PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023 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 le permita a la Entidad desarrollar y fortalecer una adecuada gestión de los riesgos de seguridad de la información a través de métodos que facilite la determinación del contexto estratégico, la identificación de riesgo y oportunidades, el análisis, la valoración y expedición de políticas, así como el seguimiento y monitoreo permanente enfocado a su cumplimiento y mejoramiento continuo.

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.
- Proteger el valor de los activos de información mediante el control de implementación de acciones de mitigación frente al riesgo y potencializar las oportunidades asociadas
- Generar una cultura y apropiación de trabajo enfocada a la identificación de los riesgos de seguridad de la información y su mitigación.
- Reducir toda posibilidad de que una brecha o evento produzca determinado impacto bien en la información o cualquier otro activo de información asociado, a través de la gestión adecuada de los riesgos de la seguridad de la información

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

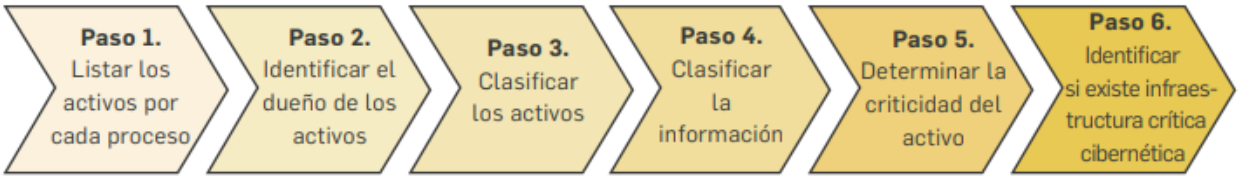
Los propietarios de activos de la información, son responsables de la clasificación, mantenimiento, actualización y valoración de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo el perfil de los usuarios, y el nivel de permisos de acceso a la información 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.

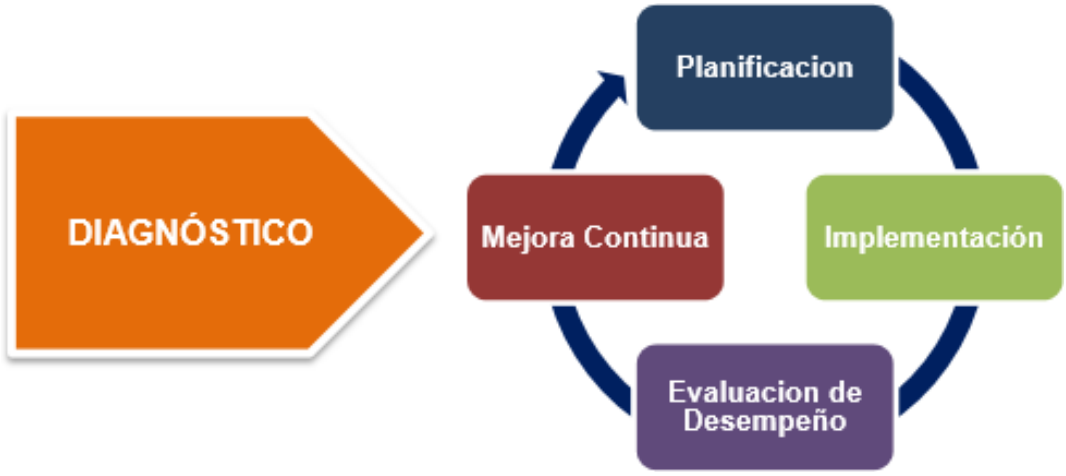
Con el fin de tener acceso a los sistemas de Información institucionales Aguas del Huila cada usuario deberá firmar el Compromiso de confidencialidad.

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.

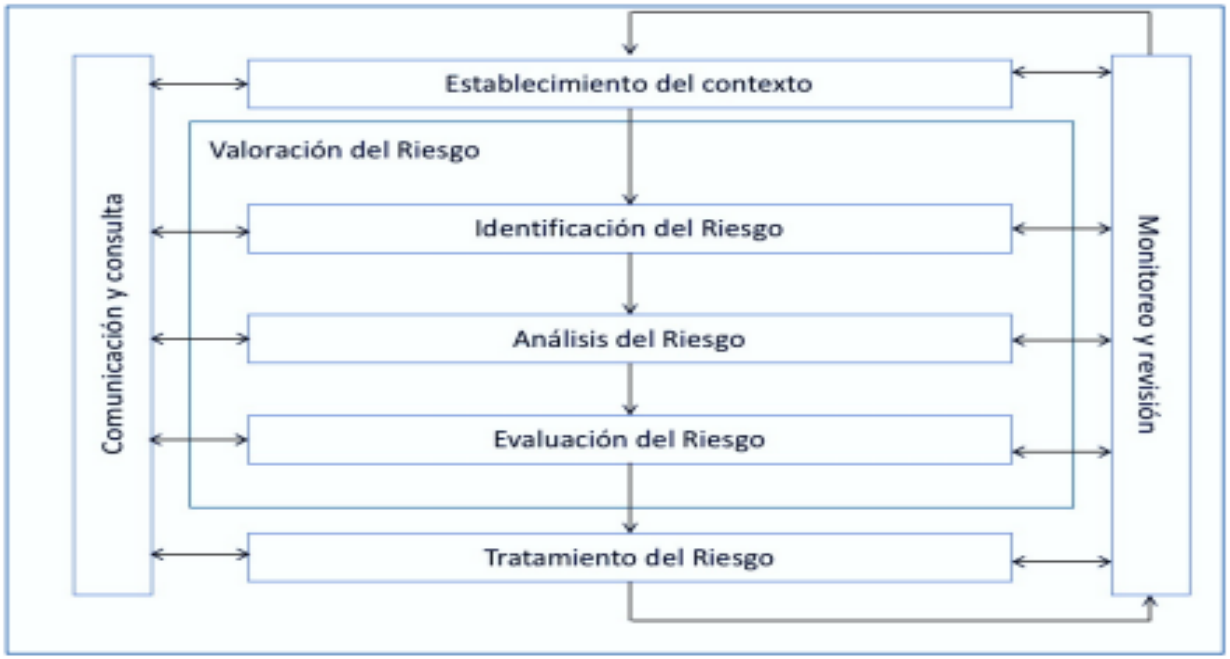
- **Fase Mejora Continua (A**ctuar**):** Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

ALINEACION NORMA ISO 27001:2013 e ISO 31000 DE 2018

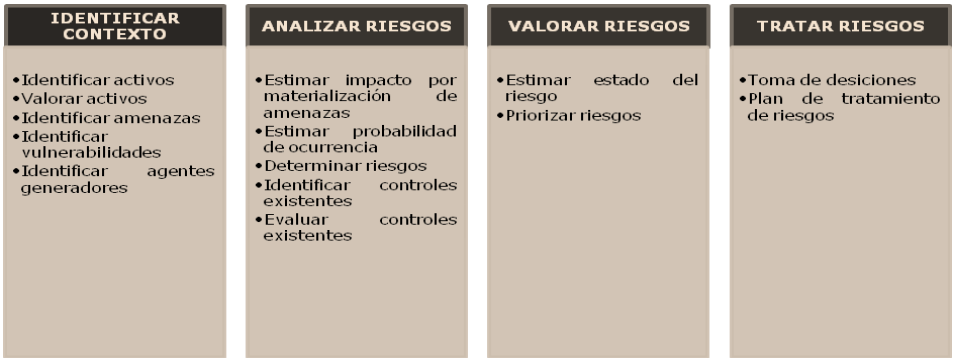
La norma ISO 27005 es el estándar internacional que se ocupa de la gestión de los riesgos relativos a la seguridad de información. La norma suministra las directrices para la gestión de riesgos, apoyándose fundamentalmente en los requisitos sobre esta cuestión definidos en la ISO 27001 y aunque esta 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:

DESCRIPCIÓN

Ejecutar acciones que protejan adecuadamente los sistemas de información y activos de la organización, al igual que implementar controles de seguridad, requiere desarrollar un proceso de Gestión de riesgos (Ver ilustración 1), basado en los activos y los factores tanto internos como externos



A continuación se exponen las actividades de cada una de las etapas del proceso de Gestión de Riegos, con el fin de identificar con claridad la situación de cada uno de sus activos: su valor, vulnerabilidades, y cómo están protegidos frente a amenazas



IDENTIFICAR EL CONTEXTO DE LA ORGANIZACIÓN

Propósito

Conocer los eventos potenciales, estén o no bajo el control de la organización y que ponen en riesgos sus activos de información

Actividades a realizar

A. Identificación de activos de información

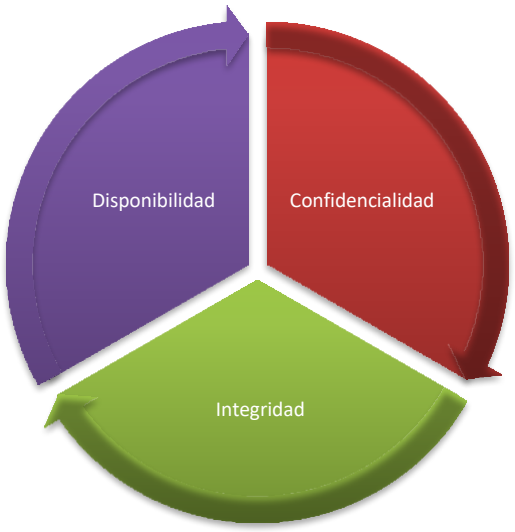
Un activo es: “cualquier elemento al cual se le asigna un valor y por tanto debe protegerse”, lo cual puede entenderse igualmente como aquello que requiere la organización para el cumplimiento de sus objetivos

1. Tipos de activos
2. Clases de activos:

Activos de información y físicos		
Activos físicos	Infraestructura física	Oficinas
	Hardware	Servidores, dispositivos de comunicaciones, computadoras de escritorio.
	Tecnología Software	Aplicaciones
Activos de información	Electrónica	Información importante para el negocio.
	Documentos	Información importante para el negocio
personal	Dueños de información	Nivel directivo dueño de la información que asigna permisos para leer utilizar y modificar la información.
		Personal que utiliza la información para su trabajo.
Servicios		Correo electrónico

Valoración de los activos de información

Una vez identificados los activos se realizará la valoración de cada uno de ellos en términos de valor para el negocio según:



Pilares de la seguridad de la información ISO 27001:2013

Disponibilidad:

Los activos de una determinada organización tendrán mayor valor en la medida que si no están disponibles se impactará gravemente el negocio. Igualmente, un activo que al no estar disponible no afecte de ningún modo el negocio, tendrá un menor valor.

Para determinar el impacto que sobre el negocio genera la indisponibilidad del activo se utilizarán los criterios relacionados en la siguiente tabla:

	Valoración de los activos			
	MINIMO (1)	**MEDIO (3)**	**GRAVE (5)**	**CATASTRÓFICO (7)**
Las pérdidas **económicas** por indisponibilidad del activo son:				
Los **servicios** prestados se ven afectados por la indisponibilidad del activo de la siguiente forma:	Interrupción leve o nula en suministro de servicios.	Obliga al cliente a cambiar de proveedor de forma transitoria.	Pérdida de algunos clientes de forma definitiva.	Pérdida de clientes clave.
La inidisponibilidad del activo afecta la **operación** así:	Retrasos en funciones no vitales	Retrasos leves en funciones vitales.	Retrasos graves en funciones vitales	Interrupción inmediata de funciones vitales
La indisponibilidad del activo afecta la **imagen** en el sentido que:	No afectar la confianza en los productos o servicios.	Pérdida de confianza en un servicio específico o en una parte de la organización.	Pérdida de confianza de parte de los clientes.	Pérdida de confianza del mercado y daños a la imagen de marca.
La indisponibilidad del activo afecta el **cumplimiento** de obligaciones en el sentido que:	Produce una falta leve en el cumplimiento de algún contrato.	Produce una falta en el cumplimiento de algún contrato que obliga a renegociar.	Produce una falta grave en el cumplimiento de algún contrato.	Deja a la organización al margen de la ley

Tabla 2: Criterios para valoración de

disponibilidad

Se asigna un valor utilizando la siguiente escala:

VALORACIÓN	VALOR
Mínimo	1
Medio	3
Grave	5
Catastrófico	7

Tabla 3. Valoración de la disponibilidad

Confidencialidad:

Los activos de información reciben una valoración alta cuando su nivel de confidencialidad es mayor, teniendo en cuenta que la divulgación no autorizada de la misma puede afectar en alguna medida los intereses, imagen y operación de la compañía.

Para realizar la valoración de los activos en la dimensión de confidencialidad tendremos en cuenta los resultados obtenidos en la Herramienta para Clasificación de Información (y con base en la clasificación obtenida para cada activo asignaremos un valor.

CLASIFICACIÓN	VALOR
Publica	5
Uso Interno	10
Confidencial	15
Reservada	20

Tabla 4. Valoración de la confidencialidad

Integridad:

Los activos son valorados con mayor valor cuando su alteración puede generar daños graves a la organización.

La valoración en la dimensión integridad se realizará utilizando los siguientes criterios:

CRITERIO	VALOR
Información que afecta mucho la operación	20
Información que afecta moderadamente el negocio	15
Información que puede tener algunos errores o cambios sin afectar su sentido principal	10
Información o activos que pueden tener errores sin tener impactos al negocio.	5

Tabla 5. Criterios para la valoración de la integridad

Para calcular el valor del activo se realiza la sumatoria de todos los factores evaluados y se establecerá el valor de activo teniendo en cuenta lo siguiente:

VALORACIÓN DE ACTIVO	SUMATORIA DE LOS FACTORES CONSIDERADOS
MB: muy bajo	De 14 a 24
B: bajo	De 25 a 35
M: medio	De 36 a 46
A: alto	De 47 a 57
MA: muy alto	De 58 a 68

Tabla 6. Valoración de la confidencialidad del activo.

Identificación de amenazas posibles

Las amenazas son resultados de actos deliberados que pueden afectar nuestros activos o los activos de información, sin embargo, existen eventos naturales o accidentales que deben ser considerados por su capacidad de generar incidentes de seguridad.

CAUSA	EVENTO O AMENAZA
Eventos naturales	Terremotos o huracanes.
Eventos externos	Pérdida de proveedores, problemas de transporte, sobrecargas.
Condiciones internas	Problemas de transporte.
Actos deliberados	Fallas de hardware, fallas de software, fallas en la red,
Actos accidentales	Destrucción de información, Incendios.
Humano	Epidemias, indisponibilidad de personal.

Tabla 7. Listado de amenazas

El impacto es la medida de daño causado por un incidente en el supuesto de que ocurra, afectando así, el valor de los activos, está perdida de valor la denominamos degradación del activo.

La medición del impacto la realizaremos utilizando la siguiente matriz:

VALORACION DEL ACTIVO	AFECTACION DEL ACTIVO				
	5%	25%	50%	75%	100%
MA: muy alto	A	A	A	A	MA
A: alto	M	M	A	A	A
M: medio	B	M	M	A	A
B: bajo	MB	MB	M	M	M
MB: muy bajo	MB	MB	MB	B	M

Tabla 8. Matriz de estimación del impacto sobre activos.

La estimación del impacto puede ser entonces**:**

1. **MA:** Muy alto
2. **A:** Alto
3. **M:** Medio
4. **B:** Bajo
5. **MB:** Muy bajo

2.3.2 Estimar probabilidad de ocurrencia

La probabilidad de ocurrencia se calcula con base en la siguiente tabla:

1) Cualitativa: La probabilidad de ocurrencia se establece acorde a la siguiente tabla:

VALOR	OCURRENCIA	FRECUENCIA
Es probable que se materialice la amenaza a diario	100	Muy frecuente
Es probable que se materialice la amenaza semanalmente	10	Frecuente
Es probable que se materialice la amenaza anualmente	1	Normal
Es probable que se materialice la amenaza cada varios años	1/10	Poco frecuente

Tabla 9. Valoración cualitativa de la frecuencia.

2) Cuantitativo: a partir de los datos históricos que la organización haya acumulado en el tiempo. La frecuencia se considera como numero de ocurrencias de la amenaza en un año.

FRECUENCIA	PROBABILIDAD
Más de 100 al año	Muy frecuente
Entre 10 y 20 al año	Frecuente
Entre 1 y 5 al año	Normal
Menos de 1/10 al año	Poco frecuente

Tabla 11. Matriz para determinación de riesgos.

2.3.3 Identificar controles existentes

Los controles existentes son las medidas con que se cuentan para reducir la exposición a los riesgos: procedimientos, mecanismos, controles tecnológicos, etc. Para identificar los controles existente puede utilizarse como referencia el anexo A del estándar ISO/IEC 27001/2013.

2.3.4 Evaluar controles existentes

Una vez identificados los controles existentes es necesario evaluar su efectividad frente a los riesgos que se pretenden mitigar.Para medir la efectividad de los controles utilizaremos los siguientes criterios:

EVALUACION DEL CONTROL	VALORES				
	NULO	DEFICIENTE	REGULAR	BUENO	EXCELENTE
El control está formalmente establecido.	0%	25%	50%	75%	100%
El control está perfectamente desplegado, configurado ymantenido.	0%	25%	50%	75%	100%
Existen procedimientos claros de uso del control y en caso deincidencias.	0%	25%	50%	75%	100%
Los usuarios están formados y concienciados sobre la aplicacióndel control.	0%	25%	50%	75%	100%
El control es funcional desde el punto de vista teórico yoperacional.	0%	25%	50%	75%	100%

Tabla 12. Criterios para valoración de controles existentes

La eficiencia del control se estima con base en la siguiente tabla:

Efectividad = Promedio de las valoraciones realizadas

SUMA	EFECTIVIDAD DEL CONTROL
Mayor de 89%	EXCELENTE
De 65% y 89%	BUENA
De 40% y 64%	REGULAR
De 15% y 39%	DEFICIENTE
Menor de 15%	NULA

Tabla 13. Valoración de controles

2.1 VALORACIÓN DE RIESGOS

2.4.1 Objetivo

Determinar el nivel o grado de exposición de la organización a los impactos del riesgo, estimando las prioridades para su tratamiento.

2.4.2 Desarrollo de actividades

2.4.3 Estimar riesgo

El riesgo se establece considerando los controles existentes, orientados a prevenir que el incidente se presente.

Controles orientados a prevenir el incidente

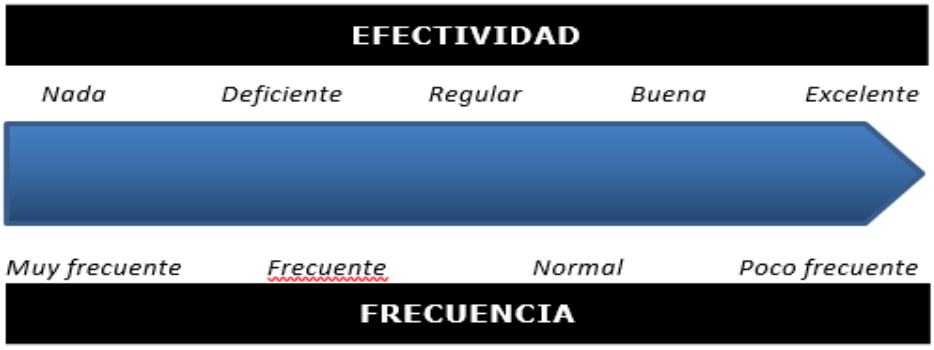


Ilustración 5. Efectividad de control y frecuencia.

En la ilustración No.5 se aprecia como a medida que la efectividad del control aumenta, la frecuencia de ocurrencia de incidentes disminuye. Controles que limitan la degradación de activos:

Ilustración 6. Efectividad de control y degradación.

En la ilustración No 6, se aprecia que la efectividad del control aumenta, la degradación del activo es menor.

Si los controles tienen niveles adecuados de efectividad la degradación de los activos ó la frecuencia de los incidentes debe ser menor a los valores hallados inicialmente.

2.4.4 Priorizar los riesgos sobre los activos

El riesgo nos muestra el grado de exposición frente a las amenazas evaluadas, es posible distinguir entre los riesgos aceptables, tolerables, moderados, importantes o inaceptables, y establecer la prioridad de las acciones requeridas para su tratamiento. Las acciones que se deben ejecutar se harán con base en la siguiente tabla:

Riesgo	Prioridad	Tiempo de ejecución de acciones
Inaceptable	Muy Alta	Inmediata
Importante	Alta	De 0 a 4 meses
Moderado	Media	De 4 a 7 meses
Tolerable	Baja	De 7 a 12 meses
Aceptable	Muy baja	De 12 a 16 meses

Tabla 14. Priorización de riesgos.

2.2 LA GESTIÓN DE RIESGOS EN LOS ACTIVOS

2.5.1 Objetivo

Estructurar los criterios para la toma de decisiones respecto al tratamiento de los riesgos, en esta etapa se establece las guías de acción necesarias para coordinar y administrar los eventos que pueden comprometer la confidencialidad, integridad y disponibilidad de los activos.

2.5.2 Desarrollo de actividades

2.5.3 Toma de decisiones

Si el riesgo se ubica en la Zona de Riesgo Aceptable, permite a la Organización aceptarlo, es decir, el riesgo se encuentra en un nivel que puede asumirse sin necesidad de tomar otras medidas de control.

Si el riesgo se ubica en la Zona de Riesgo Inaceptable, es aconsejable eliminar la actividad que genera el riesgo en la medida que sea posible.

Si el riesgo se sitúa en cualquiera de las otras zonas (riesgo tolerable, moderado o importante) se deben tomar medidas para llevar los Riesgos a la Zona Aceptable, con la implementación de los respectivos controles.

Las medidas dependen del punto en la cual se ubica el riesgo

ZONA	IMPACTO	FRECUENCIA	MEDIDA
Zona de riesgo importante	**MA:** muy alto	Poco frecuente	Prevenir riesgo: Implementar controles frente a impacto.
	MA: muy alto	Normal	Prevenir riesgo: Implementar controles frente a impacto.
	A: alto	Frecuente	Prevenir riesgo: Implementar ó mejorar controles frente a impacto y frecuencia.
	M: medio	Frecuente	Prevenir riesgo: Implementar ó mejorar controles frente a impacto y frecuencia.
	M: medio	Muy frecuente	Prevenir riesgo: Implementar ó mejorar controles frente a impacto y frecuencia.
Zona de riesgo moderado	**A:** alto	Poco frecuente	Compartir riesgos. Prevenir riesgo: Implementar ó mejorar controles frente a impacto.
	A: alto	Normal	Compartir riesgos. Prevenir riesgo: Implementar ó mejorar controles frente a impacto y frecuencia.
	M: medio	Normal	Compartir riesgos. Prevenir riesgo: Implementar ó mejorar controles frente a impacto y frecuencia.
	B: bajo	Frecuente	Realizar análisis costo beneficio para decidir si el riesgo se asume, se previene o se comparte.

ZONA	IMPACTO	FRECUENCIA	MEDIDA
	B: bajo	Muy frecuente	Realizar análisis costo beneficio para decidir si el riesgo se asume, se previene o se comparte.
Zona tolerable del riesgo	**M:** medio	Poco frecuente	Prevenir riesgo: Implementar ó mejorar controles frente a impacto.
	B: bajo	Normal	Realizar análisis costo beneficio parta decidir si el riesgo se asume, se previene o se comparte.
	MB: muy bajo	Frecuente	Realizar análisis costo beneficio parta decidir si el riesgo se asume, se previene o se comparte.
	MB: muy bajo	Muy frecuente	Realizar análisis costo beneficio parta decidir si el riesgo se asume, se previene o se comparte.

Tabla 15. Estimación de los riesgos sobre los activos.

La selección de controles se realizará tomando como referencia el Anexo A del estándar ISO/IEC 27001:2013.

Para seleccionar los controles frente a los riesgos establecidos, deberá realizarse un análisis costo-beneficio para evitar implementación de controles con costos superiores al costo de los riesgos reales.

2.5.4 Plan de tratamiento de riesgos

Una vez seleccionado los controles que serán implementados para mitigación de riesgos es necesario elaborar un plan de acción que garantice un efectivo despliegue de los mismos.

La elaboración del plan de tratamiento de riesgos será responsabilidad del Oficial de Seguridad y la respectiva aprobación de los mismos del Comité de Seguridad

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.

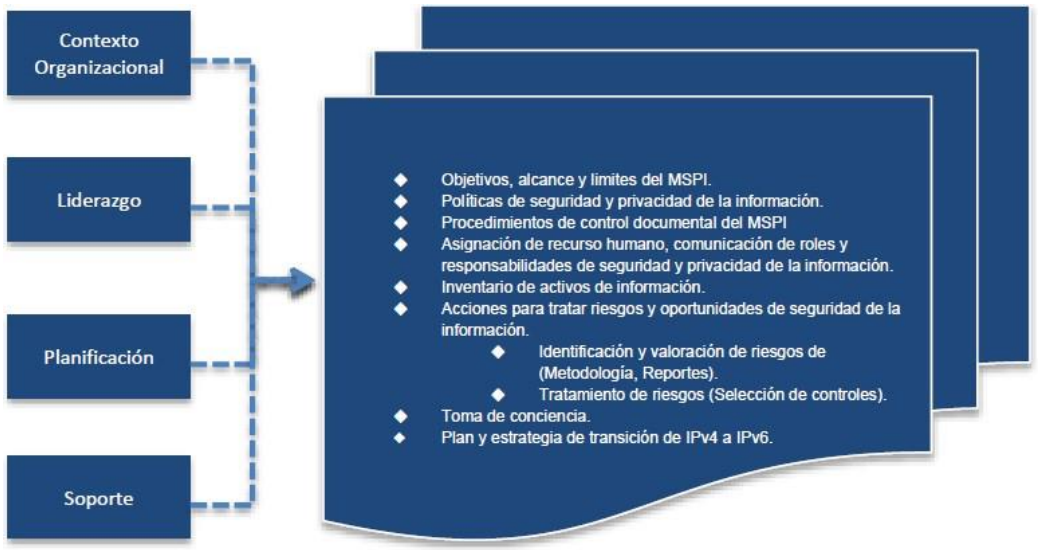


Figura 3. **Fase de planificación modelo de seguridad**

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 quecontendrá 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 sunivel 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

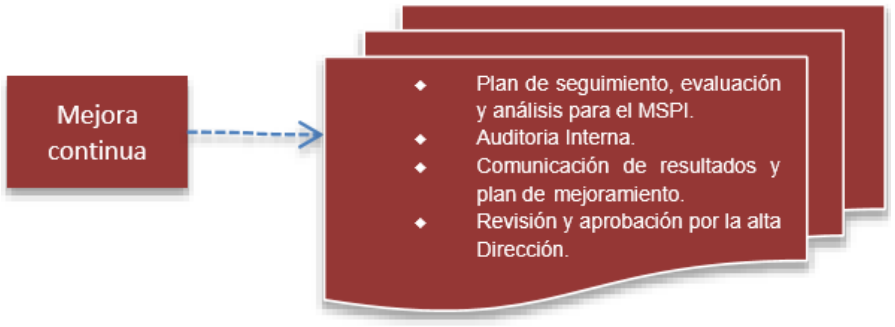


Figura 6. ***Fase Mejora Continua modelo de seguridad***
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

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

gACTIVIDAD	2023											
	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
• **ISO 27005:2018** • **ISO/IEC 31000:2018** • **ISO/27001:2013** • **ISO 22301:2012** • **ISO 27005:2005** • **ISO 31000:2009**	*“norma técnica NTC-ISO/IEC colombiana…”*

Decreto 103 de 2015	*Compendio de políticas aplican para todos los servidores públicos y contratistas de Función Pública que procesan y/o manejan información de la entidad.*
Decreto 1494 de 2015	*Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones*
Decreto 1008 de 2018	*Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.*
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