ALCALDÍA DE TULUÁ

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

AÑO 2022

NOMBRE	VERSIÓN	AUTOR	FECHA
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ALCALDIA MUNICIPAL DE TULUA.	1.0	Departamento de Informática - TIC	DICIEMBRE 2022

INTRODUCCIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, mediante resolución 911 del 26 de marzo de 2018, -"Por la cual se actualiza el Modelo Integrado de Gestión (MIG) del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se deroga la Resolución 3174 de 2014, la Resolución 3021 de 2016 y la Resolución 453 de 2016"-, artículo 9° por el cual se establecen las responsabilidades del Comité MIG, espáticamente en los numerales 7 –"Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información"- y 15 -"Aprobar y hacer seguimiento a la implementación de la Estrategia de Gobierno Digital y Seguridad de la Información en la Entidad y al Plan Estratégico de Tecnologías Información."-. además, el Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

Teniendo en cuenta lo anterior, la Alcaldía Municipal de Tuluá adopta el Plan de seguridad y privacidad de la información en el año 2021.

En atención a lo anterior, la Administración Municipal implementó el SGSI, siguiendo los lineamientos del MSPI de la Estrategia de Gobierno en Línea, a su vez reglamentado a través del Decreto 1078 de 2015 para el sector de tecnologías de la información y comunicaciones y el Decreto 2573 de 2014 por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea.

1 OBJETIVO

Presentar el Plan de Seguridad y Privacidad de la Información, el cual es el documento que dirige la implementación de controles de seguridad según el modelo del Sistema de Gestión de Seguridad de la Información, en adelante SGSI, adoptado por la Administración Municipal; este documento expone las prioridades de implementación de los controles en relación a seguridad de la información enmarcado en el ciclo de mejoramiento continuo PHVA (planear, hacer, verificar y actuar).

2 OBJETIVOS ESPECÍFICOS

1. Comunicar e implementar la estrategia de seguridad de la información.
2. Incrementar el nivel de madurez en la gestión de la seguridad de la información.
3. Implementar y apropiar el Modelo de Seguridad y Privacidad de la Información – MSPI, con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.
4. Hacer uso eficiente y seguro de los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.
5. Asegurar los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.

3 ALCANCE

Aplica a todos los niveles del Departamento de Informática, a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones que compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier archivo de información, independientemente de su ubicación. Así mismo, esta Política aplica a toda la información creada, procesada o utilizada por el Ministerio TIC, sin importar el medio, formato o presentación o lugar en el cual se encuentre

4 CONOCIMIENTO DE LA ENTIDAD

4.1 MISION:

Servir, Construir, Avanzar y consolidar a Tuluá como Municipio moderno, acogedor, innovador, seguro, equitativo, con vocación humana, educado, deportivo, saludable y con oportunidades para todos, de la gente para la gente en paz y feliz, que brinde mejores condiciones y calidad de vida para sus habitantes, partiendo para ello de los principios de democracia, buen gobierno, unidad en torno al bien común, respeto por todos y por todo, cero tolerancia a la corrupción, administración ágil, eficiente, eficaz y transparente e inclusión de todos, que promueva el desarrollo humano integral bajo los pilares del desarrollo social, desarrollo económico, infraestructura y competitividad, transformación del campo y crecimiento verde.

4.2 VISIÓN:

Entre 2020 y 2023 Tuluá desarrollará las condiciones y capacidades para avanzar, consolidarse y posicionarse como Municipio moderno, innovador, seguro, de gente culta, con vocación humana y educada, Municipio fortalecido institucionalmente, equipado con infraestructura estratégica que atraerá la inversión y ratificará al Municipio como eje articulador del desarrollo e intercambio regional del centro, del norte del valle y la región; Tuluá será más bonita, agradable, acogedora, segura, atractiva para vivir, educarse, preparase y trabajar, con oportunidades para el progreso de la gente y para la gente.

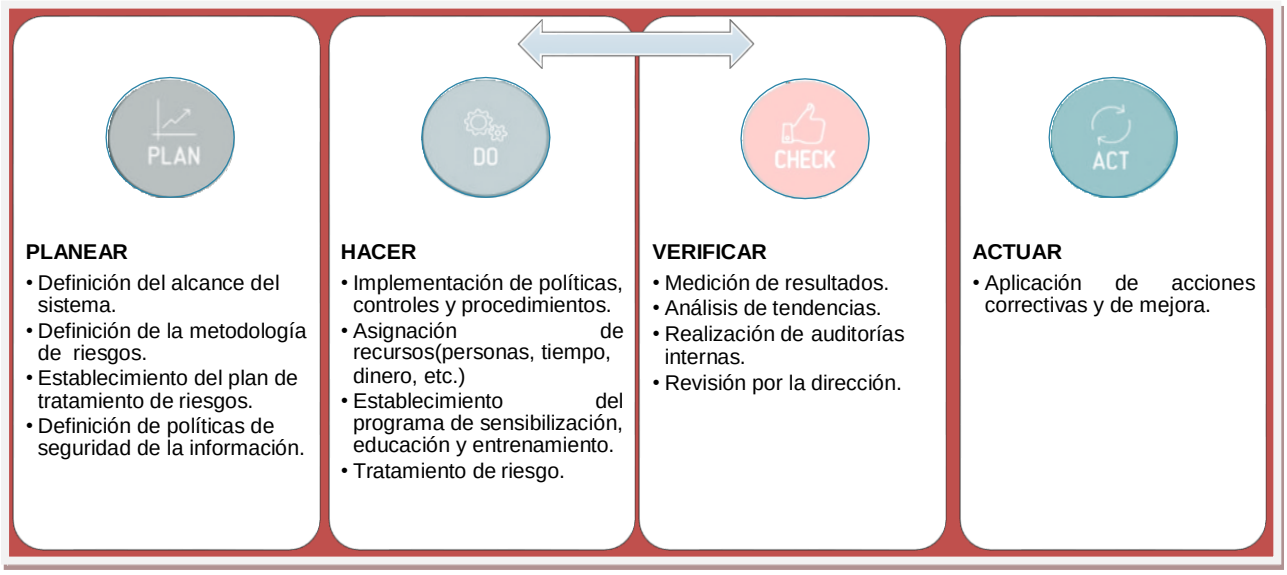
4.3 ESTRUCTURA ORGÁNICA:

5 MODELO SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

siguiendo los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL con el fin de preservar la integridad, confidencialidad, disponibilidad y privacidad de la información mediante la adecuada gestión del riesgo, la aplicación de la normatividad vigente y la implementación de mejores prácticas relacionadas con seguridad de la información.

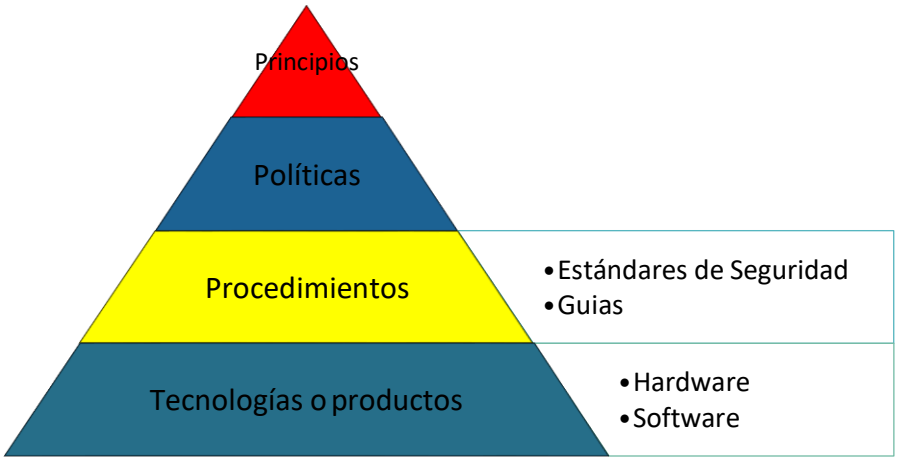
En efecto, el modelo del SGSI de la Administración Municipal se encuentra basado en el ciclo de mejoramiento continuo PHVA (Planear, hacer, actuar y verificar), el cual asegura que el SGSI esté expuesto a revisiones continuas cuando existe un cambio importante en la infraestructura o se requiera mejorar su efectividad dependiendo de las mediciones de parámetros claves de su operación. Se cuenta, entonces, con un ciclo que permite establecer, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI.

A continuación, se listan los componentes de cada una de estas fases del ciclo:



6 DESCRIPCIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN

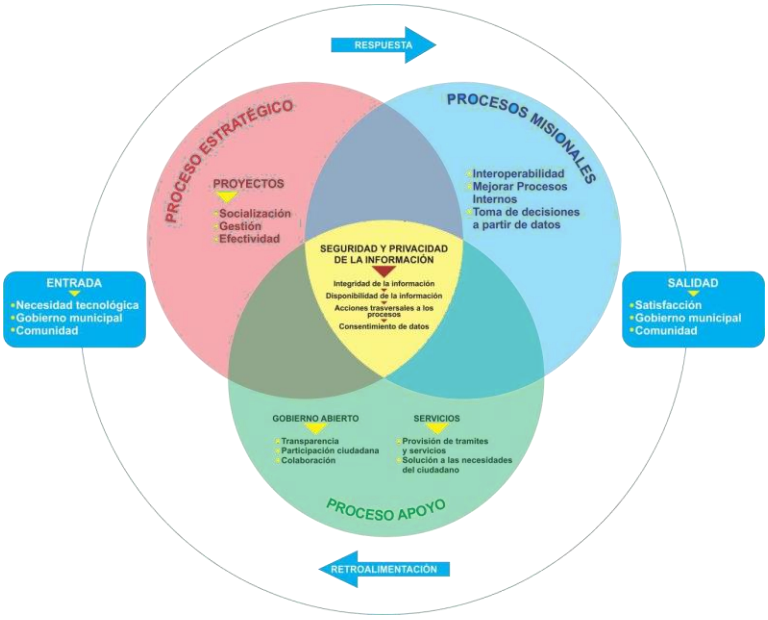
En el ámbito de la Seguridad de la información, los componentes del sistema se ubican en diferentes niveles de acuerdo con su importancia, a continuación, se ilustran dichos componentes:



6.1 ALCANCE DEL SGSI

Teniendo en cuenta el análisis del contexto externo, interno y las partes interesadas, la Administración Municipal define el alcance de SGSI, en términos de las características de la entidad, su ubicación, sus activos y su tecnología, así:

Alcance: *"La Administración Municipal adopta, establece, implementa, opera, verifica y mejora el SGSI para los procesos misionales y los procesos de apoyo que componen el mapa de procesos de la entidad".*



7 MARCO CONCEPTUAL

Para la Administración Municipal, es muy importantes tener claro el Plan de Seguridad y Privacidad de la Información con el fin de apoyar la implementación del SGSI. El plan se apoya en el Plan Estratégico Institucional.

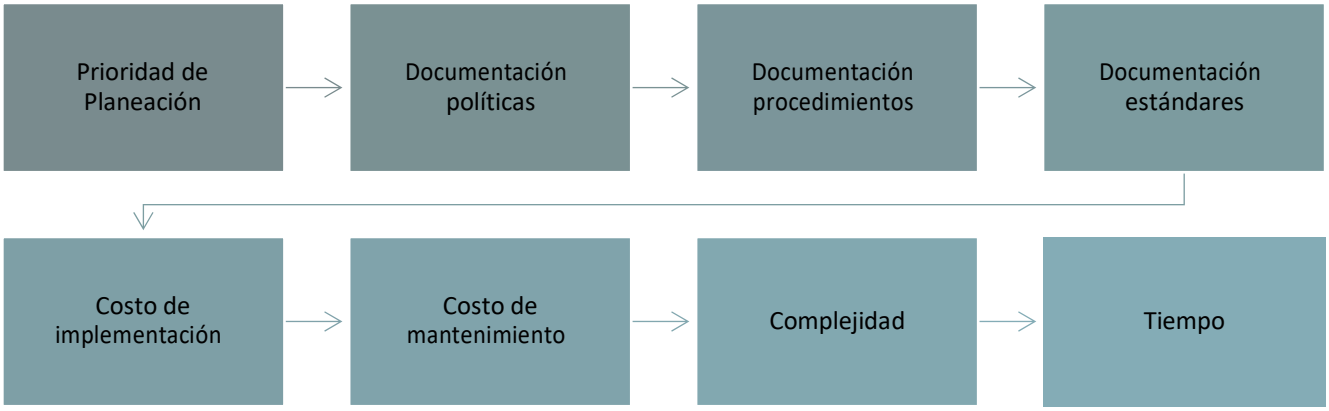
8 METODOLOGÍA UTILIZADA

Para llevar a cabo el desarrollo del Plan de seguridad se tuvo en cuenta la elaboración del Instrumento de evaluación proporcionado por MINTIC.

El cual debe darse continuidad durante el año 2021 para determinar los valores de los diagramas, los cuales quedaron pendientes por evaluar en gran parte por motivos de pandemia COVID – 19.

9 DEFINICIÓN DE LAS VARIABLES PARA EL ANÁLISIS

Para la realización del análisis dentro del Plan de Seguridad y Privacidad de la Información es necesario definir una serie de variables que ayuden a la priorización de los diferentes dominios de la NTC/ISO 27001:2013. Los 14 dominios de la norma están conformados por 114 controles. El Plan de Seguridad y Privacidad de la Información propone una estrategia para la implementación basada en una serie de variables que permiten inferir el orden de implementación de cada uno de los dominios teniendo en cuenta algunos aspectos asociados a cada uno de los controles. En la siguiente figura se presentan la matriz de valoración para cada una de las combinaciones posibles.



- ✓ **Prioridad de Planeación**: Esta variable considera los aspectos relacionados con el dominio desde el punto de vista de las categorías del tipo de control o dominio: administrativo, tecnológico y físico y los aspectos referentes a los niveles de planeación: estratégico, táctico y operativo. Dependiendo de la conjunción de estos dos criterios (nivel de planeación y categorías del tipo del control o dominio).
- ✓ **Documentación política**: El esfuerzo asociado con la documentación de políticas por cada uno de los dominios se mide en esta variable. La cantidad de políticas y normas que hay que desarrollar por dominio es un estimativo que ayuda a estimar su prioridad de implementación. Para ello implementamos el documento Políticas de Seguridad.
- ✓ **Documentación procedimientos:** El esfuerzo requerido por cada dominio en el número de procedimientos requeridos para lograr la preservación de la seguridad de la información es uno de los aspectos considerados con el fin de asignarle una prioridad a la implementación de los diferentes dominios.
- ✓ **Documentación estándares:** El esfuerzo requerido por cada dominio en el número de estándares requeridos para lograr la preservación de la seguridad de la información es uno de los aspectos considerados con el fin de asignarle una prioridad a la implementación de los dominios.
- ✓ **Costo de implementación:** Cada uno de los dominios de la norma dependiendo de la cantidad de herramientas, software, servicios, infraestructura, horas hombre, entre otros aspectos, requerirá de unos esfuerzos financieros diferentes. De tal manera que se puede

recomendar como parte de este Plan, que aquellos dominios con menor costo sean implementados en el menor tiempo posible con el fin de obtener lo que se conoce como ganancias tempranas lo que a larga beneficiará la aceptación de todo lo concerniente a la seguridad de la información por parte de la entidad y mantendrá la motivación en niveles altos durante la fase de implementación del SGSI.

- ✓ **Gasto de mantenimiento:** Todo control asociado a un dominio tiene por su misma naturaleza unos gastos asociados en mantener su efectividad en el transcurso del tiempo. Estos gastos normalmente tienden a ser reiterativos y en algunos casos se requiere de un tercero para que cumpla con la función del mantenimiento.

- ✓ **Complejidad**: La variable complejidad considera las calificaciones requeridas en el recurso humano con el fin de acometer la implementación del dominio o control en cuestión, para ello se consideran los siguientes aspectos:

    - Especialista
    - Ingeniero
    - Técnico
    - Estudiante técnico o profesional
    - Personal no calificado

- ✓ **Tiempo:** La variable tiempo le imprime al dominio unas restricciones importantes en lo referente al tema de cuándo se debe abordar su implementación. Se considera que si un control o dominio toma mucho tiempo para su implementación es recomendable abordarlo posteriormente para que de esta manera podamos implementar muchos más controles que sean de corta duración en su implementación y se aumenta rápidamente el porcentaje de cumplimiento de la norma de seguridad. No obstante, se debe considerar que estos controles de largo tiempo de implementación sean acometidos sin violar los requerimientos de tiempo de todo el proyecto.

INDICADORES DE GESTIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN AÑO 2021

A continuación, se definen una serie de indicadores para medir la gestión[2] y el cumplimiento[3] en el avance de implementación del Nuevo Modelo de Seguridad y Privacidad de la Información en el Municipio de Tuluá, dichos indicadores son:

INDICADOR 02 - CUBRIMIENTO DEL SGSI EN ACTIVOS DE INFORMACIÓN.	
IDENTIFICADOR	SGIN02
DEFINICIÓN	
El indicador permite determinar y hacer seguimiento al cubrimiento que se realiza a nivel de activos **críticos** de información de una entidad y los controles aplicados.	
OBJETIVO	
Hacer un seguimiento a la inclusión de nuevos activos críticos de información y su control, dentro del marco de seguridad y privacidad de la información.	

[2] Indicador de Gestión: Los indicadores de gestión están relacionados con las razones que permiten administrar realmente un proceso o un sistema.
[3] Indicador de Cumplimiento: De cumplimiento están relacionados con las razones que indican el grado de consecución de tareas.

INDICADOR 02 - CUBRIMIENTO DEL SGSI EN ACTIVOS DE INFORMACIÓN.					
TIPO DE INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES			**FORMULA**	**FUENTE DE INFORMACIÓN**	
VSI03: Número de activos críticos de información incluidos en el alcance de implementación del modelo, incluidos en la zona de riesgo inaceptable y la implementación del control no requiere adquisición de elementos de hardware o software.			(VSI03/VSI04)*100	Alcance del SGSI, Inventario de Activos de información, plan de tratamiento, matriz de riesgos	
VSI04: Número de activos críticos de información incluidos en el alcance de implementación del modelo; activos incluidos en la zona de riesgo inaceptable.				Inventario de Activos de información, nuevos	
METAS					
MÍNIMA	75-80%	**SATISFACTORIA**	80-90%	**SOBRESALIENTE**	100%
OBSERVACIONES					
El indicador de cada proceso debe ser recolectado y promediado para construir un indicador que refleje el estado a nivel empresa. El terminó “incluir un activo” debe ser entendido como realizar la correcta clasificación del activo, tratamiento, evaluación de riesgos sobre el mismo y determinación de controles para minimizar el riesgo calculado. Para este indicador, solo se tienen en cuenta los controles que no implican adquisición de hardware o software.					

INDICADOR – VERIFICACIÓN DEL CONTROL DE ACCESO			
IDENTIFICADOR	SGIN07		
DEFINICIÓN			
Grado control de acceso en la entidad.			
OBJETIVO			
INDICADOR – VERIFICACIÓN DEL CONTROL DE ACCESO			
Busca identificar la existencia de lineamientos, normas o estándares en cuanto al control de acceso en la entidad.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
VSI14: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar el acceso de los usuarios a sus servicios de Gobierno en línea y a sus redes de comunicaciones?		VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Usuarios Internos.
VSI15: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar el uso y el acceso a los sistemas de información, las aplicaciones y los depósitos de información con las que cuenta la entidad? VSI16: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar las terminales móviles y accesos remotos a los recursos de la entidad?			Usuarios Internos.
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

<table>
<tr><th colspan="4">INDICADOR – IMPLEMENTACIÓN DE LOS PROCESOS DE REGISTRO Y AUDITORÍA</th></tr>
<tr><td colspan="2">DEFINICIÓN</td><td colspan="2">SGIN10</td></tr>
<tr><td colspan="4">Grado de implementación de los mecanismos encaminados a la detección de anomalías e irregularidades.</td></tr>
<tr><td colspan="4">OBJETIVO</td></tr>
<tr><td colspan="4">Busca medir el nivel de mecanismos encaminados a la detección de anomalías e irregularidades</td></tr>
<tr><td colspan="4">TIPO INDICADOR</td></tr>
<tr><td colspan="4">Indicador de Cumplimiento</td></tr>
<tr><td colspan="4">DESCRIPCIÓN DE VARIABLES</td></tr>
<tr><td colspan="2">VSI21: VAPRSG005: ¿La entidad ha implementado mecanismos para detectar periódicamente vulnerabilidades de seguridad en el funcionamiento de:

a) su infraestructura,

b) redes,

c) sistemas de información,

d) aplicaciones y/o

e) uso de los servicios?</td><td>FORMULA</td><td colspan="2">FUENTE DE INFORMACIÓN</td></tr>
<tr><td colspan="2"></td><td rowspan="2">VSI0X = 1 (SÍ se evidencia)

VSIOX = 0 (NO se evidencia)</td><td colspan="2">Usuarios Internos, No Conformidades</td></tr>
<tr><td colspan="2">METAS</td><td colspan="2"></td></tr>
<tr><td colspan="4">CUMPLE</td></tr>
<tr><td>OBSERVACIONES</td><td>1</td><td>NO CUMPLE</td><td>0</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4"></td></tr>
</table>

INDICADOR – POLÍTICAS DE PRIVACIDAD Y CONFIDENCIALIDAD			
IDENTIFICADOR	SGIN11		
DEFINICIÓN			
Grado de implementación de políticas privacidad y confidencialidad de la entidad.			
OBJETIVO			
Busca identificar el nivel de implementación de políticas privacidad y confidencialidad de la entidad.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
VSI22: ¿La entidad ha implementado lineamientos, normas y/o estándares para proteger la información personal y privada de los ciudadanos que utilicen sus servicios?		VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Usuarios Internos.
VSI23: ¿La entidad ha implementado lineamientos, normas y/o estándares para proteger la información privada de las entidades que utilicen sus servicios?			Usuarios Internos.
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

INDICADOR – VERIFICACIÓN DE LAS POLÍTICAS DE INTEGRIDAD DE LA INFORMACIÓN			
IDENTIFICADOR	SGIN12		
DEFINICIÓN			
Grado de implementación de mecanismos para la integridad de la información de la entidad.			
OBJETIVO			
Busca identificar el nivel de implementación de políticas privacidad y confidencialidad de la entidad.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
VSI24: ¿La entidad ha implementado lineamientos contra modificación o pérdida accidental de información?		VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Usuarios Internos.
VSI25: ¿La entidad ha implementado lineamientos, normas y/o estándares para recuperar información en caso de modificación o pérdida intencional o accidental?			Usuarios Internos.
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

INDICADOR – VERIFICACIÓN DE LAS POLÍTICAS DE INTEGRIDAD DE LA INFORMACIÓN

INDICADOR – ATAQUES INFORMÁTICOS A LA ENTIDAD.			
IDENTIFICADOR	SGIN14		
DEFINICIÓN			
Porcentaje de ataques informáticos recibidos en la entidad que impidieron la prestación de alguno de sus servicios.			
OBJETIVO			
Busca conocer el número de ataques informáticos que recibe la entidad			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
VSI28: ¿Cuántos ataques informáticos recibió la entidad en el último año?		VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Herramientas de Monitoreo/Usuarios Internos.
VSI29: ¿Cuántos ataques recibió la entidad en el último año que impidieron la prestación de algunos de los servicios que la entidad ofrece a los ciudadanos y empresas?			Herramientas de Monitoreo/Usuarios Internos.
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

INDICADOR – PORCENTAJE DE IMPLEMENTACIÓN DE CONTROLES					
IDENTIFICADOR	SGIN16				
DEFINICIÓN					
grado de avance en la implementación de controles de seguridad					
OBJETIVO					
Busca identificar el grado de avance en la implementación de controles de seguridad					
TIPO INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES		**FORMULA**		**FUENTE DE INFORMACIÓN**	
VSI32: Número de Controles Implementados		(VSI032/VSI33)*100		Plan de tratamiento de riesgos	
VSI33: Número de Controles que se planearon implementar				Plan de Tratamiento de riesgos.	
METAS					
MÍNIMA	75-80%	**SATISFACTORIA**	80- 90%	**SOBRESALIENTE**	100%

10 RECOMENDACIONES PARA LA IMPLEMENTACIÓN

10.1 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

La política determina los objetivos de seguridad, lo que se quiere hacer en temas de seguridad, se basa en los análisis de riesgos y en los resultados de la gestión de incidentes de seguridad. Las políticas siempre responden a la pregunta ¿Qué voy a hacer? y en ese sentido hay que darle seguimiento a la política que tiene implementada el Departamento TIC. La política define los objetivos a alcanzar y no cómo se va a implementar, es un error incluir en una política algo operativo por ej. *"la contraseña debe tener 8 caracteres alfanuméricos, al menos una mayúscula y números"*, esto no es una política, sino la forma como cumpliría el objetivo, responde a cómo lo voy a hacer y no a ¿qué voy a hacer? una política correcta podría ser algo como "*Todos los usuarios que acceden a los sistemas de información de la Administración Municipal deben disponer de un medio de identificación y el acceso debe ser controlado a través de una autenticación personal."*. Lo anterior, lo que se refería a las características de las contraseñas, es lo que se conoce como norma, la cual, no es otra cosa, que enunciados de obligatorio cumplimiento, que responden a la forma en que se cumplirá una política.

Como se mencionó anteriormente, la política determina los objetivos de seguridad, y la forma de cumplir con estos objetivos en el modelo de seguridad es a través de normas y procedimientos. Las normas y procedimientos siempre deben responder a una política, por lo tanto en cada norma o procedimiento debe especificarse a qué política responde, si no se puede determinar a qué política corresponde debe razonarse, o que el procedimiento o norma no es necesario, o que el documento de políticas está incompleto. El documento de políticas SIEMPRE debe ser conocido y firmado por la alta gerencia.

10.2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información realmente es una cultura, en la cual se deben involucrar todos los colaboradores, tanto servidores públicos, usuarios y contratistas para que contribuyan a crear un clima de seguridad tanto al interior como al exterior de la entidad. La organización de seguridad debe estar distribuida por toda la entidad en diferentes funciones con responsabilidades relacionadas con la seguridad de la información.

Se deben utilizar roles para la realización de las actividades que los colaboradores realizan en cada procedimiento, y posteriormente asociar a los cargos, los roles previamente definidos, que contienen las actividades y las funciones de cada rol.

A la hora de realizar esta asignación de roles a cargos se debe:

- ✓ Realizar una matriz de trabajo para cada procedimiento, de tal forma que puedan ser controladas las actividades por diferentes personas.
- ✓ Realizar una matriz de segregación de funciones entre los roles con el fin de asegurarse que para un cargo no se presenten conflictos de intereses en temas de

seguridad de la información.

Dentro del modelo de seguridad, la organización de seguridad debe tener al menos:

- Un **comité de seguridad de la información** en el cual se debe integrar la alta gerencia mediante actas. Este comité es el órgano máximo del modelo de seguridad. Sus funciones principales, entre otras, podrían ser:

    - Definir los lineamientos y estrategias de Seguridad de la información en función de los objetivos del negocio.
    - Aprobar el modelo de seguridad de la entidad (políticas, normas, procedimientos, etc.).
    - Aprobar el Plan de seguridad y Privacidad de la Información, así como los resultados de su implementación.

- **Líder de seguridad de la Información de la Entidad.** Es el encargado de coordinar todo el modelo de seguridad. Debería estar dedicado tiempo completo a temas de seguridad y debe velar por el mejoramiento continuo del modelo de seguridad. Debe establecer contacto con las autoridades pertinentes, así como con grupos de interés en temas de seguridad.
- **Analista de seguridad de la información.** Son funcionarios dedicados tiempo completo a temas de seguridad de la información y que realizan labores operativas del modelo de seguridad. Son dirigidos por el líder de seguridad de la información. En lo posible, la entidad debe contar como mínimo con dos funcionarios para este rol.

Este dominio también contempla el aseguramiento de dispositivos móviles y el teletrabajo. Con referencia a este tema se sugieren las siguientes recomendaciones:

- Contar con un inventario con el registro de todos los equipos de la Administración Municipal, en el cual se registre al menos: la persona responsable del equipo, los activos de información que maneja el equipo y los lugares a los que tiene acceso.
- Contar con estándares de seguridad para equipos que pueden contener entre otras, cifrado de disco duro, restricciones de instalación de software,

actualización de parches de seguridad, restricción a conexiones de acceso de información, protecciones contra software malicioso, deshabilitar borrado remoto, copias de respaldo, entre otros.

- Contar con un documento formal de normas para uso de equipos, donde se den recomendaciones sobre el uso de los equipos y los cuidados de seguridad que se deben tener.

10.3 SEGURIDAD DEL RECURSO HUMANO

Con relación a la seguridad de los recursos humanos se debe tener en cuenta el ciclo de vida del recurso humano, esto es, antes, durante y después de su contratación. En este sentido se darán recomendaciones en estas tres etapas.

- **Antes de la contratación:**

Contar con un procedimiento de selección de personal siguiendo los parámetros de contratación que, de acuerdo con las leyes y reglamentos de ética pertinentes, incluya:

- Verificación de referencias
- Verificación de la hoja de vida completa
- Verificación de la identidad del aspirante
- Verificación de competencia
- Pruebas psicotécnicas
- Verificar en términos generales que sea una persona confiable.

- **Durante el periodo de contratación: (de este deben hacerse cargo los funcionarios de planta).**
    - Todos los colaboradores y contratistas que accedan a información reservada o sensible deben firmar un acuerdo de confidencialidad y no divulgación ANTES de tener acceso a dicha información por cualquier medio.
    - Todos los colaboradores deben firmar una cesión de derechos de propiedad intelectual a favor de la entidad sobre los desarrollos que se realicen fruto de su trabajo en la entidad.
    - Todos los colaboradores deben seguir fielmente las normas sobre el manejo de cada tipo de información de acuerdo con lo definido en la clasificación de activos de información.
    - Contar con un proceso disciplinario sí se incumple cualquiera de las normas de seguridad establecidas.
    - Contar con un proceso disciplinario frente a la responsabilidad en incidentes de seguridad de la información en los que se demuestre la participación de algún colaborador.
    - Brindar capacitaciones del modelo de seguridad aprobado, así como capacitaciones periódicas en temas de seguridad con el fin de tomar conciencia sobre la seguridad de la información pertinente a sus roles, y lograr crear una cultura de seguridad al interior y exterior de la entidad.
    - Contar con un canal anónimo mediante el cual los colaboradores puedan reportar posibles incidentes de seguridad de la información.

Se debe crear un programa de capacitaciones continuas en seguridad que deberán cubrir como mínimo los siguientes aspectos

- Concientización sobre riesgos de seguridad.
- Conocimiento del modelo de seguridad.
- Conocimiento de las normas y procedimientos de seguridad.
- Puntos de contacto para información de problemas de seguridad.
- Mecanismos para el reporte de incidentes de seguridad de la información.
- Tips prácticos de seguridad orientado a las labores que realiza cada colaborador según sus funciones.

- **Al terminar la contratación:**

Dentro del procedimiento de terminación de contrato se debe incluir: backup de la información que el colaborador manejaba, eliminación de todos los usuarios y contraseñas del colaborador, eliminación de los accesos remotos de teletrabajo a los que tenía acceso el colaborador.

El área de seguridad de la información debe dar un visto bueno, o un paz y salvo después de analizar que los activos de información permanezcan en la entidad. Este paz y salvo debe ser requisito para completar el proceso de desvinculación.

10.4 GESTIÓN DE ACTIVOS

Este dominio pretende identificar los activos de información de la entidad, clasificarlos, asignarles responsables a dichos activos y brindarles un tratamiento apropiado de acuerdo a su clasificación.

Las recomendaciones en este punto son:

- Realizar un inventario de todos los activos de información, para este fin normalmente se realiza una búsqueda de los activos de información en los procesos y procedimientos, buscando el flujo de información en los mismos.
- Incluir en el inventario, el tipo de activo (físico o digital), ubicación, activos de soporte, redes, medios, servidores o servicios en las que se encuentra, proceso al que pertenece, entre otros.
- Asignar a cada activo de información un dueño. El dueño del activo de información es el responsable del activo de información y velará por salvaguardar dicho activo y hacer cumplir el tratamiento de seguridad del mismo de acuerdo con su clasificación. Se considera a los activos de información como cualquier otro activo, con un valor financiero y estratégico.
- Realizar una clasificación de los activos de información teniendo en cuenta criterios de disponibilidad, integridad y confidencialidad de dicha información.
- Asignar un tratamiento de seguridad detallado para cada nivel de la clasificación de los activos de información, definiendo normas de uso, etiquetado, y controles de seguridad para cada nivel de clasificación.

Cuando se terminen los vínculos contractuales con la entidad se debe devolver todos los activos de información a los que el colaborador tuvo acceso.

Con respecto a la gestión de medios removibles, se debe:

- Inicialmente bloquear todos los accesos a medios removibles en todos los equipos de la entidad (bloqueo de USB)
- Habilitar los puertos USB, sólo con una justificación escrita y debe ser autorizada por el área de seguridad. Sólo se deberá habilitar el uso de medios removibles, si hay una razón de negocio para hacerlo.
- Se deben redactar normas para el uso de dispositivos removibles
- Se debe tener registro de la información en medios removibles
- Sí la información ya no se requiere tener en dispositivos removibles o cuando el colaborador se retire de la entidad, debe realizarse un borrado seguro del medio removible.
- Sí la confidencialidad o integridad de la información contenida en un medio removible se considera importante, debería utilizar mecanismos criptográficos apropiados para cada medio.
- La disposición final para los medios removibles debe realizarse en forma segura, por ejemplo, incineración o borrado seguro.

10.5 CONTROL DE ACCESO

El objetivo del dominio de control de acceso consiste en limitar el acceso a la información y a las instalaciones con el fin de salvaguardar los activos de información.

- Se debe realizar unas políticas de control de acceso, con sus respectivas normas y procedimientos que las implementen. Las recomendaciones para esta política son:
    - Tener en cuenta para este fin la clasificación de la información, la legislación pertinente de acuerdo con las leyes de protección de datos.
    - Implementar un procedimiento de gestión de derechos de acceso a los

diferentes tipos de activos de información en los que se involucre a los dueños de los activos de información.

- El criterio fundamental a la hora de definir la política de control de acceso debería ser: “Permitir sólo lo que necesita conocer para realizar sus funciones, de lo contrario no se permite”.

- Se debe realizar unas políticas de control de acceso a redes y servicios de red, con sus respectivas normas y procedimientos que las implementen. Las recomendaciones al respecto son:

  - El acceso a redes o servicios de red debe justificarse en función de los activos a los que se necesita acceder, en la clasificación de los activos puede encontrar en qué redes o a que servicios se le debe permitir acceso para acceder al activo de información.

- Se debe incluir procedimientos para monitorear las redes, tráfico y quién tiene acceso de acuerdo con la política, y en caso de accesos no autorizados, considerarlos como un incidente de seguridad e iniciar inmediatamente una investigación de seguridad.
- Se debe implementar un procedimiento de gestión de acceso a usuarios. Este procedimiento incluye la creación, modificación y eliminación de usuarios. Generalmente está asociado con el proceso de contratación y desvinculación. El procedimiento debe tener en cuenta la autorización al acceso de activos de información, redes y servicios, y estas autorizaciones deben ser avaladas por el dueño del activo de información y por el área de seguridad de la información como mínimo.
- Se debe revisar periódicamente todos los accesos a los activos de información, redes y servicios. En estas revisiones identificar y eliminar o deshabilitar permisos redundantes y obsoletos de acuerdo con las solicitudes de acceso.
- Se debe tener especial cuidado con usuarios con altos privilegios.
- Se debe habilitar logs de acceso a los sitios restringidos.
- Se debe realizar auditoría periódica a los permisos de acceso
- A nivel de aplicativos, durante su desarrollo, desde la etapa de diseño, se debe tener en cuenta:

- La posibilidad de restringir el acceso a la información de la aplicación, para esto utilizar roles, permitir auditar el acceso a información sensible y a operaciones sensibles dentro del aplicativo, entre otras.
- Utilizar técnicas de autenticación adecuadas para corroborar la identidad de un usuario.
- Durante el log-on se debe proteger de intentos de ingreso por fuerza bruta, evitar mensajes de ayuda en el log-on, utilizar contraseña protegida (que no se vea la contraseña al momento de ingresarla), llevar registro de intentos de log-on (exitosos y fallidos). No transmitir las contraseñas en texto plano.
- Se debe cerrar las sesiones por inactividad.

10.6 CRIPTOGRAFÍA

El objetivo de este dominio es asegurar la confidencialidad mediante el uso de métodos apropiados de criptografía. Los sistemas centralizados de gestión de llaves garantizan la seguridad de las diferentes llaves utilizadas por los sistemas de cifrado.

Los proyectos recomendados para este dominio son:

✓ SEGURIDAD FÍSICA Y DEL ENTORNO:

La seguridad no es una tecnología, ni un producto, es un proceso que se apoya en la tecnología para lograr sus objetivos a lo largo de toda la entidad. La seguridad debe ser un enfoque sistémico realizado por profesionales en la materia, que propongan una serie de actividades, procesos y productos para que todos funcionando de manera sincronizada ejerzan un control, factores disuasivos, e información; que en su conjunto garanticen que la entidad pueda lograr sus objetivos de manera oportuna y productiva.

La seguridad física en Colombia es y ha sido un aspecto muy importante de la forma

como las empresas protegen sus activos económicos. Se requiere contar con una metodología que permite evaluar qué tan efectivos son los controles existentes en la infraestructura de la Entidad con el fin de actuar como factor disuasivo y control, contra eventos que pongan en peligro la disponibilidad, confidencialidad e integridad de la información.

Es importante considerar que factores como el control de variables ambientales, tecnologías de control de acceso, y sistemas de CCTV, permiten implementar los controles. Estos controles deben ser el resultado del análisis de riesgo, en donde se determinan las prioridades de cada uno de los elementos anteriormente mencionados.

Espacios de mejora o posibles proyectos (mejora de controles de acceso y protección contra amenazas naturales)

1. Centros de Procesamiento normales o de emergencia
2. Áreas con servidores, ya sean de procesamiento o dispositivos de comunicación
3. Áreas donde se encuentren concentrados dispositivos de información
4. Áreas donde se almacenen y guarden elementos de respaldo datos (CD, Discos
5. Duros, Cintas etc.)
6. Áreas donde se deposite salidas de impresoras.

10.7 SEGURIDAD EN LAS OPERACIONES

El objetivo de este dominio consiste en asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información. Para ello, lo divide en siete grandes subdominios que se tratarán individualmente:

- ✓ PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES:

Para este subdominio se debe:

- Tener procedimientos documentados de cada uno de los elementos de procesamiento de información, como servicios, aplicativos, dispositivos de red y de infraestructura. La documentación por cada elemento debería incluir como mínimo:
    - Instalación y configuración de los sistemas

- Procedimientos de encendido y apagado
- Procedimientos de respaldo tanto de los datos como de la configuración

- Contar con un procedimiento de gestión de la capacidad. El principio fundamental consiste en monitorear todos los recursos de procesamiento y comunicación, tales como ancho de banda de los canales, memoria, capacidad de almacenamiento, capacidad de cálculo, entre otros, y alertar cuándo lleguen a valores críticos con el fin de gestionar la capacidad de cómputo, bien sea optimizando o adquiriendo más capacidad.
    - Contar con separación de ambientes, la norma se refiere a que el ambiente de desarrollo debe ser diferente al ambiente de producción. Cuando se refiere a ambientes, lo ideal sería que fuesen ambientes totalmente independientes. En lo posible, se debe procurar cinco ambientes como se describen a continuación:
        - **Terceros**: cuando se desarrolla software por terceros y es necesario que tengan acceso a los sistemas de la entidad, es recomendable construir un ambiente independiente para el proveedor que no interfiera con la entidad ni afecte la seguridad de la misma. La información con la que se realiza estos desarrollos debe ser información de prueba, nunca con datos reales.
        - **Desarrollo**: El ambiente de desarrollo es un ambiente diseñado para este fin no debe tener acceso directo a los sistemas de producción. Debería brindarle a los desarrolladores una infraestructura lo más similar posible a la que se tiene para producción. La información con la que se realiza estos desarrollos debe ser información de prueba, nunca con datos reales.
        - **Pruebas y Calidad de Software**: Es un ambiente destinado para todas las pruebas de software: funcionales, no funcionales y pruebas de seguridad. Debería tener una infraestructura lo más similar posible a la que se tiene para producción. La información con la que se realiza estos desarrollos debe ser información de prueba, nunca con datos reales.

- **Producción**: Es el ambiente productivo, donde se realizan las operaciones reales de la entidad.
- **Contingencia**: Es el ambiente de respaldo que se analiza en detalle en la gestión de continuidad, debe ser lo suficientemente robusto para soportar los servicios mínimos requeridos por la entidad.

10.8 REGISTRO Y SEGUIMIENTO

El objetivo de este subdominio es dejar rastro de los eventos y evidencia de todas las operaciones relevantes con el fin de que sirvan de apoyo en una investigación de seguridad en un momento dado. Se debe tener en cuenta para estos registros que contengan entre otros la siguiente información:

- Identificación de usuarios;
- Actividades del sistema;
- Fechas, horas y detalles de los eventos clave, por ejemplo, entrada y salida;
- Identidad del dispositivo o ubicación, si es posible, e identificador del sistema;
- Registros de intentos de acceso al sistema exitosos y rechazados;
- Registros de datos exitosos y rechazados y otros intentos de acceso a recursos;
- Cambios a la configuración del sistema;
- Uso de privilegios;
- Uso de utilidades y aplicaciones del sistema;
- Archivos a los que se tuvo acceso, y el tipo de acceso;

- Direcciones y protocolos de red;
- Alarmas accionadas por el sistema de control de acceso;
- Activación y desactivación de los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusión;
- Registros de las transacciones ejecutadas por los usuarios en las aplicaciones.

10.9 SEGURIDAD EN LAS COMUNICACIONES

La transferencia de información está expuesta a múltiples riesgos, por ello la entidad debe implementar medidas preventivas para evitar su divulgación o modificación. Para lograr esto la Administración Municipal debe:

Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte y mantener la seguridad de la información transferida dentro de la entidad y con cualquier entidad externa.

10.10 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

La seguridad en los procesos de desarrollo de software debe estar a lo largo de cada parte del ciclo de desarrollo de software, las recomendaciones por cada parte son:

Análisis de Requerimientos

- Definir claramente con el usuario final el alcance de los requerimientos.
- Determinar la confidencialidad de la información que se maneja
- Definir el control de autenticación requerido
- Definir los roles y los privilegios de cada rol

Diseño

- Acceso a componentes y administración del sistema
- Logs para auditoría
- Gestión de sesiones
- Datos históricos
- Manejo apropiado de errores
- Segregación de funciones

- Defina adecuadamente la administración de identidades
    - Exija el uso de contraseñas seguras
    - En el caso de que se produzca un error en la autenticación, devuelva la mínima información posible
- Compruebe siempre la validez de los datos de entrada
    - Suponga que todos los datos especificados por los usuarios tienen mala intención
    - Compruebe la validez del tipo, longitud e intervalo de los datos
- Administración de la configuración y las sesiones
- Datos confidenciales y criptografía
- Auditoría y registro, siempre dejar registro de las actividades sensibles del aplicativo, (log- in y log-out, Tiempo de sesión, accesos a la base de datos)

Codificación

- Aseguramiento de los ambientes de desarrollo
- Mantener documentación técnica
- Seguridad en las interfaces de comunicación
- Buenas prácticas de codificación:
    - Validación de entradas
    - Codificación de las salidas
    - Estilo de programación limpio
    - Código autodocumentado
    - Control de código fuente (log de cambios)
    - Buena utilización de recursos (memoria, acceso a base de datos)
    - Estandarización y reutilización de código

Pruebas

- Controles de calidad en controles de seguridad
- Inspección de código por fases
- Comprobación de gestión de configuraciones
- Realizar pruebas de caja blanca y caja negra (owasp top 10)

Instalación, actualización y parches

- Tener en cuenta control de cambios

10.11 RELACIONES CON LOS PROVEEDORES

Los proveedores por su naturaleza son una de las fuentes externas de riesgos, pero a su vez son importantes para el cumplimiento de la misión y la visión de la entidad, por esta razón se deben implementar controles para: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores y mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con proveedores.

Las auditorías nos ayudan a determinar el nivel de cumplimiento de los proveedores con respecto a la seguridad de la información:

10.12 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Construir un proceso consistente para gestionar los incidentes de seguridad de la información, el cual debe contener como mínimo:

- Reporte de incidente de seguridad de la información
- Investigación de incidente de seguridad de la información
- Adecuado control de cadena de custodia para gestión de evidencias.

La adecuada gestión de los incidentes de seguridad de la información permite proteger los tres pilares de la seguridad: la confidencialidad, la integridad y la disponibilidad de la información. La implementación de estos controles permite asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

10.13 CUMPLIMIENTO

Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad es importante para no incurrir en demandas, multas u otra clase de afectación a la imagen o a las finanzas de la entidad.

Definir procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados, en el marco de la Ley 719 de 2001.

Establecer una política de privacidad y protección de la información de datos personales, en el marco de la Ley 1581 de 2012 y mantener una capacitación continua sobre estas leyes con expertos en el tema.

Adicionalmente, como parte del ciclo de mejoramiento continuo del SGSI, la entidad debe garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos organizacionales.

10.14 DEFINICIONES

- **Activo**: En cuanto a la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Contratistas**: Entenderemos por contratista aquella persona natural o jurídica que ha celebrado un contrato de prestación de servicios o productos con una entidad.
- **Control**: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Guía**: documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de información.
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Norma**: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.
- **Parte interesada**: (Stakeholder) Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Política del SGSI:** Manifestación expresa de apoyo y compromiso de la alta dirección con respecto a la seguridad de la información.
- **Política**: Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la entidad.
- **Privacidad de datos:** La privacidad de datos, también llamada protección de datos, es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una

organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros

- **Procedimiento**: Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Rol:** Papel, función que alguien o algo desempeña.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).