PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION AGENCIA NACIONAL DE TIERRAS (ANT)

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION DE LA ANT

SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN
2019

CONTENIDO

ILUSTTRACIONES

TABLAS

INTRODUCCIÓN

La información en la Agencia Nacional de Tierras (ANT) está definida como uno de los activos más valiosos y primordiales, la cual, sólo tiene sentido cuando esta conserva los principios de disponibilidad, integra y confidencialidad, además si esta es oportuna, responsable y segura, lo que nos lleva a la necesidad de que la ANT tenga una adecuada gestión de sus activos de información con el objetivo de asegurar y controlar el debido tratamiento, acceso y uso de la información.

Cualquier organización de régimen público o privado, debe ser consciente que las amenazas existentes que atentan contra la seguridad y privacidad de la información, representan un riesgo latente que al materializarse no solo les puede generar costos económicos, sanciónales legales y afectación de su buena imagen, sino que pueden afectar la continuidad del negocio.

En la medida que las entidades tengan una visión general de los riesgos que pueden afectar la seguridad y privacidad de la información, podrán establecer controles y medidas eficientes, efectivas y transversales con el propósito de salvaguardar la disponibilidad, integridad y confidencialidad de la información y del negocio. Es importante resaltar la necesidad de que las organizaciones realicen una adecuada identificación, clasificación y valoración de los riegos que pueden afectar su seguridad, con el propósito de implementar medidas y controles efectivos que les permitan estar preparados ante situaciones adversas que puedan comprometer tanto la seguridad física como lógica, así como también las personas, recursos y sistemas.

La ANT es consciente que la protección y aseguramiento de su información es fundamental para garantizar debidamente la gestión de tierras del país. Razón por la cual debe establecer un marco normativo de un Sistema de Gestión Seguridad de la Información que apalanque las políticas, lineamientos, responsabilidades y obligaciones para que sus colaboradores se concienticen del tratamiento necesario para dar un excelente manejo a la seguridad y privacidad de la información de la ANT.

El presente documento contiene el plan de seguridad y privacidad de la información para el establecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información de la ANT, el cual tomará como referencia el Modelo de Seguridad y

Privacidad de la estrategia de Gobierno en Línea y la norma ISO 27001[1], los cuales proporcionan un marco metodológico basado en buenas prácticas.

[1] https://www.normas-iso.com/iso-27001/

1. OBJETIVOS.

1.1. Objetivo general

Establecer un Plan de Seguridad y Privacidad de la Información que apoye la creación y establecimiento del Sistema de Gestión de Seguridad de la Información (SGSI) de la Agencia Nacional de Tierras, teniendo en cuenta los requerimientos del modelo de seguridad de la estrategia de gobierno en digital y los requerimientos del negocio de la ANT, dando cumplimiento a las disposiciones legales vigentes de nuestro país.

1.2. Objetivos específicos

A. Definir las etapas para establecer la estrategia de seguridad de la información y el SGSI de la ANT.

B. Optimizar la gestión de la seguridad de la información al interior de la ANT.

C. Gestionar la implementación del Sistema de Gestión de Seguridad de la Información de la ANT de acuerdo con los requerimientos establecidos en el modelo de seguridad de la estrategia de Gobierno en digital.

D. Establecer lineamientos para la implementación y/o adopción de mejores prácticas de seguridad en la ANT.

2. ALCANCE

Este Plan de Seguridad de la Información identifica la situación actual (AS-IS) y propone la situación deseada (TO-BE) para los siguientes tres años, de 2019 a 2021, en términos de los siguientes temas:

- ✓ Implementación del Sistema de Gestión de Seguridad de la Información - SGSI
- ✓ Certificación del Sistema de Gestión de Seguridad de la Información - SGSI
- ✓ Activos de Seguridad de la Información

- ✓ Riesgos de Seguridad de la Información
- ✓ Clasificación y Prevención de Fuga de Información
- ✓ Acceso a la información
- ✓ Seguridad Perimetral
- ✓ Transferencia Segura de la Información
- ✓ Monitoreo de eventos de Seguridad
- ✓ Seguridad en redes y comunicaciones
- ✓ Seguridad en proyectos de TI
- ✓ Gestión de Vulnerabilidades
- ✓ Continuidad del Negocio
- ✓ Capacitación y Sensibilización en Seguridad de la Información

3. BASE LEGAL

NORMA	FECHA	DESCRIPCIÓN
Ley 599	24-jul-2000	Por la cual se expide el Código Penal. Título III capítulo séptimo de la violación a la intimidad, reserva e interceptación de comunicaciones. Art 192, 193, 194,196 y 197.
Ley 1273	05-ene-2009	Por medio de la cual se modifica el Código Penal. Título VII Bis "De la protección de la información y de los datos". Artículos 269A a 269J.
Ley 1581	17-oct-2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1712	06-mar- 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Ley 1915	12-jul-2018	Por la cual se modifica la ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
Decreto 1377	27-jun-2013	Por la cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto 886	13-may-2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos
Decreto 103	20-ene-2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014.
Decreto 1078	26-may-2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Capítulo 1, Título 9, Libro 2, Parte 2 subrogado por el Decreto 1008 de 2018.
Decreto 1081	26-may-2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector Presidencia de la República. Parte 1, Titulo 1.
Decreto 1008	14-jun-2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. Política de Gobierno Digital.
NTC-ISO/IEC COLOMBIANA 27001:2013	11-dic-2013	Norma Técnica Colombiana NTC-ISO-IEC 27001.Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información.Requisitos.
Guías MPSI	29-jul-2016	Modelo de Seguridad y Privacidad de la Información, MINTIC.

Tabla 1. Base Legal

RECURSOS.

HUMANO: La Dirección de Gestión del Ordenamiento Social de la Propiedad, la Subdirección de Sistemas de Información de Tierras, la Secretaría General, la Mesa Tecnológica Directiva, la Subdirección de talento humano, los líderes de proceso, Oficina de Control Interno y un profesional especializado en seguridad informática.

FÍSICO: Infraestructura tecnológica y controles de acceso físico.

4. RESPONSABLES.

- Dirección de Gestión del Ordenamiento Social de la Propiedad.
- Subdirección de Sistemas de Información de Tierras.
- Secretaria General.
- Mesa Tecnológica Directiva.
- Subdirección de Talento Humano.
- Profesional Especializado en seguridad informática.

5. METODOLOGÍA IMPLEMENTACIÓN MODELO DE SEGURIDAD.

5.1. Ciclo operación.

El Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno en Línea contempla el siguiente ciclo de operación compuesto por cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

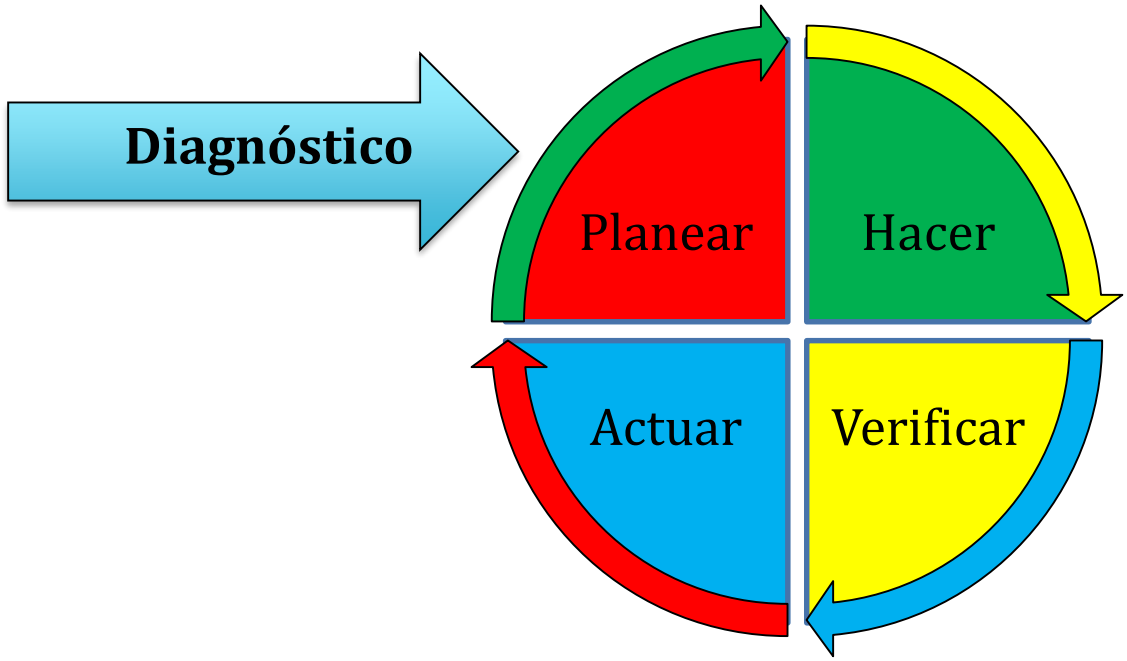


Ilustración 1. Ciclo de operación Modelo de Seguridad y Privacidad de la Información

Fuente: Elaborada con base en la información publicada en la página web: https://www.pmg-ssi.com/2015/01/iso-27001-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/

- **Fase Diagnóstico**: Permite identificar el estado actual de la ANT con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.
- **Fase Planear**: Se establecen los objetivos a alcanzar y las actividades susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.

- **Fase Hacer**: Se ejecuta el plan establecido que consiste en implementar las acciones para lograr las mejoras planteadas en la fase de planear.
- **Fase Verificar**: Una vez implantadas las mejoras, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas en la fase del hacer.
- **Fase Actuar**: Se analizan los resultados de las acciones implementadas y si estas no cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones, dando un diagnóstico y un nuevo punto de partida en la fase del planear.

La implementación del SGSI en la ANT, siguiendo el Modelo de Seguridad y Privacidad de la Información también involucra el modelo de madurez descrito en la guía, el cual permite identificar el nivel de madurez del SGSI en el que se encuentra la ANT, midiendo la brecha entre el nivel actual de la ANT y el nivel optimizado. A continuación, se muestran los diferentes niveles que hacen parte del modelo de madurez y sus características.

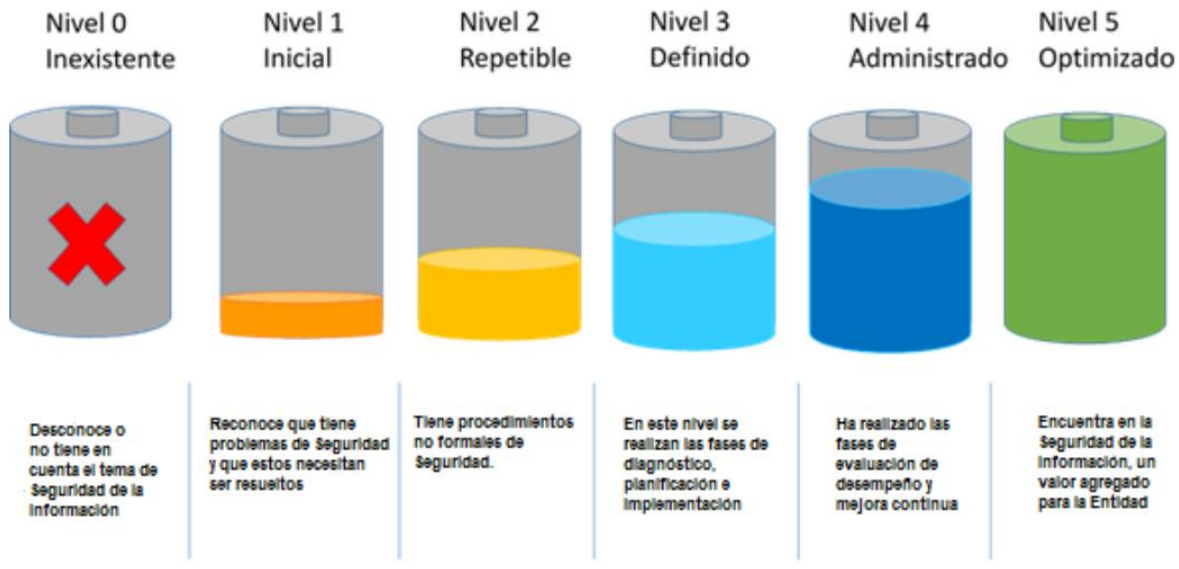


Ilustración 2. Niveles de Madurez del MSPI - MINTIC

5.2. Alineación norma ISO 27001:2013 vs Ciclo de operación

Aunque en la norma ISO 27001:2013 no determina un modelo de mejora continua (PHVA) como requisito para estructurar los procesos del Sistema de Gestión de Seguridad de la Información, la nueva estructura de esta versión se puede alinear con el ciclo de mejora continua de los modelos de gestión de la siguiente forma:

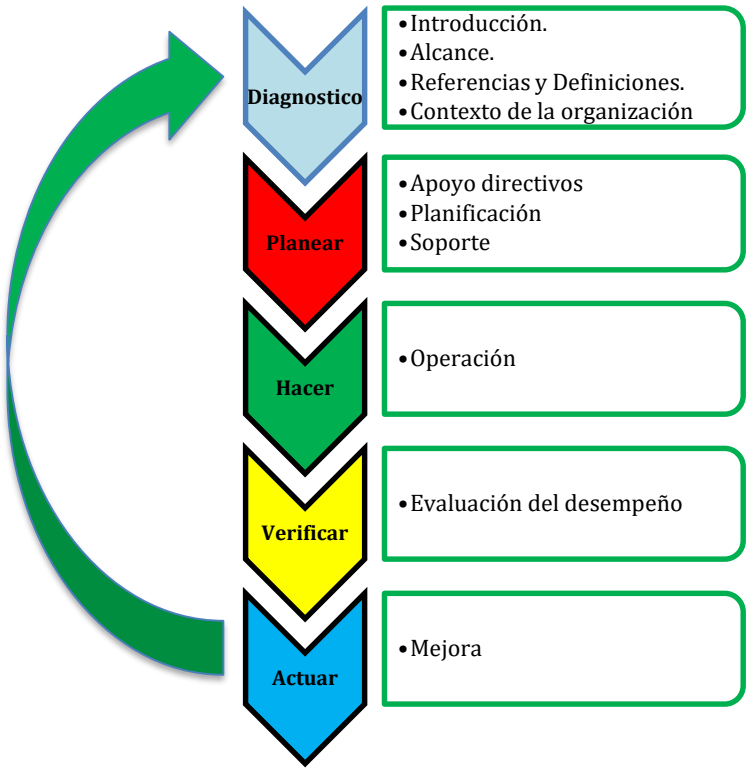


Ilustración 3. Norma ISO 27001:2013 alineado al Ciclo de mejora continua

Fuente: Elaborada con base en la información publicada en la página web https://www.welivesecurity.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-la-norma-para-gestionar-la-seguridad-de-la-informacion/

Trasladando a las necesidades del SGSI, el ciclo PHVA planteado por la ISO 27001 se dividiría en las siguientes fases, cada una de ellas ligada a una serie de acciones:

Fases	Acciones
PLANEAR	• Definir la política de seguridad. • Establecer el alcance del SGSI. • Realizar el análisis de riesgos. • Seleccionar los controles. • Definir competencias. • Establecer un mapa de procesos. • Definir autoridades y responsabilidades.
HACER	• Implantar el plan de gestión de riesgos. • Implantar el SGSI. • Implantar los controles de seguridad. • Administrar los dispositivos de seguridad.
VERIFICAR	• Revisar internamente el SGSI. • Realizar auditorías internas del SGSI. • Poner en marcha indicadores y métricas. • Hacer una revisión por parte de la Dirección.
ACTUAR	• Adoptar acciones correctivas • Adoptar acciones de mejora

Tabla 2. Estructura PHVA ISO 27001:2013 y acciones

5.3. Fase I (Diagnóstico)

Objetivo: Identificar el estado de la ANT con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

6.3.1 Situación actual (AS-IS)

A partir del análisis de la información y documentación proporcionada se identificó:

- Objetivos de seguridad de la información para la ANT:
  - ✓ Establecer la capa de seguridad para todos los sistemas de información.
  - ✓ Brindar confidencialidad, integridad y disponibilidad a la información de la ANT.
  - ✓ Establecer políticas y planes de la seguridad orientada a las personas.
  - ✓ Brindar los mecanismos de seguridad para todos los procesos de tecnología tercerizados.

- Requerimientos de cumplimiento establecidos para la ANT:
  - ✓ Todos los establecidos por MINTIC y Gobierno Digital por ser una entidad pública
  - ✓ Las normativas de gestión documental y ley general de archivo.
  - ✓ Toda la normatividad vigente en Colombia sobre manejo de información

- Requerimientos de apoyo en temas de seguridad de la información con los que se cuenta para apoyar proyectos estratégicos:
  - ✓ Gestión Documental
  - ✓ Análisis de información sobre data estructurada y no estructurada
  - ✓ Portal Web

La evaluación del cumplimiento de Requisitos/Cláusulas 4 al 10 de la norma NTC-ISO/IEC 27001:2013, se diligenció con la lista de validación, donde se analizó y evaluó el estado de cumplimiento.

Para las cláusulas y el establecimiento del SGSI, de acuerdo con los numerales de la norma, se documentó el porcentaje de madurez de los requisitos y dominios (cláusulas). A continuación, podemos observar la tabla de resultado del nivel de madurez de acuerdo con los objetivos de control de los dominios del Anexo A de la Norma NTC ISO/IEC 27001:2013.

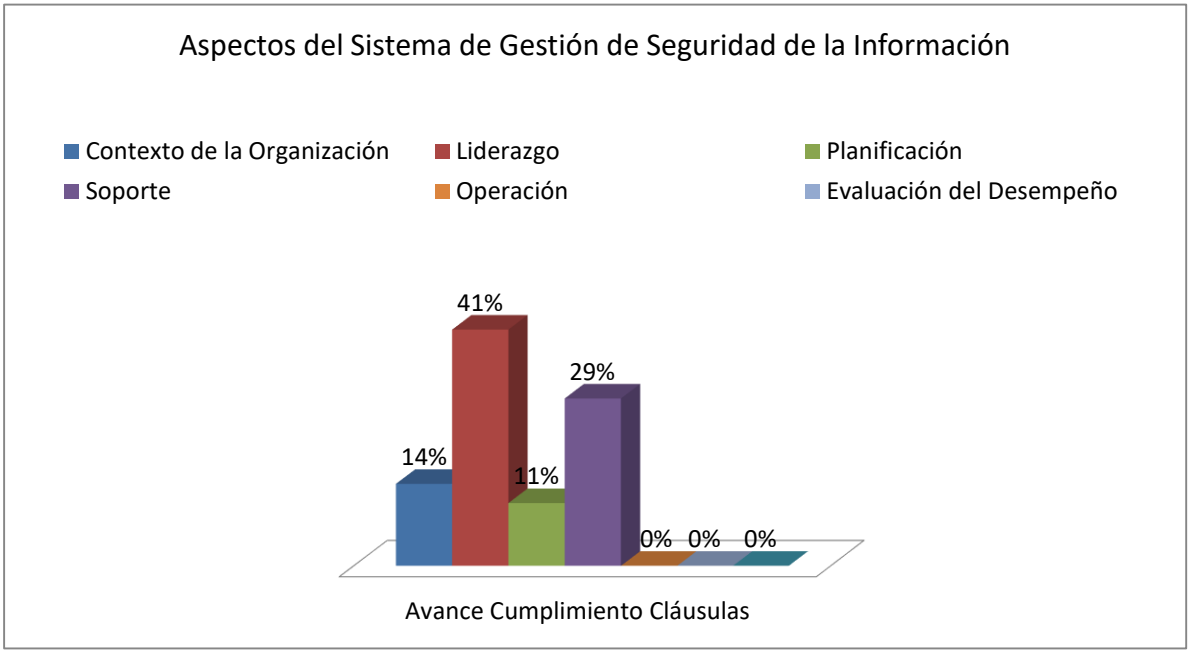
Ítem	Dominios	Controles	Madurez
A.5.	Política de Seguridad de la Información	25%	Inicial
A.6.	Organización de la Seguridad de la Información	14%	Inexistente
A.7.	Seguridad en los Recursos Humanos	42%	Repetible
A.8.	Gestión de los activos	35%	Inicial
A.9.	Control de Acceso	32%	Inicial
A.10.	Criptografía	0%	Inexistente
A.11.	Seguridad Física y del Entorno	33%	Inicial
A.12.	Seguridad de las Operaciones	36%	Inicial
A.13.	Seguridad de las Comunicaciones	50%	Repetible
A.14.	Adquisición, Desarrollo y Mantenimiento de Sistemas	62%	Repetible
A.15.	Relaciones con los Proveedores	40%	Inicial
A.16.	Gestión de incidentes de Seguridad de la Información	0%	Inexistente
A.17.	Seguridad información Gestión de Continuidad de Negocio	0%	Inexistente
A.18.	Cumplimiento	19%	Inicial
TOTAL		32%	Inicial

Tabla 3. Resultados de la evaluación del Anexo A de la Norma ISO/IEC 27001:2013

Se presenta, a continuación, los resultados de la evaluación de cumplimiento en SGSI. En la ilustración número 4. Se evidencia el cumplimento en porcentaje por cada dominio de control del anexo A de la Norma ISO/IEC 27001:2013.

Ilustración 4. Porcentaje de cumplimiento por requerimiento del SGSI

Se presenta a continuación las gráficas, en la ilustración número 5, los resultados de la evaluación de cumplimiento de controles del Anexo A de la Norma ISO/IEC 27001:2013.



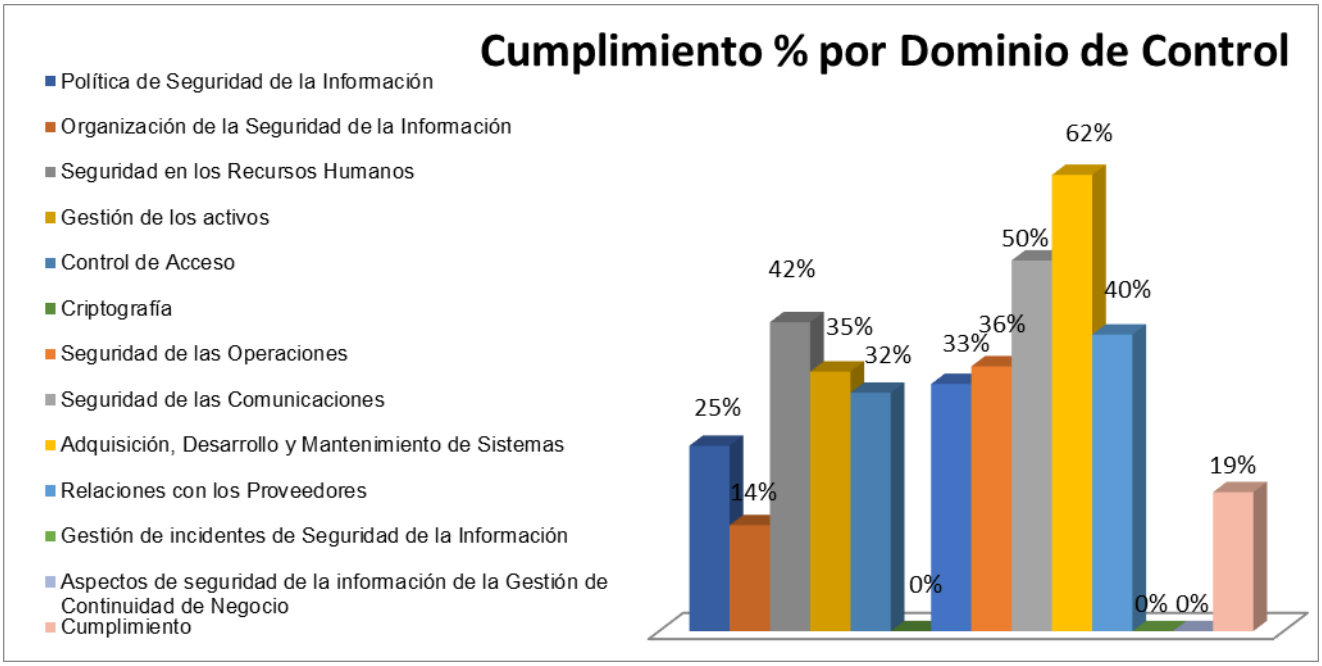


Ilustración 5. Porcentaje de cumplimiento por Dominio de Control

El diagnóstico realizado define el porcentaje máximo de cumplimiento que posee actualmente la ANT. Se presentan a continuación las conclusiones del proceso de análisis de cumplimiento de los controles del Anexo A de la norma NTC-ISO/IEC 27001:2013:

- El Diagnóstico realizado define el porcentaje máximo de cumplimiento que posee actualmente la ANT, aclarando que dichos cumplimientos están sujetos a acciones de mejoramiento una vez se esté ejecutanda la implementación.

- Los líderes de los procesos entrevistados demostraron interés y preocupación por la seguridad de la información de la ANT.

- El porcentaje de cumplimiento de las cláusulas de la norma ISO/IEC 27001:2013 es de 16**%,** lo que presenta un nivel de madurez INICIAL de implementación, es decir, (se desarrollan actividades y/o procesos, sin embargo, no han sido documentadas, ni hay entrenamiento ni comunicación formal de la misma. Se deja la responsabilidad al individuo).

- El porcentaje de implementación de controles del anexo A de la norma ISO/IEC 27001:2013 es de 32**%**, es decir, se desarrollan actividades y/o procesos, sin embargo, no han sido documentadas, ni hay entrenamiento ni comunicación formal de la misma. Se deja la responsabilidad al individuo, lo cual representa un porcentaje importante para continuar con el ajuste que requiere la norma ISO/IEC 27001:2013.

- Es necesario, de manera prioritaria, definir, aprobar, socializar e implementar las políticas de seguridad de la información para toda la ANT. La implementación de las políticas por la Alta Dirección permite aumentar el nivel de madurez del SGSI.

- La ANT debe definir un rol de responsable de la seguridad de la información y de la seguridad informática. Definir un responsable permite gestionar adecuadamente el Sistema de Gestión de Seguridad de la Información.

- Se recomienda definir y monitorear las responsabilidades de los líderes de los procesos en los controles de seguridad de la información.

- Se debe definir, aprobar, socializar y gestionar los riesgos de seguridad de la información de la ANT. Una adecuada implementación de la gestión de riesgos minimiza el impacto de la materialización de estos.

- En el documento Plan de Seguridad que entregará la consultoría de seguridad de la información se deben consignar las recomendaciones para el cumplimiento de los requisitos de la norma ISO /IEC 27001:2013.

- Es necesario continuar con las campañas de sensibilización en SGSI, con el fin de generar cultura y buenas prácticas de Seguridad de la Información.

- Es importante para el SGSI, tener una buena comunicación entre los procesos relacionados en el proyecto de certificación en ISO 27001:2013 de la ANT, por tal motivo es recomendable incentivar y difundir los productos que se desarrollen durante la planeación de seguridad de la información.

5.3.1. Fase II PLAN DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se propone la situación deseada (TO-BE) para cada uno de los temas relacionados en el alcance, así:

- ✓ **Implementación Sistema de Gestión de Seguridad de la Información – SGSI:** Se debe implementar el SGSI en lo que resta del 2019 y el 2020, con el fin de comenzar a tener registros y evidencias de su implementación, así como demostrar la verificación e implementación de la mejora continua.

- ✓ **Políticas de Seguridad de la Información:** Se debe actualizar y documentar la Política de Seguridad de la Información y las políticas específicas de seguridad de la información alineadas con lo definido por MINTIC y por lo exigido por la ISO 27001:2013, estas políticas se deben aprobar por la Alta Dirección y divulgadas a todos los interesados. Se deben continuar divulgando en el 2019 y 2020 a todos los interesados y al menos una vez en el año 2020 y 2021 revisarlas y hacer los ajustes que se consideren pertinentes.

- ✓ **Certificación del Sistema de Gestión de Seguridad de la Información – SGSI**: optar en el 2021 a la certificación ISO 27001:2013 para el alcance definido, luego para el 2022 se debe mantener la certificación e incluir dentro del alcance del SGSI la totalidad de los procesos de la ANT.

- ✓ **Activos de Seguridad de la Información**: Se debe hacer la identificación y valoración de los activos de información de todos los procesos, haciendo énfasis en los de tipo información, por la criticidad y sensibilidad de la información que en la ANT se maneja.

- ✓ **Riesgos de Seguridad de la Información:** Se deben llevar a cabo la identificación, valoración y planes de tratamiento de riesgos y hacer seguimiento permanente, realizar nuevas revisiones de seguridad que permitan identificar nuevos riesgos, la cual debe ser la dinámica durante el 2020 y 2021.

- ✓ **Clasificación y Prevención de Fuga de Información**: se debe realizar la clasificación de activos de tipo información y adquirir e implementar una solución de prevención de fuga de información, teniendo en cuenta la información confidencial que se gestiona en la ANT.

- ✓ **Acceso a la Información:** Se debe afinar los permisos a todos los recursos compartidos y sistemas de información.

- ✓ **Seguridad Perimetral:** Se debe protege la red LAN y DMZ de las amenazas externas que constantemente se encuentran en Internet, además, con el fin de mejorar el nivel de seguridad, se debe en el 2020 adquirir un Firewall de Aplicaciones Web (WAF).

- ✓ **Transferencia Segura de la Información:** se deben implementar esquemas de cifrado para los equipos móviles, unidades de almacenamiento externo o portátiles, para la información que es transportada o que es compartida con terceros, así mismo, se debe adquirir una solución de cifrado que permita compartir o transportar la información de manera segura.

- ✓ **Monitoreo de eventos de Seguridad:** Se debe adquirir una solución de monitoreo de logs y correlación de eventos de seguridad de la información (SIEM - Security Information & Event Management) o contratar un servicio de SOC (Security Operations Center), de tal manera que se permita contrarrestar de manera oportuna o prevenir eventos adversos en la plataforma tecnológica.

- ✓ **Seguridad en redes y comunicaciones:** Garantizar que todas las aplicaciones web funcionen sobre HTTPS, así mismo, se deben realizar unas pruebas de Ethical Hacking para la plataforma tecnológica y adquirir e implementar una solución de control de acceso a la red (NAC - Network Access Control) que permita blindar de mejor manera la información y los servicios de red.

- ✓ **Seguridad en proyectos de TI:** Actualmente en los proyectos de TI no se están considerando todos los aspectos de seguridad que en las diferentes fases se debe tener presentes, por lo tanto, para los proyectos que se tienen presupuestados para ser implementados entre el 2019 y el 2021, se debe considerar desde los mismos RFIs o RFPs los requisitos de seguridad que se debe atender para cada caso, y luego tener en cuenta las cláusulas que apliquen, como temas de confidencialidad, auditoria de los servicios brindados, etc. En caso que se adquieran equipos o soluciones, se debe exigir temas como Roles y Perfiles, Logs de Auditoria, Guías de Aseguramiento, Pruebas de Vulnerabilidades, entre otros.

- ✓ **Gestión de Vulnerabilidades:** Se deben generar estándares de seguridad de la plataforma tecnológica, para realizar el correspondiente hardening, luego hacer pruebas de vulnerabilidades y llevar a cabo los planes de tratamiento de las vulnerabilidades identificadas, dándole prioridad a las críticas y altas y continuar con las medias y bajas. Así mismo, se debe adquirir un escáner de vulnerabilidades con el fin de validar las brechas de seguridad la plataforma tecnológica de manera periódica.

- ✓ **Continuidad del Negocio:** Se debe llevar a cabo un Análisis de Impacto al Negocio (BIA) para poder determinar el Punto Objetivo de recuperación (RPO - Recovery Point Objetive), el Tiempo Objetivo de recuperación (RTO - Recovery Time Objetive) y demás variables importantes que respondan a las necesidades de disponibilidad de los servicios TI de la ANT, para proponer adelantar un proyecto de Plan de Continuidad del Negocio que comprende aspectos más amplios de la continuidad.

- ✓ **Capacitación y Sensibilización en Seguridad de la Información:** se debe mantener de manera periódica las campañas de sensibilización en temas de seguridad de la información, así mismo, cada año se debe proponer cursos de actualización en temas de seguridad, con el fin de que se mantengan al día en cuanto a las nuevas brechas de seguridad.

- ✓ **Privacidad y protección de información de datos personales:** se debe mantener de manera periódica las campañas de privacidad de protección de

datos personales, así mismo, se debe realizar auditorías que permitan establecer el cumplimiento de la ley.

5.3.2. Cronograma Plan de Seguridad de la Información

ID	Nombre Tarea	2019	2020		2021	
		Segundo Semestre	Primer Semestre	Segundo Semestre	Primer Semestre	Segundo Semestre
0	**DIAGNOSTICO DEL ESTADO DE IMPLEMENTACION DE ISO 27001**					
0.1	Estado actual en la gestión de seguridad y privacidad de la información en la ANT					
0.2	Identificación del nivel de madurez en la gestión de seguridad y privacidad de la información					
0.3	Levantamiento de información - Pruebas de efectividad					
1	**CONTEXTO DE LA ANT**					
1.1	Entender la situación actual de la ANT					
1.2	Comprensión de las necesidades y expectativas de las partes interesadas					
1.3	Determinación del alcance del MSPI					
2	**LIDERAZGO**					
2.1	Política de Seguridad de la Información					
2.2	Roles, Responsabilidades y Autoridades de Seguridad de la Información					
2.3	Manual de la Seguridad y Privacidad de la Información					
2.4	Procedimientos de la Seguridad y Privacidad de la Información					
3	**PLANIFICACION – Implementación**					
3.1	Gestión Clasificación de Activos					
3.2	Gestión de Riesgos / Seguridad en proyectos de TI					

3.3	Objetivos y Planes de Seguridad y Privacidad de la Información					
4	**SOPORTE**					
4.1	Toma de conciencia y sensibilización / Clasificación y Prevención de Fuga de Información / Seguridad Perimetral / Transferencia Segura de la Información					
4.2	Plan de comunicaciones / Acceso a la información / Gestión de Vulnerabilidades					
4.3	Gestión Documental / Seguridad en redes y comunicaciones					
5	**IMPACTO DEL NEGOCIO**					
5.1	Continuidad del Negocio					
5.2	Análisis de Impacto del Negocio (BIA)					
6	**CONTROL Y PLANEACIÓN OPERACIONAL**					
6.1	Valoración de Riesgos de seguridad de la información					
6.2	Tratamiento de los riesgos de seguridad de la información					
7	**EVALUACION DE DESEMPEÑO**					
7.1	Indicadores de Gestión de Seguridad y Privacidad de la Información					
7.2	Seguimiento, Medición y Evaluación de seguridad de la información					
7.3	Auditoría Interna de seguridad de la Información					
7.4	Revisión por la Dirección					
8	**INCIDENTES DE SEGURIDAD DE LA INFORMACION**					
8.1	Establecimiento del modelo de gestión de incidentes de seguridad de la información / Monitoreo de eventos de Seguridad					
8.2	Gestión de incidentes					
9	**MEJORA CONTINUA**					
9.1	No conformidades y acciones correctivas					

9.2	Mejora continua / Certificación del Sistema de Gestión de Seguridad de la Información – SGSI/Cumplimiento de ley de tratamiento de datos personales.					
10	**LINEAMIENTOS ASEGURAMIENTO INFORMACIÓN**					
10.1	Lineamientos de seguridad lógica					
10.2	Lineamientos de seguridad física					
10.3	Lineamientos de seguridad de la red					
10.4	Lineamientos de seguridad frente a la ANT proveedores					
10.5	Lineamientos de seguimiento y monitoreo de controles					
11	**PROTOCOLO DE INTERNET VERSIÓN 6 - IPv6**					
11.1	Diagnóstico					
11.2	Plan de implementación					
11.3	Implementación Piloto					
11.4	Implementación Entidad					
11.5	Aseguramiento IPv6					
11.6	Monitoreo IPv6					

Tabla 4. Cronograma Plan de Seguridad de la Información

5.4. Fase III: Implementación (Hacer)

Objetivo: Llevar acabo la implementación de la fase de planificación del SGSI, teniendo en cuenta para esto los aspectos más relevantes en los procesos de implementación del Sistema de Gestión de Seguridad de la Información de la ANT.

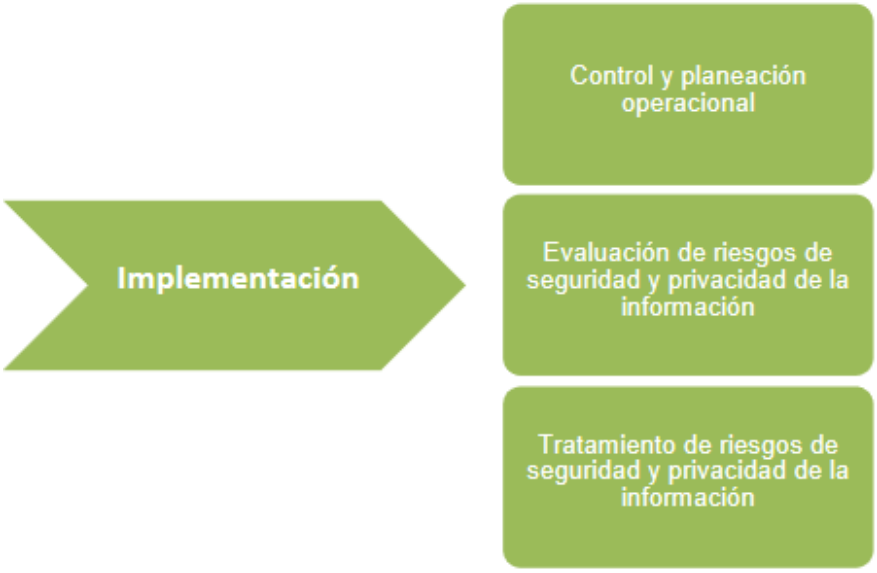


Ilustración 6. Fase de implementación modelo de seguridad.

Fuente: http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf

5.5. Fase IV: Evaluación de desempeño (Verificar).

Objetivo: realizar el seguimiento, monitoreo y la eficacia del SGSI, a través de instrumentos que permita determinar la eficacia y efectividad de los controles implementados.

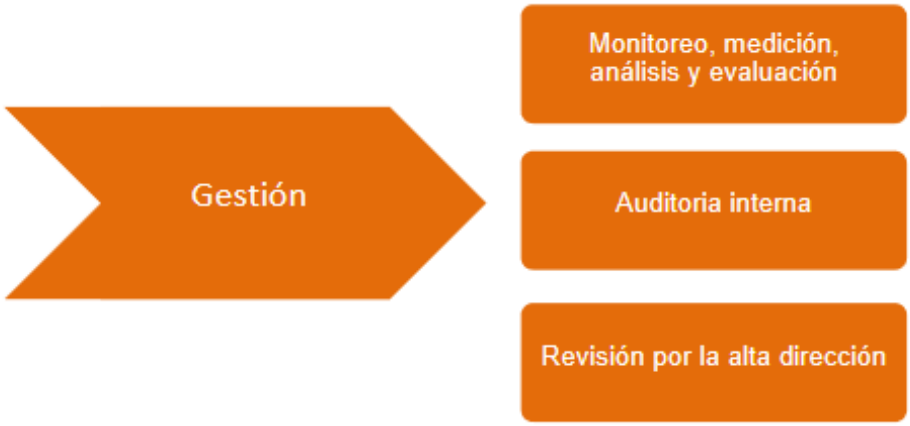


Ilustración 7.: Fase de evaluación de desempeño modelo de seguridad

Fuente: http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf

5.6. Fase V: Mejora continua (Actuar)

Objetivo: Consolidar los resultados obtenidos del componente de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el SGSI.

Ilustración 8. Fase de mejora continua modelo de seguridad.

Fuente: http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf

6. GUÍA DE OPERACIÓN DEL SGSI

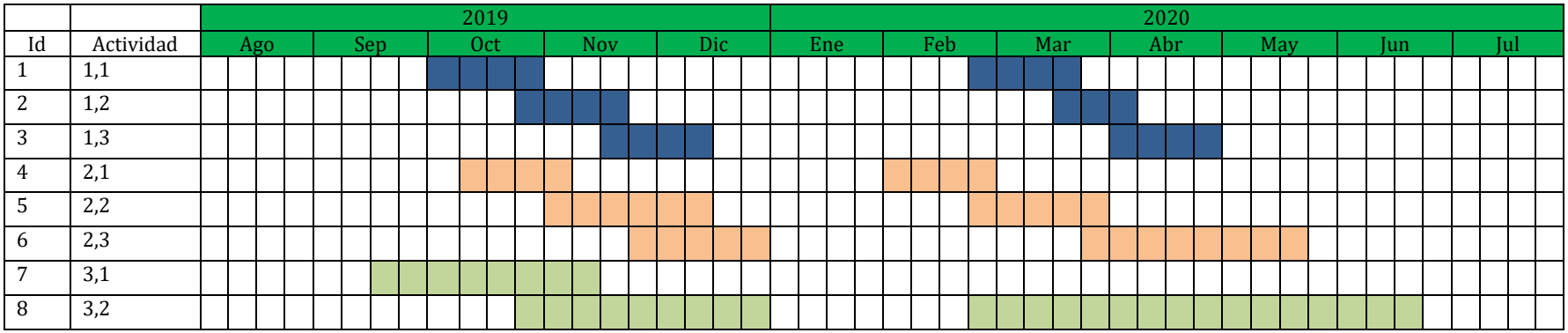
Id	Controles	Actividad 1	Actividad 2	Actividad 3
1	Política general de seguridad de la información	Revisar semestralmente el cumplimiento de política general de seguridad de la información	Revisar y/o ajustar La política de seguridad de la información al menos cada año	Hacer seguimiento a las evidencias de actualización y revisión del cumplimiento de la política de seguridad. Aprobación del Comité Institucional de desarrollo y desempeño.
2	Procedimientos de seguridad de la información	Realizar seguimiento de la implementación de los procedimientos del SGSI	Revisar y/o actualizar los procedimientos del SGSI	Hacer seguimiento a las evidencias de actualización, revisión, comunicación e implementación de los procedimientos del SGSI
3	Gestión de activos	Ejecución de pruebas de seguridad (análisis de vulnerabilidades y ethical hacking) al menos cada 12 meses.	Realizar seguimiento al cierre de vulnerabilidad técnicas de acuerdo con su nivel de criticidad. Actualización, clasificación y etiquetado de activos de información.	Verificar la ejecución del re-test de pruebas de seguridad Verificar la actualización cada 12 meses o cuando ocurra un cambio importante en los procesos del inventario de activos. Verificación de la asignación de propietarios de activos.
4	Indicadores de seguridad de la información	Realizar seguimiento al cumplimiento de las metas de los indicadores del SGSI	Realizar seguimientos a las acciones correctivas planteadas para los indicadores que no cumplen las metas.	Hacer seguimiento a las evidencias de ejecución de acciones correcticas. Reporte de indicadores del SGSI y aporte de evidencias de la medición.
5	Gestión de riesgos	Revisar y realizar seguimiento trimestral de los Planes de Tratamiento de Riesgos	Realizar valoración trimestral del riesgo residual	Realizar seguimiento a la Documentación del Plan de Tratamiento de Riesgos (Aporte de evidencias).
6	Continuidad de negocio	Elaboración del PCN, aprobación publicación. Realizar seguimiento y revisión de la ejecución de las pruebas del PCN	Realizar seguimiento a la documentación y lecciones aprendidas de los resultados de las pruebas del PCN y a la continuidad de la seguridad de la información.	Revisión de las acciones de mejora planteadas para corregir las acciones de mejora identificadas en las pruebas del PCN.

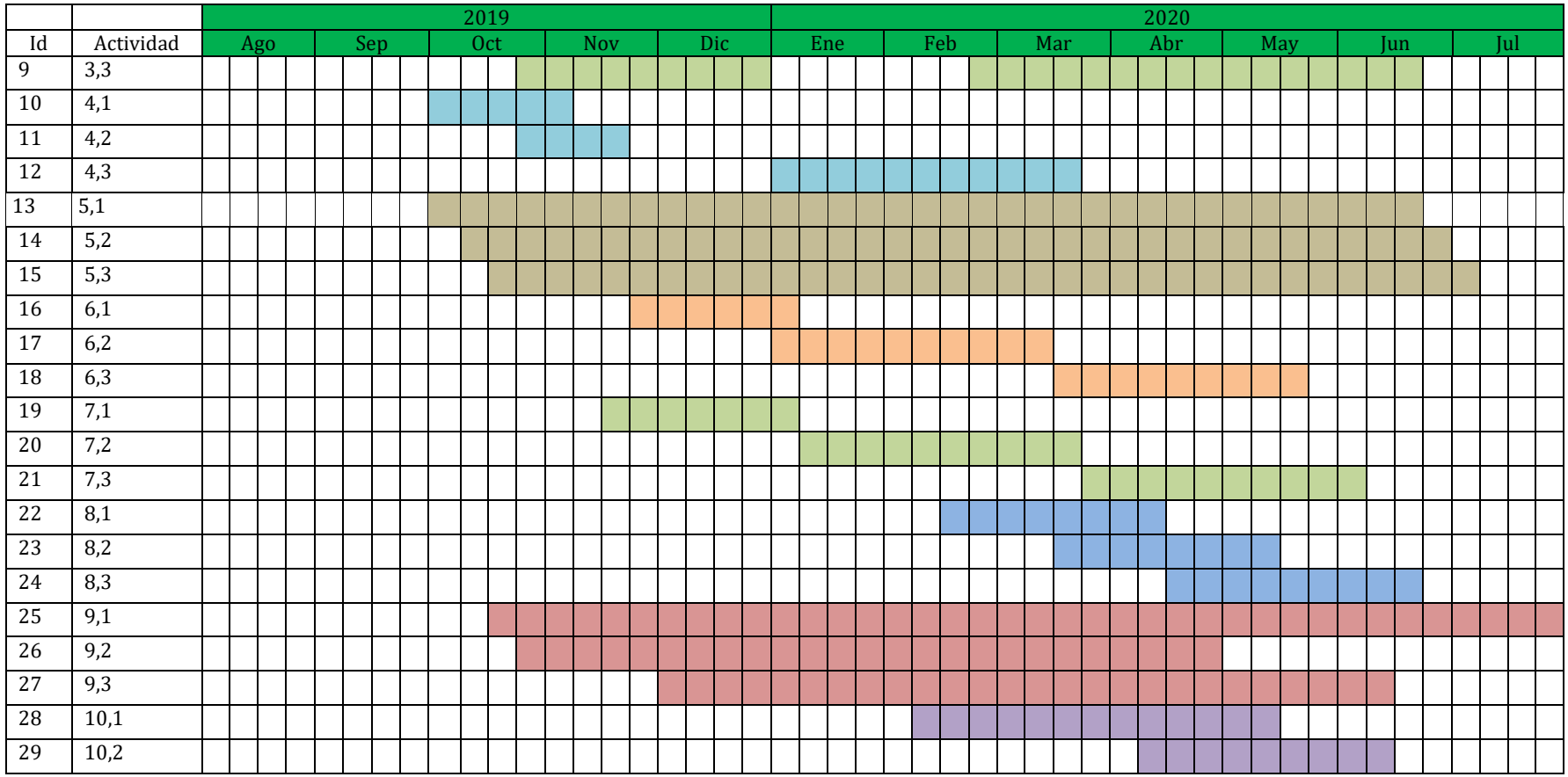
7	Plan de comunicación, socialización y sensibilización	Aprobar el Plan de comunicaciones y sensibilizaciones o capacitación de la ANT en el ítem de SGSI. Realizar al menos 2 jornadas de sensibilización en seguridad de la información en el año y al menos una jornada de reinducción en el año	Realizar evaluación de conocimientos de seguridad posterior a las capacitaciones.	Hacer seguimiento a las evidencias de socialización del SGSI. Anexar documentación a los indicadores del SGSI.
8	Auditoria	Inclusión de seguridad de la información en el programa de auditoria de Control Interno. Realizar seguimiento al cierre de las no conformidades producto de las auditorías internas y externas al SGSI.	Programar una revisión de verificación de cierre de no conformidades del SGSI. Presentación a la alta dirección de las no conformidades y su plan de mejoramiento.	Hacer seguimiento a las evidencias del cierre de las no conformidades por proceso
9	Gestión de incidentes	Realizar el seguimiento al procedimiento y a la gestión de incidentes de seguridad de la información incluyendo cierre.	Realizar seguimiento a las lecciones aprendidas producto de la gestión del incidente.	Realizar revisión y seguimiento de los reportes de eventos de seguridad de la información reportados por los funcionarios.
10	Gestión de la Seguridad de las operaciones	Creación de procedimientos documentados de operación. Gestionar los cambios para los sistemas que afecten la seguridad de la información.	Socializar reportes de la gestión de capacidad de servidores. Recolección de evidencia de separación de ambientes. Pruebas de restauración de copias de respaldo, con aporte de evidencias.	Realizar seguimiento a los riesgos identificados en las pruebas ejecutadas. Hacer revisión de registros (logs de servidores y equipos de comunicaciones). Realizar de barrido de permisos en SDI y en sistemas operativos.
11	Resultados de revisión periódicas del SGSI, por la alta dirección	Realizar revisión de los resultados de las revisiones periódicas por la dirección	Hacer seguimientos al cierre de los hallazgos de incumplimiento a las políticas y controles del SGSI	Realizar seguimiento al cierre de hallazgos que quedan pendientes |de la primera revisión.

12	Gestión de privacidad y protección de datos personales.	Desarrollo del informe de contexto (1581). Sensibilización e inclusión en el plan general de la ANT.	Actualización de políticas de protección de datos. Verificación de cumplimiento de aceptación por pare de los funcionarios.	Actualización y socialización en registros de ingreso, atención al ciudadano y en general en los formatos donde se tome información personal de funcionarios o ciudadanos. Verificación de mensajes pie de firma de correo y en videograbaciones de la ANT.
13	Administración de comunicaciones.	Gestionar el acceso de equipos a la red corporativa.	Aplicación del procedimiento de transferencia de información. Levantamiento de evidencias de aplicación del procedimiento. Revisar los acuerdos de confidencialidad con contratistas y proveedores.	Verificar la protección de la información aplicada en la mensajería electrónica, Levantamiento de evidencias y pruebas de vulnerabilidad.

Tabla 5. Guía de operación del SGSI

6.1. PLAN DE OPERACIÓN DEL SGSI




2019
2020
Id
Actividad
Ago
Sep
Oct
Nov
Dic
Ene
Feb
Mar
Abr
May
Jun
Jul
9 3,3
10 4,1
11 4,2
12 4,3
13 5,1
14 5,2
15 5,3
16 6,1
17 6,2
18 6,3
19 7,1
20 7,2
21 7,3
22 8,1
23 8,2
24 8,3
25 9,1
26 9,2
27 9,3
28 10,1
29 10,2

		2019																						2020																							
Id	Actividad	Ago				Sep				Oct				Nov				Dic				Ene				Feb				Mar				Abr				May				Jun				Jul			
30	10,3																																															
31	11,1																																															
32	11,2																																															
33	11,3																																															
34	12,1																																															
35	12,2																																															
36	12,3																																															
37	13,1																																															
38	13,2																																															
39	13,3																																															

Tabla 6. PLAN DE OPERACIÓN DEL SGSI

7. TERMINOS Y REFERENCIAS

Activos de información: aquello que es de alta validez y que contiene información vital de la empresa que debe ser protegida.

Amenaza: Es la causa potencial de un daño a un activo de información.

Análisis de riesgos: Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Controles: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.

Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
Dueño del riesgo sobre el activo: Persona responsable de gestionar el riesgo.

Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Oficial de Seguridad: Persona encargada de administrar, implementar, actualizar y monitorear el Sistema de Gestión de Seguridad de la Información.
Probabilidad de ocurrencia: Posibilidad de que se presente una situación o evento específico.

Riesgo: Grado de exposición de un activo que permite la materialización de una amenaza.

Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información (ISO 27000:2014).

Sistema de Gestión de Seguridad de la información (SGSI): permite establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma NTC-ISO-IEC 27001.

Vulnerabilidad: Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad de caracteriza por ausencia en controles de seguridad que permite ser explotada.

8. APROBACIÓN

HISTORIAL DE CAMBIOS		
Fecha	**Versión**	**Descripción**
29/01/2020	01	Primera versión del documento.

Elaboró: Cesar Daferzon Mosquera Valencia	**Revisó: Andres Fernando Cabrera Ochoa**	**Aprobó: Duberly Eduardo Murillo Barona**
Cargo: Contratista Subdirección de Sistemas de Información de Tierras	**Cargo:** Contratista Subdirección de Sistemas de Información de Tierras	**Cargo**: Subdirector de Sistemas de Información de Tierras
Firma:	**Firma:**	**Firma:**