MINAGRICULTURA

Plan Operativo Anual SGSI 2017

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

MINISTERIO DE AGRICULTURA Y DESARROLLO RURAL

OFICINA DE LAS TECNOLOGIAS DE INFORMACIÓN Y LAS COMUNICACIONES

ENERO, 2017

1. Objetivo

El plan de gestión de seguridad de la información es el documento que define la estrategia y acciones necesarias para mantener y mejorar el sistema de gestión de seguridad de la información del Ministerio de Agricultura y Desarrollo Rural. En este documento se puede encontrar la descripción de las acciones para lograr el objetivo
propuesto.

2. Alcance del plan

El plan de gestión de seguridad de la información para el año 2017, cubre seis aspectos para mantener y mejorar el SGSI de la Entidad de forma que al finalizar el año, la entidad esté preparada para lograr la certificación ISO27001 de su SGSI. Las tareas que se describen en este documento son:

Diagnóstico de situación en seguridad
Sensibilización en seguridad
Recuperación ante desastres
Preparación para certificación del SGSI
Migración IPV4 IPV6
Relacionamiento Interinstitucional

3. Diagnóstico de situación en seguridad

Debido a los constantes cambios en las amenazas informáticas es necesario actualizar periódicamente el diagnóstico de seguridad de la información institucional con el fin determinar con precisión las acciones para el tratamiento de nuevos riesgos en materia de seguridad de la información. Las acciones necesarias desarrollar durante el primer y segundo semestre del año 2017 incluyen:

3.1. Nivel de riesgo en seguridad de la información institucional

Realizar sesiones de trabajo con todos los procesos y dependencias para actualizar el mapa de riesgos institucionales, el particular en aquellos aspectos relacionados con el riesgo de seguridad de la información a nivel tecnológico. Las sesiones de trabajo se programarán con el acompañamiento del grupo de administración del SIG

3.2. Análisis de vulnerabilidades

Durante el primer y segundo semestre del año 2017 y con el uso de software libre se realizarán pruebas de detección de vulnerabilidades a los servidores y aplicaciones web.

En los casos en que la criticidad de la plataforma sea calificada como alta se intentará la explotación de la vulnerabilidad para proponer tareas concretas de remediación.

3.3. Aseguramiento de plataformas

Con el acompañamiento de los administradores de plataforma se iniciará un programa anual de aseguramiento de servidores usando los resultados de las pruebas de detección de vulnerabilidades y el uso de plantillas de aseguramiento de servidores y plataformas como: Windows Server 2012 R2 Hardening Checklist, https://wikis.utexas.edu/display/ISO/Windows+Server+2012+R2+Hardening+Checklist

https://learn.cisecurity.org/benchmarks

4. Sensibilización en seguridad

La principal línea de defensa en materia de seguridad de la información es el usuario, una cadena es tan fuerte como el más débil de sus eslabones, es por esa razón con durante el año 2017 se debe reforzar al usuario la necesidad de identificar oportunamente los riesgos de seguridad, aplicar las políticas de seguridad de la información y adoptar las medidas de seguridad de la información necesarias para reducir las posibilidades de pérdida de confidencialidad, integridad y disponibilidad de la información institucional.

4.1. Capacitación de primeros respondientes

Aprovechando los resultados del contrato de diseño del SGSI ejecutado en el año 2015, se ejecutará el curso de preparación de primeros respondientes de incidentes de seguridad de la información para mejorar las competencias de funcionarios del ministerio y de representantes de las entidades del sector.

4.2. Sensibilización funcionarios

Mediante charlas en sitio y elementos electrónicos se buscará mejorar el nivel de conciencia en seguridad de la información en los siguientes aspectos:

a) Política general de la seguridad de la información
b) Políticas técnicas de seguridad de la información
c) Clasificación de la información
d) Uso seguro de servicios de almacenamiento en la nube

5. Recuperación ante desastres

Para fortalecer las capacidades de respuesta antes contingencias de orden de mayor y preparar la Ministerio para la certificación de su sistema de gestión de seguridad de la información, durante el año 2017 se realizarán las siguientes acciones

5.1. Actualización de DRP

Verificar la documentación de procedimientos de recuperación de plataformas informáticos y mecanismos de respuesta ante incidentes tecnológicos que impidan a prestación continua de servicios de las plataformas críticas

5.2. Probar el DRP

Una vez actualizado el plan de recuperación ante desastres se programarán y realizarán dos pruebas en las modalidades de:

a) Inspección y pruebas de escritorio
b) Verificación en sitio paso a paso del plan

De acuerdo con la disponibilidad de recursos se planificará una prueba de operación real en contingencia de algunos servicios críticos.

6. Preparación para certificación del SGSI

El objetivo principal del plan de seguridad de la información para el año 2017 es preparar al ministerio para optar por la certificación ISO 27001 de su SGSI. Este objetivo principal requiere:

6.1. Actualización documental

Aunque la documentación del SGSI ha estado en permanente actualización y revisión, es necesario mejorar aspectos como estándares de almacenamiento de evidencias, nuevos procedimientos y divulgación de procedimientos del SGSI. En particular es necesario:

6.1.1. Resolución de SIG

Durante el año 2016 se preparó la resolución de actualización del SIG para incorporar las funciones específicas del rol de oficial de seguridad de la información, el proyecto de resolución requirió de diversos ajustes en lo referente a otros subsistemas lo que freno la adopción formal del rol de oficial de seguridad de la información.

6.1.2. Inventario de información clasificada y reservada

Para dar cumplimiento a las obligaciones del decreto 103 de 2015, que reglamenta parcialmente la ley 1712 de 2014 sobre transparencia y acceso a la información pública, es necesario realizar un acompañamiento a todas las áreas del MinAgricultura para que construyan y documenten el inventario de información clasificada y reservada de todos los procesos institucionales.

6.1.3. Modelo de Referencia de Arquitectura Empresarial (MRAE)

La estrategia de gobierno en línea requiere de la adopción de diversos lineamientos en materia de seguridad de la información que deben ser preparados por el SGSI a fin de cumplir las metas del decreto 1078 de 2015

6.2. Actualización de panorama de riesgos

Como ya se había mencionado, semestralmente es obligación normativa realizar una revisión y actualización de los mapas de riesgos institucionales.

6.3. Autoevaluación del SGSI

Con miras a la certificación ISO27001 y a realización de la primera auditoria interna al SGSI, durante el primer semestre de 2017, se realizará un ejercicio de autoevaluación del estado de la seguridad de la información para preparar a los procesos de la OTIC para recibir formalmente la auditoria interna por parte de la oficina de control interno.

6.4. Auditoria interna SGSI

De acuerdo con la programación de auditorías internas, en el tercer trimestre de 2017, la oficina de control interno del MinAgricultura auditará el SGSI.

7. Migración IPV4 IPV6

Dada el cambio inminente del protocolo IPV4 a su nueva versión IPV6 debido a obsolescencia y brechas de seguridad, el Ministerio debe adelantar las acciones necesarias para planificar su cambio de dispositivos en el año 2018. Esta primer etapa del proceso de migración implicará:

7.1. Inventario de infraestructura de Comunicaciones

A lo largo del primer semestre de 2017 se debe documentar el conjunto de dispositivos y plataformas tecnológicas, incluidos sistemas de información y aplicaciones que estén haciendo uso las funcionalidades del protocolo IPV4 para poder determinar el alcance y requerimientos del plan de migración a IPV6 en el año 2018.

7.2. Plan de Migración de IPV a IPV6

Con la información de diagnóstico de situación en materia de IPV4, se preparará una estrategia y plan de acción para realizar ajustes y cambios en la infraestructura actual de comunicaciones y ejecutar las adecuaciones en el año 2018.

8. Relacionamiento Interinstitucional

Un aspecto fundamental en materia de seguridad de la información es establecer vínculos permanentes con grupos de interés y organizaciones dedicadas a la seguridad de la información. Continuando con las acciones adelantas en el año 2016, en el año 2017 se fortalecerán los vínculos con el Comando Conjunto de Operaciones Cibernéticas y las entidades del sector. Las acciones concretas incluyen:

8.1. Ciberseguridad Ciberdefensa

Participación en todas las sesiones que organice el Ministerio de Defensa Nacional para la implementación de la estrategia de gestión de riesgo, ciberseguridad y ciberdefensa definidas en el documento CONPES 3854 de ciberseguridad

8.2. Estado de implementación SGSI Sectorial

8.2.1. Medición de SGSI a nivel sectorial

Aprovechando los nuevos instrumentos elaborados por el MINTIC se actualizarán los diagnósticos del estado de la seguridad de la información y se documentarán los resultados del indicador de eficacia en la implementación del SGSI en el Ministerio.

8.3. Fortalecimiento de la seguridad de la información a nivel sectorial

Retomar el liderato en materia de seguridad e implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) es otro de los retos de la vigencia 2017. En ese sentido se realizarán actividades asociadas a:

8.3.1. Divulgación de políticas de seguridad

Socializar a todas las entidades del sector las políticas de seguridad de la información diseñadas dentro del marco del PETI del Ministerio de Agricultura y realizar sesiones de trabajo para identificar mecanismos para mejorar la seguridad de la información a nivel sectorial.

8.3.2. Apoyo a entidades

Apoyar a las entidades en el fortalecimiento de su SGSI a través de acampamiento, personalizado, mesas de trabajo y difusión de buenas prácticas en materia de seguridad de la información.

9. Anexos

Cronograma de trabajo
Presentación del Plan