 MINAGRICULTURA	INSTRUCTIVO	VERSIÓN 01
	DIAGNÓSTICO DE NIVEL DE IMPLEMENTACIÓN DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD	IN-GGT-01
		FECHA EDICIÓN 22-07-2016

1. OBJETIVO

Explicar los pasos para realizar la evaluación de la eficacia en el nivel de implementación de subsistema de gestión de seguridad de la información (SGSI) en el marco del Sistema Integrado de Gestión (SIG) del Ministerio de Agricultura y Desarrollo Rural.

2. DEFINICIONES



DdA: (Declaración de Aplicabilidad). Documento en el que se registran los controles necesarios para la gestión de riesgos de seguridad de la información, ya se que se implementen o no y la justificación de las exclusiones de los controles del Anexo A de la norma ISO/IEC 27001:2013


IPv4: Es la cuarta versión del protocolo de intercambio de información sobre el que se sustenta la comunicación en Internet. La función o propósito de este protocolo es mover datos (formalmente denominados datagramas) a través de redes interconectadas hasta que se alcance el destino final

IPv6: es la nueva versión del *Internet Protocol* (IP) en el cual se sustenta la operación de Internet. Las especificaciones técnicas básicas de IPv6 se desarrollaron en la década de los 90s en el IETF (*Internet Engineering Task Force*). Al día de hoy el protocolo sigue añadiendo nuevas funcionalidades y se le considera un protocolo lo suficientemente maduro para soportar la operación de Internet en sustitución de IPv4.(Fuente: <http://portalipv6.lacnic.net/que-es/>)

MSPI: Modelo de Privacidad y Seguridad de la información: es el conjunto de lineamientos, políticas, normas, procesos e instituciones que proveen y promueven la puesta en marcha, supervisión, mejora y control de la implementación del modelo, así como a la implementación de la Estrategia de Gobierno en Línea, establecida en manual GEL. (Modelo de Privacidad y Seguridad de la Información MINTIC)

SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

REVISO	APROBO
 ANA BEIBA POVEDA Coordinadora Grupo de Gestión de Gobernabilidad de la Información y Gestión del Conocimiento FECHA: 22-07-2016	 FIDEL ANTONIO TORRES MOYA Jefe Oficina de Tecnologías de la Información y las Comunicaciones FECHA: 22-07-2016

 MINAGRICULTURA	INSTRUCTIVO	VERSIÓN 01
	DIAGNÓSTICO DE NIVEL DE IMPLEMENTACIÓN DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD	IN-GGT-01
		FECHA EDICIÓN 22-07-2016

De acuerdo con las recomendaciones formuladas por el Ministerio de las TIC sobre la implementación del Modelo de Privacidad y Seguridad de la información, las definiciones para los diferentes niveles de madurez de implementación son:

Nivel inicial

En este nivel se encuentran las Entidades, que aún no cuentan con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto, los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información.

Nivel gestionado

En este nivel se encuentran las Entidades, en las cuales existen procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentran gestionados dentro del componente de planificación del MSPI (Modelo de Privacidad y Seguridad de la información)

Nivel Definido

En este nivel se encuentran las Entidades que tiene documentado, estandarizado y aprobado por la dirección, el modelo seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.


Nivel Gestionado cuantitativamente

En este nivel se encuentran las Entidades, que cuenten con métricas, indicadores y realizan auditorías al modelo de seguridad y privacidad de la información, recolectando información para establecer la efectividad de los controles.

Nivel Optimizado

En este Nivel se encuentran las Entidades, en donde existe un mejoramiento continuo del modelo de seguridad y privacidad de la información, retroalimentación cualitativa del modelo.

Cada nivel debe estar completo en un 100% para poder iniciar la implementación del siguiente nivel. Es decir, no es posible cumplir parcialmente un nivel e iniciar la ejecución de actividades del siguiente nivel de madurez.

 MINAGRICULTURA	INSTRUCTIVO	VERSIÓN 01
	DIAGNÓSTICO DE NIVEL DE IMPLEMENTACIÓN DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD	IN-GGT-01
		FECHA EDICIÓN 22-07-2016

3. DESARROLLO

La determinación del nivel de eficacia en la implementación del subsistema de gestión de seguridad de la información busca establecer el grado de cumplimiento de las obligaciones del Ministerio de Agricultura y Desarrollo Rural (MADR) en la adopción del modelo de privacidad y seguridad de la información de la estrategia de gobierno en línea, de acuerdo con los lineamientos del decreto 2578 de 2015 del Ministerio de las Tecnologías de Información y Comunicaciones.

El cálculo del nivel de eficacia en implementación del SGSI se realiza usando la guía encuesta de Diagnóstico Modelo de Seguridad de la Información para las Entidades del Estado. La guía permite determinar el nivel de cumplimiento en la implementación del SGSI y el Modelo de privacidad y seguridad de la información.


En primera instancia se debe determinar el nivel de madurez que se desea lograr para el período de evaluación del SGSI. Los niveles definidos por el MINTIC son: inicial/Gestionado, Definido, Gestionado cuantitativamente, Optimizado

Para determinar el nivel de madurez se usan las siguientes tablas de evaluación. Cada pregunta se debe resolver y al final se suman los puntajes. Los puntajes son absolutos, es decir, no es posible cumplir parcialmente una obligación y asignar un puntaje proporcional al nivel de cumplimiento requerido.


3.1. Evaluación de nivel de madurez para nivel inicial y gestionado.

Responda las siguientes preguntas y al final sume el puntaje obtenido en la columna SI CUMPLE


INICIAL / GESTIONADO		SI cumple	NO cumple
Contexto Organizacional			
<i>Establecer y documentar el alcance, límites y política.</i>			
1	¿Existe una definición de la seguridad de la información y sus objetivos globales?	2	0
2	¿Existe una probación de la Dirección para la implementación del SGSI?	2	0
3	¿Los requerimientos de seguridad están articulados con las necesidades de la entidad?	3	0
4	¿Los procesos y servicios escogidos para la implementación del SGSI, están apoyando directamente a la misión Institucional?	3	0

 MINAGRICULTURA	INSTRUCTIVO	VERSIÓN 01
	DIAGNÓSTICO DE NIVEL DE IMPLEMENTACIÓN DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD	IN-GGT-01
		FECHA EDICIÓN 22-07-2016

INICIAL / GESTIONADO		SI cumple	NO cumple
5	¿Está documentado en el alcance del SGSI claramente en qué áreas de la organización se desea implantar el SGSI, como primera medida y cuáles posteriormente?	2	0
6	¿Está documentado el alcance del SGSI claramente los servicios implicados en el SGSI?	3	0
7	¿Está documentado en el alcance del SGSI las locaciones físicas relacionadas con el SGSI?	3	0
8	¿En el alcance se determinan claramente los sistemas de información relacionados con el SGSI?	2	0
9	¿En el alcance se determinan claramente los terceros y externos relacionados con el SGSI?	2	0
10	¿En el alcance se determinan claramente las Interfaces del SGSI? (¿Que procesos externos e internos tiene relación con el SGSI?).	3	0
11	¿Se ha identificado la legislación que afecta los procesos dentro del SGSI?	2	0
12	¿Se tiene una Política de seguridad de la información?	1	0
13	¿La política de seguridad de la información es de dominio público dentro de la organización?.	2	0
<i>Establecer procedimientos, roles y responsabilidades dentro del SGSI.</i>			
1	¿Se hace la definición de responsabilidades generales y específicas, en las que se incluirán los roles? (sin hacerlo para personas concretas dentro de la organización)	6	0
2	¿Se incluyen los temas de seguridad de la información en los comités de gestión interdisciplinarios de la Entidad?	6	0
3	¿Los temas de seguridad de la información se tratan en los comités directivos interdisciplinarios de la Entidad, con regularidad?	9	0
4	¿Se cuentan con procedimientos que indique a los funcionarios como manejar la información y los activos de información en forma segura?	9	0
Liderazgo			
<i>Asignación de recursos</i>			
1	¿Se establece el responsable del SGSI para la entidad?	7	0
2	¿Se identifican los propietarios de la información?	4	0
3	¿Se ha generado la asignación de recurso humano, comunicación de roles y responsabilidades de seguridad y privacidad de la información?	7	0
4	¿Se revisan y se aprueban las políticas de seguridad y privacidad de la información?	5	0
5	¿Se revisa y se aprueba la estrategia de transición del protocolo IPv4 a IPv6?	7	0

 MINAGRICULTURA	INSTRUCTIVO	VERSIÓN 01
	DIAGNÓSTICO DE NIVEL DE IMPLEMENTACIÓN DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD	IN-GGT-01
		FECHA EDICIÓN 22-07-2016

INICIAL / GESTIONADO		SI cumple	NO cumple
<i>Procedimientos de control documental del MSPI</i>			
1	¿Existe un documento de la política de seguridad de la Información?	6	0
2	¿El documento de la política de seguridad de la información esta aprobado por la dirección?	8	0
3	¿El Documento de política de seguridad de la información está revisado, evaluado y divulgado en su lectura y aplicación?	8	0
4	¿Documento con el plan y estrategia de transición de IPv4 a IPv6 está revisado y aprobado por la alta Dirección?	8	0
Planificación			
<i>Inventario de activos de información.</i>			
1	¿Con base en el inventario de activos de información clasificado, se establece la caracterización de cada uno de los sistemas de información?	8	0
2	¿Se Identifican los riesgos asociados con la información, físicos, lógicos, identificando sus vulnerabilidades y amenazas?	11	0
3	¿Los roles de seguridad y privacidad de la información están bien definidos y se lleva un registro de las actividades de cada uno?	11	0
Soporte			
<i>Acciones para tratar riesgos y oportunidades de seguridad de la información.</i>			
1	¿Se tiene una metodología para la Identificación y valoración de riesgos de seguridad de la Información?	5	0
2	¿Se tienen definidos los planes de tratamiento de riesgos de seguridad de la información?.	5	0
3	¿Se elabora un informe de los incidentes de seguridad de la información?	7	0
4	¿Existen planes de continuidad del negocio que contemplen los procesos críticos de la Entidad que garanticen la continuidad de los mismos?	7	0
5	¿Se definen los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro?	6	0
<i>Toma de conciencia.</i>			
1	¿Existe un diseño del plan de comunicación sensibilización y capacitación para el SGSI?	15	0
2	¿Existe un diseño del plan de comunicación sensibilización y capacitación para la transición al protocolo IPV6.?	15	0
Total de calificación para nivel Inicial/Gestionado			

 MINAGRICULTURA	INSTRUCTIVO	VERSIÓN 01
	DIAGNÓSTICO DE NIVEL DE IMPLEMENTACIÓN DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD	IN-GGT-01
		FECHA EDICIÓN 22-07-2016

Luego de tener la calificación compare el resultado obtenido con la siguiente tabla de evaluación de cumplimiento del nivel de madurez inicial gestionado.

Nivel de cumplimiento Nivel inicial/gestionado	Puntaje Mínimo	Puntaje Máximo
Critico	0	85
Intermedio	86	125
Suficiente	126	210

Luego calcule el índice de eficacia en implementación del SGSI mediante la siguiente fórmula.


Eficacia en implementación del SGSI = $\frac{\text{Resultado de la encuesta de diagnóstico SGSI} \times 100}{\text{Máximo puntaje según nivel de madurez inicial}}$

Si se logra el nivel 100% en el nivel de madurez inicial/gestionado se puede evaluar el indicador para el nivel definido. En caso contrario la entidad debe cumplir todas las obligaciones del nivel inicial/gestionado antes de intentar cumplir el nivel de madurez definido.


3.2. Evaluación de nivel de madurez para nivel definido.

Cuando la entidad cumpla en un 100% el nivel inicial/gestionado, puede evaluar su cumplimiento en nivel definido, para esto, responda las siguientes preguntas y al final sume el puntaje obtenido.

DEFINIDO		SI cumple	NO cumple
Planificación y control operacional.			
<i>Divulgación de las políticas de seguridad y privacidad de la información.</i>			
1	¿Se ejecutan los planes de toma de conciencia, comunicación y divulgación, de las políticas de seguridad y privacidad de la información y están, aprobados por la alta Dirección?	10	0
<i>El comité directivo divulga, las medidas de seguridad y privacidad de la información que deberán ser tomadas para la conservación de la información.</i>			
1	¿Se han implementado los controles físicos y lógicos que se han definido en la Entidad, con los cuales se busca preservar la seguridad y privacidad de la información?	10	0
Plan de tratamiento del riesgo			

 MINAGRICULTURA	INSTRUCTIVO	VERSIÓN 01
	DIAGNÓSTICO DE NIVEL DE IMPLEMENTACIÓN DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD	IN-GGT-01
		FECHA EDICIÓN 22-07-2016

DEFINIDO		SI cumple	NO cumple
<i>Lista de chuequeo de requerimientos de seguridad</i>			
1	¿Existencia del listado de requerimientos sobre la seguridad de la información en proyectos?.	15	0
<i>Elaboración del plan de tratamiento del riesgo (quién, cómo y cuándo)</i>			
1	¿Se tiene un plan de acción definido en función de los diversos controles definidos por la DdA (Declaración de Aplicabilidad)?	10	0
2	¿Se tiene una descripción de las tareas a realizar para la ejecución de los controles que lo necesiten o de las tareas de administración del SGSI?	10	0
3	¿Se tiene una descripción del personal requerido con experiencia, habilidades, funciones, dentro del plan de acción para el tratamiento de riesgos de seguridad?	10	0
<i>Implementación de controles</i>			
1	¿Se han Implementado los controles seleccionados para la gestión de riesgos de seguridad de la información con priorización de acciones evaluación de opciones de control recomendadas facilidad/efectividad, Costo/ beneficio y asignación de responsabilidades?	7	0
2	¿Se aplica el protocolo de controles preventivos y detectivos (políticas de seguridad, procedimientos, metodologías, seguridad del personal, física y ambiental) en el tratamiento de riesgos de seguridad de la información?.	7	0
3	¿Se establecen los indicadores de gestión pertinentes que permitan medir eficacia de los controles de seguridad de la información?	8	0
4	¿Se incluye un plan de contingencia para la gestión de riesgos de seguridad de la información?	8	0
<i>Seguimiento</i>			
1	Se tienen Instrumentos diseñados para hacer el seguimiento.	15	0
2	Se reconoce la importancia de ampliar los planes de continuidad del negocio a otros procesos, pero aún no se pueden incluir ni trabajar con ellos.	15	0
Gestión de recursos y procedimientos implementados para la asignación de recursos financieros			
<i>Asignación del presupuesto para Seguridad de la Información.</i>			
1	¿Se genera la documentación de la asignación del presupuesto de seguridad como % del presupuesto de TI?	20	0
Gestión de recursos y procedimientos implementados para la asignación de recursos humanos			
<i>Perfiles y experiencia del personal (descripción) para cada rol o función.</i>			
1	¿Se genera la documentación de perfiles para cada función en materia de seguridad de la información?	20	0
<i>Inventario de habilidades del personal disponible (experiencia existente).</i>			

 MINAGRICULTURA	INSTRUCTIVO	VERSIÓN 01
	DIAGNÓSTICO DE NIVEL DE IMPLEMENTACIÓN DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD	IN-GGT-01
		FECHA EDICIÓN 22-07-2016

DEFINIDO		SI cumple	NO cumple
1	¿Se genera la documentación del inventario de habilidades del personal?	20	0
<i>Procedimientos para la asignación del personal según las funciones.</i>			
1	¿Se genera la documentación de procedimientos de asignación de personal?	20	0
<i>Procedimientos para la contratación del personal</i>			
1	¿Se genera la documentación del proceso de contratación?	20	0
<i>Implementación del plan y estrategia de transición de IPv4 a IPv6.</i>			
1	¿Se posee la implementación del plan y estrategia de transición de IPv4 a IPv6?	20	0
Total de calificación para nivel Definido			

Luego de tener la calificación compare el resultado obtenido con la siguiente tabla de evaluación de cumplimiento del nivel de madurez definido.

Nivel definido

Nivel de cumplimiento	Mínimo	Máximo
Critico	0	87
Intermedio	88	147
Suficiente	148	245


Luego calcule el índice de eficacia en implementación del SGSI mediante la siguiente fórmula.

Eficacia en implementación del SGSI = $\frac{\text{Resultado de la encuesta de diagnóstico SGSI}}{\text{Máximo puntaje según nivel de madurez definido}} \times 100$

Si se logra el nivel 100% en el nivel de madurez definido se puede evaluar el indicador para el nivel gestionado cuantitativamente. En caso contrario la entidad debe cumplir todas las obligaciones del nivel definido antes de intentar cumplir el nivel de madurez gestionado cuantitativamente.

3.3. Evaluación de nivel de madurez para nivel gestionado cuantitativamente.

Cuando la entidad cumpla en un 100% el nivel definido, puede evaluar su cumplimiento en nivel gestionado cuantitativamente, para esto, responda las siguientes preguntas y al final sume el puntaje obtenido.

 MINAGRICULTURA	INSTRUCTIVO	VERSIÓN 01
	DIAGNÓSTICO DE NIVEL DE IMPLEMENTACIÓN DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD	IN-GGT-01
		FECHA EDICIÓN 22-07-2016


GESTIONADO CUANTITATIVAMENTE		SI cumple	NO cumple
Plan de seguimiento, evaluación y análisis del MSPI.			
<i>Acciones realizadas y los resultados de la implementación del SGSI</i>			
1	Se utilizan indicadores de cumplimiento para establecer si las políticas de seguridad y privacidad de la información y las cláusulas establecidas por la organización en los contratos de trabajo, son acatadas correctamente.	7	0
2	Se realizan pruebas de manera sistemática a los controles, para determinar si están funcionando de manera adecuada.	7	0
3	Se realizan pruebas y ventanas de mantenimiento (simulacro), para determinar la efectividad de los planes de respuesta de incidentes.	8	0
4	Se tiene un registro de actividades en seguridad (bitácora operativa).	8	0
Auditoria Interna.			
<i>Monitoreo a la ejecución de la política, los planes y estándares de la SI</i>			
1	¿Se realiza la revisión y verificación continua de los controles implementados?	10	0
2	¿Se revisa y monitorean periódicamente los activos de información de la Entidad?	10	0
3	¿Se realizan de planes de mejora de la seguridad de la información?	10	0
Plan de tratamiento de riesgos.			
<i>Evaluación del plan de tratamiento de riesgos.</i>			
1	¿Se realiza la revisión y actualización de la evaluación de riesgos?	10	0
2	¿Se realiza la Medición de los indicadores de gestión?	10	0
Total de calificación para nivel gestionado cuantitativamente			

Luego de tener la calificación compare el resultado obtenido con la siguiente tabla de evaluación de cumplimiento del nivel de madurez gestionado cuantitativamente.

Nivel gestionado cuantitativamente

Nivel de cumplimiento	Mínimo	Máximo
Critico	0	28
Intermedio	29	47
Suficiente	48	80

Luego calcule el índice de eficacia en implementación del SGSI mediante la siguiente fórmula.

 MINAGRICULTURA	INSTRUCTIVO	VERSIÓN 01
	DIAGNÓSTICO DE NIVEL DE IMPLEMENTACIÓN DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD	IN-GGT-01
		FECHA EDICIÓN 22-07-2016

Eficacia en implementación del SGSI = Resultado de la encuesta de diagnóstico SGSI X 100
Máximo puntaje según nivel de madurez gestionado cuantitativamente

Si se logra el nivel 100% en el nivel de madurez gestionado cuantitativamente se puede evaluar el indicador para el nivel optimizado. En caso contrario la entidad debe cumplir todas las obligaciones del nivel definido antes de intentar cumplir el nivel de madurez optimizado.


3.4. Evaluación de nivel de madurez para nivel gestionado cuantitativamente.

OPTIMIZADO		SI cumple	NO cumple
Plan de seguimiento, evaluación y análisis para el MSPI.			
<i>Plan de seguimiento, evaluación y análisis para el MSPI.</i>			
1	¿Se analizan los datos arrojados por el informe de desempeño en seguridad y privacidad de la información para definir acciones correctivas más claras?	10	0
2	¿La Entidad aprende continuamente sobre los incidentes de seguridad presentados?	10	0
3	¿Se incluyen todas las áreas de la Entidad, en los planes de respuesta de incidente?	10	0
Revisión y aprobación por la alta Dirección.			
<i>Auditoria Interna.</i>			
1	¿Los funcionarios apoyan y contribuyen al mejoramiento de la seguridad y privacidad de la información en la Entidad?	20	0
<i>Comunicación de resultados y plan de mejoramiento.</i>			
1	¿Se realiza e implementa el plan de socialización, difusión y documentación de los cambios incorporados (procesos y acciones)?	20	0
<i>Revisión y aprobación por la alta Dirección.</i>			
1	¿Se implementan las acciones correctivas y planes de mejora de la seguridad de la información?	20	0
Total de calificación para nivel Optimizado			

Luego de tener la calificación compare el resultado obtenido con la siguiente tabla de evaluación de cumplimiento del nivel de madurez optimizado.

Nivel optimizado

Nivel de cumplimiento	Mínimo	Máximo
Critico	0	31
Intermedio	32	53
Suficiente	54	90

 MINAGRICULTURA	INSTRUCTIVO	VERSIÓN 01
	DIAGNÓSTICO DE NIVEL DE IMPLEMENTACIÓN DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD	IN-GGT-01
		FECHA EDICIÓN 22-07-2016

Luego calcule el índice de eficacia en implementación del SGSI mediante la siguiente fórmula.

Eficacia en implementación del SGSI = $\frac{\text{Resultado de la encuesta de diagnóstico SGSI}}{\text{Máximo puntaje según nivel de madurez optimizado}} \times 100$

Si se logra el nivel 100% en el nivel de madurez gestionado cuantitativamente se puede evaluar el indicador para el nivel optimizado. En caso contrario la entidad debe cumplir todas las obligaciones del nivel optimizado.

Una vez la entidad logre el nivel de madurez optimizado puede definir nuevos indicadores para evaluar el desempeño o impacto de la implementación de su Sistema de gestión de seguridad de la información.

4. DOCUMENTOS DE REFERENCIA

Guía encuesta de Diagnóstico Modelo de Seguridad de la Información para las Entidades del Estado. MINTIC.

5. HISTORIAL DE CAMBIOS

Fecha	Versión	Descripción
22/07/2016	1	Primera versión del documento.