



El campo
es de todos

Minagricultura

protection



Plan de Sensibilización seguridad de la información

compute

Internet

Cyber
security



Oficina de Tecnologías de la Información y las Comunicaciones

Ministerio de Agricultura y Desarrollo Rural



1. Introducción

El objetivo de actualizar el **Plan de Sensibilización y Comunicación en materia de seguridad de la información**, del Ministerio de Agricultura y Desarrollo Rural, es incluir nuevas acciones de sensibilización y comunicación para lograr que un mayor número de colaboradores de la entidad apropien conceptos relacionados con seguridad de la información, aprendan a identificar, reportar y prevenir incidentes de seguridad de la información.

El presente documento contiene el plan general de actividades para la sensibilización en seguridad de la información en el Ministerio durante la vigencia 2020-2022.

2. Antecedentes

A lo largo de 2018 se desarrolló una campaña en dos bloques semestrales, que contempló actividades como charlas de sensibilización, medios electrónicos, concursos, personificaciones y uso de los medios de divulgación institucional como: Camponet, correo electrónico, video pantallas y una cuenta en Twitter.

3. Objetivos

3.1. Objetivo General

Definir estrategias para sensibilizar y comunicar a los colaboradores del Ministerio de Agricultura y Desarrollo Rural con el fin de aumentar la cultura de seguridad de la información.

3.2. Objetivos Específicos

- Reforzar y apropiar conceptos relacionados con la seguridad de información, que permitan salvaguardar la información institucional.
- Ejecutar las acciones establecidas en el presente Plan con el fin de fortalecer los controles de seguridad de información establecidos por los diferentes procesos en el marco del SGSI.
- Identificar las necesidades relacionadas con temas de seguridad de la información según el rol de los usuarios de la Entidad, con el fin de focalizar la estrategia de sensibilización y comunicación establecidas para la vigencia 2020-2022.



- Realizar seguimiento semestral al "Plan de comunicación y sensibilización en seguridad de información" con el fin de revisar e identificar el impacto de las actividades ejecutadas.

4. Alineación con la política general de seguridad y privacidad de la información.

El Plan de Sensibilización y Comunicación de Seguridad de la Información aporta en el cumplimiento del objetivo: "Sensibilizar a las partes involucradas (funcionarios, contratistas, terceros, proveedores) sobre aspectos relacionados con la Gestión de Seguridad de la Información, a fin de generar y fortalecer la cultura de seguridad de la información", de la política general de seguridad y privacidad de la información.

5. Usuarios y Responsabilidades

Para efectos del presente Plan se establecieron grupos de usuarios en el Ministerio de Agricultura y Desarrollo Rural y para cada grupo objetivos de conocimiento y responsabilidades, lo cual permitirá enfocar el esfuerzo de las actividades de comunicación y sensibilización.

5.1. Usuarios Directivos, coordinadores y/o líderes de proceso.

- Conocer las políticas institucionales relacionadas con la seguridad de la información y la protección de datos personales.
- Sensibilizar sobre el papel como líderes desde el ejemplo que tiene su rol al momento de orientar las actuaciones de los funcionarios y contratistas bajo su dirección, jefatura o supervisión, según aplique.
- Incentivar la aplicación de buenas prácticas en materia de seguridad de la información en las actividades laborales y en los proyectos que lideran.
- Incentivar a los colaboradores bajo su responsabilidad para participar en las sesiones (virtuales o presenciales) de sensibilización que se desarrollen.
- 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
- Participar de acuerdo con su disponibilidad en las actividades del plan de sensibilización



- Identificar necesidades particulares en materia de sensibilización o comunicación en seguridad de la información para su proceso, colaboradores o la Entidad.

5.2. Demás colaboradores (funcionarios, contratistas, terceros)

- Conocer las políticas institucionales relacionadas con la seguridad de la información y la protección de datos personales.
- Deben aplicar buenas prácticas en materia de seguridad de la información en las actividades laborales y en los proyectos en los que participan.
- Participar en las actividades del programa de sensibilización.
- Identificar formas de implementar en sus actividades diarias las recomendaciones y buenas prácticas del programa de sensibilización
- Participar en la evaluación de la calidad, impacto y efectividad de las actividades del programa de sensibilización
- Identificar oportunidades para el mejoramiento del programa de sensibilización
- Proponer actividades y temas a tratar en futuros programas de sensibilización.

5.3. Responsables del plan

El grupo de Uso y Apropiación y el Oficial de Seguridad de la Información serán los responsables de actualizar el Plan de Sensibilización y Comunicación de Seguridad de la Información, que está alineado con la misión institucional, las necesidades de la Entidad y recursos disponibles para su ejecución.

6. Canales de comunicación

6.1. Comunicación y sensibilización

6.1.1. Boletín informativo de la Oficina de Tecnologías de la Información y las Comunicaciones

- **Periodicidad:** Mensual
- **Insumo:** Noticias

Durante 2020, la Oficina TIC del Ministerio implementó un boletín informativo que tiene como objetivo dar a conocer la transformación digital del Ministerio y de sus entidades adscritas.



Este boletín tiene una sección denominada "**Seguridad de la información**" y tiene como objetivo comunicar noticias y avances de la entidad en materia de seguridad de la información.

6.1.2. Intranet Camponet

Periodicidad: Quincenal

Insumo: Recomendaciones/Tips

Para que las audiencias internas estén informadas la Intranet es una plataforma clave para este fin.

6.1.3. Correo electrónico

Periodicidad: Quincenal

Insumo: Recomendaciones/Tips

Canal de comunicación más consultado por los funcionarios y contratistas de la entidad.

6.2. Sensibilización

6.2.1. Teams- reuniones virtuales

Periodicidad: Mensual o cuando sea necesario

Insumo: Sensibilización TIC

Espacio para socializar temas de seguridad de la información en línea.

6.2.2. Videos

Periodicidad: Cada vez que sea necesario

Insumo: Resumen de información clave

Video de no más de 2 minutos con información clave sobre políticas relacionadas con la seguridad de la información.

7. Acciones de comunicación

7.1. Boletín informativo OTIC:

Contenidos propuestos:

- ABC de la Política de seguridad y privacidad de la información.



- "Editorial" sobre la seguridad de la información en el Ministerio
- Video sobre Política técnica TIC del Ministerio

7.2. Mailing (correo electrónico), ejemplos:

- Tip del mes (backup)

Tres razones por las cuales se debe hacer backup

1. Por un golpe o avería, el disco duro del computador podría estropearse junto con los archivos
2. Tienes la tranquilidad de tener los documentos más importantes a salvo
3. Si entra un virus al computador la información clave estará respaldada

- Tip del mes (contraseñas)

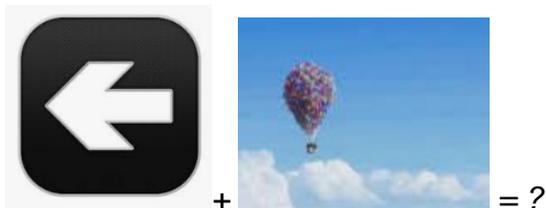
Cinco recomendaciones para proteger tus contraseñas:

1. No la compartas con ninguna persona
2. Cámbiala cada 45 días
3. No la escribas en un lugar visible
4. Evita contraseñas clásicas: 123456
5. Crea contraseñas seguras: letras, números, mayúsculas, minúsculas, caracteres especiales.

7.3. PausaTIC "Acertijo TIC", ejemplos:

1. Resuelve este acertijo TIC durante tu pausa activa del día

Ejemplo gráfico del acertijo:

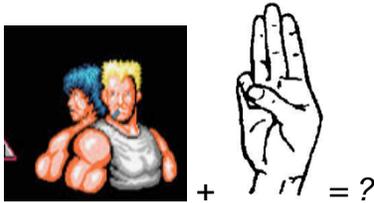


Respuesta: Back + up = Backup

2. Resuelve este acertijo TIC durante tu pausa activa del día



Ejemplo gráfico del acertijo:



Respuesta: Contra + seña = Contraseña

Teniendo en cuenta que el 30 de noviembre se celebra el "Día internacional de la seguridad de la información", la oficina TIC conmemorará este día durante todo el mes desarrollando acciones de comunicación incluidas en este Plan y visibilizándolas con un logo de "Mes de la seguridad informática".

7.4. Intranet “Camponet”

Actualización de la sección “Seguridad de la información” de la intranet con contenidos que orienten a los funcionarios y colaboradores

7.5. Postal de bienvenida sobre seguridad de la información a nuevos funcionarios y contratistas

Enviar una postal de bienvenida a cada nuevo funcionario y contratista del Ministerio de Agricultura que presente la información clave de seguridad de la información. Esta pieza llevará a un ABC de la seguridad de información en el Ministerio.

7.6. Feria virtual de seguridad de la información

Desarrollo de una jornada virtual donde se programen diferentes charlas y ejercicios de seguridad de la información para que los usuarios del Ministerio aprendan a identificar, reportar y prevenir incidentes de seguridad de la información.

7.7. Cartilla para directores y jefes de oficina



Explicar a los directivos y jefes de oficina del Ministerio de Agricultura y Desarrollo Rural, las políticas, responsabilidades y beneficios de la implementación de la seguridad de la información en la entidad.

Actividad: Cartilla en PDF

Temas para tratar: Políticas de seguridad y privacidad de la información, responsabilidades y beneficios de la ciberseguridad.

Recursos: Correo electrónico

7.8. Sesiones virtuales de sensibilización

Tema 1.

Título: **Políticas de seguridad de la información**

Objetivo:

Explicar a los colaboradores del Ministerio de Agricultura y Desarrollo Rural, la importancia del sistema de gestión de seguridad de la información, así como las políticas con las que cuenta actualmente el MADR

Tiempo estimado: 45 Min.

Actividad: Charla a cada una de las áreas del Ministerio.

Temas para tratar:

Que es información, activo de información y clasificación de los activos, que es seguridad de la información y privacidad de la información, regulación en temas de ciberseguridad en Colombia y políticas de seguridad de la información del MADR.

Recursos: Uso de la herramienta TEAMS

Resultados: Se medirá a través de una encuesta de satisfacción o de un cuestionario de evaluación.

Tema 2

Título: **Amenazas y riesgos cibernéticos**



Objetivo:

Explicar a los colaboradores del Ministerio de Agricultura y Desarrollo Rural, conceptos asociados a ciberseguridad, riesgos y vulnerabilidades, así como el modus operandi de los ataques informáticos más comunes.

Tiempo estimado: 45 Min.

Actividad: Charla a cada una de las áreas del Ministerio.

Temas para tratar:

Definición de conceptos (ciberespacio, ciberseguridad, amenazas, riesgos, ataques y vulnerabilidad), y principales ataques cibernéticos.

Recursos: Uso de la herramienta TEAMS

Resultados: Se medirá a través de una encuesta de satisfacción o de un cuestionario de evaluación.

Tema 3

Título: **Custodia digital y respuesta a incidentes**

Objetivo:

Explicar a los colaboradores del Ministerio de Agricultura y Desarrollo Rural, conceptos de custodia digital, así como temas asociados a respuesta de incidentes de seguridad de la información.

Tiempo estimado: 45 Min.

Actividad: Charla a cada una de las áreas del Ministerio.

Temas para tratar:

Definición de conceptos de delito cibernético, delito informático, cibercrimen, copias de seguridad, almacenamiento y gestión y respuesta a incidentes de seguridad de la información.

Recursos: Uso de la herramienta TEAMS

Resultados: Se medirá a través de una encuesta de satisfacción o de un cuestionario de evaluación.



Tema 4

Título: **Ataques dirigidos**

Objetivo:

Mostrar a los colaboradores del Ministerio de Agricultura y Desarrollo Rural, los resultados de los ataques dirigidos relacionados con los temas de las anteriores charlas.

Tiempo estimado: 45 Min.

Actividad: Charla a cada una de las áreas del Ministerio.

Temas para tratar:

Estadísticas de los ataques más comunes que se han materializado a nivel mundial, estadísticas de los reportes de incidentes de ciberseguridad, explicación de la forma como se realizaron los ataques.

Recursos: Uso de la herramienta TEAMS

Resultados: Se medirá a través de una encuesta de satisfacción o de un cuestionario de evaluación.