1. PRESENTACIÓN

El presente plan se elabora con el fin de dar a conocer cómo se realizará la implementación y socialización del componente de Gobierno en Línea en el Eje Temática de la Estrategia en seguridad y privacidad de la información, el cual busca guardar los datos que genera y custodia la entidad, garantizando la seguridad de la información institucional.

2. DEFINICIONES

- Acceso a la Información Pública
  Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

- Activo
  En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- Activo de Información
  En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controla en su calidad de entidad.

- Archivo
  Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

- Amenazas
  Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- Análisis de Riesgos
  Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- Auditoría

Av. La Esperanza calle 24 No. 62 – 49
Complejo Empresarial - Estación 2 Piso 9
PBX 739 9080 - www.ansv.gov.co - @ansvcol

Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

- Autorización
  Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

- Bases de Datos Personales
  Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

- Ciberseguridad
  Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

- Ciberespacio
  Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

- Control
  Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- Datos Abiertos
  Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley
  1712 de 2014, art 6).

- Datos Personales
  Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art3).

- Datos Personales Públicos
  Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos,

documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

- Datos Personales Privados
  Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

- Datos Personales Mixtos
  Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

- Datos Personales Sensibles
  Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

- Declaración de aplicabilidad
  Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

- Derecho a la Intimidad
  Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

- Encargado del Tratamiento de Datos
  Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)

- Gestión de incidentes de seguridad de la información
  Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- Información Pública Clasificada

Av. La Esperanza calle 24 No. 62 – 49
Complejo Empresarial - Estación 2 Piso 9
PBX 739 9080 - www.ansv.gov.co - @ansvcol

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- Información Pública Reservada
  Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- Plan de continuidad del negocio
  Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- Plan de tratamiento de riesgos
  Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- Privacidad
  En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a le compete realizar y que generan en las entidades destinatarias del Manual de Gobierno en Línea, correlativa obligación a proteger dicha información en observancia del marco legal vigente.

- Responsabilidad Demostrada
  Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

- Responsable del Tratamiento de Datos
  Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

- Riesgo

Av. La Esperanza calle 24 No. 62 – 49
Complejo Empresarial - Estación 2 Piso 9
PBX 739 9080 - www.ansv.gov.co - @ansvcol

Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- Seguridad de la información
  Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- Sistema de Gestión de Seguridad de la Información SGSI
  Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

- Titulares de la información
  Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

- Trazabilidad
  Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

3. OBJETIVOS

3.1. Objetivo General

- Controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes, en la Agencia Nacional de Seguridad Vial con el fin de salvaguardar los activos de información, el manejo de medios, el control de acceso y la gestión de usuarios, que acceden y procesan información en la entidad.

3.2. Objetivos Específicos

- Aplicar las metodologías y buenas prácticas establecidas en los estándares internacionales respectivamente en seguridad y riesgo de la información, para que el ANSV logre el mayor aprovechamiento de la información.

Av. La Esperanza calle 24 No. 62 – 49
Complejo Empresarial - Estación 2 Piso 9
PBX 739 9080 - www.ansv.gov.co - @ansvcol

4. RECURSOS

Humanos → Son todas aquellas personas con las que la organización cuenta para desarrollar y ejecutar de manera correcta las acciones, actividades, labores y tareas que deben realizarse de materia de seguridad y privacidad de la información.

- Director General
- Secretario General
- Director Técnico Observatorio Nacional de Seguridad Vial
- Grupo Interno de Trabajo de TIC
- Contratistas Externos

Físicos → Los recursos físicos necesarios para lograr una implementación del Plan están definidos en el cronograma de trabajo para la implementación del SGSI.

Financieros → Presupuesto pendiente de ser aprobado por la alta dirección

5. RESPONSABLES

- Director General
- Secretario General
- Director Técnico Observatorio Nacional de Seguridad Vial
- Coordinador GIT TIC

6. METODOLOGÍA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en la ANSV, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los decretos relacionados en materia de tecnología.

De acuerdo a lo anterior, se relacionan las siguientes fases de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI):

1. Diagnosticar
2. Planear
3. Hacer
4. Verificar
5. Actuar

Av. La Esperanza calle 24 No. 62 – 49
Complejo Empresarial - Estación 2 Piso 9
PBX 739 9080 - www.ansv.gov.co - @ansvcol

Ilustración 1 – Marco de Seguridad y Privacidad de la Información

7. CUMPLIMIENTO DE LA IMPLEMENTACIÓN

De acuerdo a las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar y los plazos de implementación de acuerdo a lo establecido por la ANSV en el Cronograma de Trabajo.

- Contexto de la Organización
- Liderazgo
- Planificación
- Soporte
- Operación
- Evaluación del Desempeño
- Controles de Seguridad de la Información
- Seguridad Física
- Seguridad de las Operaciones
- Seguridad de las Comunicaciones
- Incidentes de Seguridad de la Información
- Continuidad del Negocio
- Cumplimiento.

8. SEGUIMIENTO Y EVALUACIÓN

Al finalizar cada etapa se realizará una reunión con la Dirección Técnica del Observatorio Nacional de Seguridad Vial, El GIT TIC y la Secretaría General para presentar el informe del avance del proyecto y de esta manera evaluar todas las acciones que se han y no efectuado de acuerdo al cronograma planteado en el presente plan.

Av. La Esperanza calle 24 No. 62 – 49
Complejo Empresarial - Estación 2 Piso 9
PBX 739 9080 - www.ansv.gov.co - @ansvcol

9. ENTREGABLES

- Informe de avance o resumen ejecutivo
- Actas de Reunión Periódicas.
- Plan de tratamiento de riego aprobado por las partes y socializado con el personal de la entidad.
- Productos de cada etapa

Av. La Esperanza calle 24 No. 62 – 49
Complejo Empresarial - Estación 2 Piso 9
PBX 739 9080 - www.ansv.gov.co - @ansvcol

10. CRONOGRAMA

Agencia Nacional de Seguridad Vial — Construcción y Seguimiento al Sistema de Gestión y Seguridad de la Información de la Agencia Nacional de Seguridad Vial

IdTarea	Nombre Tarea	2019											
		Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
	DIAGNOSTICO DEL ESTADO DE ISO 27001												
1	CONTEXTO DE LA ORGANIZACIÓN												
1.1	Comprensión De Las Necesidades Y Expectativas De Las Partes Interesadas												
1.2	Determinación del alcance del sistema de gestión de la seguridad de la información												
2	LIDERAZGO												
2.1	Política de Segregación de Funciones												
2.2	Apoyo en la identificación de contenido de seguridad y protección de la información en Acuerdo de Confidencialidad y Transparencia												
3	PLANIFICACION												
3.1	Valoración de riesgos de la seguridad de la información (Modelo de Gestión de Riesgos)												
3.2	Tratamiento de los riesgos de seguridad de la información												
3.3	Objetivos de Seguridad de la Información y planes para su logro												
3.4	Diligenciamiento de la declaración de aplicabilidad												
4	SOPORTE												
4.1	Toma de conciencia												
4.2	Documentación de Sistema de Gestión de Seguridad de la Información (manuales, políticas, procedimientos, instructivos, formatos, etc												
5	OPERACIÓN												
5.1	Valoración de Riesgos de seguridad de la información (sala)												
	Procesos tecnológico												
	Archivo y Gestión documental												
	Seguridad Física y ambiental												
	Talento Humano												
5.2	Tratamiento de los riesgos de seguridad de la información												
	Procesos tecnológico												
	Archivo y Gestión documental												
	Seguridad Física y ambiental												
	Talento Humano												

Av. La Esperanza calle 24 No. 62 – 49
Complejo Empresarial - Estación 2 Piso 9
PBX 739 9080 - www.ansv.gov.co - @ansvcol

Av. La Esperanza calle 24 No. 62 – 49
Complejo Empresarial - Estación 2 Piso 9
PBX 739 9080 - www.ansv.gov.co - @ansvcol

Agencia Nacional de Seguridad Vial

Construcción y Seguimiento al Sistema de Gestión y Seguridad de la Información de la Agencia Nacional de Seguridad Vial

IdTarea	Nombre Tarea	2019											
		Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
6	**EVALUACION DE DESEMPEÑO**												
6.1	Seguimiento, Medición y Evaluación de seguridad de la información												
6.2	Auditoría Interna de seguridad de la Información												
6.3	Revisión por la Dirección												
7.	**CONTROLES DE SEGURIDAD DE LA INFORMACION**												
7.1	Contacto con Autoridades y grupos de interes												
7.2	Propuesta seguridad de la información en proyectos												
7.3	Inventario de Activos de Información (proceso tecnológico, evaluación de propuestas - sala, Gestión Documental												
	Inventario Procesos tecnológico												
	Inventario Archivo y Gestión documental												
	Inventario Seguridad Física y ambiental												
	Talento Humano												
7.4	Valoración de Riesgos de seguridad de la información (ver numerales 5.1 y 5.2)												
7.5	Lineamientos de uso aceptable de Activos de Información												
7.6	Procedimiento de custodia de contraseñas de usuarios privilegiados												
8	**SEGURIDAD FISICA**												
8.1	Valoración de la seguridad física y de entorno de las áreas seguras (Centro de datos y de cableados en pisos)												
8.2	Apoyo en el protocolo de seguridad de la sala de evaluación de propuestas												
9	**SEGURIDAD DE LAS OPERACIONES**												
9.1	Documentación de actividades de operación tecnológica (toma de respaldo y restauración de información de servidores y de información de aplicaciones, gestión de cambios TI, gestión de capacidad)												
9.2	Apoyo en la identificación del Catálogo de Servicios Tecnológicos												
10	**SEGURIDAD DE LAS COMUNICACIONES**												
10.1	Definición de políticas de acceso seguro y uso adecuado del servicio de internet												
10.2	Política de configuración y aseguramiento de conexión inalámbrica												
10.3	Solicitud de conexión clientes VPN												
11	**INCIDENTES DE SEGURIDAD DE LA INFORMACION**												
11.1	Establecimiento del modelo de gestión de incidentes de seguridad de la información												
12	**CONTINUIDAD DE NEGOCIO**												
12.1	Ejecución de actividades para el establecimiento del BIA (Business Impact Analysis de la ANSV)												

Av. La Esperanza calle 24 No. 62 – 49
Complejo Empresarial - Estación 2 Piso 9
PBX 739 9080 - www.ansv.gov.co - @ansvcol

11. CONTROL DE CAMBIOS

FECHA	CAMBIO	VERSIÓN
2019-01-31	Documento Original. Primera versión	00

12. CONTROL DE FIRMAS

Elaboró
Firma

Angela Riveros Sierra
Profesional Especializado TICS

Aprobó
Firma

Juana Caycedo Gutiérrez
Secretaria General (E)

Revisó: Eder Carrascal Cuadrado – Profesional Especializado Oficina Asesora de Planeación

Av. La Esperanza calle 24 No. 62 – 49
Complejo Empresarial - Estación 2 Piso 9
PBX 739 9080 - www.ansv.gov.co - @ansvcol