PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020 DE LA ENTIDAD AGUAS DEL HUILA S.A E.S.P

aguas del huila

...llevamos más que agua.

www.aguasdelhuila.gov.co

INTRODUCCIÓN

De acuerdo a lo establecido por el ministerio de las TIC, plan de gobierno en línea GEL Decreto 2573 de 2014 Lineamientos generales de la Estrategia de Gobierno en línea 2015 Decreto 1078 de 2015 Decreto Único Sectorial. Donde los componentes son:

TIC para el Gobierno Abierto: Busca construir un Estado más transparente y colaborativo, donde los ciudadanos participan activamente en la toma de decisiones gracias a las TIC.
TIC para servicios: Busca crear los mejores trámites y servicios en línea para responder a las necesidades más apremiantes de los ciudadanos.
TIC para la gestión: Busca darle un uso estratégico a la tecnología para hacer más eficaz la gestión administrativa.
Seguridad y privacidad de la información: Busca guardar los datos de los ciudadanos como un tesoro, garantizando la seguridad de la información.

Así mismo la ley 1273 de 2009 donde se crea el bien denominado "DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE DATOS" y la ley 1341 de 2009 "por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones –TIC", la ley 1712 de 2014 "Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información Pública nacional" Aguas del Huila S.A. E.S.P., se compromete a tener un sistema de gestión de Seguridad de la información actualizado.
Al mismo tiempo revisamos la diferencia entre seguridad de la información y seguridad informática con el fin de justificar el cambio de nombre del documento.

El presente documento contiene el Plan de Seguridad y Privacidad de la información, orientado por un conjunto de actividades basadas en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) para crear condiciones de uso confiable en el entorno digital y físico de la información, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información.

OBJETIVO GENERAL

Establecer un Plan de Seguridad y Privacidad de la Información que apoye el establecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información de Aguas del Huila S.A. E.S.P., acorde a los requerimientos del modelo de seguridad de la estrategia de gobierno en línea, los requerimientos de la entidad y en cumplimiento de las disposiciones legales vigentes.

OBJETIVOS ESPECIFICOS

- Definir las etapas para establecer la estrategia de seguridad de la información de la entidad.
- Apalancar la implementación del Sistema de Gestión de Seguridad de la Información de la entidad de acuerdo con los requerimientos establecidos en el modelo de seguridad de la estrategia de Gobierno en Línea.
- Establecer lineamientos para la implementación y/o adopción de mejores prácticas de seguridad e la entidad.
- Optimizar la gestión de la seguridad de la información al interior de la entidad.

ALCANCE

El del sistema de gestión de Seguridad de la información (SGSI) es un manuscrito de alto nivel que expresa el compromiso de la Alta Dirección con la seguridad de la información. Este plan contribuye a minimizar los riesgos asociados a daños, proyecta la eficiencia administrativa y asegura el cumplimiento de las funciones misionales de la entidad apoyada en el uso adecuado de TIC

Este plan es de aplicación en todas las dependencias que componen Aguas del Huila S.A. E.S.P.; a sus recursos, a la totalidad de los procesos internos o externos vinculados a la Administración Pública a través de contratos o convenios con terceros y a todo el personal de la entidad, independiente de su tipo de vinculación, la dependencia a la cual se encuentre adscrito y el nivel de funciones o labores que ejecute.

RESPONSABLES

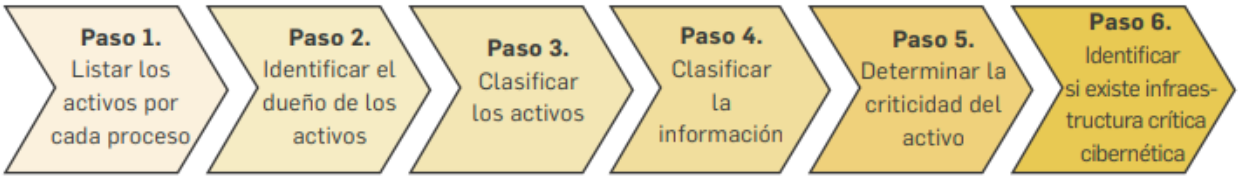
Los propietarios de activos de la información, son responsables de la clasificación, mantenimiento, actualización y valoración de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo el perfil de los usuarios, y el nivel de permisos de acceso a la información de acuerdo a sus cargos, funciones y competencias. Tienen la responsabilidad de mantener de forma integral, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

Al vincularse un funcionario a la entidad contratista o funcionario dentro de la inducción, deberá ser notificado respecto al cumplimiento de las Políticas de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas, guías y lineamientos que surjan del Sistema de Gestión de la Seguridad de la Información.

IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN

Cada área o dependencia de la Entidad, con la colaboración del encargado de seguridad de la Información, y con base en el inventario de activos de la información, debe mantener un inventario de estos activos con la que se cuenta, ya sea procesada o producida. La forma y medios en donde se incorpore la clasificación, valorización, ubicación y acceso de la información, se especifican por medio por medio del responsable de las TIC.

Los servidores públicos de la Aguas del Huila S.A. E.S.P., independiente del tipo de vinculación laboral o contractual, la dependencia o área a la cual se encuentre adscrito y el nivel de funciones, tareas o actividades que desempeñe debe contar con un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. La Dirección de Informática y Sistemas (DIS) debe mantener un directorio completo y actualizado de los perfiles creados. Así mismo deben cumplir con las políticas específicas para la prestación de servicio y salvaguardar la información.



CLASIFICACIÓN DE LA INFORMACIÓN

La información propiedad de Aguas del Huila S.A. E.S.P., se considerará por defecto, correspondiente a toda la información “Pública”, o que no haya sido declarada como “Pública”, “Pública Clasificada” o “Pública Reservada”. (Ley 1712 de 2014 de Transparencia, Artículo 6) Sólo se podrá tener acceso a información clasificada como

“Pública Clasificada” o “Pública Reservada” bajo previa aprobación del “sujeto obligado” de la información. (Art. 5 Ley 1712/2014)

De acuerdo a la Ley en Mención, la información se clasifica en:

✓Pública: Toda información que un sujeto obligado genere, obtenga, adquiera o controle en su calidad de tal.

✓Pública Clasificada: Es aquella información, que estando en poder o custodia de un sujeto obligado, pertenece al ámbito propio, particular y privado o semi-privado, 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 citada Ley.

✓Pública Reservada: Es aquella información, que estando en poder o custodia de un sujeto obligado o en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo el cumplimiento de la totalidad de los requisitos consagrados en el Artículo 19 de la citada Ley.

La responsabilidad de la clasificación de la información, recae sobre la Alta Dirección, Asesores y Jefes de Área de cada dependencia. Se debe tomar como guía para el proceso de clasificación, lo establecido en la Ley 1712 del 2014 Artículo 6.

El primer responsable de verificar que la Información cuente con controles adecuados que eviten su pérdida, daño o divulgación no autorizada es el sujeto obligado de la Información.

El nivel de protección requerido para cada nivel de clasificación, se deberá evaluar analizando los requerimientos de Confidencialidad (la información de mayor valor para la entidad solo puede ser conocida por personas autorizadas); e Integridad (la información no debe poder ser alterada o destruida de manera no autorizada para afectar la entidad).

ACUERDO DE CONFIDENCIALIDAD Y DERECHOS DE PROPIEDAD INTELECTUAL

Mientras persista una relación laboral con la Aguas del Huila S.A. E.S.P., todos sus funcionarios y contratistas ceden a la entidad los derechos de propiedad intelectual de los desarrollos que originen como parte de sus responsabilidades laborales y contractuales con la institución.

Siempre que se requiera compartir información “Pública Clasificada” y/o “Pública Reservada” con un tercero, deberá acogerse a los términos de la Ley.

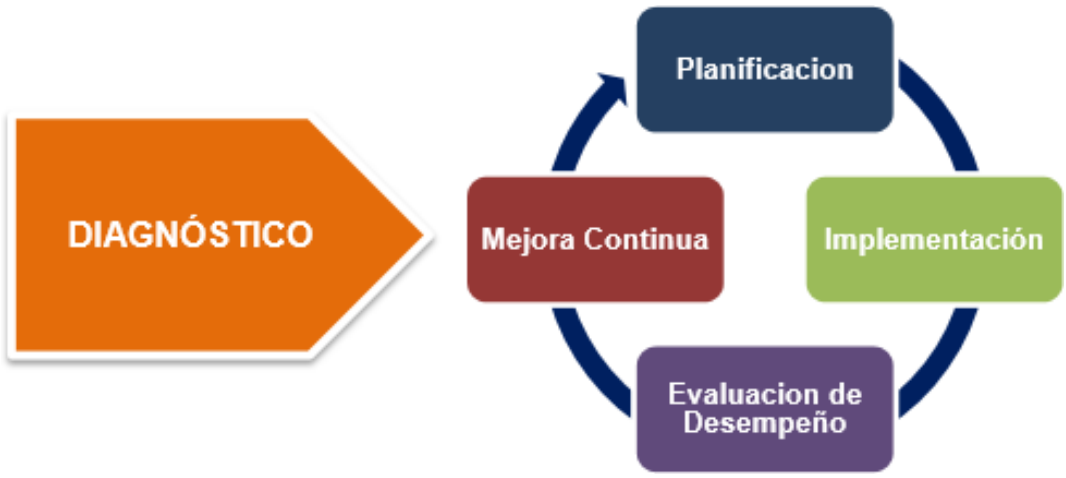
Con el fin de tener acceso a los sistemas de Información institucionales Aguas del Huila cada usuario deberá firmar el Compromiso de confidencialidad.

RIESGO DE LA INFORMACIÓN

Clasificación	Tipo	Riesgo	Tratamiento
Inventario Sistemas De Información	Software	Pérdida de Información	Aplicar control
Inventario De Bienes	Bienes	Bienes no Asegurados	Aceptado
	Almacenamiento de elementos	Falta de controles sobre los bienes almacenados	Aplicar control
Inventario De Expedientes	Documentos	Uso inadecuado de la información	Aplicar control
	Expedientes	Pérdida de expedientes	Aplicar control
Inventario Del Recurso Humano	Historias laborales	Pérdida o sustracción	Aplicar control
Manejo Inadecuado de Sistemas De información	Humano	Uso inadecuado del sistema de información	Aplicar control

Se realiza identificación y evaluación de las amenazas y vulnerabilidades relativas a los activos de información ya sean sistemas de información, infraestructura, bienes o de recurso humano, la probabilidad de que ocurran y su potencial impacto en la operación de la entidad.

METODOLOGÍA DE LA IMPLEMENTACIÓN DEL PLAN



Fuente: Ciclo de operación Modelo de Seguridad y Privacidad de la Información
http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

El Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno en Línea contempla el siguiente ciclo de operación que contempla cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información[1].

- **Fase Diagnostico**: Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información

- **Fase Planificación (P**lanear**):** En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición

para controlar y cuantificar los objetivos.

- **Fase Implementación (H**acer**):** En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.

- **Fase Evaluación de desempeño (V**erificar**):** Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.

- **Fase Mejora Continua (A**ctuar**):** Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

ALINEACION NORMA ISO 27001:2013 VS CICLO DE OPERACION

Aunque en la norma ISO 27001:2013 no se 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 las modelos de gestión de la siguiente forma:

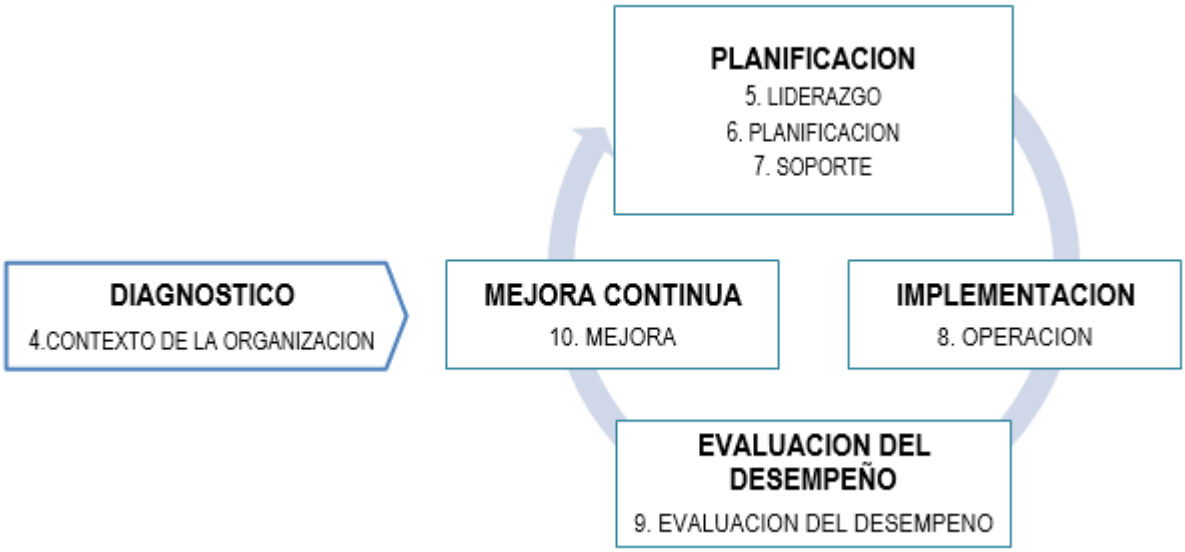


Figura 2. ***Norma ISO 27001:2013 alineado al Ciclo de mejora continua***
Fuente: Elaborada con base en la información publicada en la página web http://www.welivesecurity.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-la-norma-para-gestionar-la-seguridad-de-la-informacion/

El siguiente cuadro muestra la relación entre las fases del ciclo de operación del Modelo de Seguridad y Privacidad de la Información (Diagnostico, Planificación, Implementación, Evaluación, Mejora Continua) y la estructura de capítulos y numerales de la norma ISO 27001:2013:

Tabla 1. Fases Ciclo Operación vs Estructura ISO 27001:2013

Fase	Capitulo ISO 27001:2013[2]
Diagnostico	4. Contexto de la Organización
Planificación	5. Liderazgos 6. Planificación 7. Soporte
Implementación	8. Operación
Evaluación de desempeño	9. Evaluación de desempeño
Mejora Continua	10. Mejora

•Fase DIAGNOSTICO en la norma ISO 27001:2013.

En el capítulo 4 - Contexto de la organización de la norma ISO 27001:2013, se determina la necesidad de realizar un análisis de las cuestionas externas e internas de la organización y de su contexto, con el propósito de incluir las necesidades y expectativas de las partes interesas de la organización en el alcance del SGSI.

•Fase PLANEACION en la norma ISO 27001:2013

En el capítulo 5 - Liderazgo, se establece las responsabilidades y compromisos de la Alta Dirección respecto al Sistema de Gestión de Seguridad de la Información y entre otros aspectos, la necesidad de que la Alta Dirección establezca una política de seguridad de la información adecuada al propósito de la organización asegure la asignación de los recursos para el SGSI y que las responsabilidades y roles pertinentes a la seguridad de la información se asignen y comuniquen.

En el capítulo 6 - Planeación, se establece los requerimientos para la valoración y tratamiento de riesgos de seguridad y para la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento.

En el capítulo 7 - Soporte se establece que la organización debe asegurar los recursos necesarios para el establecimiento, implementación y mejora continua Sistema de Gestión de Seguridad de la Información.

•Fase IMPLEMENTACION en la norma ISO 27001:2013.

En el capítulo 8 - Operación de la norma ISO 27001:2013, se indica que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.

•Fase EVALUACION DEL DESEMPEÑO en la norma ISO 27001:2013.

En el capítulo 9 - Evaluación del desempeño, se define los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia del sistema de gestión de seguridad de la información.

•Fase MEJORA CONTINUA en la norma ISO 27001:2013.

En el capítulo 10 - Mejora, se establece para el proceso de mejora del Sistema de Gestión de Seguridad de la Información, que a partir de las no-conformidades que ocurran, las organizaciones deben establecer las acciones más efectiva para solucionarlas y evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repitan.

FASES I: DIAGNOSTICO

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

Metas	Actividades \ Instrumentos \ Resultados
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad	**Diagnóstico** de la **situación actual** de la entidad con relación a la gestión de seguridad de la información. **Diagnostico nivel de cumplimiento** de la entidad frente a los objetivos de control y controles establecidos en el Anexo A de la **norma ISO 27001:2013**. **Valoración estado actual** de la gestión de seguridad de la entidad

	con base en el Instrumento de Evaluación MSPI de MINTIC.
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad.	**Valoración** del **nivel de estratificación** de la entidad frente a la seguridad de la información **con base en** el método planteado en el documento '*ANEXO 3: ESTRATIFICACIÓN DE ENTIDADES*' del modelo seguridad de la información para la estrategia de Gobierno en Línea 2.0. **Valoración** del **nivel de madurez** de seguridad y privacidad de la información en la entidad de acuerdo con los lineamientos establecidos en el capítulo '*MODELO DE MADUREZ*' del documento Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea.
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	**Ejecución prueba de vulnerabilidades** con el fin de identificar el nivel de seguridad y protección de los activos de información de la entidad y definición de planes de mitigación.

Para la recolección de la información, en esta fase se utilizarán mecanismo como:

- Diligenciamiento de cuestionarios con el objetivo de determinar el nivel de cumplimiento de le entidad con relación a los dominios de la norma ISO/IEC 27001:2013.

- Documentación existente en el sistema de calidad de la entidad relacionada con la información de las partes interesadas de la entidad y los roles y funciones asociados a la seguridad de la información.

- Fuentes externas, como las guías de autoevaluación, encuesta y estratificación dispuestas por la estrategia de gobierno en línea Ministerio de Tecnologías de la Información y las Comunicaciones.

FASES II: PLANIFICACIÓN

Objetivo	Definir la estrategia metodológica, que permita establecer el alcance, objetivos, procesos y procedimientos, pertinentes a la gestión del riesgo y mejora de seguridad de la información, en procura de los resultados que permitan dar cumplimiento con las metas propuestas del SGSI.

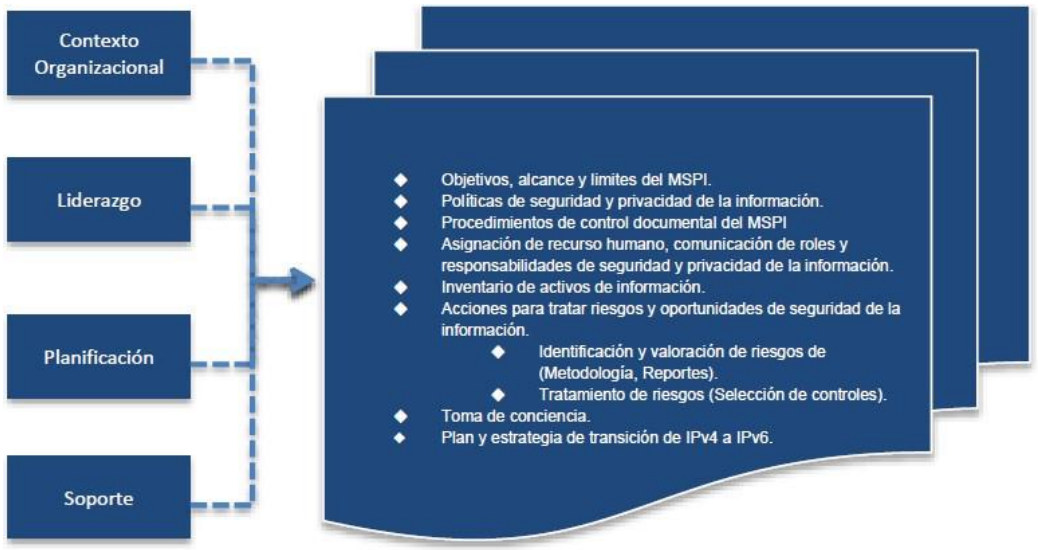


Figura 3. **Fase de planificación modelo de seguridad**

Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

Metas	Actividades \ Instrumentos \ Resultados
Realizar un análisis de Contexto y factores externos e internos de la Entidad en torno a la seguridad de la información.	**Realizar** un **Análisis de Contexto** de la entidad entorno a la seguridad de la información teniendo en cuenta el capítulo 4. CONEXTO DE LA ORGANIZACIÓN de la norma ISO 27001:2013, con el fin de poder determinar las cuestiones externas e internas de la organización que son pertinentes para la implementación del Sistema de Gestión de Seguridad de la Información.
Definir el alcance del SGSI de la entidad	**Definir** el **alcance** del **Sistema de Gestión de Seguridad de la Información** 'SGSI' de la entidad aprobado por la Alta Dirección y socializado al interior de la Entidad. Definir el alcance del SGSI, en el cual se establece los límites y la aplicabilidad del Sistema de Gestión de Seguridad de la Información.
Definir Roles, Responsables y Funciones de seguridad y privacidad de la información	**Adicionar** las **funciones de seguridad** de la información al **Comité de Riesgos** de la entidad y formalizarlas mediante acto administrativo. **Establecer** el **Rol** de **Oficial de Seguridad** de la información. **Definir** un **marco de gestión que contemple roles y responsabilidades** para la implementación, administración, operación y gestión de la seguridad de la información en l entidad. **Definir la estructura organizacional** de la Entidad que contendrá los roles y responsabilidad **pertinentes a la seguridad** de la información.
Definir la metodología de riesgos de seguridad de la información	**Definir Metodología** de Valoración de **Riesgos de Seguridad**. **Integrar** la **metodología** definida con la metodología de riegos operativos de la entidad. **Implementar** un **sistema de información** para la administración y gestión de los riesgos de seguridad de la entidad.

Elaborar las políticas de seguridad y privacidad de la información de la entidad	**Elaborar Política General de Seguridad y Privacidad** la cual debe ser aprobada por la Alta Dirección y socializada al interior de la Entidad. **Elaborar** el **manual de Políticas de Seguridad y Privacidad de la Información**, que corresponde a un documento que contiene las políticas y los lineamientos que se implementaran en la Entidad con el objetivo de proteger la disponibilidad, integridad y confidencialidad de la información. Estas políticas deben ser aprobadas por la Alta Dirección y socializadas al interior de la Entidad.
Elaborar documentación de operación (formatos de procesos, procedimientos y documentos debidamente definidos y establecidos) del sistema de seguridad de la información	**Elaborar** los **documentos de operación del sistema de seguridad** de la información, tales como: • Declaración de aplicabilidad • Procedimiento y/o guía de identificación y clasificación de activos de información. • Procedimiento Continuidad del Negocio, Procedimientos operativos para gestión de TI • Procedimiento para control de documentos (SGI) • Procedimiento para auditoría interna (SGI) • Procedimiento para medidas correctivas (SGI) • Procedimiento para la gestión de eventos e incidentes de seguridad de la información • Procedimiento para la gestión de vulnerabilidades de seguridad de la información. • Entre otros.
Identificar y valorar activos de información	**Realizar** la **identificación** y **valoración** de los **activos de información** de la entidad de acuerdo con su nivel de criticidad de acuerdo con el alcance del SGSI. Documentar el inventario de activos de información de la entidad.

FASES III: IMPLEMENTACIÓN

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 entidad.

Figura 4. **Fase de implementación modelo de seguridad**
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

Metas	Actividades \ Instrumentos \ Resultados
Establecer el plan de implementación de seguridad de la información	**Implementar** el **plan de implementación** del **modelo de seguridad y privacidad** de la información el cual debe ser revisado y aprobado por el comité de riesgos
Ejecutar el plan de tratamiento de riesgos	**Ejecutar** el **plan de tratamiento de los riesgos** transversales de seguridad de la información identificados en la fase de planificación que fue presentado en el comité de riegos.
Ejecutar del plan y estrategia de transición de IPv4 a IPv6.	**Ejecutar plan de transición a IPv6** y elaborar informe de implementación.
Establecer indicadores de gestión de seguridad	**Definir los indicadores** para medir la gestión del modelo de seguridad y establecer los mecanismos para su medición. Estos indicadores deben permitir verificar la eficacia y efectividad de los controles implementados para mitigar los riesgos de seguridad de la entidad.
Implementar procedimiento de gestión de eventos e incidentes de seguridad	**Implementar** el procedimiento y los mecanismos para la **gestión de los eventos e incidentes de seguridad** de la información**.**
Implementar procedimiento de gestión de vulnerabilidades	**Implementar** el procedimiento y los mecanismos para la **gestión de vulnerabilidades seguridad** de la información**.**
Ejecutar plan de capacitación y sensibilización de seguridad	**Ejecutar** el plan anual de capacitación, socialización y sensibilización de seguridad de la información
Ejecutar pruebas anuales de vulnerabilidades e intrusión	**Ejecutar** el plan anual de **pruebas vulnerabilidades** e intrusión con el objetivo de identificar el nivel de protección de los activos de

Ejecutar pruebas de Ethical Hacking	**Ejecutar** pruebas anuales de **Ethical Hacking** orientadas a poder determinar los niveles de riesgo y exposición de la organización ante atacantes interno o externo que puedan a comprometer activos críticos de la entidad y con esto generar interrupción en los servicios, afectar la continuidad del negocio y/o acceder de forma no autorizada a la información sensible o clasificada de la entidad o de carácter personal de los trabajadores o terceros que laboren para la entidad.
Ejecutar pruebas de Ingeniera Social	**Ejecutar** pruebas anuales de **ingeniería social** orientadas a verificar aspectos como: (i) los protocoles internos de seguridad, (ii) el nivel de concientización de los funcionarios y terceros que laboren en la entidad sobre temas de seguridad de la información, (iii) el conocimiento y/o cumplimiento de las políticas de seguridad y privacidad de la información de la entidad y (iv) el nivel de exposición de la información publicada en internet de la entidad y de sus empleados.

FASES IV: EVALUACIÓN DE DESEMPEÑO

Objetivo	Evaluar el desempeño y la eficacia del SGSI, a través de instrumentos que permita determinar la efectividad de la implantación del SGSI.

Figura 5. **Fase Evaluación Desempeño modelo de seguridad**
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

Metas	Actividades \ Instrumentos \ Resultados
Ejecución de auditorías de seguridad de la información	**Ejecución de auditorías** del modelo de seguridad y de temas normativos y de cumplimiento de seguridad de la información aplicables a la entidad, de acuerdo con el plan de auditoria revisado y aprobado por la Alta Dirección. Las auditorías internas se deberán llevar a cabo para la revisión del Sistema de Gestión de Seguridad 'SGSI' de la Información implementado en la entidad, con la finalidad de verificar que los objetivos de control, controles, procesos y procedimientos del SGSI cumpla con los requisitos establecidos en la norma ISO 27002:2013 y los del MSPI.
Plan de seguimiento, evaluación y análisis de SGSI	**Elaboración documento** con el **plan de seguimiento, evaluación y análisis del SGSI** revisado y aprobado por el Comité de Riesgos.

FASES V: MEJORA CONTINUA

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

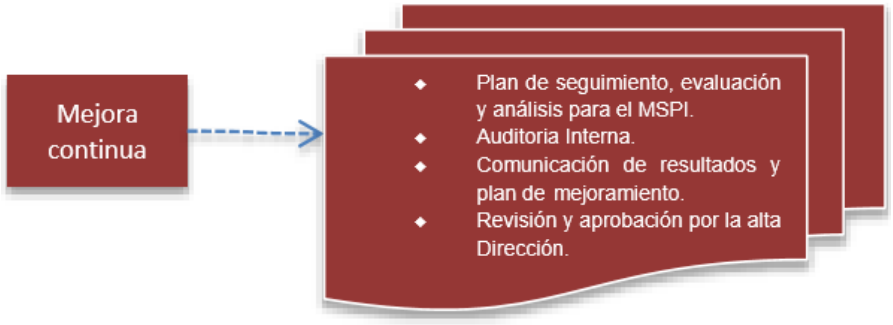


Figura 6. ***Fase Mejora Continua modelo de seguridad***
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

Metas	Actividades \ Instrumentos \ Resultados

Diseñar plan de mejoramiento	**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 Sistema de Gestión de Seguridad de la Información.

FASES VI: IMPLEMENTACIÓN DEL PLAN

ACTIVIDAD	2020											
	1	2	3	4	5	6	7	8	9	10	11	12
FASE DIAGNOSTIVO												
Determinar el estado actual de la gestión de seguridad de la entidad												
Identificar el nivel de madurez de seguridad de la entidad												
Identificar vulnerabilidades técnicas												
FASE PLANIFICACION												

Realizar análisis de Contexto de la Entidad en torno a la seguridad.												
Definir el alcance del SGSI de la entidad												
Definir Roles y Responsables de seguridad de la información												
Definir la metodología de riesgos de seguridad de la información												
Elaborar políticas de seguridad y privacidad de la información												
Elaborar documentación de operación del sistema de seguridad												
Identificar y valorar activos de Información												
Identificar y valorar los riesgos de seguridad de la información												
Definir plan de capacitación, comunicación y sensibilización												
Diagnóstico Plan de IPv4 a IPv6												
FASE IMPLEMENTACION												
Implementación medidas objetivos de control Anexo A ISO 27001												
Implementar planes de acción resultado de las auditorias												
Ejecutar plan de tratamiento de riesgos												
Ejecutar del plan y estrategia de transición de IPv4 a IPv6.												
Implementar procedimiento de gestión de eventos e incidentes de seguridad												
Implementar procedimiento de gestión de vulnerabilidades												
Ejecutar plan de capacitación y sensibilización de seguridad												
Ejecutar pruebas anuales de vulnerabilidades												
FASE EVALUACION DESEMPEÑO												
Ejecución auditoria de seguridad de la información												
FASE MEJORA CONTINUA												
Diseñar plan de mejoramiento												

TERMINOS

- Activo 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.

- Anexo SL: Nuevo esquema definido por International Organization for Standardization - ISO para todos los Sistemas de Gestión acorde al nuevo formato llamado “Anexo SL”, que proporciona una estructura uniforme como el marco de un sistema de gestión genérico.

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

- Causa: Razón por la cual el riesgo sucede.

- Ciclo de Deming: Modelo mejora continua para la implementación de un sistema de mejora continua.

- Colaborador: Es toda persona que realiza actividades directa o indirectamente en las instalaciones de la entidad, Trabajadores de Planta, Trabajadores Temporales, Contratistas, Proveedores y Practicantes.

- Confidencialidad: Propiedad que determina que la información no esté disponible a personas 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: Propiedad de determina que la información sea accesible y utilizable por aquellas personas debidamente autorizadas.

- Dueño del riesgo sobre el activo: Persona responsable de gestionar el riesgo.

- Impacto: Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo.

- Incidente de seguridad de la información: Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.

- Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.
- 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.

- Responsables del Activo: Personas responsables del activo de información.
- Riesgo: Grado de exposición de un activo que permite la materialización de una amenaza.

- Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

- Riesgo Residual: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo.

- PSE: Proveedor de Servicios Electrónicos, es un sistema centralizado por medio del cual las empresas brindan a los usuarios la posibilidad de hacer sus pagos por Internet.

- SARC: Siglas del Sistema de Administración de Riesgo Crediticio.

- SARL: Siglas del Sistema de Administración de Riesgo de Liquidez.

- SARLAFT: Siglas del Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo.

- SARO: Siglas del Sistema de Administración de Riesgos Operativos.
- Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información (ISO 27000:2014).

- SGSI: Siglas del Sistema de Gestión de Seguridad de la Información.

- 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.

MARCO NORMATIVO

NORMA	OBJETO
Norma ISO 27001:2013	*"norma técnica NTC-ISO/IEC colombiana 27001tecnología de la información. Técnicas de seguridad. sistemas de gestión de la seguridad de la información (SGSI). Requisitos"*
Decreto 2573 de 2014	*"Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta la Ley 1341 de 2009 y se dictan otras disposiciones."*
Decreto 1078 de 2015	*Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones*
Ley 1712 de 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 1273 de 2009	*"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"*

Tabla. Marco Normativo