PLAN DE SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACION 2017

MINISTERIO DE AGRICULTURA Y DESARROLLO RURAL

OFICINA DE LAS TECNOLOGIAS DE INFORMACIÓN Y LAS COMUNICACIONES

Actualización 21 de marzo de 2017

Contenido

Introducción

Este documento describe en forma detallada el plan de sensibilización en seguridad de la información para la vigencia 2017 en el MinAgricultura. En el documento se describen alcance del programa, actividades y metas a alcanzar.

Objetivos

Los objetivos principales del plan de sensibilización en seguridad para la vigencia 2017 son:

- Mejorar el conocimiento de los colaboradores del MinAgricultura en el SGSI
- Fortalecer las capacidades institucionales para dar prevenir y dar respuesta a eventos de seguridad
- Formar primeros respondientes en incidentes de seguridad.

Alineación a política institucional de seguridad de la información

El plan de sensibilización en seguridad de la información está alineado con la política de seguridad de la información en la medida que permite “la participación activa de los funcionarios, contratistas y terceros en lograr el nivel de cumplimiento adecuado de los lineamientos y requisitos de seguridad de la información”

Alcance

Todos los colaboradores del Ministerio se verán beneficiados con este plan de sensibilización al obtener un conocimiento adecuado de cómo manejar con seguridad su información en distintos dispositivos además de contextualizarse de las regulaciones que tiene el Ministerio para darle apoyo.

Roles involucrados

Directivos

Los niveles directivos del MinAgricultura apoyaran el desarrollo del plan de sensibilización en seguridad de la información mediante acciones como:

1) Autorizar a los colaboradores bajo su responsabilidad para participar en las sesiones presenciales de sensibilización que se desarrollen durante la vigencia

2) Fomentar la aplicación de las buenas prácticas de seguridad que divulgará el plan de sensibilización
3) Incluir en su revisión de plan de acción del proceso la evaluación de los resultados de las actividades de sensibilización en seguridad en las que participen su proceso
4) Participar de acuerdo con su disponibilidad en las actividades presenciales del plan de sensibilización
5) Propiciar el cumplimiento de las recomendaciones e instrucciones en materia de seguridad de la información que se divulguen dentro del marco del plan de sensibilización en seguridad de la información.

Líderes de proceso

1) Coordinar al interior de sus procesos la participación de los colaboradores en las actividades del plan de sensibilización
2) Participar en las actividades de sensibilización en seguridad programadas de acuerdo con su disponibilidad de tiempo
3) Velar porque las actividades de sus procesos apliquen las recomendaciones e instrucciones en materia de seguridad que se divulguen dentro del marco del plan de sensibilización en seguridad de la información
4) Medir la eficacia de los resultados de las actividades de sensibilización en las que participan los colaboradores de sus procesos
5) Identificar necesidades particulares en materia de sensibilización o capacitación en seguridad de la información para su proceso, colaboradores o la Entidad.

Responsables de seguridad de la información

1) Diseñar el plan de sensibilización en seguridad de la información, teniendo presente la misión de la Entidad y la relevancia que se busca para la cultura de la Entidad.
2) Identificar las necesidades y las prioridades que tenga la Entidad respecto al tema de sensibilización en seguridad de la información,
3) Estructurar el programa de sensibilización en seguridad de acuerdo con las necesidades de la Entidad y Recursos disponibles para su ejecución
4) Participar en el diseño de los materiales del programa de sensibilización
5) Participar en la implementación del programa de sensibilización
6) Consolidar los resultados de la evaluación de calidad y efectividad del programa de sensibilización
7) Identificar oportunidades de mejora para la planificación, diseño, implementación y evaluación del programa de sensibilización.

Administradores de sistemas de información

1) Participar en las actividades de sensibilización en seguridad de la información de acuerdo con su disponibilidad de tiempo y directrices de los responsables de procesos de la Entidad

2) Identificar los mecanismos que permitan implementar las recomendaciones y buenas prácticas del programa de sensibilización
3) Difundir entre los usuarios de los sistemas de información la adopción de las buenas prácticas de seguridad
4) Evaluar en conjunto con el responsable de proceso la efectividad de las actividades del programa de sensibilización en seguridad
5) Fomentar la implementación de las buenas prácticas de seguridad de la información propuestas por la campaña de sensibilización.

Funcionarios del MinAgricultura

1) Participar en las actividades del programa de sensibilización de acuerdo con la coordinación que realice el líder del proceso
2) Identificar formas de implementar en sus actividades diarias las recomendaciones y buenas prácticas del programa de sensibilización
3) Participar en la evaluación de la calidad, impacto y efectividad de las actividades del programa de sensibilización
4) Identificar oportunidades para el mejoramiento del programa de sensibilización
5) Proponer actividades y temas a tratar en futuros programas de sensibilización.

Metas del plan

El programa de sensibilización en seguridad de la información para la vigencia 2017 tiene como metas principales

1) Comunicar formalmente a toda la entidad la existencia del subsistema de gestión de seguridad de la información y sus componentes de apoyo
2) Socializar a todo el personal de la Entidad las políticas de seguridad de la información
3) Socializar los principales procedimientos de seguridad de la información
4) Fomentar la cultura de la seguridad de la información como herramienta de protección de la información institucional
5) Explicar de manera sencilla las normas legales que soportan el sistema de gestión de seguridad de la información
6) Divulgar a todos los funcionarios los principales riesgos de seguridad de la información
7) Explicar en manera sencilla en qué consisten diversos tipos de ataques informáticos y como controlarlos
8) Explicar los mecanismos de control dispuestos por la entidad para evitar ataques informáticos

Audiencia objetivo

Todos los colaboradores del Ministerio se verán beneficiados con este proyecto al obtener un conocimiento adecuado de cómo manejar con seguridad su información en distintos dispositivos además de contextualizarse de las regulaciones que tiene el Ministerio para darle apoyo.

Temáticas del plan de sensibilización 2017

Conocimiento general del Subsistema de gestión de seguridad

Se cubrirán conocimientos fundamentales de la seguridad de la información:

- Concepto de seguridad de la información
- Qué es un riesgo de seguridad de la información
- Qué la norma ISO27001 de gestión de seguridad de la información
- Cómo está estructurado el sistema de gestión de seguridad de la información
- Quienes son los actores del sistema de gestión de seguridad de la información

Conocimiento de las políticas de seguridad de la información

- Explicación de la política general de la seguridad de la información
- Explicación de las políticas de seguridad de la información con ejemplos de aplicación

Conocimiento de los procedimientos principales del Subsistema de gestión de seguridad

- Explicación del procedimiento de clasificación y etiquetado de información
- Explicación del procedimiento de Acceso a áreas seguras
- Metodología de gestión de riesgos y su anexo para identificación de riesgos de seguridad

Amenazas informáticas

- Phishing
- Ramsonware
- Robo de identidad

Generalidades sobre regulación en materia de seguridad de la información

- Ley de trasparencia y acceso a la información

Ley de protección de datos personales

Estrategia de gobierno en línea

Atención y respuesta a incidentes de seguridad de la información

Curso de primeros respondientes en incidentes de seguridad de la información

Actividades de sensibilización programadas

Campaña de sensibilización

Charlas y conferencias

Cursos

Concursos

Mensajes de correos electrónico

Publicaciones en pantallas

Elementos físicos de recordación

Materiales y recursos

mensajes electrónicos sobre que debe y que no debe hacerse.

videowalls o pantallas institucionales.

Screensavers con mensajes de sensibilización.

Elementos de oficina con mensajes alusivos.

Boletines vía email.

Eventos relacionados con seguridad (concursos, dramatizaciones)

Sesiones con instructores

Evaluación, Mejora y Seguimiento

La campaña se evaluará mediante encuesta electrónica en donde los colaboradores calificaran las diferentes actividades, su impacto y utilidad para el desarrollo de sus funciones asignadas.

Los resultados de la evaluación se incorporarán como ajustes en las actividades del programa de sensibilización en el segundo semestre de 2017

Campaña de sensibilización, INFOHÉROES 2, 2017

Justificación

- Infohéroes es un proyecto enfocado a informar y capacitar a los funcionarios del Ministerio de Agricultura y Desarrollo Rural sobre seguridad de la información y de qué manera influye en sus actividades diarias, además de cómo puede mejorar sus prácticas de seguridad informática.

- Se permitirá identificar el nivel de conocimiento relacionado con los temas impartidos dentro de la actividad por parte de los funcionarios.

Población beneficiaria

Todos los colaboradores del Ministerio se verán beneficiados con este proyecto al obtener un conocimiento adecuado de cómo manejar con seguridad su información en distintos dispositivos además de contextualizarse de las regulaciones que tiene el Ministerio para darle apoyo.

Objetivo general

Sensibilizar a los colaboradores del Ministerio de Agricultura y Desarrollo Rural en las buenas prácticas que existen entorno a seguridad de la

Objetivos específicos

- Realizar talleres de sensibilización en los distintos temas relacionados a la seguridad de la información.

    Clasificación de información

    Acceso a áreas seguras

    Criptografía

    Ley de transparencia y acceso a la información

    Escritorio limpio y pantalla limpia

- Impactar a la comunidad del Ministerio de agricultura y desarrollo Rural por medio de actividades de intervención publicitaria como lo son las actividades BTL o de reconocimiento lúdico.

- Informar a los funcionarios del Ministerio por distintos medios de comunicación sobre los avances en la implementación del subsistema de gestión de seguridad de la información

- Concientizar por medio de la entrega de elementos de merchandacing a los colaboradores del Ministerio de Agricultura y Desarrollo Rural sobre el uso responsable de los servicios informáticos y la aplicación de las políticas de seguridad de la información.

-Fomentar la participación de más funcionarios en la adopción de controles de seguridad para mitigar riesgos de pérdida de confidencialidad, integridad y disponibilidad de información institucional

Resultado esperado

Esperamos generar una cultura con respecto al uso responsable de la información, que se cambien los malos hábitos considerados como inseguros por comportamientos seguros respectos a la protección de la información institucional y de carácter personal. Dentro de las temáticas que se abordaran se contempla:

- Bloqueo de la sesión de trabajo al dejar solo el puesto de trabajo
- Uso de contraseñas seguras
- Mantenimiento del escritorio despejado y la pantalla limpia de información sensible
- Control de acceso a las áreas de almacenamiento de información reservada o sensible
- Clasificación de la información para su apropiada protección
- Políticas y procedimientos del subsistema de gestión de seguridad de la información
- Uso de técnicas de cifrado de datos para proteger la transmisión de información reservada o clasificada.

Localización

Las distintas actividades se disponen para ser realizadas en las instalaciones del MinAgricultura para facilitar el acceso de los funcionarios.

H. PLAZO ESTIMADO DE EJECUCIÓN Y FECHA DE INICIO

El proyecto de Infohéroes 2 se desarrollará en un tiempo de 1 mes para las distintas actividades planeadas, su fecha estimada de inicio es el 1 de mayo de 2017

Posibles actividades

1 Concurso trivia de la seguridad

Empleando las políticas de seguridad de la información se lanzarán trivias que debe resolver el participante para acumular puntos. Las preguntas se realizan sobre de las obligaciones descritas en las políticas TIC de la seguridad

2 Actividad No de papaya

Usando un personaje oculto en la entidad se identificarán estaciones de trabajo desatendidas en las cuales el personaje colocará un cartel con imagen de una papaya, el personaje se tomará una Selfie y la publicará en el micrositio de “no de papaya”, al finalizar la campaña se entregaran papayas a los usuarios de las estaciones desatendidas.

3 Lanzamiento de la liga de la seguridad y los villanos de la inseguridad

Mediante correos electrónicos se envían tips de seguridad y tips de inseguridad, los usuarios deben aprender que lo villanos también enviar mensajes para atacar a los usuarios.

4 Charlas y conferencias

Se propone la realización de las siguientes charlar con duración de 1 hora cada una.

- Clasificación de información
- Acceso a áreas seguras
- Criptografía
- Ley de transparencia y acceso a la información
- Escritorio limpio y pantalla limpia
- Formas comunes de ataque informático

Ideas clave a reforzar en la campaña

1) No responda a correos de desconocidos que lo invitan a establecer contacto

2) No consulte links en correos sospechosos que lo invitan a actualizar datos o resolver problema que usted no tiene

3) Siempre bloquee su sesión de trabajo cuando deje solo su puesto de trabajo

4) Guarde en lugar seguro documentos en papel cuando no los esté usando

5) Almacene en las carpetas compartidas la información vital de sus procesos

6) Adopte la práctica de escritorio despejado

7) Mejore la fortaleza de sus contraseñas

8) Porte su carnet en Lugar visible cuando este en las instalaciones del Ministerio

9) Proteja la información reservada con controles de seguridad

10) No de Papaya!

Charlas de sensibilización

Conocimiento general del Subsistema de gestión de seguridad

OBJETIVO: Explicar a todos los colaboradores del MinAgricultura qué es y para que sirve el subsistema de gestión de seguridad de la información.

ACTIVIDAD: Charla

CÓMO: exposición magistral

TIEMPO: 45 minutos

CUANDO: mayo 2017

RESPONSABLE: Juan Carlos Alarcón

RECURSOS: sala de conferencias, presentación de diapositivas

RESULTADOS: Los participantes podrán explicar cuáles son los beneficios de contar con un sistema de gestión de seguridad de la información

Conocimiento de las políticas de seguridad de la información

OBJETIVO: Explicar a los colaboradores del MinAgricultura, en dónde se pueden consultar y cuales son las principales políticas de seguridad

ACTIVIDAD: charla magistral

TIEMPO: 45 minutos

CUANDO: Junio de 2017

RESPONSABLE: Juan Carlos Alarcon

RECURSOS sala de conferencias, presentación de diapositivas

RESULTADOS: Los participantes podrán identificar cuales comportamientos de seguridad de la información se consideran correctos y cuales incorrectos.

Conocimiento de los procedimientos principales del Subsistema de gestión de seguridad

OBJETIVO: Explicar a los colaboradores del MinAgricultura, en dónde se pueden consultar y cuales son los procedimientos de uso más común del SGSI

ACTIVIDAD: charla Magistral

TIEMPO: 45 minutos

CUANDO: Julio de 2017

RESPONSABLE: Juan Carlos Alarcon

RECURSOS: sala de conferencias, presentación de diapositivas

RESULTADOS: Los participantes podrán determinar que procedimientos permiten identificar riesgos de seguridad, cómo se puede clasificar la información institucional, comó implementar áreas seguras de almacenamiento de información.

Amenazas informáticas

OBJETIVO: explicar a los colaboradores el modus operandi de los ataques informáticos mas comunes

ACTIVIDAD: charla magistral

TIEMPO: 45 minutos

(CUANDO): agosto de 2017

RESPONSABLE: Juan Carlos Alarcon

RECURSOS: sala de conferencias, presentación de diapositivas

RESULTADOS: Los participantes podrán explicar cómo se pueden identificar y proteger de los ataques informáticos más comúnmente utilizados

Generalidades sobre regulación en materia de seguridad de la información

OBJETIVO: Exponer la regulación que está directamente involucrada en el SGSI

ACTIVIDAD: charla magistral

TIEMPO: 45 minutos

CUANDO: septiembre de 2017

RESPONSABLE: Juan Carlos Alarcon

RECURSOS: sala de conferencias, presentación de diapositivas

RESULTADOS: el participante podrá identificar el objetivo de las principales regulaciones en materia de seguridad de la información.

Atención y respuesta a incidentes de seguridad de la información

OBJETIVO: Impartir un curso con certificación de primer respondiente de incidentes de seguridad de la información

ACTIVIDAD: curso formal

TIEMPO: 16 horas

CUANDO: abril de 2017

RESPONSABLE: Angelica Salinas

RECURSOS: sala de conferencias, presentación de diapositivas, instructor externo

RESULTADOS: Participantes certificados como respondientes ante incidentes de seguridad.

Mensajes propuestos sensibilización en seguridad de la información 2017

Tema: Seguridad en las estaciones de trabajo, Escritorio Limpio Pantalla Limpia

Mensaje: Bloquea tu sesión cuando dejes solo tu puesto de trabajo

¡ No doy Papaya!

Tema: Seguridad en las estaciones de trabajo, Contraseñas seguras

Mensaje:

Utiliza contraseñase que sean seguras, fáciles de recordar, difíciles de adivinar

- Evita usar tu datos personales en las claves
- Siempre memoriza tu clave, no la escribas
- Siempre incluye símbolos, letras y números en tus claves
- Cambia mensualmente tus claves

¡ No doy papaya!

Tema: Seguridad en las estaciones de trabajo, Clasificar, Ordenar, Limpiar

Mantén sobre tu escritorio únicamente los documentos necesarios para la labor que realizas

Ordena tu puesto de trabajo para saber siempre en dónde está cada cosa

Archiva documentos innecesarios que ya no utilices

¡No doy papaya!

Tema: Amenazas informáticas, Ramsonware

El ramsonware es un virus que cifra tus archivos impidiendo que se puedan leer. Después de cifrar los datos, el atacante pide dinero para recuperar los archivos.

Evita el ramsonware

- has copias de respaldo de los archivos importantes de trabajo en la carpeta compartida
- No descargues ni ejecutes adjuntos de correos electrónicos sospechosos
- Vacuna toda memoria que uses en tus cumputadores

¡No doy papaya!

Tema Amenazas informáticas, Phising

El phising es un ataque informático en el que el atacante intenta robar tus datos mediante correos o links a sitios falsos

Evita el phishing

- No hagas click en links de correos sospechosos
- No respondas a correos con invitaciones engañosas
- Recuerda. ¡De eso tan bueno no dan tanto!

¡No doy papaya!

Tema Amenazas informáticas, Robo de identidad

El robo de identidad es un delito en el cual:

1) Alguien roba tu información personal desde tus redes sociales, mediante el robo de tus documentos personales o aprovechando la información en físico que dejas descuidada
2) El atacante te suplanta y comete fraudes a tu nombre: toma créditos, crea perfiles falsos.

Evita el robo de identidad

- No hagas transacciones bancarias en café internet público
- Activa las opciones de seguridad de tus redes sociales
- Consulta regularmente tu historia financiero en CIFIN, Datacredito

¡No doy papaya!

Tema: Procedimientos SGSI, Áreas seguras

Un área segura es un espacio físico en donde se almacena o procesa información.

Las áreas seguras previenen la pérdida, daño o divulgación de la información institucional

1) Identifica si el proceso requiere uso de área seguras
2) Define el área segura con el procedimiento PR-GST-08
3) Define quienes tendrán acceso al área segura

   Todo visitante debe estar acompañado de una persona responsable cuando visite un área segura.
   Cuando no están en uso las áreas seguras deben estar cerradas.

¡No doy papaya!

Tema: Procedimientos del SGSI, Clasificación de la información

Protege la información la información personal de los beneficiarios de los programas del Ministerio de Agricultura. Evitar divulgación no autorizada de información

1) Identifica y clasifica la información usando el procedimiento PR-GST-10
2) Almacena en un área segura la información
3) Si tienes dudas… consulta con el líder del proceso si la información si la información se puede compartir

¡No doy papaya!

Tema: Procedimientos del SGSI, Transferencia de información

Antes de transferir información reservada o pública clasificada se deben establecer acuerdos para proteger la información:

1) Define qué información se va a transferir
2) Acuerda los protocolos a usar para garantizar la seguridad de los datos
3) Documenta los protocolos de intercambio
4) Verifica periódicamente el cumplimiento de los acuerdos

Oferta gratuita de cursos en seguridad de la información

Sena Sofia Plus

Controles y seguridad informática

Código 475198

http://oferta.senasofiaplus.edu.co/sofia-oferta/detalle-oferta.html?fm=0&fc=XvhTOnNfsMA

Gestión de la seguridad Informática

Código 731072

http://oferta.senasofiaplus.edu.co/sofia-oferta/detalle-oferta.html?fm=0&fc=4vVJM3GoTPA

Redes y Seguridad

Código 455101

http://oferta.senasofiaplus.edu.co/sofia-oferta/detalle-oferta.html?fm=0&fc=9CMnBjMmR6g

ESET

Curso de seguridad para padres

https://www.academiaeset.com/default/store/45327-curso-de-seguridad-para-padres

ESET

Uso seguro de medios informáticos

https://www.academiaeset.com/default/store/7116-uso-seguro-de-medios-informaticos

ESET

Seguridad en las transacciones comerciales en línea

https://www.academiaeset.com/default/store/7177-seguridad-en-las-transacciones-comerciales-en-linea

ESET

Seguridad para PyMEs

https://www.academiaeset.com/default/store/7203-seguridad-para-pymes

ESET

Navegación Segura

https://www.academiaeset.com/default/store/7383-navegacion-segura

ESET

Seguridad en dispositivos móviles

https://www.academiaeset.com/default/store/14041-seguridad-en-dispositivos-moviles