PLAN DE PROYECTO

para la implementación del Sistema de Gestión de Seguridad de la Información.

TICSOCIAL S.A.S

Versión:	002
Fecha de versión:	12 de diciembre de 2018
Creado por:	Diana Rodríguez
Aprobado por:	
Nivel de confidencialidad:	

El historial de cambios

Fecha	Versión	Creado por	Descripción del cambio
2018-11-23	0.1	Diana Rodríguez	Esquema básico del documento.
2018-12-12	0.2	Diana Rodríguez	Edición equipo del proyecto y listado de los documentos a realizar en el proyecto.

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS 43

2. DOCUMENTOS DE REFERENCIA 43

3. PROYECTO DE IMPLEMENTACIÓN SGSI 43

3.1. OBJETIVO DEL PROYECTO 43
3.2. RESULTADOS DEL PROYECTO 44
3.3. FECHAS LIMITE 45
3.4. ORGANIZACIÓN DEL PROYECTO. 46
3.4.1. Patrocinador de proyecto 46
3.4.2. Gerente del proyecto. 46
3.4.3. Equipo del proyecto. 46

***TABLA DE PARTICIPANTES EN EL PROYECTO* 46**

3.5. RIESGO PRINCIPAL DEL PROYECTO. 46
3.6. HERRAMIENTAS PARA LA IMPLEMENTACIÓN DE PROYECTOS, INFORMES. 46

4. GESTIÓN DE REGISTROS MANTENIDOS SOBRE LA BASE DE ESTE DOCUMENTO. 47

5. VALIDEZ Y GESTIÓN DOCUMENTAL. 48

1. Objetivo, alcance y usuarios

Se pretende analizar la situación actual de los procesos y estándares relacionados con la seguridad de la información en TICSOLCIAL S.A.S, para establecer un plan de implementación de un sistema de gestión de seguridad de la información, de manera que la empresa conozca la mejor manera de enfrentar los retos, cumpliendo con los estándares que integran los principios de negocio en los sistemas de gestión.

- Analizar la estructura de la organización sus características principales para proponer una metodología que permite efectuar el SGSI.
- Definir los parámetros para tener en cuenta para la implementación de SGSI junto con la norma ISO 27001 dentro de una organización.
- Ofrecer a la organización reportes, plantillas y seguimientos de las actividades y documentos realizados.

Los documentos a elaborar para el proyecto son:

- Lista de requisitos legales, reglamentarios, contractuales y otros
- Documento de alcance del SGSI.
- Política de seguridad de la información
- Evaluación de riesgos y metodología de tratamiento de riesgos.
- Plan de tratamiento de riesgos.
- Declaración de aplicabilidad.
- Requisitos legales, reglamentarios y contractuales.

Los siguientes documentos no son obligatorios para el proyecto,

- Procedimiento de control de documentos.
- Traiga su propia política de dispositivo (BYOD)
- Política de dispositivos móviles y teletrabajo.

Los usuarios involucrados en el proyecto son Robinson Salazar y Luis Fernando Morales quienes estarán a cargo de las revisiones, seguimiento y evolución del proyecto y Diana Rodríguez encargada de la realización de este.

2. Documentos de referencia

- Lista de documentos ISO 27001 (Revisión 2013)
- ISO/IEC 27001 standard

3. Proyecto de implementación SGSI

3.1. Objetivo del proyecto

Realizar la gestión documental por medio de una lista de verificación interna o checklist a través diagrama de flujo y plantillas los cuales se encontrarán a través de la herramienta CONFORMIO enfocado a la aplicación de la norma ISO 27001 para realizar el proceso de

implementación de un sistema de gestión de seguridad de la información (SGSI) para la empresa TICSOCIAL S.A.S con fecha de finalización para el día 22 de marzo de 2019.

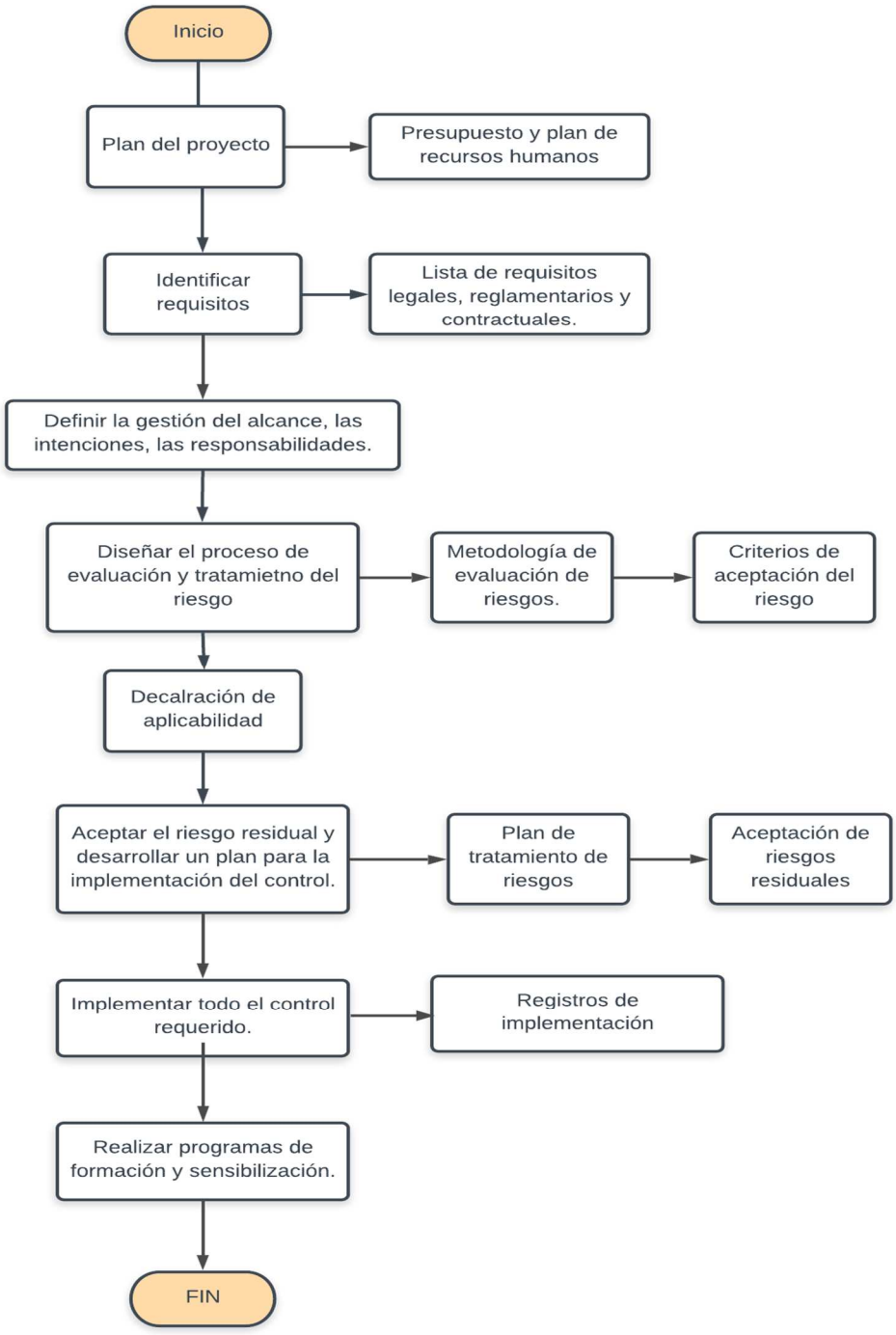


Imagen 1. Workflow Plan Implementación SGSI

3.2. Resultados del proyecto

Durante la elaboración del SGSI, se elaborarán los siguientes documentos:

- **Procedimiento para el control de documentos y registros**: procedimiento que prescribe reglas básicas para escribir, aprobar, distribuir y actualizar documentos y registros.
- **Procedimiento para la identificación de requisitos**: procedimiento para la identificación de obligaciones legales, reglamentarias, contractuales y de otro tipo.
- **Alcance del sistema de gestión de la seguridad de la información:** un documento que define con precisión los activos, ubicaciones, tecnología, etc. que forman parte del alcance.
- **Política de seguridad de la información:** este es un documento clave utilizado por la administración para controlar la administración de la seguridad de la información
- **Metodología de evaluación de riesgos y tratamiento de riesgos**: describe la metodología para administrar los riesgos de la información
- **Tabla de evaluación de riesgos:** la tabla es el resultado de la evaluación de valores de activos, amenazas y vulnerabilidades
- **Tabla de tratamiento de riesgos:** una tabla en la que se seleccionan los controles de seguridad apropiados para cada riesgo inaceptable
- **Informe de evaluación de riesgos y tratamiento de riesgos:** un documento que contiene todos los documentos clave realizados en el proceso de evaluación de riesgos y tratamiento de riesgos.
- **Declaración de aplicabilidad**: un documento que determina los objetivos y la aplicabilidad de cada control de acuerdo con el Anexo A de la norma ISO 27001
- **Plan de tratamiento de riesgos**: un documento de implementación que especifica los controles a implementar, quién es responsable de la implementación, los plazos y los recursos.

3.3. Fechas Limite

A continuación, se establece las fechas para la aceptación de los documentos individuales durante la implementación del SGSI:

Documento	***Fecha límite para la aceptación de documentos***
Lista de requisitos legales, reglamentarios, contractuales y otros.	15/03/2019
Documento de alcance del SGSI.	15/03/2019
Política de seguridad de la información	15/03/2019
Evaluación de riesgos y metodología de tratamiento de riesgos.	15/03/2019
Análisis de brechas	15/03/2019
Apéndice 1 - Tabla de evaluación de riesgos.	15/03/2019
Apéndice 2 - Tabla de tratamiento de riesgos.	15/03/2019
Apéndice 3 - Evaluación de riesgos e informe de tratamiento.	15/03/2019
Declaración de aplicabilidad.	15/03/2019
Plan de tratamiento de riesgos.	15/03/2019

La presentación final de los resultados del proyecto estará prevista para el día 25 de marzo de 2018

3.4. Organización del proyecto.

3.4.1. Patrocinador de proyecto.

Cada proyecto tiene un "patrocinador" asignado que no participa activamente en el proyecto. El gerente del proyecto debe informar regularmente al patrocinador del proyecto sobre el estado del proyecto e intervenir si el proyecto se detiene.

Guillermo Palacio, Gerente ha sido nombrado patrocinador del proyecto.

3.4.2. Gerente del proyecto.

El rol del gerente de proyecto es asegurar los recursos necesarios para la implementación del proyecto, coordinar el proyecto, informar al patrocinador sobre el progreso y llevar a cabo el trabajo administrativo relacionado con el proyecto. La autoridad del gerente del proyecto debe ser tal que garantice la implementación ininterrumpida del proyecto dentro de los plazos establecidos.

Robinson Salazar, Líder de desarrollo y tecnología.

3.4.3. Equipo del proyecto.

Tabla de participantes en el proyecto

Nombre	*Cargo*	*E-mail*
Robinson Salazar	Líder de desarrollo y tecnología	robinsonsalazar@ticsocial.com.co
Luis Fernando Morales	Líder de desarrollo y tecnología	luisfernandomorales@ticsocial.com.co
Diana Rodríguez	Analista de desarrollo	dianarodriguez@ticsocial.com.co

3.5. Riesgo Principal del proyecto.

El riesgo que mas puede afectar el proyecto es la extensión en los plazos en fases fundamentales del plan de implementación, que retasen de manera considerable la evolución del proyecto, no tener claridad en los riesgo e inseguridades sobre los cuales se desea hacer el plan de implementación ya que para un futuro cuando se desee llevar a cabo la implementación puede generar perdidas tanto en tiempo como económicas.

Para solventar dicho riesgo TICSOCIAL S.A.S tomo la decisión de asesorarse por una persona experta en temas de seguridad quien apoyara el proyecto, para proporcionar una guía y apoyo necesarios al plan de implementación y permitirá aclarar las dudas que vayan surgiendo en las diferentes fases del proyecto, para que al momento de dar inicio a la implementación de la norma se pueda ir a las fases de auditoria y certificación.

3.6. Herramientas para la implementación de proyectos, informes.

Mediante la herramienta Conformio se llevará a cabo el seguimiento del proyecto principalmente porque proporciona las plantillas de la documentación necesaria para la norma ISO/IEC 27001, y además que esta permite realizar una gestión de documentos en la nube en

donde esta disponible para los usuarios que la gerencia considere necesarios, asignar tareas sobre los documentos cargados, versiones y llevar a cabo revisiones.

4. Gestión de registros mantenidos sobre la base de este documento.

Todo el almacenamiento de los archivos se gestionará desde la plataforma CONFORMIO.

Nombre de Registro	*Ubicación de almacenamiento*	*Responsable del almacenamiento*	*Control para la protección de registros*	*Tiempo de retención*
Plan de proyecto	Carpeta compartida Inicio Plan implementación	Diana Rodríguez	Robinson Salazar	1 años
Procedimiento para el control de documentos y registros	Carpeta compartida Inicio Plan implementación	Diana Rodríguez	Robinson Salazar	3 años
Lista de requisitos legales, reglamentarios, contractuales y otros	Carpeta compartida Inicio Plan implementación	Diana Rodríguez	Robinson Salazar	1 años
Documentos de alcance del SGSI	Carpeta compartida Inicio Plan implementación	Diana Rodríguez	Robinson Salazar	1 años
Política de seguridad de la información	Carpeta compartida Inicio Plan implementación	Diana Rodríguez	Robinson Salazar	3 años
Evaluación de riesgos y metodología de tratamiento de riesgos	Carpeta compartida Inicio Plan implementación	Diana Rodríguez	Robinson Salazar	1 años
Tabla de evaluación de riesgos	Carpeta compartida Inicio Plan implementación	Diana Rodríguez	Robinson Salazar	1 años
Tabla de tratamiento de riesgos	Carpeta compartida Inicio Plan implementación	Diana Rodríguez	Robinson Salazar	1 años

Evaluación de riesgos e informa de tratamiento	Carpeta compartida Inicio Plan implementación	Diana Rodríguez	Robinson Salazar	1 años
	Carpeta compartida Inicio Plan implementación	Diana Rodríguez	Robinson Salazar	1 años
Declaración de aplicabilidad	Carpeta compartida Inicio Plan implementación	Diana Rodríguez	Robinson Salazar	1 años
Plan de tratamiento de riesgos	Carpeta compartida Inicio Plan implementación	Diana Rodríguez	Robinson Salazar	1 años

5. Validez y gestión documental.

Este documento es válido a partir de 23 de noviembre de 2018.

El propietario de este documento es TICSOCIAL S.A.S

Al evaluar la efectividad y la adecuación de este documento, se deben considerar los siguientes criterios:

- Si todos los empleados que participan en el proyecto realizan sus actividades de acuerdo con este documento
- Si se cumplen todos los plazos del proyecto

Ingeniero de Sistemas - Líder de Desarrollo y Tecnología
Robinson Salazar Grimaldos

_____

PROCEDIMIENTO PARA EL CONTROL DE DOCUMENTOS Y REGISTROS

TICSOCIAL S.A.S

Versión:	001
Fecha de versión:	30 de noviembre de 2018
Creado por:	Diana Rodríguez
Aprobado por:	
Nivel de confidencialidad:	

El historial de cambios

Fecha	Versión	Creado por	Descripción del cambio
2018-11-30	0.1	Diana Rodríguez	Esquema básico del documento.

Tabla de contenido

1. PROPÓSITO, ALCANCE Y USUARIOS 51

2. DOCUMENTOS DE REFERENCIA 51

3. CONTROL DE DOCUMENTOS INTERNOS 51

3.1. FORMATO DE DOCUMENTO 51
3.2. APROBACIÓN DE DOCUMENTOS 51
3.3. PUBLICACIÓN Y DISTRIBUCIÓN DE DOCUMENTOS. 51
3.4. ACTUALIZACIONES DE DOCUMENTOS Y CONTROL DE REGISTROS 52

4. VALIDEZ Y GESTIÓN DOCUMENTAL 52

6. Propósito, alcance y usuarios

El propósito de este documento es llevar un control sobre la creación, apropiación, distribución, uso y actualización de los documentos que se llevaran a cabo a lo largo del desarrollo del proyecto.

Los usuarios que estarán involucrados en este seguimiento son Robinson Salazar y Luis Fernando Morales.

7. Documentos de referencia

- Norma ISO / IEC 27001, cláusula 7.5

8. Control de documentos internos

Para poder llevar un adecuado seguimiento del proceso y los avances del proyecto, se cuenta con la herramienta CONFORMIO en donde se irán cargando los documentos que se vayan realizando y donde se permite realizar comentarios sobre los archivos.

Ya que a medida que el proyecto avance pueden surgir cambios en los documentos, se llevara un control de estos cambios por versiones dentro del documentos mediante una tabla para ver el histórico de los cambios.

8.1. Formato de documento

El texto del documento se escribe con la fuente Calibri, tamaño 11. Los títulos de los capítulos se escriben con el tamaño de fuente 14 en negrita, mientras que los títulos de los capítulos del nivel 2 se escriben en tamaño de fuente 12 en negrita. Los títulos de los capítulos del nivel 3 están escritos en tamaño de fuente 11 negrita cursiva.

El encabezado del documento contiene el nombre de la organización y el nivel de confidencialidad. El pie de página contiene el nombre del documento, la versión actual y la fecha del documento, y el número de páginas.

Tabla de historial de cambios.

Cada documento también debe definir sus usuarios.

8.2. Revisión y aprobación de documentos

Todos los documentos sean nuevos o versiones nuevas, llevará un proceso de revisión y aprobación a cargo de la gerencia, la aprobación se llevará a cabo a través de la plataforma Conformio, desde donde se irá subiendo cada uno de los documentos nuevos o sus nuevas versiones.

8.3. Publicación y distribución de documentos.

La publicación y distribución de los documentos también se realizará mediante la plataforma Conformio, por esta razón la confidencialidad de los documentos estará dada solamente para los usuarios que tengan acceso a dicha plataforma, los cuales son Robinson Salazar y Luis Fernando Morales como representantes del área de gerencia y Diana Rodríguez quien está a cargo de la elaboración del plan de implementación.

8.4. Actualizaciones de documentos y control de registros.

Para cada actualización o cambio que se realice dentro de un documento se llevara el seguimiento y un historial de cambios y quien estuvo a carga de realizar dichos cambios y/o actualizaciones

De igual manera si otra persona dentro de la organización solo tendrá acceso a estos documentos una vez se le haya gestionado el permiso.

9. Validez y gestión documental

Establecer la fecha de validez y el propietario del documento, y los compromisos que tendría para con dicho documento a lo largo de la duración del proyecto. Para evaluar la efectividad y la adecuación de los documentos definir criterios de realización y evaluación para llevar un estándar.

Ingeniero de Sistemas - Líder de Desarrollo y Tecnología
Robinson Salazar Grimaldos

_____

TICSOCIAL S.A.S

Apéndice - Lista de requisitos legales, reglamentarios, contractuales y otros

A continuación, se listan los requisitos normativos y estatutarios que se deberán cumplir para la implementación el sistema de seguridad de la información.

Requisito	***Documento que estipula el requisito***
Artículo 9º. Integridad de un mensaje de datos.	LEY 527 DE 1999
Artículo 11. Criterio para valorar probatoriamente un mensaje de datos.	LEY 527 DE 1999
Artículo 12. Conservación de los mensajes de datos y documentos.	LEY 527 DE 1999
Artículo 18. Concordancia del mensaje de datos enviado con el mensaje de datos recibido	LEY 527 DE 1999
Artículo 20. Acuse de recibo	LEY 527 DE 1999
Artículo 7°. Deberes de los operadores de los Bancos de Datos	LEY ESTATUTARIA 1266 DEL 31 DE DICIEMBRE DE 2008
ARTÍCULO 1o. (Artículo 269B.) Obstaculización ilegitima de sistema informático o red de telecomunicación	LEY 1273 DE 2009
ARTÍCULO 1º. (Artículo 269F.) Violación de datos personales	LEY 1273 DE 2009
Artículo 2º. Naturaleza.	LEY 1065 DE 2006 (Modificada en la resolución 284, 21 de febrero, 2008)
Artículo 2º. Ámbito de la aplicación.	Ley Estatutaria 1581 de 17 de octubre de

	2012
Artículo 3º. Definiciones	Ley Estatutaria 1581 de 17 de octubre de 2012
Artículo 4º. Principio para el Tratamiento de datos personales	Ley Estatutaria 1581 de 17 de octubre de 2012
Artículo 5º. Datos sensibles	Ley Estatutaria 1581 de 17 de octubre de 2012
Artículo 6º. Tratamiento de datos sensibles.	Ley Estatutaria 1581 de 17 de octubre de 2012
Artículo 8º. Derechos de los titulares.	Ley Estatutaria 1581 de 17 de octubre de 2012
Artículo 9º. Autorización del titular.	Ley Estatutaria 1581 de 17 de octubre de 2012
Artículo 11º. Suministro de la información.	Ley Estatutaria 1581 de 17 de octubre de 2012
Artículo 12º. Deber de informar al titular.	Ley Estatutaria 1581 de 17 de octubre de 2012
Artículo 13º. Personas a quien se les puede suministrar la información	Ley Estatutaria 1581 de 17 de octubre de 2012
Artículo 14º. Consultas.	Ley Estatutaria 1581 de 17 de octubre de 2012
Artículo 15º. Reclamos.	Ley Estatutaria 1581 de 17 de octubre de 2012
Artículo 17º. Deberes de los responsables del Tratamiento	Ley Estatutaria 1581 de 17 de octubre de 2012
Artículo 18º. Deberes de los encargados del tratamiento	Ley Estatutaria 1581 de 17 de octubre de 2012
Artículo 19º.Autoridad de protección de datos	Ley Estatutaria 1581 de 17 de octubre de 2012
Artículo 27º. Normas Corporativas Vinculantes	Ley Estatutaria 1581 de 17 de octubre de 2012

REFERENCIAS

[1] https://www.sisben.gov.co/Documents/Informaci%C3%B3n/Leyes/LEY%20TRATAMIENTO%20DE%20DATOS%20-%20LEY%201581%20DE%202012.pdf

Ingeniero de Sistemas - Líder de Desarrollo y Tecnología

Robinson Salazar Grimaldos

_____

DOCUMENTOS ALCANCE DEL SGSI

TICSOCIAL S.A.S

Versión:	002
Fecha de versión:	5 de enero de 2019
Creado por:	Diana Rodríguez
Aprobado por:	
Nivel de confidencialidad:	

El historial de cambios

Fecha	**Versión**	**Creado por**	**Descripción del cambio**
2018-12-10	0.1	Diana Rodríguez	Esquema básico del documento.
2019-01-05	0.2	Diana Rodríguez	Reestructura del alcance del SGSI.

Tabla de Contenido

1. PROPÓSITO, ALCANCE Y USUARIOS 58

2. DOCUMENTOS DE REFERENCIA 58

3. DEFINICIÓN DEL ALCANCE DEL SGSI 58

3.1. PROCESOS Y SERVICIOS 59
3.2. UNIDAD ORGANIZACIONAL 60
3.3. UBICACIÓN 60
3.4. RED E INFRAESTRUCTURA DE TI 60

4. VALIDEZ Y GESTIÓN DOCUMENTAL 61

5. REFERENCIAS 61

1. Propósito, alcance y usuarios

El propósito de este documento es definir el alcance que tendrá el plan de implementación dentro de TICSOCIAL S.A.S, basado y guiado con la documentación pertinente a las actividades dentro del SGSI.

Los usuarios involucrados en este seguimiento son Diana Rodríguez a cargo de la construcción del alcance y Robinson Salazar quien supervisara que lo plasmado este acorde a las necesidades de la empresa.

2. Documentos de referencia

- ISO/IEC 27001 standard, clausula 4.1, 4.2, 4.3
- Plan de proyecto

3. Definición del alcance del SGSI

La definición del alcance del SGSI esta vinculados con el contexto en el que se desenvuelve la empresa, las necesidades y las expectativas de las partes interesadas y en la necesidad de proteger la información que se manipula por medio de autentificaciones y controles de seguridad.

Para realizar un plan de implementación del SGSI adecuado, se debe comprender el contexto en el que se encuentra la organización, evaluando factores internos y factores externos que influyan en los propósitos de la empresa y un análisis sobre los procesos efectuados en la empresa para poder evaluar si los resultados esperados se están consiguiendo y como se daría la relación con el SGSI. Los puntos a tener en cuenta para una adecuada definición del alcance son:

a) **Factores Internos:** Al analizar estos factores se encuentra la falta de definición de objetivos, políticas y estrategias para el crecimiento, ampliación en los procesos que se efectúan los cuales a la hora de elaborar el SGSI son necesario para definir escalas de riesgo. [1]
b) **Factores Externos:** Ya que en estos factores no se puede tener el control de cómo se afectará de manera directa, se hace necesario tener planes de contingencia que permitan disminuir sus impactos en los siguientes aspectos:
    - Social.
    - Legal.
    - Tecnológico.
    - Cultura.

El alcance que tendrá el SGSI es de manera interna de tal forma que las actividades que se van a realizar sean más fáciles para controlar y verificar que se cumpla bajo los requisitos normativos y leyes que rigen dichas actividades:

Ley 527 de 1999 [2]

> **ARTÍCULO 2° DEFINICION.** Mensajes de datos: La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudiera ser, entre otros, el intercambio electrónico, internet, correo electrónico, etc.
>
> Intercambio Electrónico de datos: La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo las normas técnicas convenidas al efecto
>
> Sistema de Información: Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna u otra forma mensajes de datos.

Ley 1581 de 17 octubre de 2012 [3]

> Artículo 2°. Ámbito de aplicación. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.
>
> Tener en cuenta el documento de lista de requisitos legales, reglamentarios, contractuales y otros, en el cual se especifica los artículos aplicables

Se debe tener en cuenta las necesidades y expectativas de las partes interesadas en la implementación del SGSI, para el caso de TICSOCIAL sus clientes requieren que se les asegure la confidencialidad de la información que es brindada a la empresa.

Siguiendo la metodología de la norma ISO 27001 la cuál esta basada en el ciclo de mejora continua PDCA, se hace necesario aclarar que de las fases que componen este ciclo (Planear, Hacer, Verificar, Actuar), se enfatizará principalmente en la primera fase **Planear** ya que es hasta donde el alcance del plan implementación desea llegar y que de tal manera que al ingresar a las demás fases ya todo se encuentre definido de manera correcta.

3.1. Procesos y servicios

Al revisar el alcance a través del enfoque de los procesos, se evidencia que TICSOCIAL no cuenta con un mapa de procesos de las actividades que realiza, se informa de esto a la parte de gerencia ya que es necesario tener definido dicho mapa para la identificación de los activos, riesgos y amenazas que son vitales en este plan de implementación. Para garantizar la continuidad del plan de implementación se crea un mapa de procesos macro, que permita tener claridad sobre las áreas involucradas.

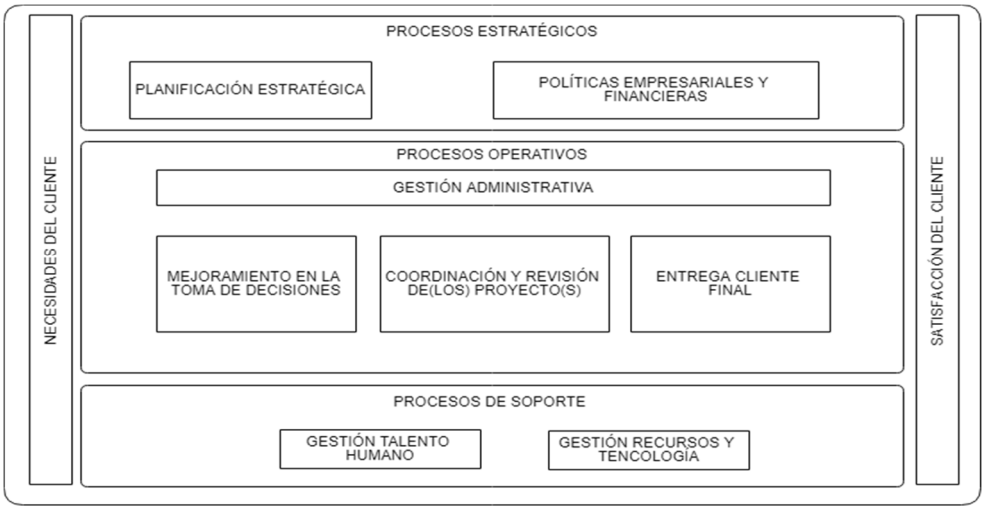


Imagen 2. Mapa Procesos TICSOCIAL

Los procesos que estarían dentro del alcance del SGSI serian:

Mejoramiento en la toma de decisiones: Al tomar este proceso se podrá evidenciar de manera directa cuales son los riesgos en los que se está incurriendo a nivel de las decisiones tomadas y cuanto impactan en los demás procesos asociados.

Coordinación y revisión de (los) proyecto(s): Verificar la elaboración de planes de acción para cada uno de los proyectos que se encuentran vigentes, donde se podrán evaluar posibles riesgos y buscar soluciones anticipadas.

Entrega cliente final: En este proceso donde está la intervención del cliente es importante para poder evidenciar otras vulnerabilidades que dentro de la empresa no se haya evidenciado, se hagan las correcciones necesarias y se tengan en cuenta para los próximos proyectos.

En cuanto a los servicios que se usan dentro de la empresa, el principal proveedor es Amazon Web Service (AWS), allí se encuentran gran parte de la información que se maneja, con servicios en la nube, escritorios virtuales y repositorios, además de este, el servicio de soporte que se le brinda a los clientes es de los más valiosos, ya que permite que los proyectos vigentes tengan un apoyo en tiempo real para que este funcione de la manera correcta y ayuda a los usuarios a entender el funcionamiento del mismo.

3.2. Unidad organizacional

Los equipos y activos físicos son los equipos usados por el área de desarrollo y el área gerencial que consta de 15 computadores con SO entre Linux y Windows.

3.3. Ubicación

La oficina de TICSOCIAL se encuentra ubicada en la Calle 26 a- 13 -97 Oficina 2202 - 2203

3.4. Red e infraestructura de TI

- Router TP-LINK TL-WR720N
- TP-LINK TL-SG1024D
- UNIFI| AP Indoor 802.11n Acces Point
- Modem ZTE
- Impresora Laser Samsung M2070FW

4. Validez y gestión documental

Este documento será revisado y podrá ser modificado por Diana Rodríguez, Robinson Salazar y Luis Fernando Morales a medida que el desarrollo del plan de implementación se vaya efectuando y si se cree conveniente para lograr la efectividad del documento.

5. Referencias

[1] Web TICSOCIAL S.A.S (11 diciembre de 2018) [Internet]. Disponible en: http://www.ticsocial.com.co/nosotros/

[2] Ley 527 de 1999 (11 diciembre de 2018) [Internet]. Disponible en: http://www.hostingred.com/ley_527_1999.pdf

[3] Ley 1581 de 2017 (11 diciembre de 2018) [Internet]. Disponible en: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf

Ingeniero de Sistemas - Líder de Desarrollo y Tecnología
Robinson Salazar Grimaldos

_____

POLITICA DE SEGURIDAD DE LA INFORMACIÓN



TICSOCIAL S.A.S

Versión:	002
Fecha de versión:	12 de febrero de 2019
Creado por:	Diana Rodríguez
Aprobado por:	
Nivel de confidencialidad:	

El historial de cambios

Fecha	**Versión**	**Creado por**	**Descripción del cambio**
2018-12-10	0.1	Diana Rodríguez	Esquema básico del documento.
2019-02-12	0.2	Diana Rodríguez	Correcciones al documento

Tabla de contenido

1. PROPÓSITO, ALCANCE Y USUARIOS 64

2. DOCUMENTOS DE REFERENCIA 64

3. TERMINOLOGÍA BÁSICA DE SEGURIDAD DE LA INFORMACIÓN [1] 64

4. GESTIONANDO LA SEGURIDAD DE LA INFORMACIÓN. 65

4.1. OBJETIVOS Y MEDIDA 65

4.2. REQUISITO DE SEGURIDAD DE LA INFORMACIÓN. 66

4.3. CONTROLES DE SEGURIDAD DE LA INFORMACIÓN. 66

4.4. RESPONSABILIDADES. 66

4.4.1. Responsabilidades de la alta dirección: 66

4.4.2. Responsabilidades del área de gestión administrativa: 66

4.4.3. Responsabilidades del área TIC: 67

4.4.4. Responsabilidades de gestión de riegos de la S.I.: 67

4.4.5. Responsabilidades de los funcionarios, contratistas y terceros: 67

5. SOPORTE PARA LA IMPLEMENTACIÓN DEL SGSI. 67

6. VALIDEZ Y GESTIÓN DOCUMENTAL 67

7. REFERENCIAS 68

1. Propósito, alcance y usuarios

El objetivo de este documento es definir el propósito, las instrucciones, los principios y las reglas básicas a tener en cuenta para ser implementado en el SGSI siguiendo lo definido en el documento de alcance y acorde al propósito que se tiene en TICSOCIAL S.A.S y en el cual se evidencia el compromiso por parte de la gerencia a realizar las medidas necesarias para garantizar la política de seguridad.

Los usuarios involucrados en este seguimiento son Diana Rodríguez a cargo de la construcción del alcance y Robinson Salazar quien supervisara que lo indicado tenga la finalidad adecuada y sea posible.

2. Documentos de Referencia

- ISO/IEC 27001 standard, clausulas 5.2, 5.3, 6.2
- Documento de alcance del SGSI
- Evaluación de riesgos y metodología de tratamiento de riesgos.
- Declaración de aplicabilidad
- Lista de requisitos legales, reglamentarios, contractuales y otros

3. Terminología básica de seguridad de la información [1]

- **Confidencialidad:** Requisito de seguridad que indica que el acceso a los recursos de sistema debe estar limitado exclusivamente a los usuarios con acceso autorizado.
- **Disponibilidad:** Requisito de seguridad que implica que la información y los servicios del sistema continúen en funcionamiento y que los usuarios autorizados puedan acceder a los recursos cuando lo necesiten, dónde lo necesiten, y en la forma en que lo necesiten.
- **Integridad:** Requisito de seguridad que indica que la información deberá ser protegida ante alteraciones.
- **Privacidad:** Estar libre de accesos no autorizados.
- **Amenaza**: Situación o evento con que puede provocar daños en un sistema.
- **Análisis de vulnerabilidades**: Análisis del estado de la seguridad de un sistema o sus componentes mediante el envío de pruebas y recogida de resultados en intervalos.
- **Cortafuegos:** Herramienta de seguridad que proporciona un límite entre redes de distinta confianza o nivel de seguridad mediante el uso de políticas de control de acceso de nivel de red.
- **Gestión de seguridad:** 1. Proceso de establecer y mantener la seguridad en un sistema o red de sistemas informáticos. Las etapas de este proceso incluyen la prevención de problemas de seguridad, detección de intrusiones, investigación de intrusiones, y resolución. 2. En gestión de redes, controlar (permitir, limitar, restringir, o denegar) acceso a la red y recursos, buscar intrusiones, identificar puntos de entrada de intrusiones, y reparar o cerrar estas posibles vías de acceso.

- **Política de seguridad:** 1. Conjunto de estatutos que describen la filosofía de una organización respecto a la protección de su información y sistemas informáticos. 2. Conjunto de reglas que ponen en práctica los requisitos de seguridad del sistema.
- **Vulnerabilidades:** Debilidades en un sistema que pueden ser utilizadas para violar las políticas de seguridad.
- **Control de acceso:** Controlar quién tiene acceso a una computadora o servicio en línea y la información que almacena.
- **Autenticación:** El proceso para verificar que alguien es quien dice ser cuando intenta acceder a una computadora o servicio en línea.
- **Identificación:** El proceso de reconocimiento de un usuario particular de una computadora o servicio en línea.
- **Contraseña:** una serie secreta de caracteres que se utiliza para autenticar la identidad de una persona.
- **Servidor:** computadora que proporciona datos o servicios a otras computadoras a través de una red.

4. Gestionando la seguridad de la información.

4.1. Objetivos y medida

El objetivo en el que se va a centrar el plan implementación del SGSI es establecer, mantener y mejorar de forma continua la seguridad de la información dentro de TICSOCAL S.A.S, y proteger mediante controles que lo anterior se cumpla para beneficio de la empresa logrando que la información se mantenga actualizada, completa y veraz para el cumplimiento de las actividades de la organización.

Para lograr esto se debe contar con el apoyo de la gerencia en donde se tenga claras las políticas que las áreas de la empresa deberán cumplir para garantizar la seguridad de la información. La política de seguridad de la información debe [2]:

a) Estar disponible como información documentada
b) Comunicarse dentro de la empresa
c) Estar disponible para las partes interesada

La alta dirección debe establecer una política de la seguridad de la información que:

a) Sea adecuada al propósito de la organización
b) Incluya objetivos de seguridad de la información o proporcione el marco de referencia para el establecimiento de los objetivos de la seguridad de la información
c) Incluye el compromiso de cumplir con los requisitos aplicables que se relacionan con la seguridad de la información
d) Incluya el compromiso de mejora continua del Sistema de Gestión de Seguridad de la Información

Para poder llevar a cabo de la mejor manera el uso y ejecución de estas políticas se deberá nombrar una persona la cual estará encargada de la aprobación dichas políticas y quien

asignará roles para verificar la seguridad, coordinar y revisar que la implementación de la seguridad sea efectuada en toda la empresa y según sea el enfoque de cada área.

4.2. Requisito de seguridad de la información.

Seguir los lineamientos de los requisitos legales mencionados en le documento Lista de requisitos legales, reglamentarios, contractuales y otros de acuerdo al enfoque empresarial, garantizando el cumplimiento de las obligaciones legales y contractuales.
Garantizar para los clientes y usuarios la ley de protección de la información y ley orgánica de protección de datos.
Debe contemplar todo lo relacionado al acceso de la información, el uso de los recursos de la organización y el comportamiento en caso de que se produzcan incidentes de seguridad.

4.3. Controles de seguridad de la información.

Para verificar que todas los objetivos y políticas que se hayan definido se estén cumpliendo a cabalidad se deberán seguir los siguientes controles [2]:

A. *Asignación de responsabilidades para la seguridad de la información (SI):* se tiene que definir y asignar claramente todas las responsabilidades para la SI y quienes estarán encargados.
B. *Segregación de tareas:* se deben segregar tareas y las áreas de responsabilidad lo antes posible para evitar conflictos de interés con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada.
C. *Contacto con grupos de interés especial:* se debe mantener el contacto con diferentes grupos o foros de seguridad que estén especializados y asociados a profesionales.
D. *S.I. en la gestión de proyectos:* se debe contemplar la seguridad de la información en la gestión de proyectos e independientemente del tipo de proyecto a desarrollar por la empresa.

4.4. Responsabilidades.

4.4.1. Responsabilidades de la alta dirección:

Debe velar por el establecimiento de las políticas de S.I. y lo objetivos de seguridad alineados a las necesidades de TICSOCIAL, garantizar la integridad de los lineamientos del SGSI en los procesos definidos, por último, apoyar y promover a las personas que contribuyan al desarrollo del SGSI.

4.4.2. Responsabilidades del área de gestión administrativa:

Proteger de manera adecuada la información interna de la organización y velar por la seguridad de esta como los son contratos con clientes y proveedores, hojas de vida de todos

los empleados de la organización, etc., implementar los controles se seguridad necesarios para la protección de esta información la cual es vital para la organización.

4.4.3. Responsabilidades del área TIC:

Promover que el personal cumpla las políticas de S.I.; registrar y mantener la información requerida para auditar y evaluar la ejecución de los controles específicos de S.I.; establecer, documentar y dar mantenimientos a los procedimientos de seguridad que apliquen a las plataformas tecnológicas de información administrada por la empresa; implementar y administrar los controles de seguridad sobre los datos y conexiones de la red; custodiar la información y los medios de almacenamiento.

4.4.4. Responsabilidades de gestión de riegos de la S.I.:

El objetivo de la gestión de riesgos es identificar y evaluar los riesgos de la S.I. a los cuales están expuestos los activos de la entidad, para seleccionar y aplicar el plan de tratamientos más adecuado. La evaluación de riesgos esta basada en el impacto y la probabilidad de ocurrencia de estos para la entidad y los requerimientos de los niveles de seguridad, tomando en cuenta los controles existentes.

4.4.5. Responsabilidades de los funcionarios, contratistas y terceros:

Deberán salvaguardar la información institucional de la empresa, garantizando así la confidencialidad, integridad y disponibilidad de la información teniendo en cuenta como funciones:

- Cumplir con las políticas y normas de la S.I.
- Reportar a través de los canales establecidos, la sospecha u ocurrencia de situaciones considerados incidentes de seguridad de información.
- Realizar sugerencias para la mejora de procesos relacionados con los activos de la organización y poder optimizar así el SGSI.
- Utilizar únicamente software y demás recursos tecnológicos autorizados por la empresa.

5. Soporte para la implementación del SGSI.

Se deberá garantizar que las áreas involucradas en el proceso de implementación tengan varios puntos a considerar, como una adecuada comunicación, cumplimiento de los objetivos dentro del alcance propuesto en el Documento de alcance del SGSI y los requisitos previamente definidos, siguiendo las responsabilidades dadas a cada uno.

6. Validez y gestión documental

Este documento será revisado y podrá ser modificado por Diana Rodríguez, Robinson Salazar y Luis Fernando Morales a medida que el desarrollo del plan de implementación se vaya efectuando y si se cree conveniente para lograr la efectividad del documento.

7. Referencias

[4] Glosarios Términos seguridad (12 diciembre de 2018) [Internet]. Disponible en: https://safemode-cl.blogspot.com/2006/07/glosario-de-terminos-de-seguridad.html

[5] ¿Qué objetivo persigue la seguridad de la información? (13diciembre de 2018) [Internet]. Disponible en: https://www.pmg-ssi.com/norma-27001/

Ingeniero de Sistemas - Líder de Desarrollo y Tecnología
Robinson Salazar Grimaldos

_____

GAP BASADO EN REQUISITOS

Resultados Gap				
ISO/IEC 27001				
Área del Estandar ISO/IEC 27001	**Número de requisitos en la sección**	**No. requerimientos cumplidos**	**% Conformidad**	
4 CONTEXTO DE LA ORGANIZACIÓN	4	2	50%	
5 LIDERAZGO	6	3	50%	
6 PLANIFICACIÓN	16	2	13%	
7 SOPORTE	8	4	50%	
8 OPERACIÓN	4	1	25%	
9 EVALUACIÓN DEL DESEMPEÑO	6	1	17%	
10 MEJORA	2	0	0%	
A.5 Políticas de la Seguridad de la Información	2	2	100%	
A.6 Organización de la Información de la Seguridad	7	3	43%	
A.7 Seguridad de los Recursos Humanos	6	2	33%	
A.8 Gestión de Activos	10	2	20%	
A.9 Control de Acceso	14	3	21%	
A.10 Criptografía	2	0	0%	
A.11 Seguridad Fïsica y del Entorno	15	12	80%	
A.12 Seguridad de las Operaciones	14	2	14%	
A.13 Seguridad de las Comunicaciones	7	3	43%	
A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas	13	5	38%	
A.15 Relación con los Proveedores	5	2	40%	
A.16 Gestión de Incidentes de la Seguridad de la Información	7	0	0%	
de la Continuidad del Negocio	4	3	75%	
A.18 Cumplimiento	8	5	63%	
Totales	**160**	**57**	**36%**	