



SISTEMA DE GESTIÓN DE LA CALIDAD

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO Ó ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO
PROCEDIMIENTO PLAN DE CULTURA Y SENSIBILIZACIÓN DEL “SGSI”	

# PLAN DE CULTURA Y SENSIBILIZACIÓN DEL “SGSI” DEL INSTITUTO COLOMBIANO AGROPECUARIO “ICA” 2022

**Marzo 2022**

*Aprobado en Sesión III – 2022. Comité Institucional de Gestión y Desempeño (Ordinaria) del 18 de Marzo de 2022.*



SISTEMA DE GESTIÓN DE LA CALIDAD

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO Ó ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO
PROCEDIMIENTO PLAN DE CULTURA Y SENSIBILIZACIÓN DEL "SGSI"	

## CONTENIDO

INTRODUCCIÓN .....	3
1. POLÍTICA DE CULTURA Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN.....	3
2. METAS A CUMPLIR.....	3
2.1. Objetivo General.....	3
2.2. Objetivo Especifico .....	3
3. ETAPA No.1 – PLANEACIÓN .....	4
3.1. Roles y Responsabilidades.....	4
3.2. Audiencia Objetivo .....	4
3.3. Temas a tratar en cada sesión.....	5
3.4. Medios De Comunicación.....	5
3.5. Sensibilización.....	5
3.5.1. Frecuencias de la sensibilización .....	5
3.5.2. Evidencia del programa de sensibilización.....	5
3.5.3. Evaluación y renovación del plan de cultura de sensibilización del "SGSI" .....	6
3.5.4. Eslogan.....	6
3.5.5. Diseño de instrumento de medición .....	6
3.6. Cronograma De Actividades .....	6
3.6.1. Charlas de Sensibilización:.....	6
3.6.2. Difusión de Seguridad de la Información: .....	7
4. ETAPA No.2 – EJECUCIÓN .....	9
5. ETAPA No.3 – EVALUACIÓN.....	9

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO Ó ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO
PROCEDIMIENTO PLAN DE CULTURA Y SENSIBILIZACIÓN DEL "SGSI"	

## INTRODUCCIÓN

Para el Instituto Colombiano Agropecuario "ICA", la Seguridad de la Información es una parte esencial dado que permite mantener los pilares fundamentales como son: la Confidencialidad, Integridad y Disponibilidad de los activos más importante para la Entidad como es la INFORMACIÓN.

Para ello se requiere dar entrenamiento a los Funcionarios, Contratistas, Proveedores y/o Terceros de la Entidad, frente a la importancia de la Seguridad de la Información y los Riesgos asociados a los activos de información que se generan por el desconocimiento de las Políticas y controles establecidos, los cuales permiten minimizar el impacto y la probabilidad de la materialización de los mismos.

Por lo tanto, el Sistema de Gestión de Seguridad de la Información "SGSI" del Instituto Colombiano Agropecuario "ICA" se ve en la necesidad de implementar campañas de sensibilización dirigidas a los Funcionarios, Contratistas, Proveedores y/o Terceros; con el fin de crear cultura frente a los Riesgos de Seguridad de Información y coadyuvar en la búsqueda de medidas preventivas para establecer una mejora continua del "SGSI" para la Entidad.

Por lo anterior, con este Plan de Cultura y Sensibilización del SGSI, permite dar a conocer las Políticas de Seguridad establecidas y los temas del SGSI en todas las sedes de la Entidad.

### 1. POLÍTICA DE CULTURA Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

- **Dominio:** A.7.2.2 Toma de conciencia, educación y formación en la Seguridad de la Información.
- **Objetivo:** Sensibilizar a los Funcionarios, Contratistas, Proveedores y/o Terceros para la toma de conciencia frente a la Seguridad de la Información y sus responsabilidades.
- **Alcance del Plan de Cultura de Sensibilización del "SGSI":** La presente Política aplica para todos los Funcionarios, Contratistas, Proveedores y Terceros ubicados en: Oficinas Nacionales, las treinta y dos (32) Seccionales del ICA para el año 2020, los cuales deben participar activamente en el Plan de Cultura y Sensibilización del "SGSI" que realiza en la Entidad a través de la Oficina de Tecnología de Información "OTI". Esto se realizará según cronograma anexo.

### 2. METAS A CUMPLIR

#### 2.1. Objetivo General

Sensibilizar y crear conciencia a los Funcionarios, Contratistas, Proveedores y/o Terceros del Instituto Colombiano Agropecuario "ICA", frente a las buenas prácticas de Seguridad de Información, con el fin de proteger y resguardar los activos de Información a través de campañas y estrategias definidas en el Plan de Cultura de Sensibilización del "SGSI".

#### 2.2. Objetivo Especifico

- Definir campañas de sensibilización para el Instituto Colombiano Agropecuario "ICA".
- Utilizar los medios de difusión institucionales como herramientas para fomentar el Plan de Cultura de Sensibilización del "SGSI" del Instituto Colombiano Agropecuario "ICA".
- Promover las campañas de sensibilización al interior de la Entidad.
- Definir encuestas y evaluaciones para medir la percepción de la Seguridad de la Información en los Funcionarios, Contratistas, Proveedores y/o Terceros del Instituto Colombiano Agropecuario "ICA".

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO Ó ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO
PROCEDIMIENTO PLAN DE CULTURA Y SENSIBILIZACIÓN DEL “SGSI”	

### 3. ETAPA No.1 – PLANEACIÓN

#### 3.1. Roles y Responsabilidades

Se definen los roles y responsabilidades para la ejecución del Plan de Cultura de Sensibilización del “SGSI” dentro del Instituto Colombiano Agropecuario “ICA” así:

ROLES	RESPONSABILIDADES
Oficina Tecnología de Información (OTI).	<ul style="list-style-type: none"> <li>Definir las actividades para la ejecución del Plan de Cultura de Sensibilización del “SGSI” en Oficinas Nacionales, las treinta y dos (32) Seccionales del ICA para el año 2022.</li> <li>Diseñar instrumento de medición del Plan de Cultura de Sensibilización del “SGSI” en Oficinas Nacionales, las treinta y dos (32) Seccionales del ICA para el año 2022.</li> <li>Realizar seguimiento en el Plan de Cultura de Sensibilización del “SGSI” en Oficinas Nacionales, las treinta y dos (32) Seccionales del ICA para el año 2022.</li> <li>Aplicar instrumento de medición del Plan de Cultura de Sensibilización del “SGSI” en Oficinas Nacionales, las treinta y dos (32) Seccionales del ICA para el año 2022.</li> <li>Realizar análisis y consolidación de los resultados del Plan de Cultura de Sensibilización del “SGSI” en Oficinas Nacionales, las treinta y dos (32) Seccionales del ICA para el año 2022..</li> </ul>
Oficina Asesora de Comunicaciones	<ul style="list-style-type: none"> <li>Apoyar en la creación de piezas gráficas y material de diseño que se requiera para el Plan de Cultura de Sensibilización del “SGSI” en la Entidad.</li> <li>Apoyar en la publicación y difusión de las actividades del Plan de Cultura de Sensibilización del “SGSI”, en los diferentes medios de comunicación oficiales y existentes en la Entidad.</li> </ul>
Líder u oficial de seguridad	<ul style="list-style-type: none"> <li>Ejecutar las actividades relacionadas con el Plan de Cultura de Sensibilización del “SGSI” en Oficinas Nacionales, las treinta y dos (32) Seccionales del ICA para el año 2022.</li> <li>Aplicar los instrumentos de medición del Plan de Cultura de Sensibilización del “SGSI” en Oficinas Nacionales, las treinta y dos (32) Seccionales del ICA para el año 2022, los cuales fueron definido por la Oficina de Tecnología de Información “OTI”.</li> </ul>

Tabla No. 1 - Roles y Responsabilidades

#### 3.2. Audiencia Objetivo

**Quienes deben ser capacitados:** Los Funcionarios, Contratistas, Proveedores y/o Terceros ubicados en Oficinas Nacionales, las treinta y dos (32) Seccionales del ICA para el año 2022.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO Ó ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO
PROCEDIMIENTO PLAN DE CULTURA Y SENSIBILIZACIÓN DEL “SGSI”	

### 3.3. Temas a tratar en cada sesión

CRONOGRAMA JORNADAS DE SENSIBILIZACION PARA EL AÑO 2022	
ITEM	TEMA
1	Vishing – Smishing - Pautas para reconocer un sitio o mensaje de Phising
2	Protección de redes sociales (WhatsApp)
3	Autenticación de Doble Factor
4	Características de Contraseñas seguras
5	Gestión de Seguridad en Redes Sociales.
6	Suplantación de identidad o marca - registro abusivo de nombre de dominio
7	Continuidad del negocio
8	Gestión de riesgos
9	Reconocimiento de los principales ataques cibernéticos (tipos de malware, explotaciones día cero y conocidas)
10	Sistema de Gestión de Seguridad de la Información SGSI

Tabla No. 2 - Temas para sesiones

### 3.4. Medios De Comunicación

Para la gestión del Plan de Cultura y Sensibilización del “SGSI” en el Instituto Colombiano Agropecuario “ICA”, se tendrán en cuenta los siguientes medios de comunicación dentro de la Entidad, los cuales deberán ser publicados y socializados con el apoyo de la Oficina Asesora de Comunicaciones:

MEDIOS DE COMUNICACIÓN	DETALLE
Intranet.	<ul style="list-style-type: none"> <li>Se propone subir a la intranet los temas tratados en las charlas del “SGSI”, boletines emitidos por la policía nacional “PONAL”, videos de Seguridad, artículos publicados en la revista virtual, entre otros.</li> </ul>
Correo Masivo.	<ul style="list-style-type: none"> <li>A través de la Oficina Asesora de Comunicaciones, se propone dar a conocer a toda la Entidad temas detallados en el cronograma referente a:               <ol style="list-style-type: none"> <li>Boletines de CSIRT-PONAL.</li> <li>Correos de buenas prácticas de seguridad y tipos de ataques.</li> <li>NEW Informativos referente a fechas especiales con temas de Tecnología.</li> <li>Sesiones de Charlas virtuales programadas a través de la Oficina de Tecnologías.</li> </ol> </li> </ul>
Charlas Virtuales	<ul style="list-style-type: none"> <li>Se generarán charlas virtuales mediante herramientas tecnológicas definidas por el ICA como (Teams, Yammer, entre otros); para Oficinas Nacionales y Seccionales a través de La Oficina de Tecnología de Información “OTI”, Organizaciones y/o Proveedores de Seguridad de la Información en caso de ser necesario.</li> </ul>
Charlas Presenciales	<ul style="list-style-type: none"> <li>Se generarán charlas presenciales para Oficinas Nacionales a través de La Oficina de Tecnología de Información “OTI”, Organizaciones y/o Proveedores de Seguridad de la Información en caso de ser necesario.</li> </ul>

Tabla No. 3 - Medios de Comunicación

### 3.5. Sensibilización

#### 3.5.1. Frecuencias de la sensibilización

De acuerdo al cronograma de sensibilización definido para el año 2022.

#### 3.5.2. Evidencia del programa de sensibilización.

Lista de asistencia, registro fotográfico o evidencia generadas mediante herramientas tecnológicas y/o los medios de comunicación definidos.

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO Ó ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO
PROCEDIMIENTO PLAN DE CULTURA Y SENSIBILIZACIÓN DEL “SGSI”	

### 3.5.3. Evaluación y renovación del plan de cultura de sensibilización del “SGSI”

El Plan de Cultura y Sensibilización del “SGSI” de la Entidad, debe ser revisado y actualizado al inicio del año; teniendo en cuenta los resultados del año anterior con base a los instrumentos de medición definidos.

### 3.5.4. Eslogan

Se propone a través de la Oficina de Tecnología de Información “OTI”, la creación del eslogan que permite tener mayor recordación entre los funcionarios, contratistas, proveedores y/o terceros de la Entidad:

**“HAZ PARTE DE LA SEGURIDAD DE INFORMACIÓN, LA SEGURIDAD ES RESPONSABILIDAD DE TODOS”.**

### 3.5.5. Diseño de instrumento de medición

Para medir la percepción de la Seguridad de la Información dentro del Plan de Cultura y Sensibilización del “SGSI”, en los Funcionarios, Contratistas, Proveedores y/o Terceros, se define:

- a. **Matriz de medición:** tiene por objetivo medir las actividades definidas dentro del cronograma del Plan de Cultura y Sensibilización del “SGSI”, como son las charlas y los diferentes medios de comunicación.
- b. **Indicador:** tiene por objetivo medir la efectividad del Plan de Cultura y Sensibilización del “SGSI” en la Entidad, teniendo en cuenta los Funcionarios, Contratistas, Proveedores y/o Terceros.

**Nota:** Estos resultados serán el insumo al cumplimiento de los requisitos obligatorios de la Norma ISO 27001:2013 en el numeral 9.3 Revisión por la Dirección.

## 3.6. Cronograma De Actividades

### 3.6.1. Charlas de Sensibilización:

Se realizará sesiones virtuales con base a los diferentes temas propuestos, en conjunto con varias entidades del estado y proveedores, con el fin de llegar a cada uno de los Funcionarios, Contratistas, Proveedores y/o Terceros en Oficinas Nacionales y en las demás seccionales del ICA

CRONOGRAMA JORNADAS DE SENSIBILIZACION PARA EL AÑO 2022	
ITEM	TEMA
1	Vishing – Smishing – Pautas para reconocer un sitio o mensaje de Phising
2	Protección de redes sociales (WhatsApp)
3	Autenticación de Doble Factor
4	Características de Contraseñas seguras
5	Gestión de Seguridad en Redes Sociales.
6	Suplantación de identidad o marca - registro abusivo de nombre de dominio
7	Continuidad del negocio
8	Gestión de riesgos
9	Reconocimiento de los principales ataques cibernéticos (tipos de malware, explotaciones día cero y conocidas)
10	Sistema de Gestión de Seguridad de la Información SGSI

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO Ó ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO
PROCEDIMIENTO PLAN DE CULTURA Y SENSIBILIZACIÓN DEL "SGSI"	

Tabla No. 4 - Charlas de sensibilización.

**ESPECIFICACIONES:**

- ✓ Deben asistir a la charla de sensibilización Funcionarios, Contratistas, Proveedores y/o Terceros.
- ✓ La duración de la sesión es de una (1) hora, en la franja de 10:00am a 11:00am.
- ✓ Se realizará por medio de sesiones virtuales por medio de la aplicación Teams o por medio de la aplicación que se utilice para la sesión.
- ✓ Se enviará mediante correo electrónico la invitación a la reunión como también el agendamiento de la misma a través de la gerencia general.
- ✓ Se realizará medición de la charla de sensibilización con la utilización del "Indicador".

**3.6.2. Difusión de Seguridad de la Información:**

**3.6.2.1. Correo masivo miércoles de Buenas Practicas de Seguridad:**

A continuación, se describen las actividades a realizar los miércoles dos (2) veces en el mes desde mayo a diciembre del 2022, con el apoyo de la Oficina Asesora de Comunicaciones, a través del correo masivo a toda la Entidad:

ACTIVIDADES		MAY		JUN		JUL		AGO		SEP		OCT		NOV		DIC	
		11	25	8	22	6	27	10	24	7	21	12	26	21	16	7	21
1	Buenas Practicas: No almacenar contraseñas en el navegador	X															
2	Buenas Practicas: Cambio periódico la contraseña de sesión		X														
3	Buenas Practicas: Usar contraseñas robustas			X													
4	Buenas Practicas: Uso de doble Factor de autenticación				X												
5	Buenas Practicas: Mantener equipo y navegadores actualizados					X											
6	Buenas Practicas: No descargar programas o complementos						X										
7	Buenas Practicas: Verificar remitente de correo y abrir solo correos conocidos							X									
8	Buenas Practicas: Bloqueo de Sesión al retirar del puesto de trabajo								X								
9	Buenas Practicas: Utilizar solo equipos de confianza									X							
10	Buenas Practicas: Realizar copia de información importante en la nube										X						
11	Que es un Incidente de Seguridad											X					
12	Peligros en Redes Sociales												X				
13	Tipos de Ataques Informáticos - Ingeniería Social													X			
14	Tipos de Ataques Informáticos - Phising														X		
15	Tipos de Ataques Informáticos - Vishing															X	
16	Tipos de Ataques Informáticos - Malware																X

Tabla No. 6 – Cronograma de Miércoles de Buenas Practicas de Seguridad.

**ESPECIFICACIONES:**

- ✓ Se debe realizar para toda la Entidad.
- ✓ Se realizará los miércoles cada quince (15) días, como indica el cronograma anterior mediante correo masivo durante los meses de mayo a diciembre.
- ✓ Esta campaña debe tener el contenido según el tema definido en el cronograma anterior, y se debe publicar en la fecha definidas, debe ser llamativo y no denso de información manteniendo la imagen institucional con el apoyo de la Oficina Asesora de Comunicaciones.
- ✓ Se realizará medición de la campaña con la utilización de la "Matriz de medición".

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO Ó ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO
PROCEDIMIENTO PLAN DE CULTURA Y SENSIBILIZACIÓN DEL “SGSI”	

### 3.6.2.2. NEWS Informativos:

A continuación, se describen las actividades a realizar para los temas de “News Informativos”, de acuerdo a las fechas definidas para el año 2022, con el apoyo de la Oficina Asesora de Comunicaciones, a través del correo masivo a toda la Entidad y nota en la intranet:

CRONOGRAMA NEWS INFORMATIVOS PARA EL AÑO 2022		
ITEM	TEMA	FECHA
1	Día Mundial de la Copia de Seguridad	31 de Marzo
2	Día Mundial del Internet de las Cosas	09 de Abril
3	Día Mundial de la Ciencia y Tecnología	10 de Abril
4	Día Mundial de la Propiedad Intelectual	26 de Abril
5	Día Mundial de la Contraseña	05 de Mayo
6	Día Mundial del Internet	17 de Mayo
7	Día Mundial Contra la Falsificación y la Piratería	07 de Junio
8	Día Mundial de las Redes Sociales	30 de Junio
9	Día de la Tecnología Apropriada	15 de Julio
10	Día del Ingeniero	17 de Agosto
11	Día Mundial del Software Libre y Código Abierto	18 de Septiembre
12	Día Internacional de la Seguridad Informática	30 de Noviembre

Tabla No.7 – Cronograma de News Informativos.

#### ESPECIFICACIONES:

- ✓ Se debe realizar para toda la Entidad.
- ✓ Se realizará solo en la fecha especial de acuerdo al cronograma anterior.
- ✓ Esta campaña debe tener el contenido según el tema definido en el cronograma anterior, y se debe publicar en la fecha definidas, debe ser llamativo y no denso de información manteniendo la imagen institucional con el apoyo de la Oficina Asesora de Comunicaciones.
- ✓ Se realizará medición de la campaña con la utilización de la “Matriz de medición”.

### 3.6.2.3. Día de la Seguridad de La Información:

A continuación, se describen las actividades a realizar para el día Internacional de Seguridad de la Información, de acuerdo a las fechas definidas para el año 2022, con el apoyo de la Oficina Asesora de Comunicaciones, a través del correo masivo a toda la Entidad:

CRONOGRAMA JORNADA DE SENSIBILIZACION DIA DE LA SEGURIDAD DE LA INFORMACION		
ITEM	TEMA	FECHA
1	Temas de Seguridad con apoyo de Entidades Especializadas	30 de Nov

Tabla No.8 – Cronograma de Día de la Seguridad de la Información.

#### ESPECIFICACIONES:

- ✓ Se debe realizar para toda la Entidad.
- ✓ Se realizará solo en la fecha especial de acuerdo al cronograma anterior.



PROCESO GOBERNABILIDAD TICS	
SUBPROCESO Ó ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO
PROCEDIMIENTO PLAN DE CULTURA Y SENSIBILIZACIÓN DEL "SGSI"	

- ✓ Esta campaña debe tener el contenido según el tema definido en el cronograma anterior, y se debe publicar en la fecha definidas, debe ser llamativo y no denso de información manteniendo la imagen institucional con el apoyo de la Oficina Asesora de Comunicaciones.
- ✓ Se realizará medición de la campaña con la utilización de la "Matriz de medición".

#### 4. ETAPA No.2 – EJECUCIÓN

En esta etapa se establece la puesta en marcha del Plan de Cultura de Sensibilización del "SGSI", la cual fue definida en la "ETAPA No.1 – PLANEACIÓN".

##### Ejecución:

- a. Se debe tener lista de asistencia como evidencia.
- b. Se debe contar con registro fotográfico como evidencia.
- c. Se debe tener el contenido de las charlas como evidencia
- d. Se debe realizar evaluación sobre los temas socializados como evidencia.
- e. Se debe destinar un lugar de almacenamiento de las anteriores evidencias.

#### 5. ETAPA No.3 – EVALUACIÓN

En esta etapa se realiza el análisis de la información suministrada por los instrumentos de medición en la etapa No.1 del ítem 3.5.5 de este documento, que permiten mejorar en los siguientes ítems:

- a. Implementación del SGSI y el MSPI de la Entidad.
- b. Implementación de Controles del SGSI.
- c. Cambios o mejoras en el Plan de Cultura de Sensibilización del "SGSI" de la Entidad.
- d. Definición de los instrumentos de medición.

##### Evaluación:

- a. Documentados con el fin de identificar las lecciones aprendidas.
- b. Permite obtener los resultados de los instrumentos de medición diseñados etapa No.1 del ítem 3.5.5, para los resultados obtenidos de las actividades planteadas y ejecutadas del Plan de Cultura de Sensibilización del "SGSI".

<b>Nombre de quien Elabora:</b> DANNY PETER GUTIERREZ BELTRAN	<b>Nombre de quien Revisa:</b> JONATHAN ARDILA GALVIS	<b>Nombre de quien Aprueba:</b> JONATHAN ARDILA GALVIS
<b>Firma:</b>	<b>Firma</b>	<b>Firma</b>
<b>Cargo:</b> LÍDER U OFICIAL DE SEGURIDAD DE LA INFORMACIÓN	<b>Cargo:</b> JEFE DE OFICINA DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN	<b>Cargo:</b> JEFE DE OFICINA DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN