INFORME DE SEGUIMIENTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

INTRODUCCIÓN

La Oficina De Control Interno de Gestión, en desarrollo de sus funciones, acorde con la Ley 87 de 1993 y en cumplimiento del Plan Anual de Auditoría vigencia 2019, realizó el seguimiento a la implementación del Sistema de Gestión de Seguridad de la Información - SGSI conforme con el Decreto 2693 de 2012, el cual fue derogado por el Decreto Nacional 2573 de 2014 "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones".

El Sistema de Gestión de Seguridad de la Información preserva la confidencialidad, integridad y disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas.

Para la implementación del Sistema de Gestión de Seguridad de la Información, es importante tener en cuenta la Norma ISO/IEC 2702:2013 en cuanto su Anexo A "Objetivos de Control y Controles de Referencia" en sus numerales 5 al 18 toda vez que van alineados al numeral 6.1.3 "Tratamiento de riesgos de la seguridad de la información" de la Norma ISO/IEC 27001:2013

OBJETIVO

Verificar que los controles sobre la confidencialidad, integridad y disponibilidad de la información, para proteger la información de las partes interesadas sean los adecuados para la implementación del Sistema de Gestión de Seguridad de la Información del Minagricultura.

MARCO LEGAL

- Constitución Política de Colombia.
- Ley Estatutaria 1581 DE 2012, "*Por la cual se dictan disposiciones generales para la protección de datos personales*".
- Decreto Nacional 1377 de 2013, "*Por el cual se reglamenta parcialmente la Ley 1581 de 2012*".
- Ley 1712 de 2014, "*Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones*".
- Decreto Reglamentario Único 1081 de 2015 – Decreto 103 de 2015, *"Disposiciones generales en materia de transparencia y del derecho de acceso a la información pública nacional"*.

- Resolución 3564 de 2015, "Por la cual se reglamentan aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública".
- Decreto 415 de marzo de 2016. "*Por el cual se adiciona el Titulo 35 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de la Función Pública 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones*".
- Circular 20191000000117 del 29 de julio de 2019, "*Por la cual se imparten lineamientos frente a la aplicación de las disposiciones contenidas en la Ley 1960 de 27 de junio de 2019, en relación con la vigencia de la ley - procesos de selección, informe de las vacantes definitivas y encargos*".
- Decreto 2693 de 2014, "Por el cual se establecen los lineamentos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011, y se dictan otras disposiciones".
- Decreto Nacional 2573 de 2014, "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones".
- Decreto 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones" Titulo 9, "Políticas y Lineamientos de Tecnologías de la Información".

MUESTRA Y ALCANCE

Se toma como referencia el Anexo A "Objetivos de control y controles de referencia" en observancia de la Norma NTC ISO/IEC 27002:2013, Dominios del 5 al 9.

METODOLOGÍA EMPLEADA

a) Con el objetivo de realizar el seguimiento al avance de la implementación del Sistema de Gestión de Seguridad de la Información dentro del Ministerio de Agricultura y Desarrollo Rural, se solicitó a las oficinas de Tecnologías de la Información y las Comunicaciones, Talento Humano y Contratos, información referente al alcance presentado anteriormente.

b) Se realizaron entrevistas con las áreas vinculadas al seguimiento.

c) Se procedió a verificar el cumplimiento de los controles descritos en la Norma antes mencionada.

SEGUIMIENTO

El Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001 tiene el objetivo de asegurar que las entidades implementen todos los controles adecuados sobre la confidencialidad, integridad y disponibilidad de la información,

para proteger la información de las partes interesadas, incluyendo clientes, empleados, socios comerciales y la sociedad en general.

Es de aclarar que los controles que contiene la Norma NTC ISO/IEC 27002:2013 no son los únicos para la implementación del Sistema; en caso que la entidad observe que hacen falta algunos controles, se pueden tomar los que considere necesarios.

Las Dimensiones seleccionadas para este seguimiento son:

A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
A.5.1 Orientación de la Dirección para la gestión de la seguridad de la información

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
A.6.1 Organización Interna
A.6.2 Dispositivos móviles y teletrabajo

A.7 SEGURIDAD DE LOS RECURSOS HUMANOS
A.7.1 Antes de asumir el empleo
A.7.2 Durante la ejecución del empleo
A.7.3 Terminación y cambio de empleo

A.8 GESTIÓN DE ACTIVOS
A.8.1 Responsabilidad por los activos
A.8.2 Clasificación de los activos
A.8.3 Manejo de medios

A.9 CONTROL DE ACCESO
A.9.1 Requisitos del negocio para control de acceso
A.9.2 Gestión de acceso a los usuarios
A.9.3 Responsabilidad de los usuarios
A.9.4 Control de acceso a sistemas y aplicaciones

Para realizar seguimiento a las Dimensiones antes mencionadas, se realizó un muestreo y se utilizó una herramienta donde se incluyeron diferentes preguntas alusivas a los controles seleccionados y descritos anteriormente, con el ánimo de conocer el estado de la implementación del Sistema de Gestión de Seguridad de la Información del Minagricultura. Una vez resultas las preguntas por los encargados, se toman valores para conocer el porcentaje de avance que tiene cada Dominio. La tabla de evaluación está dada de la siguiente manera:

100	Requerimiento Establecido al 100%

SP	Requerimiento parcialmente implementado
0	Requerimiento No Establecido
N/A	Requerimiento no aplica a la compañía

Las preguntas, observaciones encontradas y porcentaje de conformidad se describen a continuación.

NTC/ISO/IEC 27002 CÓDIGO DE PRÁCTICA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Fecha de elaboración: **23/09/19**

Anexo A ISO 27002 OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA				
			Porcentaje de cumplimiento	**0**
A.5	POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN			
A.5.1	Orientación de la dirección para la gestión de seguridad de la información Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y reglamentos pertinentes.			
# ISO/IEC 27002:2013	**Requisito**	**Aspectos a verificar**	**Situación observada**	**Porcentaje conformidad**
A.5.1.1	Políticas para la seguridad de la información	¿Es clara la Política de seguridad de la información? ¿Los colaboradores de la Compañía conocen las políticas de seguridad de la información y sitio de publicación?	La política de seguridad de la información que se encuentra en el SIG, no es clara. No se cuenta con evidencias de capacitación	

A.5.1.2	Revisión de las políticas para seguridad de la información	¿La política de Seguridad de la Información es revisada periódicamente?	No se cuenta con un seguimiento periódico a la Política de Seguridad de la Información.	
			Porcentaje de cumplimiento	**78.57**

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

A.6.1 Organización interna

Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.

# ISO/IEC 27002:2013	Requisito	Aspectos a verificar	Situación observada	Porcentaje conformidad
A.6.1.1	Roles y responsabilidades de Seguridad de la información	¿Conoce sus responsabilidades para la seguridad de la información?	El encargado del Sistema conoce perfectamente las responsabilidades las cuales se encuentran descritas en la Resolución 297 de 2017.	100
A.6.1.2	Segregación de funciones	¿Están separadas las funciones en conflicto y áreas de responsabilidad de Seguridad de la Información?	Se tienen separadas las funciones, por medio de perfiles de usuario, donde no se permite el ingreso a varias funciones.	100
A.6.1.3	Contacto con las autoridades	¿Con qué organizaciones de Seguridad de la Información se mantienen contacto?	Se tiene contacto con el Comando Conjunto Cibernético (CCOCI), donde se envían reportes periódicos	100
A.6.1.4	Contacto con grupos de interés especial	¿Con qué grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad se mantiene contacto?	Se cuenta con Equipo de Respuesta ante Incidencias de Seguridad Informáticas (SCIRT), que envían boletines de interés.	100
A.6.1.5	Seguridad de la información en gestión de proyectos	¿Se identifican los requisitos de la seguridad de la información en los proyectos ejecutados?	Se identifican únicamente en proyectos de TI, para las demás áreas no se tiene identificados.	50

A.6.2 Dispositivos móviles y teletrabajo

Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

# ISO/IEC 27002:2013	Requisito	Aspectos a verificar	Situación observada	Porcentaje conformidad

A.6.2.1	Política para dispositivos móviles	¿Se tienen políticas y medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles?	Se cuenta con políticas y medidas de seguridad de soporte publicada en el Sistema Integrado de Gestión del Minagricultura, sin embargo esta se encuentra desactualizada.	50
A.6.2.2	Teletrabajo	¿Se tiene implementada una política y unas medidas de seguridad de soporte, para proteger la información que es accesada, procesada o almacenada en los lugares en los que se realiza teletrabajo?	Se cuenta con la política de teletrabajo publicada en el SIG, sin embargo no se ha trabajado en conjunto con el Grupo de talento Humano para su implementación. Adicionalmente la política se encuentra desactualizada.	50
			Porcentaje de cumplimiento	**41.67**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS			
A.7.1	Antes de asumir el empleo			
	Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.			
# ISO/IEC 27002:2013	**Requisito**	**Aspectos a verificar**	**Situación observada**	**Porcentaje conformidad**
A.7.1.1	Selección	¿Se verifican los antecedentes de todos los candidatos a un empleo de acuerdo con las leyes, reglamentos y ética pertinentes? ¿Son proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos?	El encargado de realizar la revisión de antecedentes de los candidatos al empleo, realiza esta actividad, dejando en las hojas de vida seleccionadas consignación de ello.	100
A.7.1.2	Términos y condiciones del empleo	¿Se firman acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información?	No se observa en los contratos los deberes y responsabilidades tanto del contratista como de la Entidad en temas de seguridad de la información.	
A.7.2	Durante la ejecución del empleo			

Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.

# ISO/IEC 27002:2013	Requisito	Aspectos a verificar	Situación observada	Porcentaje conformidad
A.7.2.1	Responsabilidades de la dirección	¿Se exige a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización?	No se cuenta con evidencias que soporten la aplicación de la seguridad de la información.	
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	¿A todos los empleados de la organización y los contratistas, se les da la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo?	Se cuenta con evidencias que soporten la aplicación de la seguridad de la información. Sin embargo debido a la rotación del personal, puede ser reforzada.	50
A.7.2.3	Proceso disciplinario	¿Se encuentra definido un proceso formal y comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información?	No se cuenta con el documento que emprenda acciones disciplinarias a quienes hayan violado la seguridad de la información	

A.7.3 Terminación y cambio de empleo

Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.

# ISO/IEC 27002:2013	Requisito	Aspectos a verificar	Situación observada	Porcentaje conformidad
A.7.3.1	Terminación o cambio de responsabilidades de empleo	¿Se comunican las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo?	Se cuenta con la comunicación que al término del contrato, se solicite el bloqueo de la cuenta de usuario.	100

			Porcentaje de cumplimiento	45
A.8	GESTIÓN DE ACTIVOS			
A.8.1	Responsabilidad por los activos			
	Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.			
# ISO/IEC 27002:2013	Control	Descripción del control	Observaciones	**Porcentaje de conformidad**
A.8.1.1	Inventario de activos	Dichos activos de información, deben ser revisados y monitoreados periódicamente por su responsable o dueño del proceso, razón por la cual deben ser actualizados periódicamente. ¿La actualización de activos de información por ingreso, modificación o retiro de los mismos se ha realiza periódicamente por parte del dueño del proceso o a quien este haya delegado?	El área encargada, realiza una revisión periódica de los activos actualizando el software que se tiene para ello.	100
A.8.1.2	Propiedad de los activos	¿Se identifican los activos de propiedad propia en el inventario de los activos?	Se evidencia que cada activo cuenta con un propietario de acuerdo con el inventario realizado por el Grupo de Almacén.	100
A.8.1.3	Uso aceptable de los activos	¿Están definidas las condiciones para el uso aceptable de los activos?	Se cuenta con un procedimiento para el buen uso del activo	100
A.8.1.4	Devolución de activos	¿Se realiza la devolución inmediata de los activos de propiedad de la compañía al terminar un usuario su empleo o contrato laboral? ¿Solicita evidencia de borrado seguro de la información de los equipos?	La devolución de los activos se realiza dentro de la Entidad y se encuentra documentada. Sin embargo, no se cuenta con una evidencia de borrado seguro de la información al entregar los activos que se han dado de baja.	50
A.8.2	Clasificación de la información			

Objetivo: Asegurar que la organización recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.

# ISO/IEC 27002:2013	Requisito	Aspectos a verificar	Situación observada	Porcentaje conformidad
A.8.2.1	Clasificación de la información	¿Se clasifica la información en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada?	Se cuenta con una parte del esquema de clasificación de la información, haciendo falta otra parte dado que se realiza solo para cumplir con la ley 1712.	
A.8.2.2	Etiquetado de la información	¿Se etiqueta la información, de acuerdo con el esquema de clasificación de información adoptado por la organización?	Se cuenta con una parte del esquema de clasificación de la información, haciendo falta una parte dado que se realiza solo para cumplir con la ley 1712.	50
A.8.2.3	Manejo de activos	¿Se tiene implementado un procedimiento para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización?	No se cuenta con un procedimiento para el manejo de activos de acuerdo con el esquema de clasificación de la información.	

A.8.3 Manejo de los medios

Objetivo: Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte.

# ISO/IEC 27002:2013	Requisito	Aspectos a verificar	Situación observada	Porcentaje conformidad
A.8.3.1	Gestión de medios removibles	¿Se tiene implementado un procedimiento para la gestión de medios removibles?	Se cuenta con un documento que maneja la gestión de medios removibles, sin embargo se encuentra desactualizada y no socializado.	50
A.8.3.2	Eliminación de los medios	¿Se utilizan procedimientos formales para desechar los medios de forma segura cuando ya no son necesarios?	No se cuenta con un documento formal que hable de la disposición de los medios cuando ya no se requieran.	

A.8.3.3	Transferencia de medios físicos	El intercambio de información confidencial en medios removibles tanto a nivel interno como con terceras partes debe ser a través de mecanismos que garanticen su protección y seguridad. ¿Para el transporte e intercambio de información confidencial con los clientes, se realiza cifrado u otro control complementario a los medios removibles (USB, disco externo, CD/DVD, otros)?	No se cuenta con seguridad para el transporte de la información en los medios removibles.	
			Porcentaje de cumplimiento	**70**

A.9	CONTROL DE ACCESO
A.9.1	Requisitos del negocio para control de acceso Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.

# ISO/IEC 27002:2013	Requisito	Aspectos a verificar	Situación observada	Porcentaje conformidad
A.9.1.1	Política de control de acceso	¿Se revisa la política de control de acceso con base en los requisitos del negocio y de seguridad de la información?	Se cuenta con un procedimiento para la política del control de acceso, sin embargo se encuentra desactualizado	**50**
A.9.1.2	Acceso a redes y a servicios en red	¿Se verifica que los usuarios solo tengan disponible el acceso a la red y servicios en red a los cuales han sido específicamente autorizados para su uso?	Se cuenta con un procedimiento para la política del control de acceso a redes y/o servicios de red, sin embargo se encuentra desactualizado	**50**

A.9.2	Gestión de acceso de usuarios Objetivo: Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.

# ISO/IEC 27002:2013	Requisito	Aspectos a verificar	Situación observada	Porcentaje conformidad

A.9.2.1	Registro y eliminación de usuarios	De acuerdo con políticas de seguridad de la información, todo aquel colaborador con acceso a sistemas de información debe disponer de una cuenta exclusiva y nombrada bajo su responsabilidad. Conforme a lo anterior, ¿El acceso a los sistemas de información (bases de datos, aplicaciones, sistemas operativos, otros) se realiza con cuentas nombradas?	Se maneja el procedimiento para la gestión de cuentas de usuario, sin embargo se encuentra desactualizado.	**50**
		Con el fin de garantizar que se disponga un acceso autorizado y privilegios necesarios para el ejercicio de sus funciones, los colaboradores se encuentran bajo una catalogación por cargo y responsabilidades, dado ello, para realizar su gestión empleando los sistemas de información se dispone de perfilamiento y roles asignados a nivel de aplicación, DB y sistema operativo? ¿Cuenta con la matriz de roles y perfiles actualizada?	Se maneja el procedimiento para la gestión de cuentas de usuario, sin embargo se encuentra desactualizado.	**50**
A.9.2.2	Suministro de acceso de usuarios	¿Se implementa un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios a todos los sistemas y servicios?	Se maneja el procedimiento para la gestión de cuentas de usuario, sin embargo se encuentra desactualizado.	**50**

A.9.2.3	Gestión de derechos de acceso privilegiado	¿Se restringe y controla la asignación y uso de derechos de acceso privilegiado?	Se controla al crear el perfil del usuario, ingresándolo al grupo al cual pertenece, el cual ya viene con los accesos predefinidos	100
A.9.2.4	Gestión de información de autenticación secreta de usuarios	¿Se tiene definido el proceso para la asignación de información de autenticación secreta?	Se cuenta con un instructivo para la creación de claves secretas	100
A.9.2.5	Revisión de los derechos de acceso de usuarios	Como propietario de los activos, realiza una revisión periódica de los derechos de acceso de los usuarios a su cargo?	No se cuenta con la revisión periódica de los accesos a los usuarios	
A.9.2.6	Cancelación o ajuste de los derechos de acceso	El cumplimiento de las políticas de seguridad de la información se orienta a minimizar los riesgos que afecten sus pilares, entre los cuales se relaciona la gestión de cuentas de usuario y sus privilegios, tanto para el personal que ingresa, como aquel que se ausenta por permisos, licencias, retiros, entre otros. ¿Se solicita cancelación y/o desactivación y retiro de permisos de las cuentas de usuario cuándo el colaborador termina su contrato?	Se cuenta con un procedimiento en el cual se define la gestión de la cancelación de los usuarios retirados.	100
A.9.3	Responsabilidades de los usuarios Objetivo: Hacer que los usuarios se responsabilicen por salvaguardar su información de autenticación.			
# ISO/IEC 27002:2013	**Requisito**	**Aspectos a verificar**	**Situación observada**	**Porcentaje conformidad**
A.9.3.1	Uso de información de autenticación secreta	¿Se verifica que los usuarios cumplan con las prácticas definidas para el uso de información de autenticación secreta?	Existen claves sencillas de descifrar, el control podría ser más fuerte.	50
A.9.4	Control de acceso a sistemas y aplicaciones Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.			

# ISO/IEC 27002:2013	Requisito	Aspectos a verificar	Situación observada	Porcentaje conformidad
A.9.4.1	Restricción de acceso a información	¿Se restringe el acceso a la información y a las funciones de los sistemas de las aplicaciones de acuerdo con la política de control de acceso?	Se restringe el acceso a la información al crear el perfil del usuario, ingresándolo al grupo al cual pertenece, el cual ya viene con los accesos predefinidos	100
A.9.4.2	Procedimiento de ingreso seguro	¿Cómo se controla el acceso a sistemas y aplicaciones que requieren un proceso de ingreso seguro?	Se controla al crear el perfil del usuario, ingresándolo al grupo al cual pertenece, el cual ya viene con los accesos predefinidos	100
A.9.4.3	Sistema de gestión de contraseñas	¿Los sistemas de gestión de contraseñas son interactivos y aseguran la calidad de las contraseñas?	Se cuenta con un procedimiento, sin embargo este se encuentra desactualizado.	50
A.9.4.4	Uso de programas utilitarios privilegiados	¿Están restringidos y controlados el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones?	Se restringe el uso de programas por medio de la solicitud de un usuario administrador al instalar programas que están fuera de las políticas de la Entidad.	100
A.9.4.5	Control de acceso a códigos fuente de programas	¿Se restringe el acceso a códigos fuente de programas?	Se cuenta con un programa TFS para proteger el acceso a los códigos fuentes de la Entidad	100

De acuerdo con el porcentaje de conformidad, a continuación se presenta un resumen el cual indica el número de requisitos de acuerdo con el Dominio y el porcentaje de cumplimiento, con la cantidad de aspectos a verificar.

DOMINIOS - ANEXO A ISO/IEC 27002:2013	% DE CUMPLIMIENTO DOMINIOS - ANEXO A ISO/IEC 27002:2013	% DE CUMPLIMIENTO			
		100	50	0	N/A
A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	0	0	0	2	0
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	78,57	4	3	0	0

A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	41.67	2	1	3	0
A.8 GESTIÓN DE ACTIVOS	45,00	3	3	4	0
A.9 CONTROL DE ACCESO	70,00	7	7	1	0

De igual manera se observa que de 40 Aspectos a verificar, 10 no cumplen con los requerimientos que equivalen al 25%; 16 de ellos cumplen con el requerimiento, equivalente al 40% y con el 35% no cumplen en su totalidad 14 actividades.

Así mismo se observa el porcentaje de cumplimiento de cada uno de los Dominios, observando que el mayor porcentaje de avance corresponde al Dominio A6 que corresponde al 78.57%, y el Dominio A9 con el 70%; por los demás Dominios el porcentaje de cumplimiento es bajo.

Una vez analizada la información suministrada por los encargados de las diferentes áreas, podemos observar que, si bien hay avance de cumplimiento de requisitos, no se cuenta con un cronograma de trabajo para la implementación del Sistema de Seguridad de la Información.

Así mismo el Minagricultura cuenta con una Política de Seguridad y Privacidad de la Información, sin embargo esta se encuentra incompleta, toda vez que no se describen los controles y políticas que debe tener el Sistema.

A continuación se realizará una descripción por cada Dominio con las observaciones encontradas.

A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

A.5.1 Orientación de la Dirección para la gestión de la seguridad de la información

El porcentaje de cumplimiento de este Dominio es 0%, toda vez que la Entidad no cumple con los 2 controles propuestos en la normatividad; por lo que se hace un llamado a la ejecución de actividades que puedan cumplir con este requisito.

El anterior análisis se puede observar en la siguiente gráfica.

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

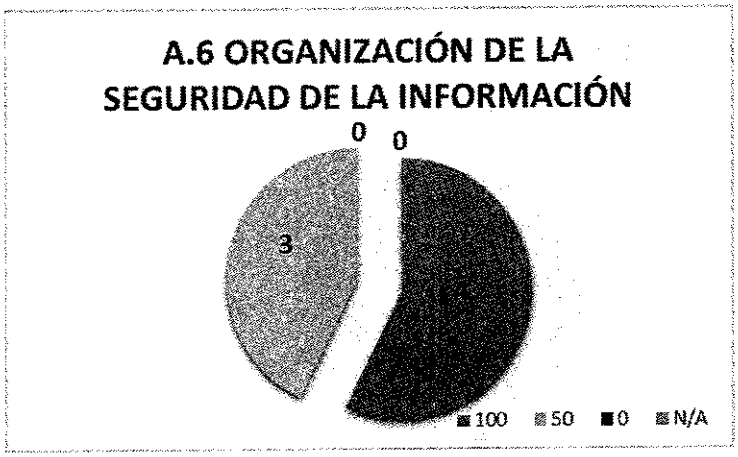
A.6.1 Organización Interna
A.6.2 Dispositivos móviles y teletrabajo

El porcentaje de evaluación de este Domino es de 78.57% dado que se cumplen 4 de los 7 controles equivalentes al 57.1% de la Norma y 3 de ellos cumplen parcialmente equivalente al 42.9%. Es importante verificar las observaciones dadas y realizar actividades que cumplan con los requisitos toda vez que no se tienen políticas para la Gestión de Seguridad de la Información en gestión de proyectos en los diferentes procesos sin incluir a TI. De igual manera se cuenta con políticas para dispositivos móviles y el teletrabajo pero no se ha implementado y su documentación se encuentra desactualizada.

Lo anterior se puede observar en la siguiente gráfica, donde 4 actividades cumplen y 3 cumplen parcialmente.

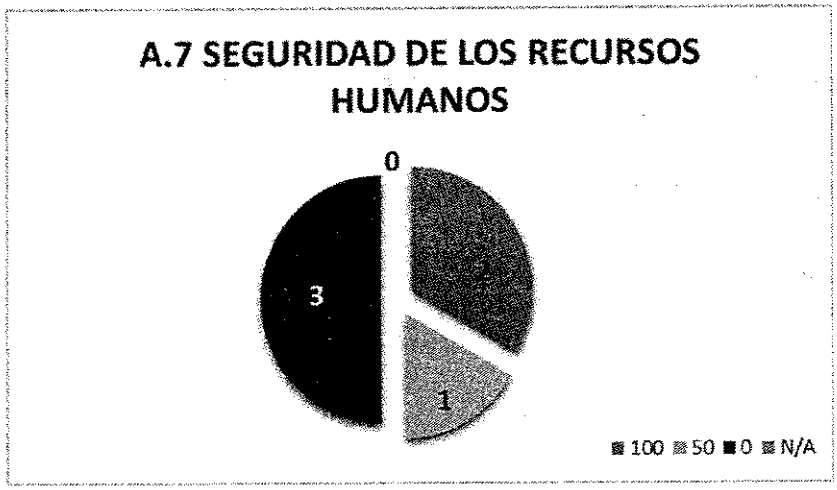
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS

A.7.1 Antes de asumir el empleo
A.7.2 Durante la ejecución del empleo
A.7.3 Terminación y cambio de empleo



Una vez analizada la información suministrada por el Grupo de Contratación y Talento Humano, se tomaron 40 carpetas de contratistas en diferentes cargos, se verificó el perfil con respecto al objeto contratado, observando el cumplimiento de la normatividad, en lo que se refiere a la selección de los postulantes a los cargos que se encuentran disponibles. Así mismo se seleccionaron 27 hojas de vida de funcionarios de planta del Ministerio, con el ánimo de verificar su perfil y si el nombramiento se realizó de acuerdo con la normatividad, observando que se está cumpliendo con la normatividad vigente. No obstante lo anterior, en las carpetas de los contratistas y funcionarios, no se encuentra descritos los deberes y responsabilidades en temas de seguridad de la información, así como tampoco se cuenta con un documento que emprenda acciones disciplinarias a quienes hayan violado la seguridad de la información.

El análisis anterior puede verse reflejado en la siguiente gráfica.



En este Dominio observa que el porcentaje de cumplimiento es bajo pues su valor es del 33.33% que corresponden a 3 actividades no cumplidas que equivalen a 50%, 2 cumplidas que equivale al 33.33% y 1 cumplida parcialmente con 16.67%.

A.8 GESTIÓN DE ACTIVOS

A.8.1 Responsabilidad por los activos
A.8.2 Clasificación de los activos
A.8.3 Manejo de medios

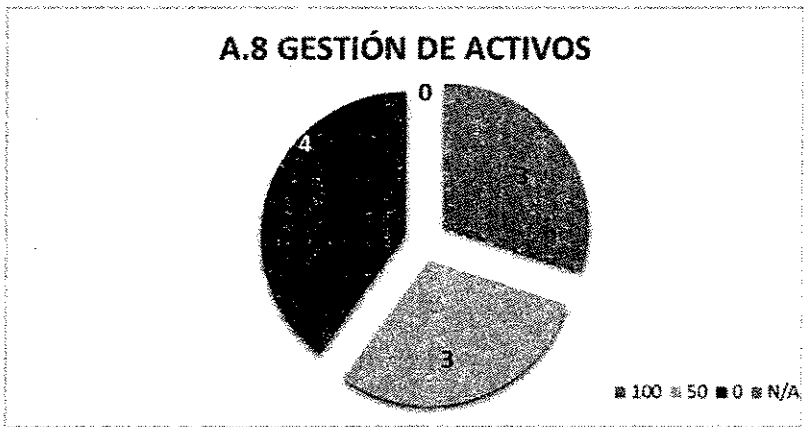
Para este Dominio, se observa que se cuenta con un software donde reposa la información de los activos los cuales son revisados periódicamente por los funcionarios encargados de realizar esta actividad. En cuanto a la devolución de los activos, se observa que al generarse el retiro de un funcionario o contratista, este queda a cargo del supervisor o funcionario delegado para ello.

Así mismo se evidencia mediante entrevista al área de Tic's, que no se cuenta con un documento que cumpla con un borrado seguro de los computadores al momento de darlos de baja en el Ministerio.

De igual manera se cuenta con la información clasificada y reservada de la ley 1712, pero no se cuenta con un etiquetado de la información por ende tampoco se cuenta con un documento de manejo de activos en temas de clasificación de la información.

Aunado a lo anterior, se observa que se cuenta con el documento que maneja la gestión de los medios removibles, sin embargo no ha sido actualizado ni socializado; no se cuenta con un documento que maneje la disposición final de los medios que ya no se requieran, así como tampoco la seguridad para el transporte de la información en medios removibles.

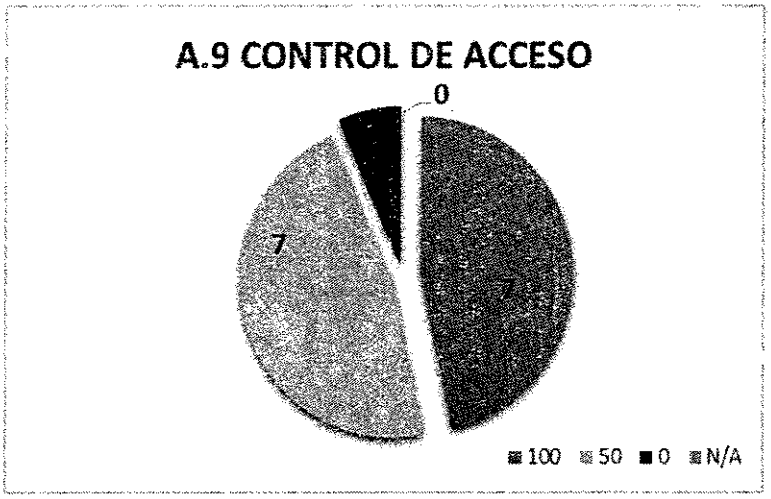
Esta información se puede observar en la siguiente gráfica donde se indica que de los 10 requisitos 4 no cumplen y corresponden al 40%, 3 que cumplen en su totalidad equivalen al 30% y 3 que cumple parcialmente equivale al 30%, por lo que se hace un llamado para realizar la gestión al cumplimiento de estos controles.



A.9 CONTROL DE ACCESO

A.9.1 Requisitos del negocio para control de acceso
A.9.2 Gestión de acceso a los usuarios
A.9.3 Responsabilidad de los usuarios
A.9.4 Control de acceso a sistemas y aplicaciones

EL porcentaje de evaluación de este Dominio, se encuentra en 70% dado que de los 15 requisitos, se cumplen 7 que equivalen al 46.67%, 7 requisitos que cumplen al 50% equivalen al 46.67% y 1 que no cumplen el requisito equivalen al 6.67%. A continuación se presenta la gráfica.



El análisis a la gráfica anterior está dada porque la documentación de Controles de Acceso se encuentra desactualizada, no se realiza una revisión periódica de los derechos de acceso de los usuarios así como tampoco se verifica que los usuarios cumplan con las prácticas definidas para el uso de información de autenticación secreta pues el sistema no valida las claves fáciles de descifrar.

ASPECTOS A MEJORAR

Es importante realizar un diagnóstico al Sistema de Gestión de Seguridad de la Información, generando un cronograma de actividades que permita agotar periódicamente las etapas de implementación.

CONCLUSIONES

Se evidencia compromiso de la Alta Dirección hacia la seguridad de la información actualmente expresada en infraestructura tecnológica y en las bases del sistema de gestión de seguridad de la información.

Se cuenta con recurso humano calificado y comprometido con las labores de gestión de seguridad.

Proyectó: Efraín Palacios M.
Revisó: Marlenne Huertas.
Octubre de 2019