepto	Activos Identificados	Concepto	Activos Identificados
Acuerdos	6	Manual de procesos y procedimientos	5
Base de Datos Estructurada	3	Nomina	1
Certificaciones	3	Planes	10
Comprobantes	2	Políticas	5
Conceptos	6	PQRSD	34
Conciliaciones	1	Procesos	4
Control de documentos	3	Programas	3
Deposito Legal de Obras	1	Proyectos	10
Diagnósticos	1	Registros	1
Estudios	1	Reportes	3
Historias	2	Soportes Documentales	15
		Total	225

Tabla 22 Elaborada equipo auditor con base a la información publicada en la página web de la entidad de los Activos de Información.

Igualmente, se procedió a revisar la información suministrada por la Oficina de Tecnologías de la Información y las Comunicaciones, documento denominado "Inventario_Activos_Actualizado", y se procedió para su evaluación una reclasificación global con los siguientes resultados:

Concepto	Activos Identificados	Concepto	Activos Identificados
Acciones de Tutela y Desacatos	1	Manual de procesos y procedimientos	6
Actas	8	Nóminas	2
Actos administrativos	2	Personas	149
Base de datos	62	Personería Jurídica	1
Boletines	3	Piezas Gráficas	2
Certificaciones	6	Planes	13
Comprobantes	3	Políticas	8
Conceptos	1	PQRSD	24
Documentos	5	Procesos	11
Equipos	14	Proyectos	9
Estudios	1	Registros	3
Hojas de Vida	1	Reportes	4
Informes	38	Servicios digitales	6
Instrumentos	22	Soportes Documentales	34
Inventarios	1	Total, General	440

Tabla 23 Elaborada equipo auditor con base a la información Suministrada por la Oficina de Tecnologías de la Información relacionada con los Activos de Información.

Como se puede observar entre las tablas anteriores, existe una diferencia entre la

información de los activos de Información que actualmente están publicados en la página web y la información suministrada por la Oficina de Tecnologías de la Información y registrada en el aplicativo que la entidad tiene destinada para tal fin, teniendo en cuentas los siguientes aspectos:

En el primer archivo (publicado en la página web) cuenta con 225 activos de información y el segundo archivo con 440, presentándose una diferencia notable de 215 registros. Adicionalmente se encuentran activos de información repetidos como es el caso de "*Conocimiento Profesional Especializado en Contabilidad*" y "*Formatos diligenciado de solicitud de trámites en el SIIF Nación*", adscritos al subdirector financiero, por las anteriores razones, no se encuentra identificados todos los activos de información en el Ministerio de Agricultura y Desarrollo Rural de acuerdo con los lineamientos y normativa del Ministerio de las Tecnologías y las Comunicaciones publicados en la página web de la entidad, presentando una No Conformidad.

Igualmente, al realizar la discriminación en la diferencia de registros, corresponde a los siguientes conceptos: 149 registros de personas, 14 de equipos, 6 de Servicios digitales, 46 registros de Base de Datos (Sistemas, credenciales, software, administración de herramientas). Adicionalmente al realizar el cruce de información entre ambas tablas por campo nombre de los activos de información (225 registros) no coinciden en su totalidad, solo coinciden 34 registros publicados, presentando una No conformidad en la Identificación de los riesgos asociados a los activos de información de acuerdo con lo dispuesto por la política de la entidad: "*Para el establecimiento de los riesgos de seguridad de la información se deben tener en cuenta los activos de información identificados en cada proceso, donde se pueden identificar tres (3) tipos de riesgos: pérdida de confidencialidad, de la integridad y de la disponibilidad de los activos de información. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice*".

Se continuo con el análisis por parte del equipo auditor, con respecto al cumplimiento de los lineamientos de la información básica que debe contener los activos de información según el Manual "maestro MSPI Inventario de Activos", se presenta la siguiente evaluación:

Información Básica	Descripción	Cumple Publicada en WEB	Cumple Suministrada TI
Identificador	Número consecutivo único que identifica al activo en el inventario.	No	No
Proceso	Nombre del proceso al que pertenece el activo	No	No
Nombre Activo	Nombre de identificación del activo dentro del proceso al que pertenece.	Sí	Sí
Descripción/Observaciones	Es un espacio para describir el activo de manera que sea claramente identificable por todos los miembros del proceso.	Sí	Sí
Ubicación	Describe la ubicación tanto física como electrónica del activo de información.	Sí	Sí

Información Básica	Descripción	Cumple Publicada en WEB	Cumple Suministrada TI
Propietario	Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso se clasifican adecuadamente. Deben definir y revisar periódicamente las restricciones y clasificaciones del acceso.	Sí	Sí
Custodio	Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de hacer efectivos las restricciones y clasificaciones de acceso definidos por el propietario. (Para sistemas de información o información consignada o respaldada, generalmente es TI o para información física, los custodios pueden ser los funcionarios o el proceso de archivo o correspondencia, el custodio generalmente se define donde reposa el activo original).	No	No
Tipo	Define el tipo al cual pertenece el activo. Para este campo se utilizan los siguientes valores:	No	Sí

Tabla 24 Elaborada equipo tomando como base los lineamientos del Mintic en el Manual de MSPI – Activos de Información.

Como se puede observar en la tabla 24, la matriz publicada en el web cumple con algunos de los lineamientos establecidos por el Ministerio de TIC, y en la información suministrada por la Oficina de Tecnología de la Información - OTIC y las Comunicaciones, también cumple parcialmente.

Adicionalmente para el campo “Tipo”, la OTIC, no tiene en cuenta las posibles opciones relacionadas en el “Maestro mpsi Inventario de Activos” y “maestro mpsi gestión del Riesgo” por ejemplo: activos de información identificados como “equipos de cómputo”, su clasificación corresponde a “Hardware”, pero la tiene clasificada como “físicos”.

Posteriormente el equipo auditor procedió a revisar el documento “Riesgos Intelisis” enviada por la Oficina de Tecnologías de la Información y las Comunicaciones a través de correo del 16 de junio de 2023, el archivo consta de 414 registros de activos de información de los 440 registros inicialmente identificados, presentándose una diferencia de 26 registros, el equipo auditor, con los elementos suministrados, no puedo establecer a que corresponde esta situación y la Oficina de Tecnologías de la Información y las Comunicaciones, preguntado, tampoco nos informó al respecto.

Igualmente, para la valoración del Riesgo, se consultó la política de riesgo de la entidad, y para el nivel de Riesgo se cuenta con la siguiente interpretación en la calificación:

Nivel de Riesgo	Descripción
1 – 24 Bajo	No es necesario adoptar ninguna medida. El nivel de riesgo es suficientemente bajo y no justifica la implantación de controles adicionales.
25 – 48 Moderado	La dirección de la empresa, o un delegado de esta, determinará el nivel de los riesgos que son aceptables o no a su juicio. El responsable de Seguridad que gestiona el SGSI determinará los controles que tendrán que aplicarse para mitigar los riesgos.

Nivel de Riesgo	Descripción
49 – 75 Alto	El nivel de riesgos no es aceptable, y sólo se podrán excluir controles que los mitiguen justificando dicha exclusión por parte de la dirección de la empresa. El responsable de Seguridad que gestiona el SGSI determinará los controles que tendrán que aplicarse para mitigar los riesgos.

Tabla 25 Extracción del documento de Política de Administración del Riesgo V12 de la entidad

De acuerdo con la anterior descripción se presenta la siguiente estadística de los activos de información de acuerdo con el reporte entregado por la Oficina de Tecnologías de la Información y las Comunicaciones:

1. Riesgo inherente, presenta la siguiente evaluación por parte de las dependencias:

Nivel de Riesgo	Riesgo Inherente		
	Confidencialidad	Integridad	Disponibilidad
1 – 24 Bajo	122	7	34
25 – 48 Moderado	105	219	380
49 – 75 Alto	0	0	0
Sin Valoración	187	188	0
Total	414	414	414

Tabla 26 Elaborada equipo auditor teniendo como base la información suministrada por la Oficina de Tecnología la Información y las comunicaciones.

Riesgo Residual, después de aplicar los respectivos controles, se presenta la siguiente evaluación por parte de las dependencias de la entidad:

Nivel de Riesgo	Riesgo Residual		
	Confidencialidad	Integridad	Disponibilidad
1 – 24 Bajo	227	226	414
25 – 48 Moderado	0	0	0
49 – 75 Alto	0	0	0
Sin Valoración	187	188	0
Total	414	414	414

Tabla 27 Elaborada equipo auditor teniendo como base la información suministrada por la Oficina de Tecnología la Información y las comunicaciones.

Nota: Con respecto a los activos sin valoración de los componentes de Confidencialidad e Integridad corresponde a: administración de herramientas (Inversión, Sisconpes, leche, aplicaciones, legalización de tiquetes), Sistemas (misionales, operacionales, usuario final), equipos (almacenamiento, conectividad, telefonía, disco externo, usuario final) y sistema (Agrocomercio, KOHA, Gestión de activos, SIOC, SIRIAGRO, SPI, EKOGUI, FURAG, SGR, ORFEO, Traza). Se contacto a la Oficina de Tecnologías de la Información y las Comunicaciones, a través de la reunión el 23 de junio de 2023, para solicitar las respectivas

explicaciones, pero expresaron que realizaran las consultas pertinentes.

Con respecto a los controles, el equipo auditor solicitó a la Oficina de Tecnologías de la Información y las Comunicaciones, a través de la mencionada reunión, la necesidad de contar con la información en un archivo Excel de los controles aplicados a los activos de información, con el fin, de realizar el respectivo análisis y evaluación. Pero no fue posible, debido a que la OTI, realizó consultas al proveedor, y este a través de correo del 23 de junio de 2023 respondió que:

"*En cuanto a los puntos 1 a 3, no hay función de exportar esa información, básicamente por la complejidad del modelo de datos y las relaciones, dependencias y restricciones entre registros del análisis de riesgos. Esa información se presenta "en vivo" durante el proceso de auditoría ya que la propia herramienta es el elemento de operación de la gestión de la seguridad y contenedor de las evidencias completamente trazables que genera. Respondiendo al punto 4, los activos se categorizan por tipo, cada tipo tiene un árbol de amenazas / vulnerabilidades inherentes que hay que evaluar según el entorno de amenaza del activo. Este entorno puede dar lugar a que existan amenazas que no están presentes en el entorno, y que, entre activos del mismo tipo, con diferente entorno, las mismas amenazas tengan diferentes valores. Las valoraciones se hacen según este entorno, con lo cual, el resultado del riesgo es el riesgo existente para ese activo. Luego, tras la definición de la gestión del riesgo (aceptar, tratar, eliminar, evitar) se valora el riesgo residual. Todo esto definido en la metodología de análisis de riesgos*".

El equipo auditor recomienda a la Oficina de Tecnologías de la Información evaluar este aspecto en cuanto a las limitantes del Sistema Intelisis, este aunado a que, no es posible la creación de un usuario de consulta para su verificación y evaluación por parte de la Oficina de Control Interno. Sin embargo, se cuenta con las descripciones de los controles aplicados en la respectiva herramienta de Intelisis, con el mencionado agravante, de no tener identificados los riesgos a todos los activos de información publicados en la página web de la entidad. Al revisar los riesgos de seguridad de la información publicados en la página web de la entidad, se presenta diferencia entre los activos de información registrados en la herramienta y los publicados en la web, implicando que no se encuentran aprobados todos los riesgos y controles por los responsables de los procesos, razón por la cual, se recomienda revisar y ajustar dicha información.

En conclusión, el equipo auditor realizó la respectiva evaluación, encontrando que se está cumpliendo con los lineamientos relacionados con los activos de información con las siguientes excepciones:

- Existe una diferencia entre los activos de Información que actualmente están publicados en la página web y la información suministrada por la Oficina de Tecnologías de la Información, teniendo en cuenta que el archivo publicado en la página web cuenta con 225 y el segundo con 440 respectivamente, presentándose una diferencia notable de 215 registros y

encuentran activos de información repetidos como es el caso de "*Conocimiento Profesional Especializado en Contabilidad*" y "*Formatos diligenciado de solicitud de trámites en el SIIF Nación*", adscritos al subdirector financiero, razones por las cuales, no se encuentra identificados todos los activos de información en el Ministerio de Agricultura y Desarrollo Rural de acuerdo con los lineamientos y normativa del Ministerio de las Tecnologías y las Comunicaciones y que deben estar publicados en la página web de la entidad, presentando una No Conformidad.

- Al realizar el cruce entre la información publicada en la web y la suministrada por la Oficina de Tecnologías de la Información por campo "*nombre de los activos de información*", de los 225 registros, tan solo coinciden 34 registros publicados, presentando una No conformidad en la Identificación de los riesgos asociados a los activos de información de acuerdo con lo dispuesto por la política de la entidad: "*Para el establecimiento de los riesgos de seguridad de la información se deben tener en cuenta los activos de información identificados en cada proceso, donde se pueden identificar tres (3) tipos de riesgos: pérdida de confidencialidad, de la integridad y de la disponibilidad de los activos de información. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice*".

3.7. Evaluar la ejecución presupuestal asignada al SGSI.

Para el año 2022, la Oficina de Tecnologías de la Información y las Comunicaciones, estableció un presupuesto de $704.975.250, para el Sistema de Gestión de Seguridad de la información - SGSI.

De acuerdo la información suministrada por la Subdirección Financiera la ejecución presupuestal para el rubro C-1799-1100-15-0-1799065-02, relacionado con el objetivo "*4. Fortalecer la gestión de servicios tecnológicos y de seguridad de la información*" del proyecto de inversión: *"Fortalecimiento de la Gestión de Tecnologías de la Información - TI en el Ministerio de Agricultura y Desarrollo Rural en Función de la Transformación Digital del Sector Agropecuario"*; se procedió a consultar la información a 31 de diciembre de 2022, el cual, contine el siguiente resumen:

DESCRIPCIÓN	APR. VIGENTE	CDP	COMPROMISO	OBLIGACIÓN	ORDEN PAGO
ADQUISICIÓN DE BIENES Y SERVICIOS - SERVICIOS TECNOLÓGICOS - FORTALECIMIENTO DE LA GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN - TI EN EL MINISTERIO DE AGRICULTURA Y DESARROLLO RURAL EN FUNCIÓN DE LA TRANSFORMACIÓN DIGITAL DEL SECTOR AGROPECUARIO. BOGO	$ 7.867.797.700,00	$ 7.595.698.895,15	$ 7.121.717.556,27	$ 5.782.555.491,55	$ 5.782.555.491,55

Tabla 28 Elaborada equipo tomando como base la Información suministrada por la Subdirección Financiera de la entidad.

Igualmente, el mencionado objetivo cuenta con dos actividades, uno específicamente relacionado con SGSI y tiene definida una asignación presupuestal de $704.975.250, incluida en el rubro mencionado y de acuerdo con

la información suministrada por la Oficina de Tecnologías de la Información y las Comunicaciones tiene la siguiente discriminación:

ACTIVIDAD	APR. ASIGNADA	COMPROMISO	OBLIGACIÓN	PAGOS
4.1.2. Evaluar, planificar, implementar y realizar seguimiento a la estrategia de seguridad de la información institucional.	$ 704.975.250,00	$ 704.780.682,50	$ 704.780.682,50	$ 704.780.682,50

Tabla 29 Elaborada equipo tomando como base la Información suministrada por la Oficina de Tecnologías de la Información.

Como se puede observar se ejecutó 99.97% del presupuesto asignado para el tema de la estrategia de seguridad de la información institucional.

Para la vigencia 2023, el objetivo 4, se encuentra actividad relacionada con la seguridad de la Información: "*4.1.2. Evaluar, planificar, implementar y realizar seguimiento a la estrategia de seguridad de la información institucional*", con una asignación presupuestal proyectada de $2.351.912.500, para el Sistema de Gestión de Seguridad de la información.

El equipo auditor procedió a consultar la información suministrada para la vigencia 2023, para el rubro C-1799-1100-15-0-1799065-02 con corte a mayo de 2023, y que se relaciona con el objetivo 4 presenta la siguiente discriminación:

DESCRIPCIÓN	APR. VIGENTE	CDP	COMPROMISO	OBLIGACIÓN	ORDEN PAGO	PAGO
ADQUISICIÓN DE BIENES Y SERVICIOS - SERVICIOS TECNOLÓGICOS - FORTALECIMIENTO DE LA GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN - TI EN EL MINISTERIO DE AGRICULTURA Y DESARROLLO RURAL EN FUNCIÓN DE LA TRANSFORMACIÓN DIGITAL DEL SECTOR AGROPECUARIO. BOGO	$ 10.172.888.474,00	$ 6.315.168.657,44	$ 3.317.552.159,25	$ 371.230.241,18	$ 316.845.935,97	$ 316.845.935,97

Tabla 30 Elaborada equipo tomando como base la Información suministrada por la Subdirección Financiera de la entidad.

De acuerdo con la información suministrada por la Oficina de Tecnologías de la Información y las Comunicaciones, entre el periodo comprendido enero – abril de 2023, aun no se ha comprometido los recursos destinados para la actividad relacionada con el Sistema de Gestión de Seguridad de la Información - SGSI y se encuentran en el proceso de contratación. Aun, no se ha comenzado la ejecución de los $2.351.912.500, asignados para el desarrollo del SGSI.

En Conclusión, de acuerdo con los resultados de la evaluación, el sistema de Gestión de Seguridad de la Información – SGSI, para la vigencia de 2022, contó con los recursos para su operación. Con respecto a la vigencia 2023, se tiene previsto un presupuesto de $2.351.912.500, pero que aun, no se han comprometido para la vigencia. La OCI recomienda a la Oficina de Tecnologías de la Información y las Comunicaciones, realizar todas las gestiones para asegurar el funcionamiento óptimo del SGSI para esta vigencia.

3.8. Evaluar los riesgos del SGSI y controles los procesos de Gestión y Gobierno de la Información - TI y Gestión de Servicios Tics.

La evaluación del riesgo se realizó a través de los ítems tratados con anterioridad, sin embargo, se presenta la siguiente consideración con respecto al Riesgo: "P*osibilidad de afectación reputacional por no tener en cuenta los lineamientos de MinTic en materia de TI, para la orientación en la formulación de estrategias, instrumentos y herramientas, debido al desconocimiento de la normatividad y lineamientos existentes*". De acuerdo con el desarrollo del ítem 1, es posible la materializó el riesgo, razón por la cual, se recomienda evaluar los controles para mitigar este posible riesgo para el proceso de Gestión y Gobierno de las Tecnologías de la Información y las Comunicaciones.

Con respecto al riesgo: "*Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin del uso indebido de privilegios de TI para acceder a los sistemas de información*".

La Oficina de Tecnologías de la Información y las Comunicaciones estableció el siguiente control: "*El jefe de la Oficina TIC y los profesionales designados deben establecer acuerdos de confidencialidad y de manejo de la información para aquellos roles que cuentan con privilegios de TI, con el fin de evitar fugas de información y usos inadecuados de esta*".

A través del correo del 21 de junio de 2023, la Oficina de Tecnologías de la Información y las comunicaciones nos informa: "*Se alojan en la ruta indicada los acuerdos de confidencialidad de todos los integrantes de la Mesa de Servicios*", el equipo auditor procedió a revisar las respectivas evidencias las cuales consta de 23 archivos con los acuerdos de confidencialidad que cuentan con privilegio de TI para la mesa de servicio, la cual, se encuentra conforme.

Con respecto al riesgo mencionado con anterioridad, su clasificación corresponde a Riesgo de Corrupción, la Guía para la Administración del riesgo en entidades públicas presenta la siguiente definición para riesgo de corrupción: "*Riesgo de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado*", y fraude Interno como "*Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros*". De acuerdo con la definición de Riesgo de Corrupción, es usar el poder para desviar la gestión de lo público hacia beneficio privado, no se observa explícitamente en el riesgo identificado, razón por la cual, se recomienda la evaluación de este riesgo para establecer dicha condición.

En conclusión, para el equipo auditor es posible se materialice el riesgo: "P*osibilidad*

de afectación reputacional por no tener en cuenta los lineamientos de MinTic en materia de TI, para la orientación en la formulación de estrategias, instrumentos y herramientas, debido al desconocimiento de la normatividad y lineamientos existentes", de acuerdo con lo manifestado en el ítem 3.1 de la evaluación del Sistema de Gestión de Seguridad de la información, para lo cual se recomienda la evaluación de los controles y así mismo la revisión y evaluación del riesgo de corrupción.

ASPECTOS ENCONTRADOS: (Conformidades y no conformidades)

ASPECTOS PARA MEJORAR:			
ÍTEM	**NC[1]/O [2]**	**SITUACIONES ENCONTRADAS**	**RECOMENDACIÓN Y/O SUGERENCIAS[3]**
1	NC	**Oficina de Tecnologías de la Información y las Comunicaciones – Oficial de Seguridad – Oficina Asesora de Planeación y Prospectiva** En relación con los roles y responsables se evidenció un cumplimiento parcial, de acuerdo con los lineamientos establecidos en el documento "*maestro MSPI - Roles y Responsabilidad*", entre ellos hace falta la creación del Comité de Seguridad y privacidad de la información, dependiente del Comité Institucional de Gestión y Desempeño Institucional (este comité es opcional, pero al interior de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC, existe un comité o grupo que se encarga de mitigar el riesgo, dirigido a la información digital, cuyo objeto sería la definición para todo el SGSI) , de la falta de la definición de los roles de la Oficina Asesora Jurídica, del Grupo de Gestión Documental y de los demás que se requieran el SGSI, en el caso del Oficial de Seguridad, el lineamiento es, que no pertenezca a la OTIC.	Tener en cuenta todos los lineamientos establecidos por Mintic en el documento maestro mspi Roles y Responsabilidad, tal y como se tuvo en cuenta en el "MN-GGT-01 Manual de Tratamiento y Protección de Datos Personales", incluyendo a los roles del Grupo de Gestión Documental, Grupo de Contratos entre otros.
2	NC	**Grupo de Gestión Documental y Biblioteca y Oficial de Seguridad – Oficina Asesora de Planeación y Prospectiva**. El procedimiento "PR-ALI-26 - Esquema de publicación de Información Pública", versión 2, no determina la periodicidad de la actualización de la identificación y clasificación de la información de acuerdo con los lineamientos del MSPI ".	Actualizar el inventario y la clasificación de los activos por los propietarios y custodia de los activos de forma periódica o toda vez que exista un cambio en el proceso.
3	NC	**Oficina de Tecnologías de la Información y las Comunicaciones – Oficial de Seguridad – Oficina Asesora de Planeación y Prospectiva**	Incluir en el PIC de cada Vigencia el Plan de Cambio, cultura, apropiación, capacitación y sensibilización de seguridad y Privacidad de la Información

[1] *NC: No Conformidad. Significa incumplimiento de un requisito legal o de cualquier requisito especificado en los procedimientos de nuestro sistema de gestión de la calidad, por lo que ameritan la implementación de un Plan de Acción, diligenciando el formato Solicitud de Acciones Preventivas, Correctivas o de Mejora - F01-PR-SIG-06.*

[2] *O: Oportunidad de mejora. Son deficiencias del proceso que, aunque no sean recurrentes o relevantes, pueden convertirse en incumplimientos o en riesgos potenciales.*

[3] *Propuesta constructiva y objetiva frente a la situación identificada.*

ASPECTOS PARA MEJORAR:			
ÍTEM	**NC[1]/O [2]**	**SITUACIONES ENCONTRADAS**	**RECOMENDACIÓN Y/O SUGERENCIAS[3]**
		Plan de Cambio, cultura, apropiación, capacitación y sensibilización de seguridad y Privacidad de la Información y seguridad digital, para la vigencia 2023 no cuenta con la respectiva información. Adicionalmente se revisó el PIC, y no contempla actividades asociadas con el tema de Seguridad, presentando una No Conformidad.	y seguridad digital.
4	O	**Oficina Asesora de Planeación y Prospectiva** Con respecto al contexto y las partes interesadas de la entidad, evidencia el cumplimiento de estos factores. Sin embargo, se recomienda establecedor una oportunidad de mejora, para que los documentos del contexto y de las partes interesadas formen parte del Sistema Integrado de Gestión de la entidad, con el fin, que Planeación Institucional tenga instrumentos generales de planeación para los procesos y para el Sistema de Gestión de la Seguridad de la Información.	Elaborar, por parte de la Oficina Asesora de Planeación y Prospectiva con apoyo de todas las dependencias de la entidad los documentos del Contexto Interno y Externo, y de las partes interesadas como documentos independientes y se publique en el Sistema Integrado de Gestión.
5	NC	**Grupo de Gestión documental y Biblioteca – Oficial de Seguridad.** En el marco de la presente auditoría la Oficina de Control Interno evidencio que no se tiene identificado los activos de información relacionados con archivo central e histórico y del archivo digital (cintas digitales), en la herramienta dispuesta (Matriz de Instrumentos de Gestión de Información Pública, publicada en la web de la entidad), presentando una No conformidad en la Identificación de los activos de Informe conforme a lo dispuesto por el artículo 13 de la ley 1712 de 2014 “Todo sujeto obligado deberá crear y mantener actualizado el Registro de Activos de Información haciendo un listado de: a) Todas las categorías de información publicada por el sujeto obligado; b) Todo registro publicado; c) Todo registro disponible para ser solicitado por el público”; al no presentar Activo de Información relacionado no se tiene la identificación documental del riesgo y los controles asociados.	Evaluar la matriz de los activos de información con el ánimo de mantener la identificación documental del riesgo y los controles asociados.
6	NC	**Grupo de Gestión Documental y Biblioteca y Oficial de Seguridad – Oficina Asesora de Planeación y Prospectiva, con la participación y aprobación de las dependencias del MADR.** Existe una diferencia entre los activos de Información publicados en la página web y la información suministrada para la evaluación del riesgo. El archivo publicado en web cuenta con 225 registros y el segundo con 440 respectivamente, presentándose una diferencia notable de 215 registros y se encuentran activos de información repetidos como es el caso de	

ASPECTOS PARA MEJORAR:			
ÍTEM	**NC[1]/O [2]**	**SITUACIONES ENCONTRADAS**	**RECOMENDACIÓN Y/O SUGERENCIAS[3]**
		"Conocimiento Profesional Especializado en Contabilidad" y "Formatos diligenciado de solicitud de trámites en el SIIF Nación", adscritos al subdirector financiero, razones por las cuales, no se encuentra identificados todos los activos de información en el Ministerio de Agricultura y Desarrollo Rural de acuerdo con los lineamientos y normativa del Ministerio de las Tecnologías y las Comunicaciones.	
7	NC	**Oficina de Tecnologías de la Información y las Comunicaciones – Oficial de Seguridad con la participación y aprobación de las dependencias del MADR.** Al realizar el cruce entre la información publicada en la web y la valoración del riesgo por campo "nombre de los activos de información", de los 225 registros, tan solo coinciden 34 registros publicados, contraviniendo lo dispuesto por la política de la entidad: "*Para el establecimiento de los riesgos de seguridad de la información se deben tener en cuenta los activos de información identificados en cada proceso, donde se pueden identificar tres (3) tipos de riesgos: pérdida de confidencialidad, de la integridad y de la disponibilidad de los activos de información. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice*".	Actualizar constantemente la información de las bases de datos a fin de que, al consultarla, esta sea real y verídica.
8	NC	**Oficina de Tecnologías de la Información y las Comunicaciones.** Incumplimiento a la Política Específica de Seguridad y Privacidad de la Información, dado que no se cuenta con elementos necesarios para la realización de copias de respaldo para salvaguardar la información al exterior de la Entidad.	Mantener la continuidad del contrato de copias de respaldo con el ánimo de que, si ocurre alguna catástrofe, se pueda respaldar la información en cualquier otro sitio.
9	NC	**Oficina de Tecnologías de la Información y las Comunicaciones.** Se incumple con la Políticas Específicas de Seguridad y Privacidad de la Información toda vez que se evidencian elementos tecnológicos (switches) que se encuentran ubicados fuera del rack del Data Center y cuartos técnicos, corriendo el riesgo de dañarse por algún golpe de los usuarios.	Recoger los elementos tecnológicos (switches) e instalarlos en los racks que se encuentran ubicados en los diferentes pisos del edificio Pedro A. López
10	NC	**Oficina de Tecnologías de la Información y las Comunicaciones.** Se incumple con la Políticas Específicas de Seguridad y Privacidad de la Información toda vez que, en los cuartos técnicos, se evidencian elementos que no pertenecen a Tecnología,	Realizar una revisión periódica de los cuartos técnicos a fin de mantenerlos libre de elementos que no sean tecnológicos.

ASPECTOS PARA MEJORAR:			
ÍTEM	**NC[1]/O [2]**	**SITUACIONES ENCONTRADAS**	**RECOMENDACIÓN Y/O SUGERENCIAS[3]**
		generando riesgos que puedan dañar el cableado instalado en los racks.	
11	O	**Oficina de Tecnologías de la Información y las Comunicaciones.** De igual forma el cableado no se encuentra ordenado, elemento que puede afectar a los usuarios conectados en el caso que se necesite un soporte directamente en el rack.	Tomar acciones urgentes que subsanen las actividades de la correcta instalación del cableado estructurado del Ministerio.
12	O	**Oficina de Tecnologías de la Información y las Comunicaciones.** Parte de la red del Edificio Bancol se encuentra conforme lo establecido a las Políticas de las TIC y a las Política Específica de Seguridad y Privacidad de la Información del Ministerio. No obstante, la otra parte no ingresa al dominio del Ministerio, permitiendo así que cualquier computador ingrese sin los permisos necesarios.	Configurar la red del Edificio Bancol, a fin de que ingrese al Dominio del Ministerio a fin de proteger la información y posible ingreso de personas ajenas a la Entidad.

Tabla 31 – Resultado de la Auditoria.

RECOMENDACIONES DE LA AUDITORÍA

A continuación, se presentan recomendaciones, enfocadas al mejoramiento continuo del proceso del Sistema de Gestión de Seguridad de la información y del cumplimiento de la normativa aplicable:

- Se recomienda a la Oficina Asesora de Planeación y Prospectiva, para el contexto Institucional se elabore un documento estratégico que publique en el Sistema Integrado Gestión - SIG, donde recoja el contexto interno como externo de la entidad de acuerdo con los lineamientos de MIPG - "Analizar el contexto interno y externo de la entidad para la identificación de los riesgos y sus posibles causas, así como retos, tendencias y oportunidades de mejora e innovación en la gestión". Así mismo con las partes interesadas.
- Se recomienda a la Oficina de Tecnologías de la Información y las Comunicaciones aplicar los lineamientos establecidos en el “Documento Maestro del Modelo de Seguridad y Privacidad de la Información”, versión 4 y sus actualizaciones con sus anexos.
- Se recomienda revisar, actualizar y ajustar la resolución No. 297 de 2017, teniendo en cuenta los lineamientos actuales de MINTIC y la normativa vigente.
- Revisar la red del Edificio Bancol, dado que parte de ella no se encuentra configurada para ingresar al dominio del Ministerio.
- Incluir en los informes de vulnerabilidades, el resultado de las actividades ejecutadas una vez se haya resuelto lo encontrado.

- Realizar gestión para comprometer los recursos destinados para la actividad relacionada con el Sistema de Gestión de Seguridad de la Información – SGSI, para así evitar que en la próxima vigencia castiguen el presupuesto.
- Generar controles necesarios para realizar la actividad de terminación de contratos en los tiempos establecidos por la ley, dado que el contrato 20190514 terminó en febrero del 2020 y la solicitud de liquidación en junio del 2022.
- Se recomienda establecer un procedimiento para la creación de áreas seguras, los mecanismos para la identificación del área, sus condiciones de seguridad y controles ambientales con el fin de que sea coherente con el procedimiento: "*PR–GST–08 - Acceso a Áreas Seguras de Almacenamiento de Información*", o su modificación e inclusión de estos aspectos.

CONCLUSIONES DE LA AUDITORÍA

La Oficina de Tecnologías de la información y las Comunicaciones, de acuerdo con la muestra evaluada, cumple con las disposiciones para el Sistema de Gestión de Seguridad de la Información y las Comunicaciones, con las excepciones planeadas en el desarrollo de la Auditoria y plasmadas en este informe en las cuales se establecieron oportunidades de Mejora y No Conformidades.

El Sistema de Gestión de Seguridad de la Información, y acorde con los resultados de la evaluación, para la vigencia de 2022, contó con los recursos financieros para operación del sistema y cuya ejecución se encuentra en el 100%. Para vigencia 2023, el sistema tiene previsto un presupuesto de $2.351.912.500, pero a fecha de 30 de abril de 2023, no se había comprometido.

Con respecto a los riesgos, *"Posibilidad de afectación reputacional por no tener en cuenta los lineamientos de Mintic en materia de TI, para la orientación en la formulación de estrategias, instrumentos y herramientas, debido al desconocimiento de la normatividad y lineamientos existentes*", es posible que se materialice, de acuerdo con lo manifestado en el ítem 3.1 de la evaluación del Sistema de Gestión de Seguridad de la información. Así mismo se recomienda que se evalué la clasificación del riesgo de corrupción: "*"Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin del uso indebido de privilegios de TI para acceder a los sistemas de información"*.

El proveedor contratado, viene cumpliendo con el indicador de incidentes dado que en promedio han solucionado más del 95% durante el periodo evaluado.

Se contó con disponibilidad y compromiso por parte del delegado de la Oficina de Tecnologías de la Información y las Comunicaciones durante la etapa de ejecución de la auditoria de la información requerida por el equipo auditor.

Se resalta que, debido a las limitaciones de cualquier estructura de control interno, pueden ocurrir errores o irregularidades que no hayan sido detectadas bajo la ejecución de los procedimientos de auditoría, evaluación o seguimiento, previamente planeados.

Los soportes producto de la presente auditoria se encuentran en la carpeta denominada Auditoria al Sistema de Gestión de Seguridad de la Información, la cual, reposa en la compartida de la Oficina de Control Interno, los cuales pueden ser objeto de verificación de los hechos reflejados en este ejercicio.

	Jefe oficina de Control Interno Auditor líder	Auditores asignados
Firma		
Nombre	Ana Marlenne Huertas López	Efraín Palacios Montaña
		
		Orlando Báez Gómez