Diseño de un plan de seguridad informática para el sistema de información de la Alcaldía Municipal de Támesis en base a la política de Gobierno Digital.

Autor

Andres Mauricio Román Toro

Para optar al título de Ingeniero de Telecomunicaciones otorgado por UdeA

Tutor
Ana María Cárdenas Soto, PhD en Telecomunicaciones

Universidad de Antioquia

Facultad de Ingeniería

Pregrado

Medellín - Colombia

2022

Cita	(Andrés Mauricio Román Toro, 2022)
Referencia **Estilo APA 7 (2020)**	Andrés Mauricio Román Toro (2022). *Diseño de un plan de seguridad informática para el sistema de información de la Alcaldía Municipal de Támesis en base a la política de Gobierno Digital.* [Semestre de Industria]. Universidad de Antioquia, Medellín – Colombia.

Tabla de Contenido

Índice de Tablas

Índice de Gráficos

1. Definiciones

Gobierno Digital: Desde sus inicios, la Estrategia Gobierno en Línea centró sus esfuerzos en introducir las TIC en los procesos y procedimientos de las entidades del Estado, con el objetivo de mejorarlos, automatizarlos y volverlos más eficientes, para mejorar la gestión pública y la relación del Estado con los ciudadanos. Bajo este enfoque, desde el Decreto 1151 de 2008 se estableció como objetivo de la Estrategia Gobierno en Línea "Contribuir con la construcción de un Estado más eficiente, más transparente y participativo, y que preste mejores servicios a los ciudadanos y a las empresas, a través del aprovechamiento de las Tecnologías de la Información y la Comunicación". La "Estrategia de Gobierno en Línea", que evoluciona a "Política de Gobierno Digital", es la política pública liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, que tiene como objetivo "Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital" [1].

MSPI: El Modelo de Seguridad y Privacidad de la Información - MSPI, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital, para que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.[2]

Norma ISO 27001: El amplio uso de las tecnologías de información en los negocios hace que cada vez sea más fácil la expansión de éstos. La comunicación con clientes que se encuentran en una ciudad o país diferente al de ubicación de la empresa, la posibilidad de realizar transacciones comerciales vía web y en general, la facilidad del uso de la tecnología y la globalización de la información para todas las personas ha contribuido a que las organizaciones crezcan cada vez más rápido. Sin embargo, toda esta cercanía y facilidad de uso de la tecnología ha generado ciertos problemas a las organizaciones, que día tras día son más vulnerables a las amenazas que se presentan en el medio, las cuales pueden llegar a convertirse en un verdadero riesgo para la organización afectando el correcto funcionamiento de las actividades del negocio. Para contrarrestar dichas amenazas, las organizaciones deben generar un plan de acción frente a éstas. Este plan de acción es conocido como Sistema de Gestión de Seguridad de la Información (SGSI) y contiene los lineamientos que deben seguirse en la organización, los responsables y la documentación necesaria para garantizar que el SGSI sea aplicado y genere una retroalimentación.[3]

Seguridad de la información: Se puede definir a la seguridad informática o seguridad de la información de la siguiente manera.

> *La seguridad informática es la disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a lo que está expuesta.*

Muchos investigadores y autores especializados en el tema de la seguridad informática por lo común se centran solo entre características de la información mencionada; no obstante, de acuerdo con el marco de gestión y de negocio global para el gobierno y la gestión de las tecnologías informáticas de la empresa (COBIT), las características que debe poseer la información son: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, apego a los estándares y confidencialidad.[4]

Hardening: el endurecimiento informático, es el término que se le da al proceso de reducción de vulnerabilidades en el sistema. Esto se consigue, estableciendo unas medidas de seguridad con el objetivo de estar preparados ante un ataque informático, por ejemplo, sería el del cerrado de puertos que no son utilizados ni necesarios para nuestro sistema. El Hardening también se logra eliminando software que no está siendo utilizado.
El *hardening* de sistemas trata de encontrar un punto de equilibrio entre la protección y hermetismo y la libertad de uso, creando un entorno seguro y cómodo de trabajo donde el usuario pueda realizar sus funciones sin estar bajo la amenaza de continuos ataques informáticos.[5]

2. Resumen

La Alcaldía Municipal de Támesis como entidad pública del Estado en la rama ejecutiva, está obligada a dar cumplimiento a las políticas de Seguridad Digital y Gobierno Digital que rige el Ministerio de las TIC (MinTIC) y que hace parte del Modelo Integrado de Planeación y Gestión. Dentro de la política se establecen los lineamientos y recomendaciones a seguir en cuanto a seguridad digital, un pilar fundamental para el desarrollo de las actividades de cualquier organización independiente de la índole a la que pertenezca. En la Alcaldía Municipal de Támesis no se contaba con un modelo de seguridad de la información que estuviera amparado por las normas del Modelo de Seguridad y Privacidad de la Información (MPSI) y que a su vez siguiera las reglas y recomendaciones de la norma ISO/IEC 27001:2013; La no existencia de un manual de reglas y políticas de seguridad informática ha propiciado en parte las intrusiones, las malas prácticas, la filtración de información sensible para la organización y los delitos informáticos,

dichos actos tienen un largo historial de ocurrencia en la entidad, algunos con mayor gravedad que otros.

El trabajo que se ha adelantado en la Alcaldía Municipal de Támesis, representa un punto de inflexión en la presente administración *¡Támesis nos pertenece!* La incorporación e implementación de políticas de seguridad de la información permitirá no solo el aumento de los indicadores de las políticas de Seguridad Digital y Gobierno Digital, sino que permitirá alcanzar ciertos objetivos del plan de desarrollo para esta administración y más importante aún, permitirá el aumento de la seguridad informática dentro de la entidad.

3. Introducción

Vivimos en la era de la información, en la sociedad del conocimiento y en las economías de los datos, ya hemos pasado por una tercera revolución tecnológica marcada y caracterizada por el salto de las tecnologías analógicas a las digitales, se nos ha abierto la posibilidad de registrar y monitorizar todas aquellas fuentes de información que sean propensas a tener valor. Esta capacidad nos ha dado un control nunca antes visto de nuestro entorno y de nuestras actividades y nos ha encaminado hacia un mundo en el que podemos entregar a la tecnología muchas de nuestras responsabilidades con la plena confianza que ella nos hará más eficientes, más focalizados y más productivos.

Desde la aparición y masificación de internet, la tendencia es a dejar de lado el uso de información física en papel y reemplazarla por su versión digital, con los beneficios en cuanto a costos, practicidad y logística que eso implica, pero con la aparición de estos métodos se han popularizado también ciertos tipos de delincuencia que se enfocan en el robo de información digital y en general a crear perjuicios por este medio.

Las empresas no son ajenas a esto y dan especial importancia a la seguridad informática como ítem importante para asegurar la integridad de sus datos, pero en aquellas entidades públicas que manejan información sensible es crítico prestar atención a estos temas. Lastimosamente muchas entidades de este tipo dejan de lado los temas informáticos por centrar sus recursos en cosas más inmediatas y es algo que no excluye a la Alcaldía Municipal de Támesis Antioquia, quien tiene un antecedente de haber sufrido un delito informático que terminó con el robo de recursos públicos, así como capturas y una preocupación sobre las vulnerabilidades que existen y que pueden ser explotadas por los delincuentes en el futuro.

Como respuesta a esta vulnerabilidad se da el surgimiento de la política de Gobierno Digital [1], como estrategia para la integración de la ciudadanía a los

procesos de su gobierno y los grandes retos que su implementación supone, ya que se basa en 5 propósitos que implican el despliegue de sistemas y el tratamiento de una mayor cantidad de información, dichos propósitos son: servicios digitales de confianza y calidad, procesos internos seguros y eficientes, decisiones basadas en datos, empoderamiento ciudadano a través de un Estado abierto y territorios, y ciudades inteligentes a través de las TIC. Tal despliegue de servicios y soluciones TIC demandan una alta seguridad en la red de la alcaldía municipal.

Actualmente desde la Alcaldía Municipal de Támesis, no se tiene un plan de seguridad informática, sus problemáticas van desde el uso de equipos de cómputo con sistemas operativos de versiones obsoletas y una gran falta de licencias en muchas de ellas, además de una clara falta de equipos destinados a seguridad en su red de datos. En el momento se está haciendo el despliegue de un programa antivirus en los equipos y se está llevando a cabo un plan de capacitación en temas de seguridad para todo el personal, con el fin de evitar ataque e infiltraciones por medio de phishing[1]. Es urgente la puesta en marcha de un plan de seguridad de la información en la red que incluya de forma imperativa técnicas y metodologías que mejoren la confiabilidad e integridad de los datos en los sistemas informáticos.

4. Objetivos

4.1. General

Diseñar una guía de seguridad informática de aplicación en la red interna de la Alcaldía Municipal de Támesis Antioquia, que permita una mejora en temas de confidencialidad, integridad y disponibilidad de la información basada en las métricas y recomendaciones de la norma ISO 27001 y más específicamente mediante el Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC en su guía número 3, que sirva como base para los requerimientos de la política de Gobierno Digital.

4.2. Específicos

- Identificar las posibles amenazas existentes dentro de la red, mediante la implementación de una fase de exploración en la cual se verifique el estado de los equipos conectados, las licencias y el grado de capacitación de los usuarios para identificar y evitar amenazas.

- Establecer estrategias y rutas que posibiliten cumplir con las políticas de seguridad informática del sistema de información de la Alcaldía Municipal de Támesis, según lo dicta la guía número 3 de MSPI del MinTIC.

[1] Suplantación de identidad

- Plantear las medidas correctivas, procedimientos, equipos, capacitaciones y acompañamiento necesario, según la información recopilada para el cumplimiento de las políticas de seguridad informática de la guía número 3 de MSPI del MinTIC, apoyados en las métricas y recomendaciones de la norma ISO 27001.

5. Marco Teórico

5.1. Planteamiento del problema.

La Alcaldía Municipal de Támesis como entidad pública, en virtud de su obligación de servicio y salvaguarda de la comunidad, está amparada bajo las leyes y normas de los diversos Ministerios del Estado Colombiano; precisamente uno de ellos es el Ministerio de las TIC, los cuales ordenan a las entidades bajo su jurisdicción, que se asuman, se cumplan y se implementen una serie de normativas para el uso correcto y seguro de las tecnologías de la información en el devenir de las labores de gobernanza. Es por esto que dentro de las 17 políticas que enmarca el Modelo Integrado de Planeación y Gestión, se han introducido múltiples políticas relacionadas con las tecnologías de la información, como lo son *Gobierno Digital, Seguridad Digital* y *Transparencia y acceso a la información pública*, además de la introducción de algún componente tecnológico en las demás políticas, lo que se busca con esto es precisamente fortalecer la seguridad de la información al interior de las instituciones y con la introducción de los 5 pilares de la política de *Gobierno Digital*, se busca una forma de gobierno mas transparente, mas eficaz y con una participación mucho mayor de la ciudadanía.

Lastimosamente en la Alcaldía de Támesis no se ha hecho una extensiva aplicación de la norma, aunque si se han implementado ciertas estrategias y medidas para la protección de la información. Por desgracia la entidad y muchos de sus funcionarios y contratistas han sido victimas de fraudes, robos (monetarios y de información), ataques y demás perjuicios como institución y como individuos; esta situación llegó a niveles preocupantes cuando en 2021 la institución recibió un agresivo ataque, puntualmente a la secretaria de *Hacienda y Rentas Municipales*, con la que se pretendía robar una fuerte suma de dinero, la cual por fortuna fue frustrada y por la cual se llegó a la captura de los implicados.

En resumen la entidad no cuenta con la implementación de muchos de los esquemas de seguridad informática y de uso de tecnologías de la información en general, su red es vulnerable, sus activos de información son propensos a se

corruptibles y algunas de las personas que laboran allí, son preocupantemente propensos a ser víctimas de delitos informáticos, por esto se hace imperativo la aplicación de medidas que ayuden a mitigar los riesgos desde todos los aspectos, el técnico, el humano y el político.

5.2. Descripción de la solución al problema encontrado.

La creación de un plan de seguridad de la información se hace imperativa dentro de la institución para evitar, mitigar, evadir y proteger los datos confidenciales y que son de suma importancia para ejercer las labores de gobernanza y de desarrollo del territorio.

La solución mas oportuna es la aplicación del Modelo de Seguridad y Privacidad de la Información, la cual pertenece al habilitador transversal de Seguridad y Privacidad, de la política de Gobierno Digital. Este está acorde con las buenas prácticas de seguridad y reúne los cambios técnicos de la norma 27001 del 2013, la legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Publica, entre otras, las cuales se deben tener en cuenta para la gestión de la información.

La implementación del Modelo de Seguridad y Privacidad por parte de las Entidades del Estado, está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos. Mediante la adopción del Modelo de Seguridad y Privacidad por parte de las Entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.[2]

De modo que la posible solución que se plantea para mejorar las prácticas es la creación y aplicación de una guía de seguridad de la información tal y como lo exige la política de Gobierno Digital por medio de las guías del MSPI, haciendo especial énfasis en la guía 3 de *procedimientos de Seguridad de la Información*. El MSPI está basada en la norma ISO 27001 como estándar internacional de seguridad de la información, como el conjunto de buenas practicas para el establecimiento mantenimiento y mejora de un **Sistema de Gestión de la Seguridad de la información.**

[2] Extraído de https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

La norma internacional ISO 27001:2013 está basado en un ciclo de Deming, el cual permite la retroalimentación de la aplicación del modelo, lo que lleva a la corrección de fallos para mejorar la eficiencia y eficacia del modelo. En el caso de la norma ISO 27001:2013, el ciclo se conoce como PHVA.

Ciclo PHVA

La ISO 27001 se basa en ciclo PHVA, el cual busca una optimización constante de las actividades al interior de la organización, es un modelo de 4 etapas que se ejecutan en un orden estricto. Una vez se llega a la última etapa, la organización debe volver a comenzar, promoviendo así una autoevaluación constante que permita identificar oportunidades de mejora en los procesos relacionados a la seguridad informática.

Las diversas etapas del ciclo PHVA son:

Planificar: se establecen objetivos, se disponen recursos, se identifican requisitos de la política organizativa y se identifican los riesgos y oportunidades.

Hacer: Se implanta y se ejecuta lo planificado.

Verificar: Controlar y medir los procesos para establecer el rendimiento de la política, objetivos, requisitos y actividades planificadas e informar los resultados.

Actuar: Tomar acciones para mejorar el rendimiento, en la medida de lo necesario.

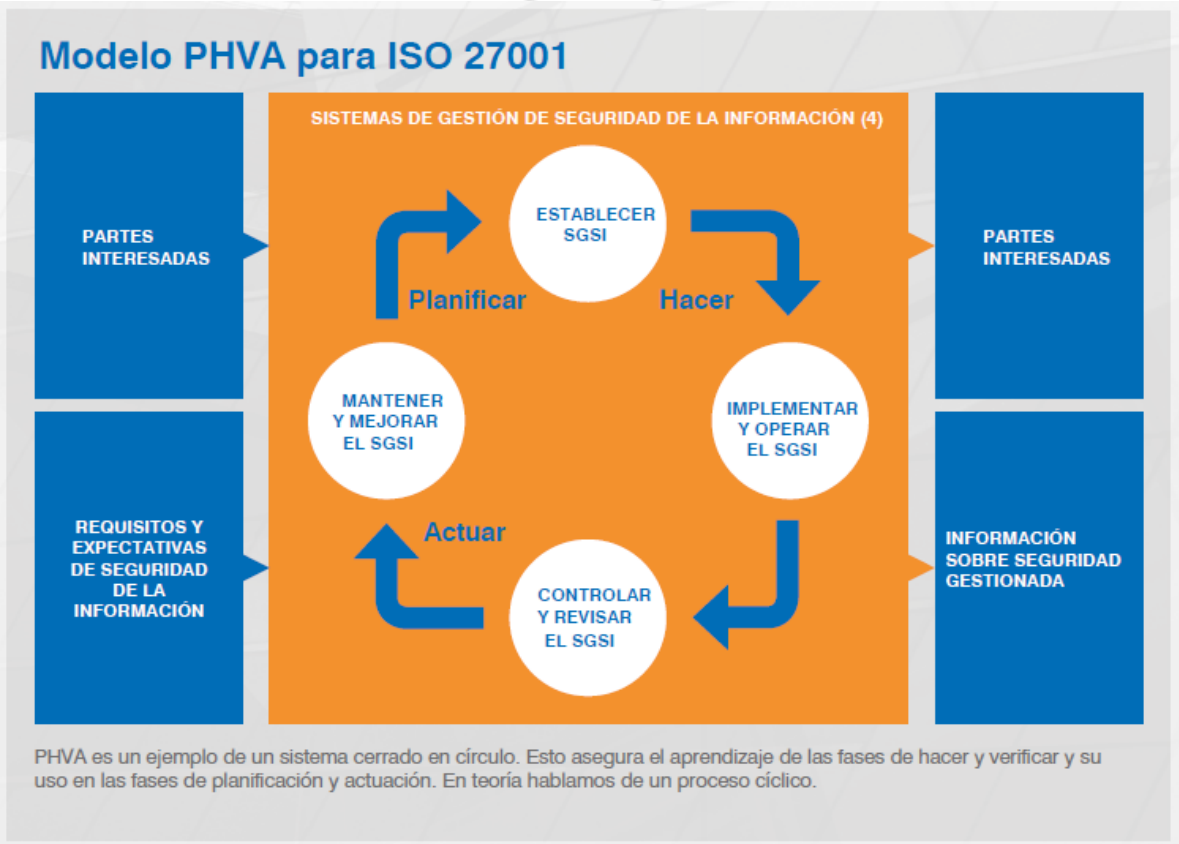


Figura 1. Modelo PHVA para ISO 27001[3]

Cláusulas del modelo ISO 27001

La ISO 27001:2013 se compone de 10 secciones conocidas como clausulas.

Al igual que con la mayoría de normas del sistema de gestión ISO, los requisitos de la ISO 27001 que deben cumplirse se especifican en las cláusulas 4 a 10. A diferencia de la mayoría de las demás normas ISO, una organización debe cumplir con todos los requisitos de las cláusulas 4 a 10, no puede declararse una o más clausulas como no aplicables.

[3] Tomado de: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Figura 2. Clausulas Normas ISO 27001[4]

Para la creación de la guía de seguridad de la información se siguieron una serie de pautas, la recolección de información, la evaluacion de los sistemas y el nivel de capacitación del personal, la solución de vulnerabilidades de alta criticidad y por último la formulación del ***Plan de Seguridad Informática Para el Sistema de Información de la Alcaldía Municipal le Támesis.***

6. Levantamiento de inventarios de equipos

Como primera medida se debe hacer un reconocimiento de todos los insumos de TI existentes y en operación con los que cuenta la alcaldía, para ello se debe

[4] Tomado de https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

realizar un inventario que incluya la hoja de vida de cada dispositivo que se integre con la red de la alcaldía y la forma en que está estructurada la red, de este modo se tenga el conocimiento de todos aquellos recursos obsoletos tanto de hardware como de software.

La Administración Municipal consta de una sede principal ubicada en la zona central del municipio, pero además cuenta con 5 sedes más dedicadas a actividades específicas de las diferentes secretarias, además de dos empresas públicas que son filiales de la Administración Municipal, las cuales son la Empresa de Servicios Públicos Domiciliarios y el Hospital San Juan de Dios, todas estas oficinas están distribuidas de la siguiente manera.

Secretarias de Despacho	Entidades descentralizadas
Alcalde del municipio de Támesis	
✓ Secretaria de Gobierno y Participación Ciudadana ✓ Secretaria de Planeación y Desarrollo Territorial. ✓ Secretaria de Turismo y Cultura. ✓ Secretaria de Hacienda y Rentas Municipales ✓ Secretaria de Educación, Salud y Deporte ✓ Secretaria de la Mujer y Bienestar Social ✓ Secretaria de Desarrollo Rural y Medio Ambiente	✓ Concejo Municipal ✓ Personal Municipal ✓ Empresa de Servicios Públicos Domiciliarios. ✓ Casa de la Salud Hospital San Juan de Dios

Tabla 1. Esquema organizacional de las empresas públicas de Támesis.

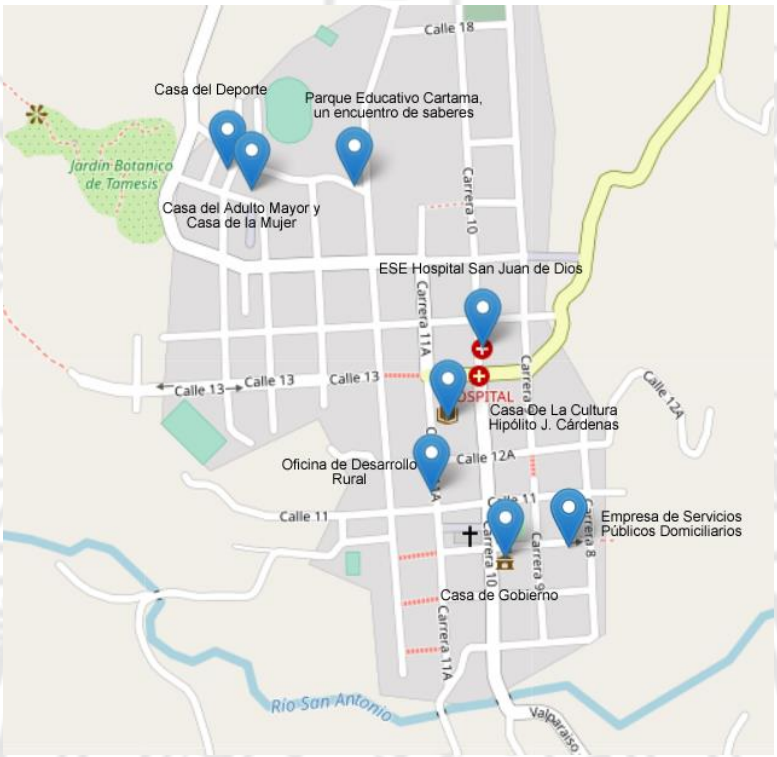


Figura 3. Referenciación geográfica de las oficinas.[5]

La información completa de la referenciación geográfica de las diferentes oficinas se encuentra en la página web oficial de la Administración Municipal "*Támesis nos pertenece*": http://www.tamesis-antioquia.gov.co/

Los inventarios existentes de los activos informáticos de cada sede estaban desactualizados, incompletos, tenían inconsistencias o eran inexistentes, por lo que se dio a la tarea de crear un inventario centralizado, en el cual se registró la hoja de vida de cada equipo de cómputo, impresora o dispositivo en red, en las que se plasma las especificaciones físicas y de software, además de las necesidades de software específico para cada oficina o funcionario. La información aquí plasmada corresponde únicamente a los equipos bajo inventario de la oficina de archivo de la administración, que contempla la Casa de Gobierno y la demás oficinas, pero no incluye a las demás entidades filiales, ya que estas no hacen parte de los activos de la Administración Municipal y su operación es independiente, aunque existen acuerdos contractuales de apoyo a ciertas tareas por parte de diferentes dependencias, incluyendo el área de sistemas y sus aportes a MIPG.

[5] Fuente. http://www.tamesis-antioquia.gov.co/

Sede	Oficina	Numero de equipos	Información de sistema			Numero de impresoras
			Windows 7	Windows 10	Otro S.O	
Inspección Rural Palermo	Inspección	2	1	1	0	2
Parque Educativo Cártama	Sala de informática	15	14	1	0	0
	Portátiles de uso académico	50	0	50	0	0
	Oficina de comunicaciones	5	1	3	1	1
	Oficina Principal	1	1	0	0	0
Casa de la mujer y adulto mayor	Oficina principal	5	0	5	0	1
	Sala de informática	16	0	16	0	0
Casa del deporte	Oficina principal	5	1	4	0	1
Casa de la cultura	Oficina secretaria de cultura	1	0	1	0	1
	Biblioteca	3	0	3	0	1
Casa de Gobierno	Banco de proyectos	5	1	3	1	1
	Sisbén	2	0	2	0	1
	Archivo	4	2	2	0	1
	Hacienda	8	0	8	0	1
	Comisaria de familia	4	1	3	0	0
	Despacho Alcaldía	2	0	2	0	1
	Enlace victimas	1	0	1	0	0
	Jurídica	2	0	2	0	0
	Oficina de control interno	1	0	1	0	0
	Inspección de policía y transito	2	0	2	0	0
	Oficina de Gobierno y participación ciudadana	2	0	2	0	0
	Educación	5	1	4	0	1
	Catastro	3	0	2	1	0
	Planeación	6	0	6	0	2
Desarrollo rural	Oficina de Desarrollo Rural	6	0	6	0	1

Tabla 2. Inventario de equipos de cómputo.

Con la información resultante se pueden identificar posibles vulnerabilidades de seguridad en los elementos de TI, comenzando por las licencias de los equipos, los dispositivos de red obsoletos y las redes WIFI clandestinas que se conectan directamente a la red, con el fin de tener un insumo que permita la creación de un plan para mitigar los riesgos más inmediatos.

Las vulnerabilidades más críticas que pudieron identificarse en una primera inspección, es la relacionada con la falta de licencias o el uso de sistemas operativos obsoletos que ya no cuentan con soporte. Además, como administrador de redes y plataformas se ha tenido acceso a las contraseñas de las plataformas y cuentas de correo institucional, y se pueden catalogar de forma general como inseguras. Aunque se tienen buenas prácticas en cuanto a longitud y uso de caracteres alfanuméricos y especiales, los empleados tienen la tendencia a poner referencias personales o institucionales en sus contraseñas, así como números que reflejan fechas o secuencias contiguas de número y letras, por lo general tienen patrones similares entre sí en cuanto a la forma en las que se estructuran las contraseñas y que las hace vulnerables para un atacante.

En cuanto a los dispositivos en red, estos presentan un buen nivel de seguridad, los equipos son de generaciones recientes, usan el estándar Gigabit Ethernet, están bien resguardados en un cuarto de telecomunicaciones con acceso restringido, aunque con una ventilación deficiente. El cableado de red es vulnerable, este no cuenta con una especificación identificable y su disposición en algunas oficinas compromete la seguridad de la información de la red de datos y la integridad de los usuarios, el cableado no está debidamente rotulado y no se cuenta con buenas prácticas para el ponchado y la distribución en el edificio, por otro lado el edificio tiene un sistema de canaletas que si cumple con las especificaciones, al separar las conexiones eléctricas de las de datos y estas se distribuyen de forma adecuada en la casa de gobierno, pero estas no se han sabido adaptar a los cambios que se han requerido, en gran parte por la ausencia de equipo y personal en el área de sistemas capacitado en temas de cableado estructurado.

7. Planeación de capacitaciones

Es de vital importancia la aplicación de métodos de evaluación como encuestas, cuestionarios y simulacros que permitan evaluar la capacidad de respuesta de los funcionarios y contratistas de la administración ante un posible ataque a la seguridad informática, y a su vez medir la capacidad para identificar una amenaza y evadirla.

La información de esta actividad corresponde con los avances en la política de *Seguridad Digital* en la dimensión de *Gestión con valores para resultados* del *Modelo Integrado de planeación y Gestión* que fue revisado y aprobado por la coordinadora de dicha dependencia. El objetivo de esta actividad es aumentar la

capacidad del personal de la entidad para reaccionar de forma adecuada ante la presencia de una amenaza para la seguridad de la información, para lograrlo se impartieron una serie de capacitaciones en la Alcaldía Municipal y en su entidad filial, la empresa de servicios públicos domiciliarios, en dichas capacitaciones se tocaron temas como el phishing y como evitarlo, el ransomware[6] y su conexión con el phishing para propagarse a través de redes locales.

Tras impartir cada capacitación se evaluó el nivel de comprensión e interiorización de las temáticas. A continuación, se presentan los resultados más relevantes:

7.1 Capacitación Alcaldía Municipal

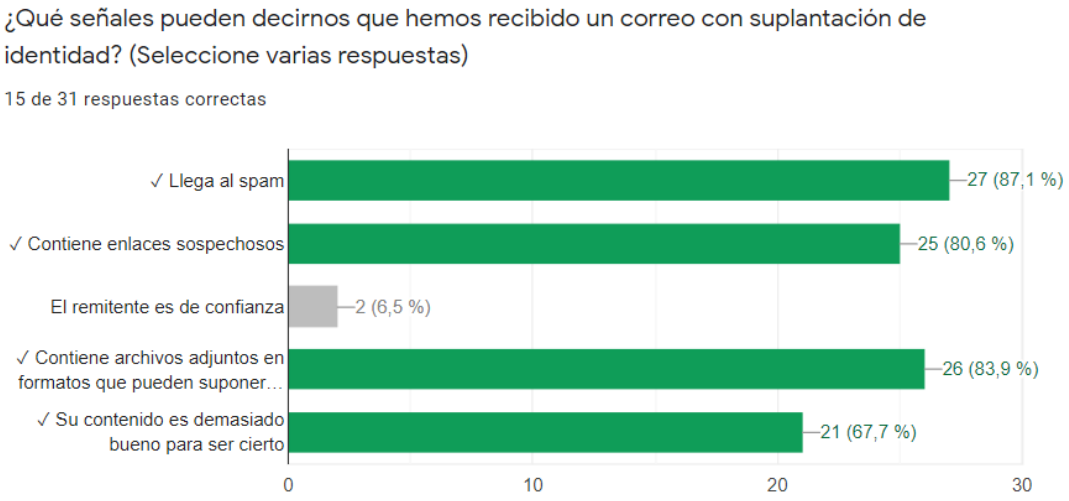
Tras cada capacitación fue aplicado un test corto para evaluar el entendimiento de los temas tratados y que a la vez sirva como un primer diagnóstico del nivel de conocimiento del personal sobre la seguridad informática. El balance general muestra una calificación media de 5.39/10, que, si bien puede parecer baja, el criterio de evaluación aplicado contempla un valor mayor a las preguntas de selección múltiple con múltiple respuesta, las cuales deben ser respondidas de forma correcta para que el punto sea válido, la intención de este método es acercar el ejercicio un poco más a la realidad, en la cual si se ignora alguno de los signos de alarma se puede ser víctima de un delincuente informático.

Figura 4. Resultados evaluación Alcaldía Municipal

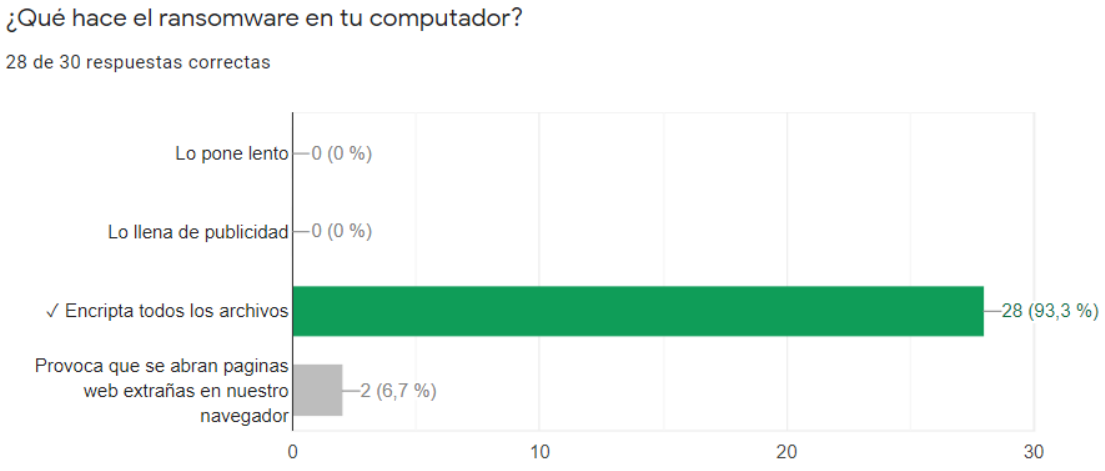
La primera pregunta hace alusión a los signos de alerta que pueden indicar que se está frente a un correo con suplantación de identidad o un intento de fraude por correo electrónico, tan solo el 6.5% de las personas evaluadas reconocen a un remitente de confianza como una amenaza, pero reconocen la mayoría de las

[6] Software malicioso para el secuestro de información

amenazas verdaderas. Este punto tiene un criterio de calificación exigente, ya que ignorar un indicador de peligro puede significar un agujero en la seguridad de la red de la entidad, eso explica porque solo 15 de 31 personas respondieron de forma perfecta a la pregunta.

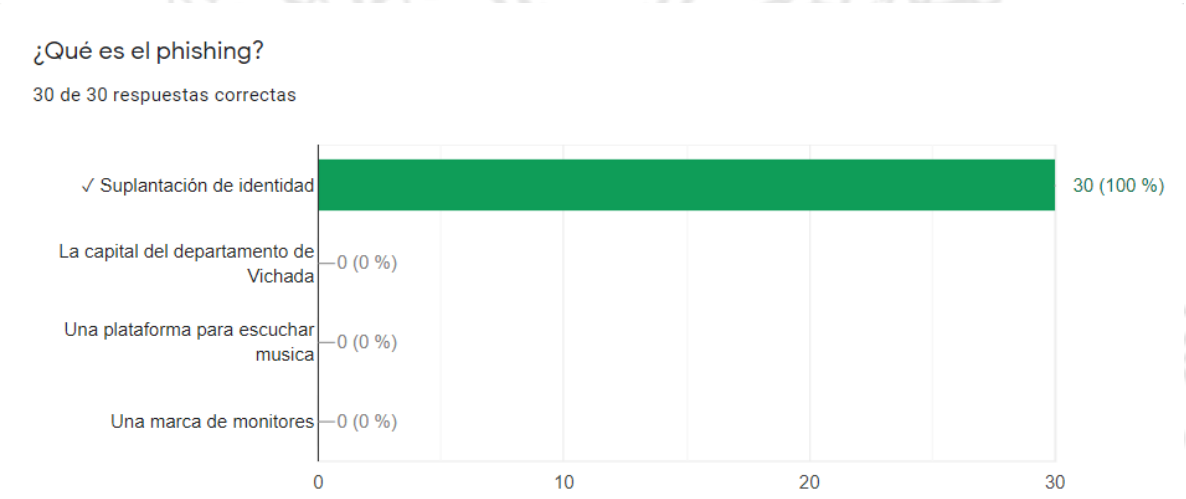


Dentro de los temas tratados, se habló sobre los peligros, las formas de contagio y como pueden suponer un gran riesgo para el desempeño de nuestras actividades y la información tratada al interior de la red de la alcaldía. El 93.3% de las personas evaluadas reconoció correctamente el efecto que tiene el contagio y la ejecución de un ransomware en el equipo.



El phishing fue el tema central de las charlas, respecto a este se explicó y dieron ejemplos de correos suplantando la identidad de entidades, así como las distintas modalidades usadas para engañar a sus víctimas aprovechándose de su ingenuidad. En esta pregunta el 100% de los asistentes reconoció correctamente

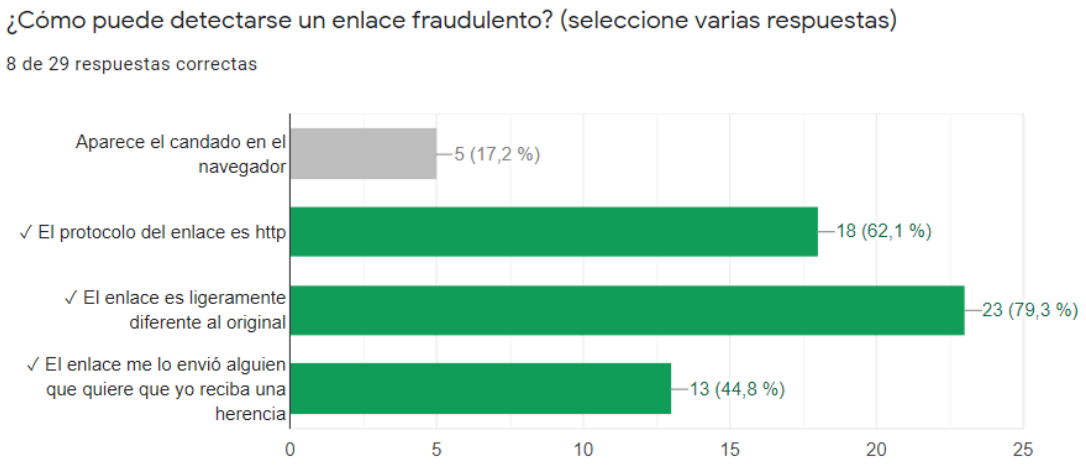
que el phishing corresponde a una suplantación de identidad para, ya sea extraer información o credenciales de acceso, así también como ingresar software malicioso al interior de la red.



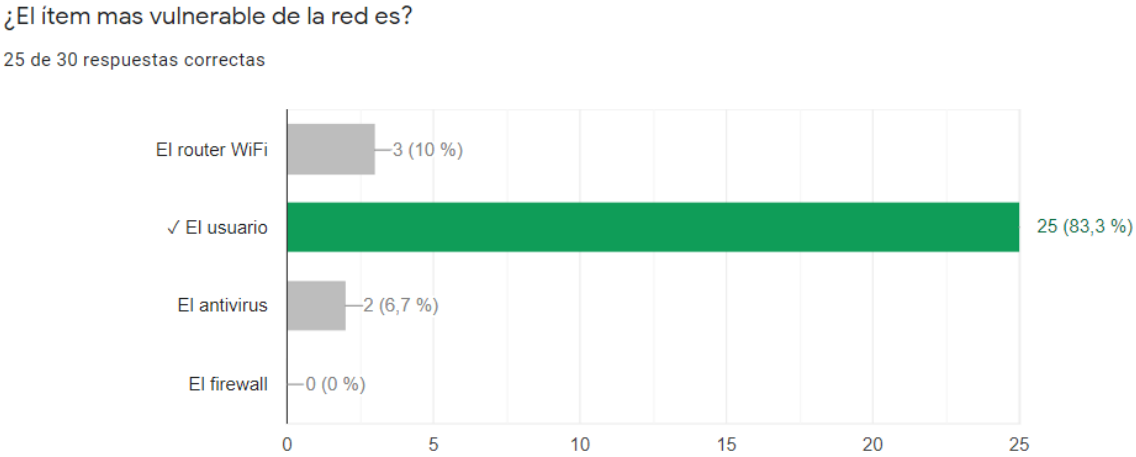
Para detectar un enlace fraudulento se vieron temas como los certificados SSL[7] y el protocolo https[8] para asegurar la seguridad de las páginas web que se visiten, así mismo se explicó cómo el navegador alerta de una página potencialmente peligrosa al carecer de dichos requisitos. El 79.3% de los asistentes reconocieron que los enlaces fraudulentos tienen pequeñas diferencias con los enlaces reales cuando se trata de la suplantación de una entidad o empresa, sin embargo, el 17.2% identificó erróneamente el símbolo del candado[9] en el navegador como una señal de riesgo, dado que este indica que la conexión esta encriptada de punto a punto.

Tan solo 8 de las 29 respuestas recibidas seleccionaron todos los ítems de forma correcta, lo que indica un desconocimiento muy generalizado de las amenazas en la web, esto sirve como indicador de cuál es una de las principales falencias y que temas hay que reforzar.

[7] certificado digital que autentica la identidad de un sitio web
[8] Protocolo seguro de transferencia de hipertexto
[9] Símbolo que indica que un sitio web emplea el protocolo *https*



El 83.3% de los asistentes reconocen que son el elemento más vulnerable dentro de la red, esto es muy diciente sobre la concientización lograda en las charlas ya que no existe un sistema que sea impenetrable y una de las puertas de acceso son las personas que hacen uso de dichos sistemas. Al reconocerse a sí mismo como vulnerabilidad se tendrá un mayor cuidado en el uso de los sistemas.



7.2 Capacitación Empresa de Servicios Públicos Domiciliarios

Tras la capacitación se aplicó el mismo método de evaluación empleado en la Alcaldía Municipal, con algunas modificaciones en el criterio de evaluación. El balance general muestra una calificación media de 4/6, en este caso el criterio de evaluación fue el de otorgar un punto por cada respuesta correcta, debido a que las altas exigencias arrojaban valores negativos que no necesariamente reflejaban

una mala compresión de las temáticas, en este caso además se impartió un tema adicional referente a los métodos para la creación de contraseñas seguras

Teniendo en cuenta que se dio un tema adición y que se modificó la metodología de evaluación, se obtuvo una calificación media de 4 respuestas correctas de 6 para las 8 personas que realizaron el test. Es un resultado que indica de forma general un buen entendimiento de las temáticas tratadas.

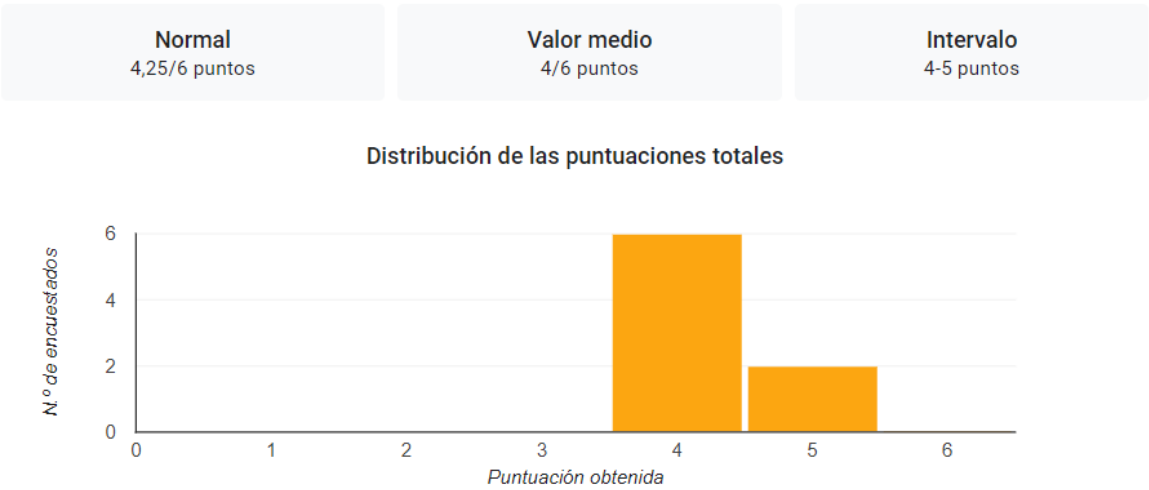
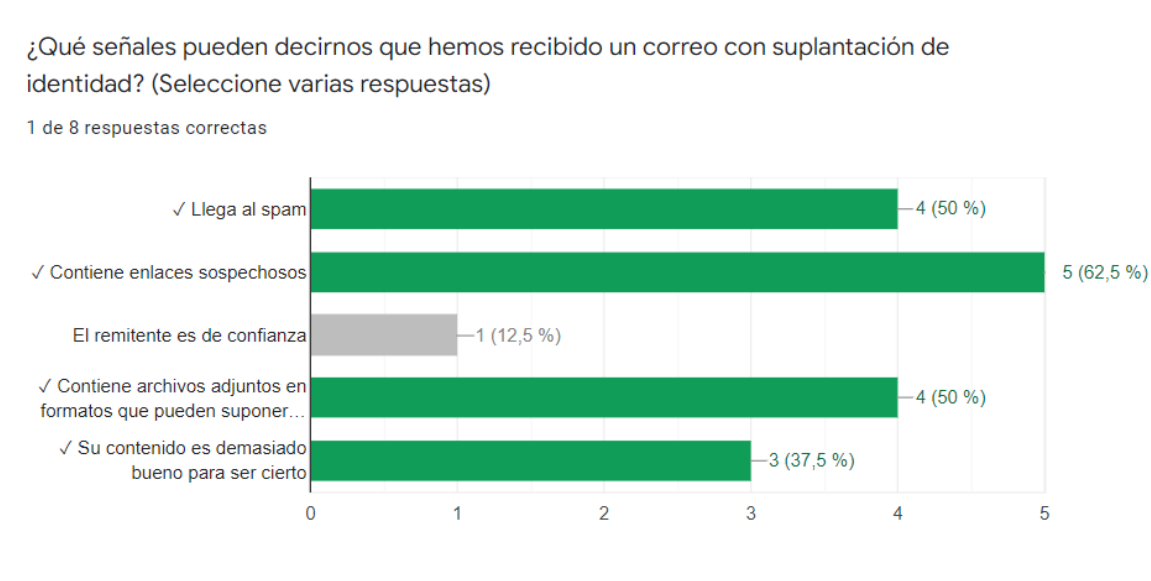
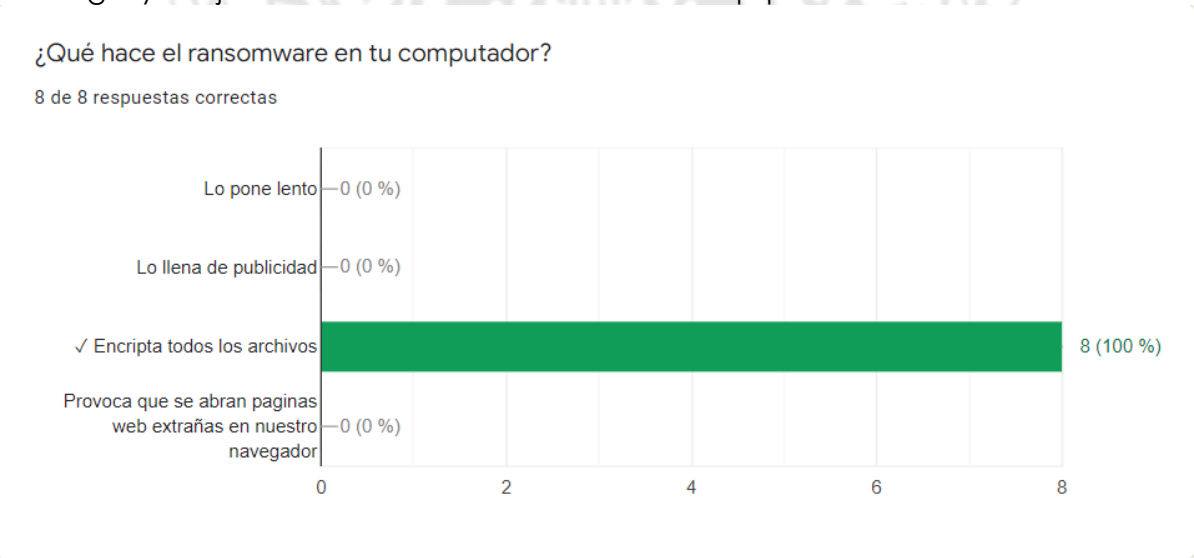


Figura 5. Resultados evaluación Empresa de Servicios Públicos Domiciliarios.

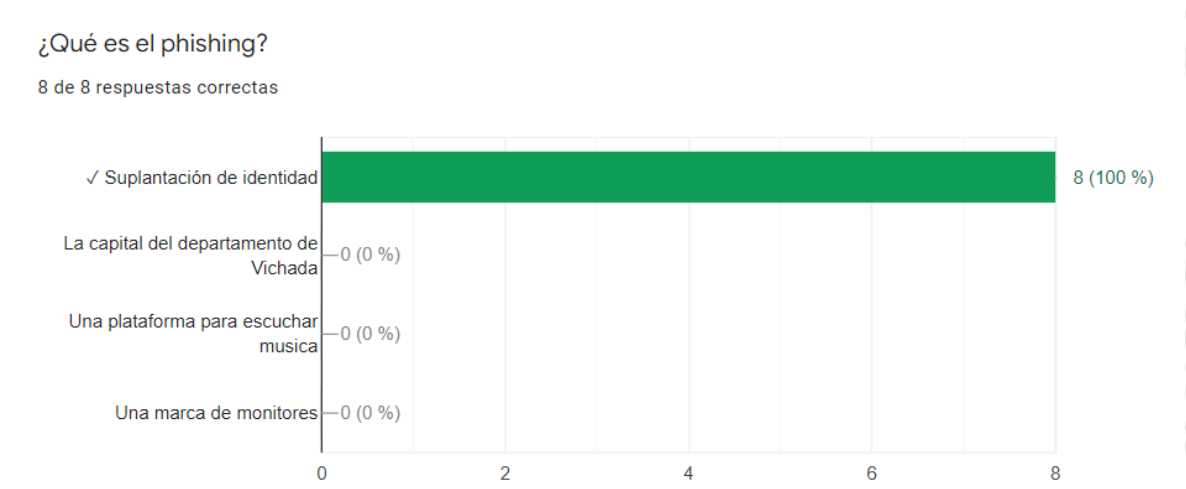
Tan solo el 12.5% de las personas evaluadas reconocen a un remitente de confianza como una amenaza, pero reconocen la mayoría de las amenazas verdaderas. Solo una de las 8 personas evaluadas identificó correctamente todas las señales de alerta para calificar un correo electrónico como una suplantación de identidad, por lo que este es un punto a reforzar.



El 100% de las personas evaluadas reconoció correctamente el efecto que tiene el contagio y la ejecución de un ransomware en el equipo.

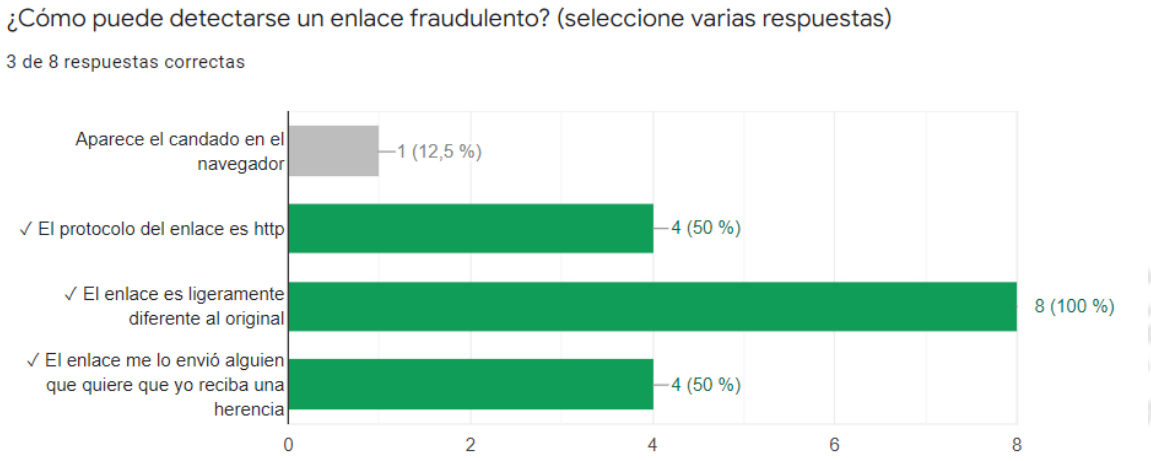


En esta pregunta el 100% de los asistentes reconoció correctamente que el phishing corresponde a una suplantación de identidad para, ya sea extraer información o credenciales de acceso, así también como inyectar software malicioso al interior de la red.

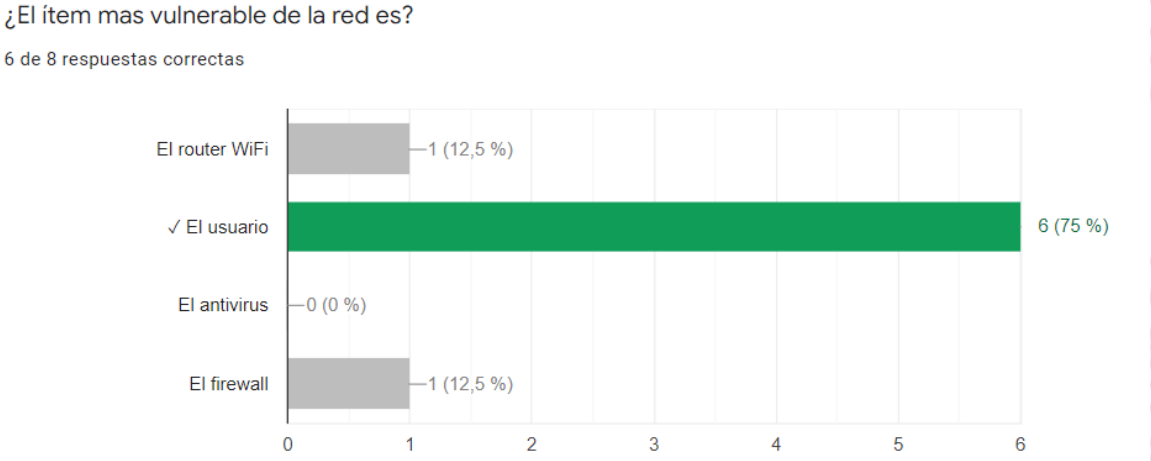


El 100% de los asistentes reconocieron que los enlaces fraudulentos tienen pequeñas diferencias con los enlaces reales cuando se trata de la suplantación de una entidad o empresa, sin embargo, el 12.5% identificó erróneamente el símbolo del candado en el navegador como una señal de riesgo, dado que este indica que la conexión esta encriptada de punto a punto.

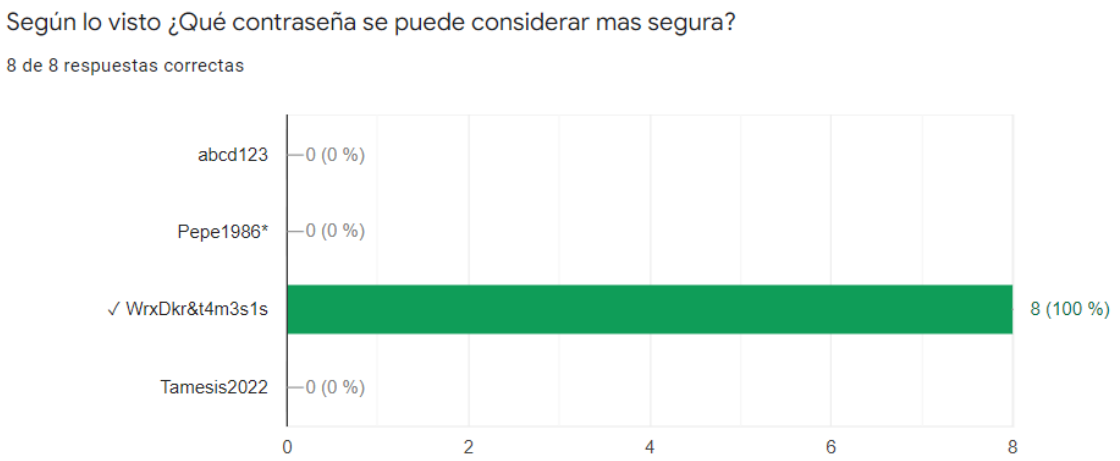
Tan solo 3 de las 8 respuestas recibidas seleccionaron todos los ítems de forma correcta, lo que indica un desconocimiento muy generalizado de las amenazas en la web, esto sirve como indicador de cual es una de las principales falencias y que temas hay que reforzar.



El 75% de los asistentes se reconocen a sí mismos de forma correcta como él elemento más vulnerable de la red; tan solo dos personas reconocen erróneamente otros sistemas como los más vulnerables.



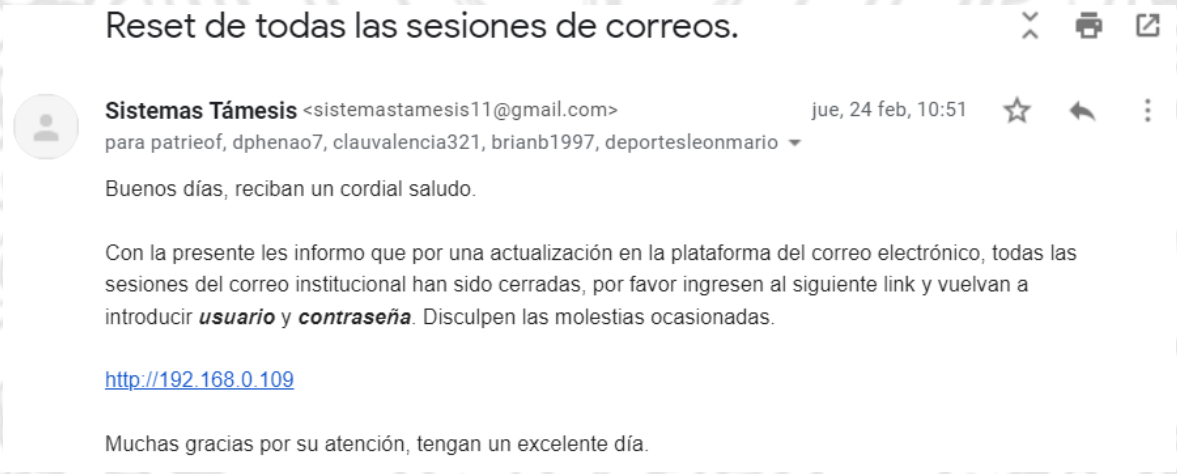
Dentro de las temáticas impartidas, se dedicó un espacio para explicar y dar consejos para la creación de contraseñas seguras, de los asistentes evaluados en su totalidad reconocen que las contraseñas más seguras son aquellas que tienen una mayor longitud y que su entropía entre caracteres es la mayor posible, de modo que la contraseña debe tener una alta diversidad de caracteres, no debe contener información personal y debe ser cambiada con frecuencia.



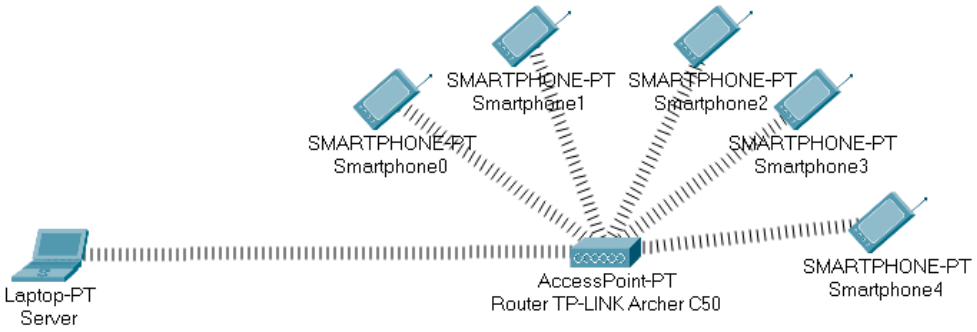
7.3 Procedimiento Simulacro De Ataque Phishing

Durante los días 22, 23, 24 y 25 de febrero, se impartieron una serie de capacitaciones sobre seguridad informática en las diferentes dependencias de la alcaldía municipal de Támesis y el día 26 de abril en la empresa de servicios públicos domiciliarios. El objetivo fue introducir a los asistentes a uno de los ataques informáticos más comunes hoy en día.

En cumplimiento de las actividades de la política de *Seguridad Digital* se aplicó un simulacro de ataque por medio de phishing. La dinámica de la actividad fue enviar un correo electrónico con suplantación de identidad en la que de forma controlada se hace pasar por personal de sistemas de la entidad, donde se solicita ingresar los datos del correo electrónico institucional a través de un enlace en el cuerpo del correo electrónico.

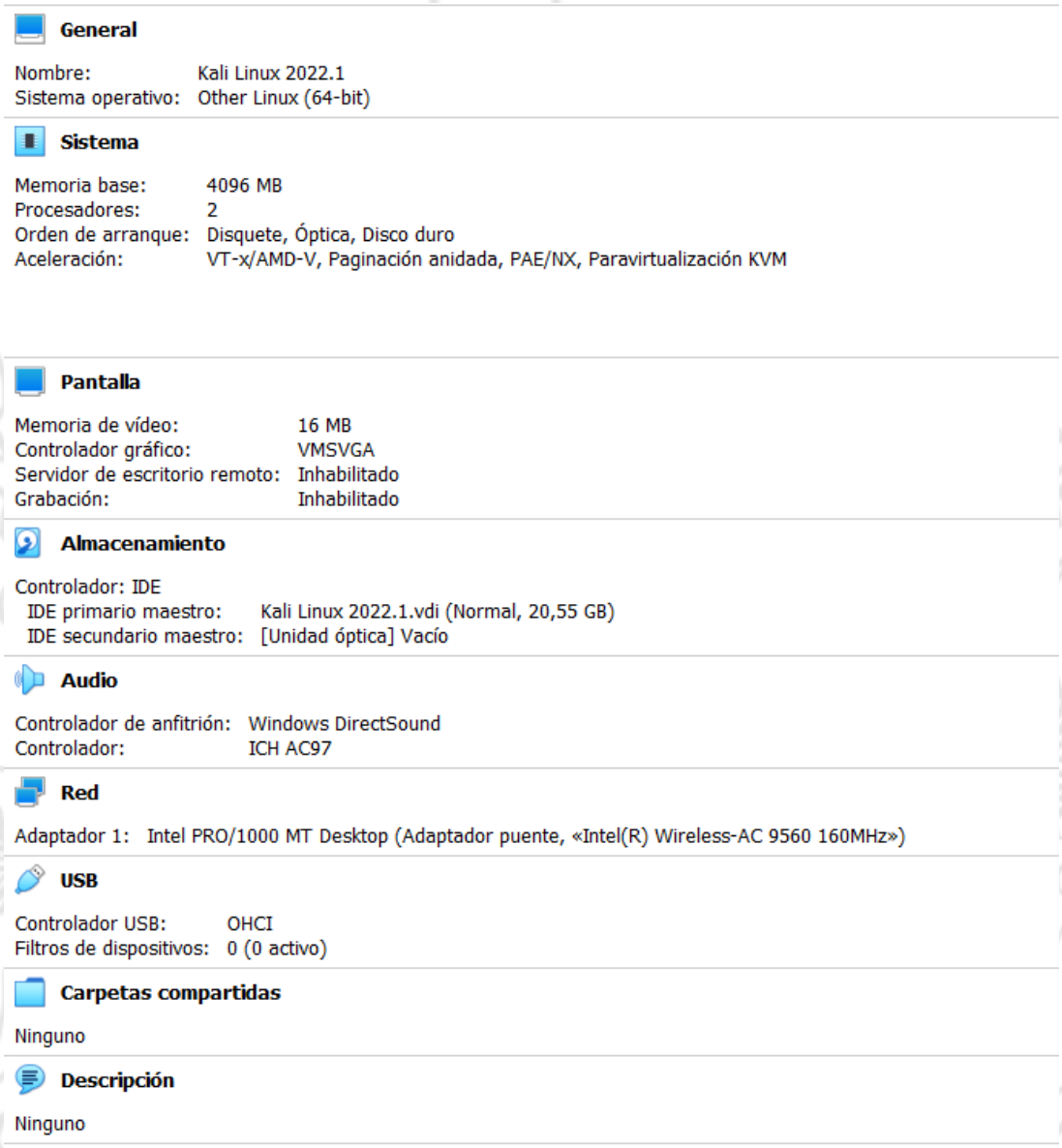


Para el funcionamiento del ejercicio se les solicitó a los asistentes que se conectaran a una red WiFi creada con un Router TP-LINK Archer C50 configurado como Access Point, la intención de esto es hacer que todos los asistentes estén conectados a la misma red local y tengan acceso al servidor donde se aloja el enlace, por lo que se da la siguiente topología.

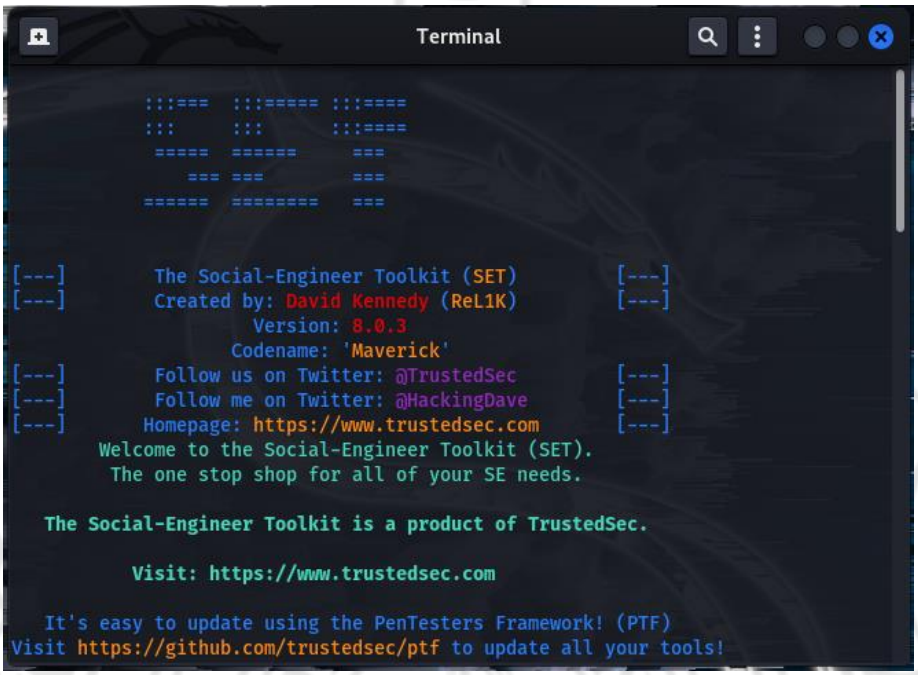


El servidor es un equipo Acer con procesador Intel Core i5 8300H y 12 GB de RAM en la que corre una máquina virtual en ***Oracle VM VirtualBox*** con el sistema operativo ***Kali Linux 2022.1 x64***, la maquina está configurada con 2 núcleos sin Hyper-Threading[10] del procesador sin restricción de frecuencia de reloj y 4 GB de RAM, con una configuración de red en modo puente con la tarjeta de red WiFi del equipo anfitrión.

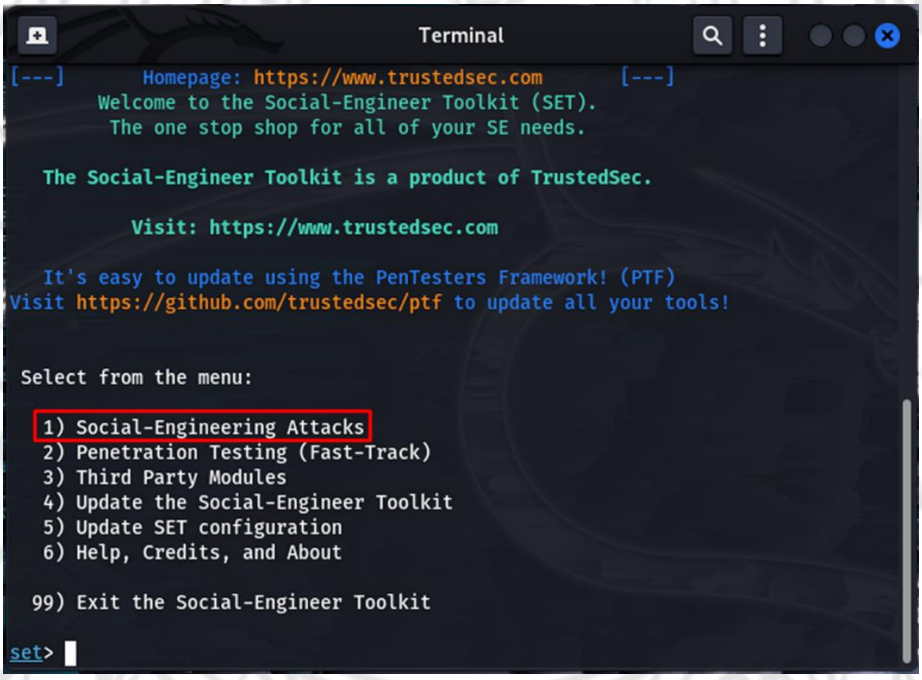
[10] Procesamiento multihilo



Dentro del sistema se ejecuta un aplicativo que permite la creación de ataques de ingeniería social, en este caso se trata de la herramienta ***The Social Engineer Toolkit (SET)***

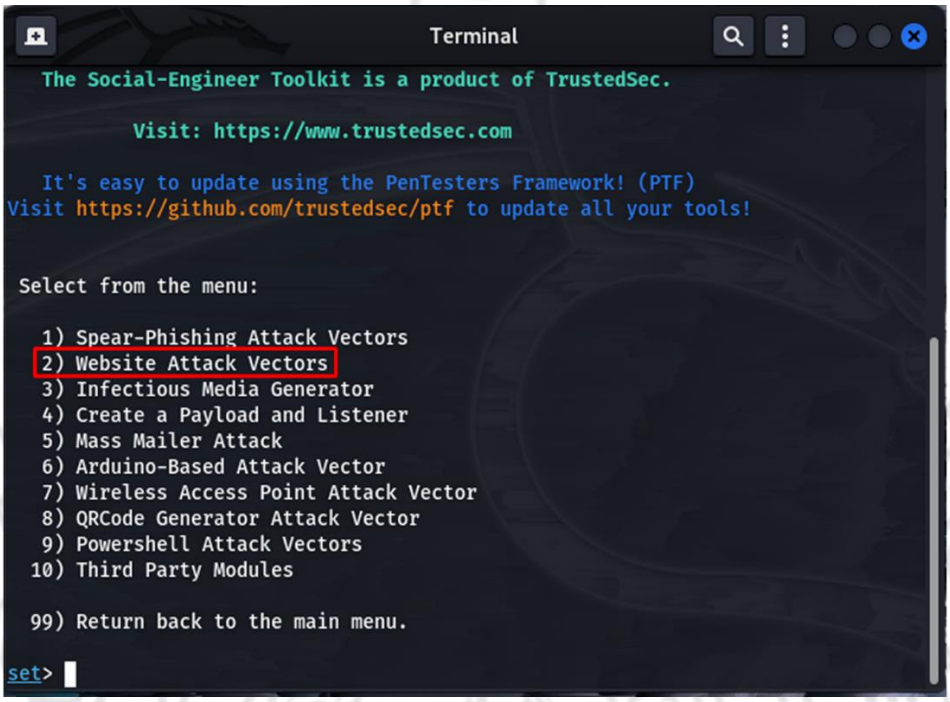


Se emplea el módulo ***Social-Engineering Attacks*** en la opción 1.

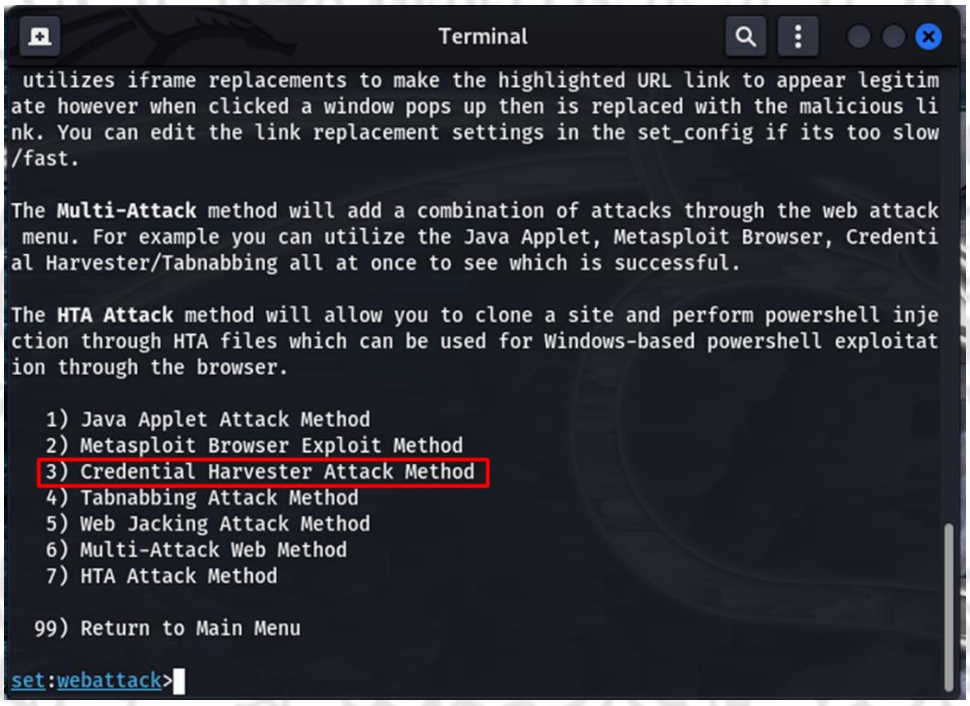


Dentro del módulo se selecciona el set de aplicaciones ***Websites Attack Vectors***, para realizar ataques mediante el protocolo http[11].

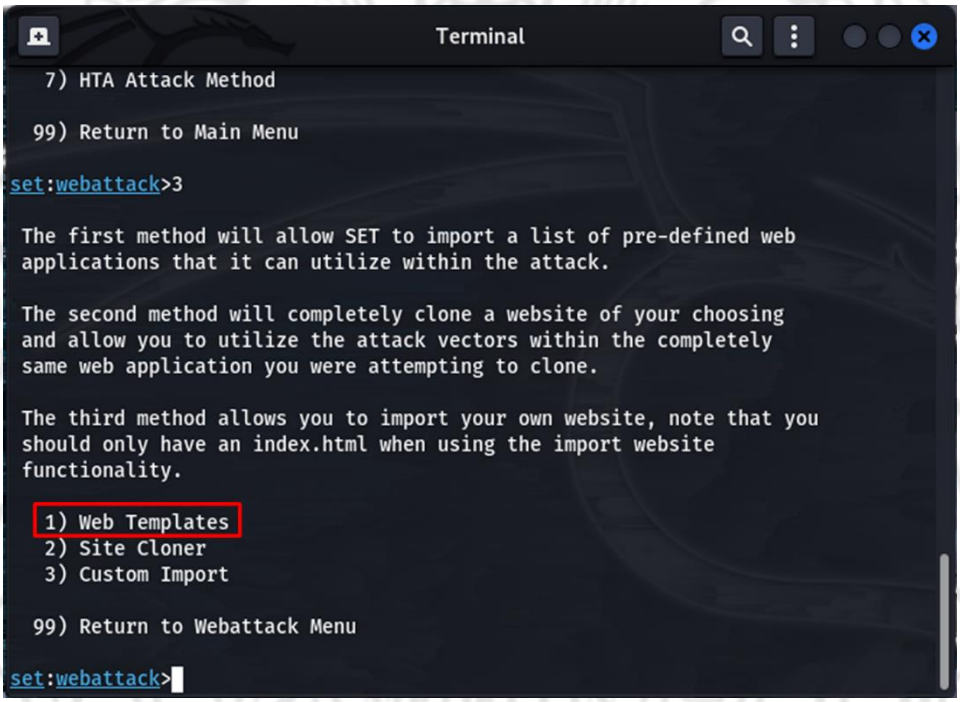
[11] Protocolo de transferencia de hipertexto.



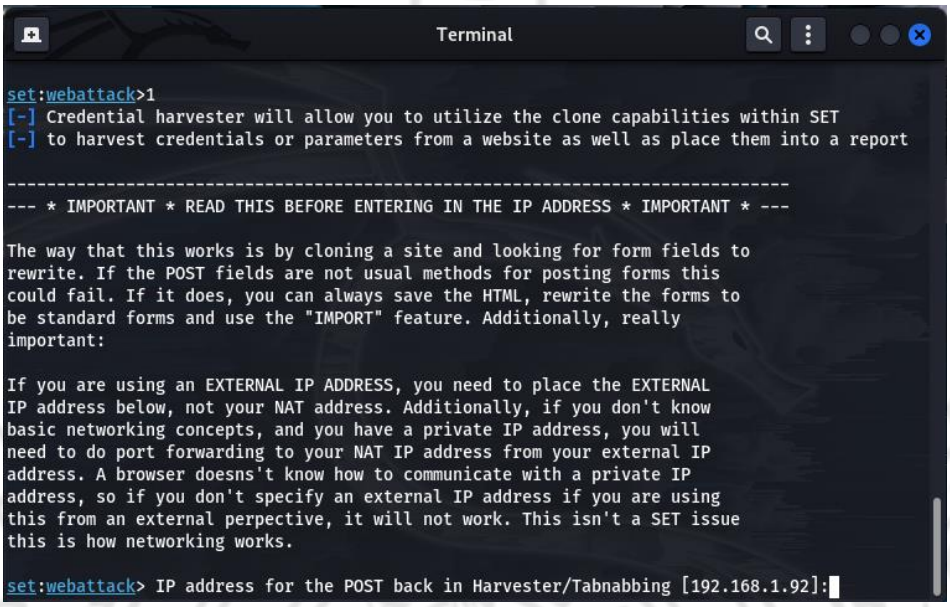
Se selecciona ahora el método de ataque de recolección de credenciales ***Credential Harvester Attack Method***, para usar alguna de las herramientas de phishing para la recolección de credenciales de inicio de sesión.



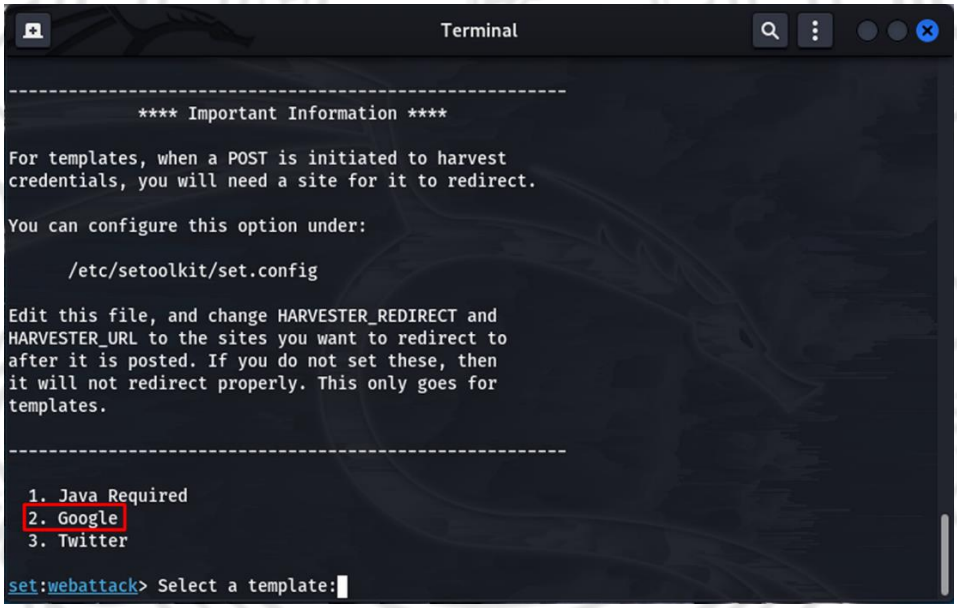
Dentro de este menú se tienen 3 algoritmos útiles, se pueden usar plantillas de algunas páginas web o se puede usar un algoritmo que puede clonar una página web. En este caso es necesario usar una plantilla de página web que solicite las credenciales de acceso a cuentas de Google como es el caso de las cuentas institucionales de la entidad, para hacer esto se puede usar alguna de las plantillas prediseñadas de la opción 1.



El programa solicita que se especifique una dirección IP sobre la cual montar el servicio http con la plantilla de la página web, esta puede dejarse por defecto para usar la dirección de la máquina virtual.

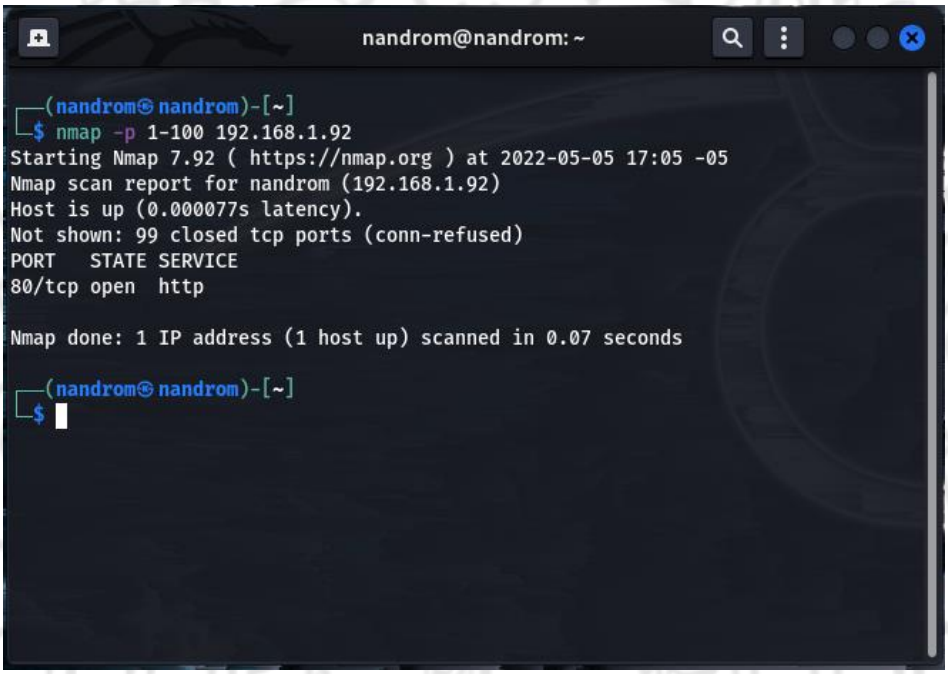


Ahora el programa solicita que se especifique la plantilla que se va a usar, en este caso se emplea la de Google para capturar credenciales de Gmail.



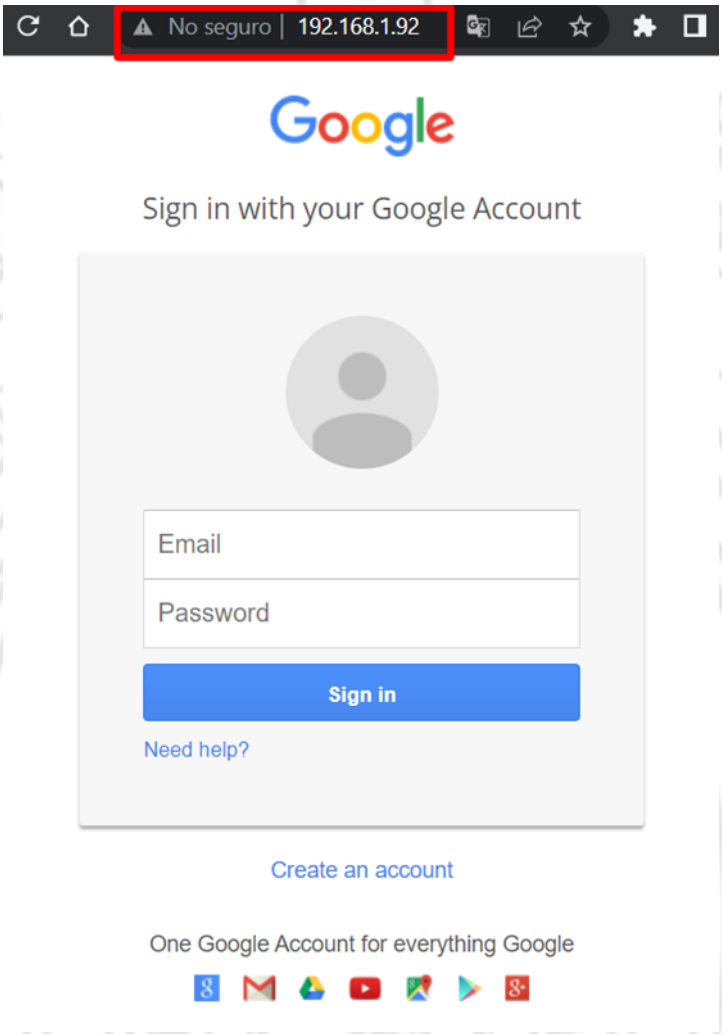
Una vez terminada la configuración, el programa inicia el servicio http en el puerto 80 por defecto, por lo que para cualquier equipo conectado a la misma red se puede acceder a la página web clonada desde el navegador invocando una solicitud HTTP, lo cual se hace ingresando la dirección http://192.168.1.92 en este caso.

Usando la herramienta ***nmap***[12] en una nueva terminal, la cual permite analizar dispositivos de la red en busca de puertos a la escucha de conexiones, se puede hacer un análisis apuntando a la misma dirección de la máquina, especificando el intervalo de puertos que se desea analizar, el resultado indica que el puerto 80 correspondiente al servicio http se encuentra a la espera de conexiones.



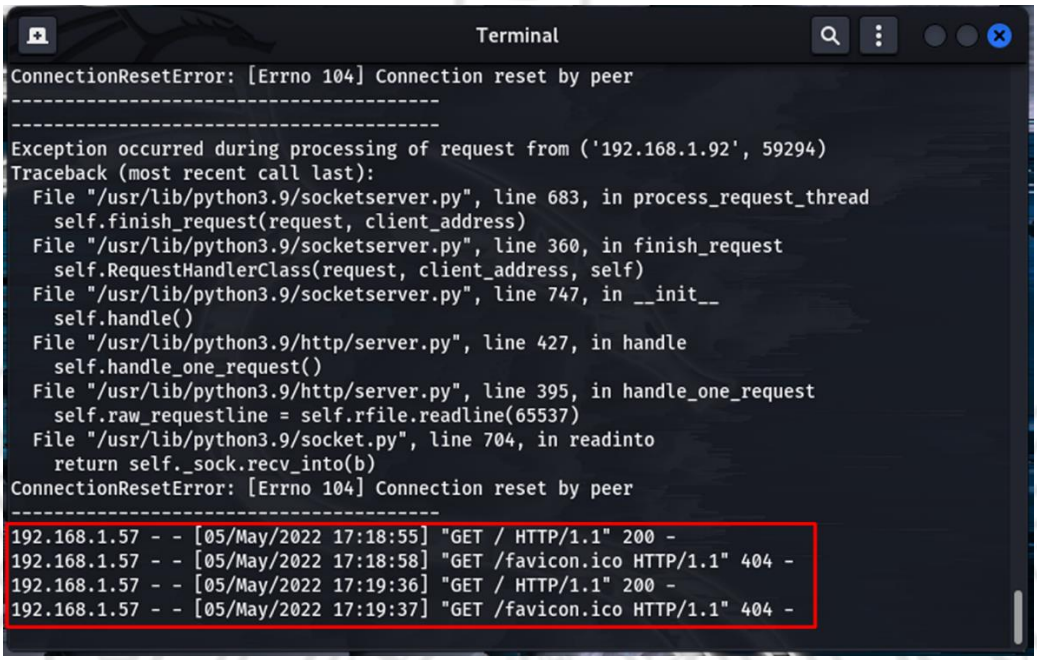
Al entrar al enlace contenido en el correo electrónico, los asistentes eran redirigidos a la siguiente página web, en la cual se nota que el enlace se aloja en una dirección IP sin traducción de nombres de dominio DNS[13], además el navegador muestra la alerta de sitio ***No seguro*** por la ausencia del protocolo https.

[12] Software para rastreo de puertos
[13] sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP

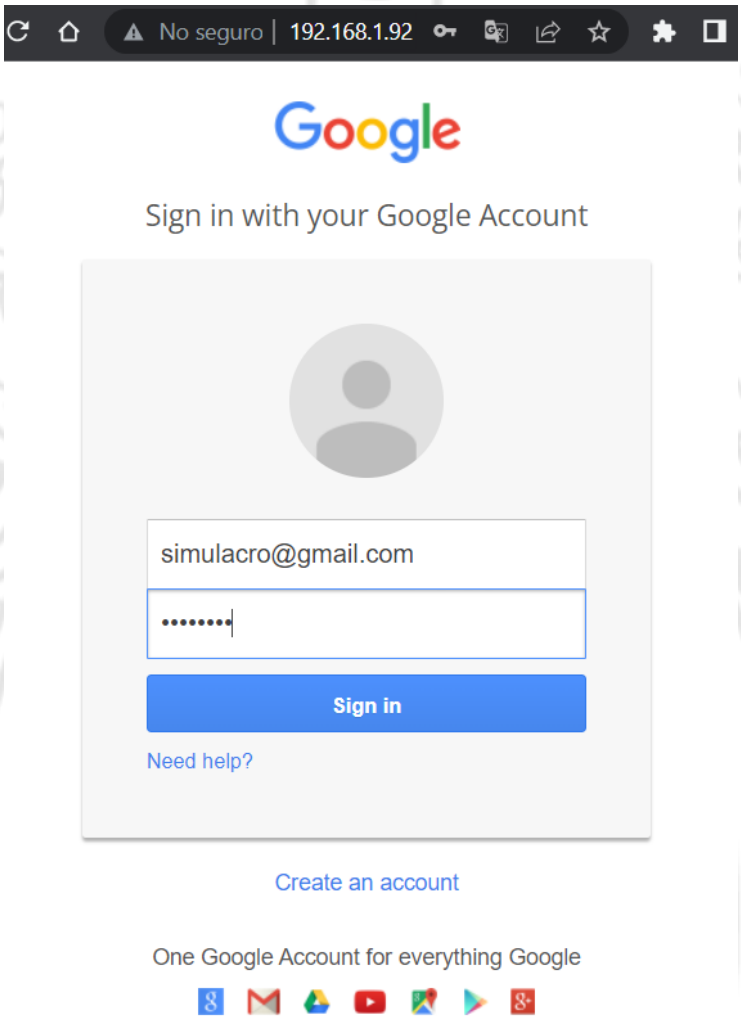


Volviendo a la herramienta ***SET***, en la consola se ve como registra de forma exitosa el handshake[14] del protocolo y se entrega la página de forma exitosa con la bandera 200[15].

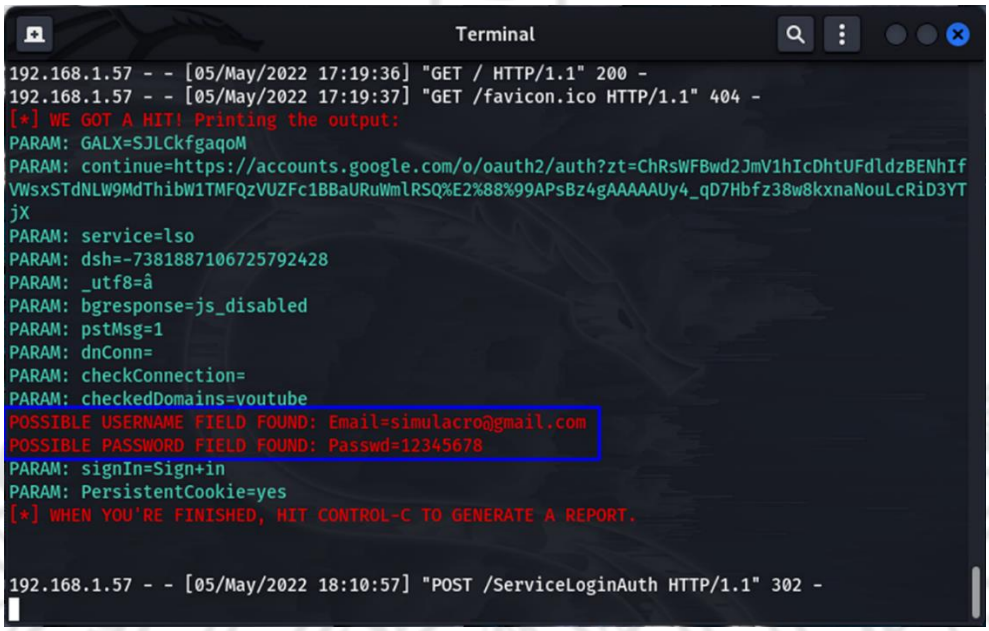
[14] Tipo de señalización utilizado para establecer una comunicación entre sistemas.
[15] En http es la bandera que indica que la conexión es exitosa.



De forma controlada se solicitaba a los asistentes que entraran al link y se hiciera un análisis de las características que sugerían que se trataba de una página falsificada. Después de ellos se solicitó que ingresaran información en los campos, enfatizando en que no fuera información real de sus cuentas de correo, tanto institucionales como personales.



Finalmente, tras el ingreso de información con el botón **Sign in**, los asistentes eran reenviados a la página real de Google, pero las credenciales eran dirigidas hacia el servidor web creado en la red local con la máquina virtual y se muestran en la consola del programa, la cual se proyectó a los asistentes para que visualizaran el resultado del simulacro, con lo cual quedaba en evidencia que las credenciales que habían ingresado en los campos de texto de página web habían sido hackeados.



Al final del ejercicio, los asistentes adquirieron conocimientos que puede ayudarlos a mitigar el efecto de los intentos de ataques phishing en sus correos electrónicos, lo que automáticamente genera el mismo efecto en las redes de las entidades donde se imparten las charlas. La mejor forma de mejorar la seguridad de un sistema es dar la capacidad a los usuarios de identificar amenazas y emprender acciones para evadir los riesgos de una intrusión o una infección.

8. Corrección de vulnerabilidades prioritarias

Se dio atención a las necesidades de seguridad más urgentes, las vulnerabilidades con un mayor grado de criticidad deben atenderse de forma prioritaria, así como crear jornadas pedagógicas en temas de TI en general y de seguridad de la información, haciendo especial énfasis en que los usuarios somos los elementos más vulnerables en la red, en la que los delincuentes informáticos se valen de la inocencia y el desconocimiento de las personas.

Las vulnerabilidades más críticas están directamente relacionadas con el software obsoleto, el uso de sistemas operativos sin soporte, como el caso de Windows 7 y Windows 8 de Microsoft, dichos sistemas operativos contienen vulnerabilidades conocidas que pueden ser fácilmente explotadas sin el refuerzo de un software de antivirus o un firewall.

La medida que se está tomando de forma paulatina es la de readecuar los equipos para que puedan soportar Windows 10 y Windows 11, también de Microsoft, esto con el fin de tener en toda la administración municipal versiones de sistemas operativos que reciban actualizaciones constantes y vigentes que incluyen

parches de seguridad para vulnerabilidades de **día cero**[16], opciones de optimización y servicios esenciales para la seguridad del software. Adicionalmente tras la adquisición de 100 licencias de antivirus se ha hecho la instalación del mismo en los equipos para dar seguridad extra.

Sede	Oficina	Número de equipos	Información de sistema			Numero de impresoras
			Windows 7	Windows 10	Otro S.O	
Inspección Rural Palermo	Inspección	2	1	1	0	2
Parque Educativo Cártama	Sala de informática	15	0	15	0	0
	Portátiles de uso académico	50	0	50	0	0
	Oficina de comunicaciones	5	0	5	0	1
	Oficina Principal	1	1	0	0	0
Casa de la mujer y adulto mayor	Oficina principal	5	0	5	0	1
	Sala de informática	16	0	16	0	0
Casa del deporte	Oficina principal	5	0	5	0	1
Casa de la cultura	Oficina secretaria de cultura	1	0	1	0	1
	Biblioteca	3	0	3	0	1
Casa de Gobierno	Banco de proyectos	5	0	5	0	1
	Sisbén	2	0	2	0	1
	Archivo	4	2	2	0	1
	Hacienda	8	0	8	0	1
	Comisaria de familia	4	1	3	0	0
	Despacho Alcaldía	2	0	2	0	1
	Enlace victimas	1	0	1	0	0
	Jurídica	2	0	2	0	0
	Oficina de control interno	1	0	1	0	0
	Inspección de policía y transito	2	0	2	0	0
	Oficina de Gobierno y participación ciudadana	2	0	2	0	0

[16] Fallo de seguridad que no ha sido detectado por el desarrollador.

	Educación	5	0	5	0	1
	Catastro	3	0	3	0	0
	Planeación	6	0	6	0	2
Desarrollo rural	Oficina de Desarrollo Rural	6	0	6	0	1

Tabla 3. Ultima actualización del inventario de equipos de cómputo.

Lo que se muestra en la tabla 3, es el proceso que se ha hecho desde la estructuración del área de sistemas y la mesa de ayuda que viene operando desde el 17 de enero de 2022 hasta la fecha de entrega del presente informe.

Tal vez una de las actividades más importantes para la mejora de la protección ha sido las capacitaciones sobre seguridad digital que se han impartido, con estas se busca crear y fortalecer la cultura de las tecnologías de la información y la seguridad digital para el trabajo.

Figura 6. Jornadas pedagógicas (Foto del 25 de febrero 2022)

9. Establecimiento del comité MIPG para las políticas de Seguridad Digital y Gobierno Digital

La creación del comité que incluya personal de sistemas, personal encargado del control interno, coordinador y demás personas implicadas en el desempeño de las actividades del Modelo Integrado de Planeación y Gestión, es de vital importancia para la evaluación de los lineamientos y el enfoque de la guía y que permita

formulación de un proyecto también desde lo administrativo que tenga en cuenta su viabilidad desde varios aspectos. Esté comité es el encargado de la coordinación, evaluación y aprobación de los proyectos que se redacten para la Administración Municipal, eso incluye la guía anexa al presente trabajo.

De acuerdo con las directivas del Modelo Integrado de Planeación y Gestión, se crea el comité MIPG, el cual se encarga de diseñar y evaluar los métodos para la adecuada gestión de las políticas administrativas de acuerdo con los lineamientos establecidos en los diferentes ministerios. En este caso, el ministerio de las TIC (MinTIC) establece la política de Gobierno Digital y Seguridad Digital, para la vigilancia de los 5 pilares de la adecuada gestión de los procesos relacionados con temas TIC.

De modo que el comité que coordina las tareas en lo que se refiere a Gobierno Digital en la Alcaldía Municipal de Támesis queda conformada como sigue.

Comité MIPG		
Nombre	Cargo	Rol
Anyi Milena López Rendón	Coordinadora MIPG	Coordinadora
Carlos Mario Velásquez Ramírez	Banco de proyectos	Apoyo
Diego Alejandro Builes	Control Interno	Revisor
Andres Mauricio Román Toro	Administrador de redes y plataformas	Gobierno Digital y Seguridad Digital
Daniel Darío Marín Paniagua	Secretario de Gobierno	Supervisor
María Elcy Ospina Mejía	Secretaria de Planeación	Supervisora

Tabla 4. Conformación del comité MIPG para las políticas de Gobierno Digital y Seguridad Digital.

Actualmente el comité coordina las actividades de Gobierno y Seguridad Digital, y la elaboración de varios proyectos relacionados con tecnologías de la información. Entre los proyectos esta la elaboración del Plan Estratégico de las Tecnologías de la información (PETI) y el Modelo de Seguridad y Privacidad de la Información, del cual hace parte el presente proyecto.

10. Plan de seguridad informática

La creación de una guía general de aplicación a la red de datos de la alcaldía basado sobre todo en la guía número 3 de MSPI del MinTIC apoyado en las métricas y recomendaciones de la norma ISO 27001, que integre seguridad del recurso humano, gestión de activos, control de acceso, seguridad física y del entorno, así como la adquisición, desarrollo y mantenimiento de sistemas de información y la creación de planes de acción de incidentes de seguridad de la información.

Políticas y objetivos de seguridad de la información

Los Sistemas de Gestión de la Seguridad de la Información (SGSI) son marcos para proteger la información al interior de una red, que puede ser adaptada para su aplicación en organizaciones de todo tipo y dimensión; la importancia de su fundamentación en la norma ISO 27001, viene de la importancia y la necesidad de garantizar la integridad, disponibilidad y confidencialidad de los datos al interior de la organización y que es vital para su correcto funcionamiento y optimo desempeño. Las organizaciones más expuestas a los riesgos relacionados con la seguridad de la información eligen cada vez más implementar un SGSI que cumpla con la norma ISO 27001.

Las políticas de seguridad informática generalmente son un documento breve de alto nivel que detalla el principal objetivo del SGSI. Dado que es común que las organizaciones ignoren la importancia que estas tienen para la seguridad de la información.

El fin de estos documentos es que las áreas administrativas de la organización definan lo que se quiere conseguir al implementar la norma ISO 27001 y comprender bajo que herramientas se dará control de lo que suceda en la entidad en lo que se refiere a seguridad de la información.

Se anexa al presente proyecto ***El Plan de Seguridad Informática Para el Sistema de Información de la Alcaldía Municipal de Támesis***. Los datos recopilados como hojas de vida de equipos, topologías de red, metodologías demás datos técnicos no son consignados en este trabajo por considerarse privados y confidenciales, la Alcaldía se reserva dicha información hasta que el Plan Estratégico de las Tecnologías de la Información sea publicado.

11. Conclusiones

La recopilación de los valores de los activos, aunque no de forma precisa, permitió completar el análisis y extraer resultados con lo que se pudieron evidenciar los riesgos de seguridad que podrían estar afectando el desempeño de las diferentes áreas y la seguridad de estas. Algunas de las vulnerabilidades pueden ser subsanadas con la aplicación de ciertas técnicas que no demandan demasiados recursos, como las jornadas pedagógicas, otras vulnerabilidades a diferencia requieren de un diseño y una planificación exhaustiva que requiere de una inversión considerable.

El desarrollo de una política de Seguridad en cualquier organización cubre la gran parte de los aspectos que componen un Sistema de Gestión de la Seguridad de la Información. El análisis de riesgos permitió tener una noción real del estado actual de la empresa a nivel de seguridad en el entorno relacionado con el Datacenter. El análisis realizado a partir de la norma ISO/IEC 27001:2013 permitió identificar la necesidad de implementar un plan y una política de seguridad, con el fin de mitigar los riesgos o vulnerabilidades a los que pueda estar expuesta la organización. Con la implementación de la herramienta de monitoreo, aplicando los controles de seguridad pertinentes y haciendo uso de la zonificación de red establecida se logró evidenciar que es posible mitigar vulnerabilidades de los sistemas, haciendo de estos unos equipos con alto nivel de seguridad. Con el desarrollo de este trabajo se logró el cumplimiento del 100% de los objetivos planteados a corto plazo, aun hacen falta procedimientos de hardening más exhaustivos que ayuden a mitigar aún más los riesgos.

12. Referencias Bibliográficas

MinTIC: *Política de Gobierno Digital*. [Consultado: 25 de febrero de 2022]. https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/

MinTIC: *¿QUÉ ES EL MSPI?*. [Consultado: 30 de Marzo de 2022] https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

Ladino, M. I., Villa, P. A., & López, A. M. (2011). Fundamentos de iso 27001 y su aplicación en las empresas. *Scientia et technica*, *17*(47), 334-339.

Urbina, G. B. (2016). *Introducción a la seguridad informática*. Grupo editorial PATRIA.

BlogSEAS, *Hardening: qué es y cómo endurecer las medidas de seguridad informáticas, [Consultado 1 de marzo de 2022]. https://www.seas.es/blog/informatica/hardening-que-es-y-como-endurecer-las-medidas-de-seguridad-informaticas/*

Página Web. Administración Municipal de Támesis – Antioquia. http://www.tamesis-antioquia.gov.co/

ACADEMIA. Conceptos básicos en buenas prácticas en gestión de TI y seguridad de la información. {En línea}. {Consultado mayo 2022}. Disponible en: https://www.academia.edu/11494593/Conceptos_basicos_en_buenas_practicas_de_TI_y_seguridad_informatica

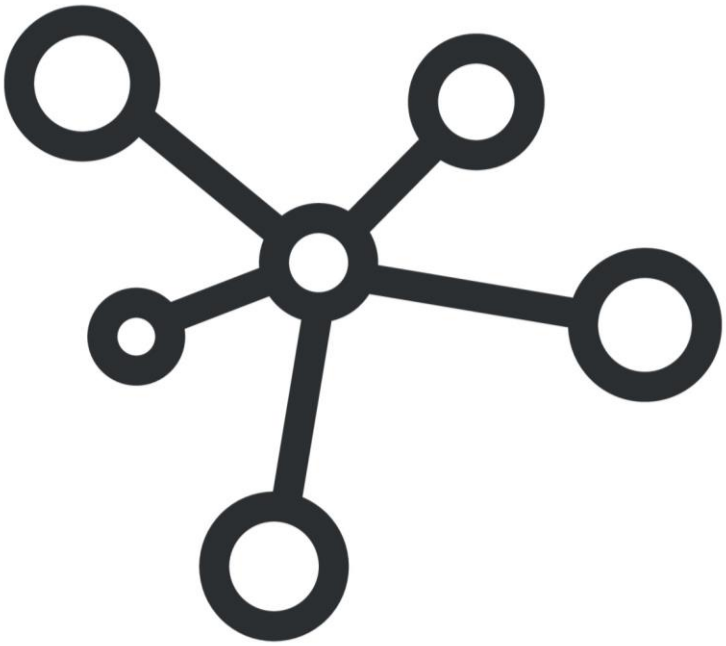
CISCO. Ciberseguridad. {En línea}. {Consultado mayo 2022}. Disponible en: https://www.cisco.com/c/es_co/solutions/smb/security/infographic-basic-concepts.html

MINIEDUCACIÓN. MANUAL DE SEGURIDAD INFORMÁTICA. {En línea}. {Consultado junio 2022}. Disponible en: https://www.mineducacion.gov.co/1759/articles-322548_Manual_de_Seguridad_Informatica_.pdf

MUÑOZ ÑAUTA, J. D. (2016). Diseño de políticas de seguridad informática para la dirección de tecnologías de la información y comunicación (DTIC) de la Universidad de Cuenca. Obtenido de Repositorio Digital de la Universidad de Cuenca: http://dspace.ucuenca.edu.ec/handle/123456789/25646

SEGU-INFO. Implementación de una Política de Seguridad. {En línea}. {Consultado junio 2022}. Disponible en: https://www.segu-info.com.ar/politicas/implementacion

PLAN DE SEGURIDAD INFORMÁTICA PARA EL SISTEMA DE INFORMACIÓN DE LA ALCALDÍA MUNICIPAL DE TÁMESIS.



Municipio de Támesis-Antioquia

Versión 2.0

2022

Contenido

Índice de tablas

Índice de ilustraciones

1. INTRODUCCIÓN.

El desarrollo de los procesos en el escenario de planeación, ejecución y control de las operaciones representa actividades tan complejas que sin la ayuda de las tecnologías de la información y las comunicaciones no sería posible prestar un servicio adecuado. Con el soporte de la informática se incrementa eficientemente los indicadores generales de desarrollo, en este caso haciendo cumplimiento al plan de desarrollo ***¡Támesis nos pertenece!***

El plan de desarrollo en su estructura refiere a la LINEA 3: BUEN GOBIERNO PARA CONSTRUIR CONFIANZA COMPONENTE, 3.1 UN GOBIERNO ABIERTO NOS ACERCA, Y PROGRAMA: 3.1.2 CONSTRUYENDO UN TERRITORIO INTELIGENTE. Además del soporte jurídico cuando: "Ley 1273 de 2009, Por medio de la cual 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"

2. JUSTIFICACION

La Alcaldía de Támesis, en el desarrollo de sus actividades como administración municipal, cimienta y hace uso constante de tecnologías informáticas para la generación, tratamiento y preservación de información relativa a los diferentes procesos emprendidos en pro del desarrollo del territorio y el bienestar de los tamesinos. Sin embargo, la alta vulnerabilidad de la información en la administración municipal es evidente, en especial en los tiempos que transcurren, con la masificación del uso de medios informáticos y la aparición de cada vez más vulnerabilidades ha puesto en evidencia que los sistemas de información de la organización no están evolucionando al mismo ritmo de las tendencias actuales, lo que ha propiciado escenarios de vandalismo, sabotaje, fraudes y aspectos antrópicos valiéndose de la versatilidad del crimen computacional, lo que por desgracia ha dejado referencia de ataques a las secretarias de despacho y activa las alarmas en cuanto a la seguridad informática de la Alcaldía de Támesis.

En ese orden de ideas, la información que se proyecta es un patrimonio material importante, donde los datos intelectuales, procesos y procedimientos, son un baluarte local al servicio comunitario; por lo tanto "Definir, lograr, mantener y mejorar la seguridad de la información puede ser esencial para mantener una eficacia en la operación de las actividades del organismo, al igual que plan de contingencia"

3. OBJETIVOS

3.1 GENERAL

Generar estrategias que reduzcan la perdida de información en las diversas plataformas tecnológicas, garantizando mecanismos de seguridad permanente con sus respectivos planes de contingencia para un servicio efectivo a la comunidad tamesina.

3.2 ESPECIFICOS

- ✓ Identificar las fases del Modelo de Seguridad y Privacidad de la Información.
- ✓ Orientar el cumplimiento del MSPI para el cumplimiento de las políticas de seguridad de la información.
- ✓ Promover la cultura de seguridad y privacidad como pilar fundamental del ejercicio de la gobernanza.
- ✓ Garantizar el manejo correcto de la información pública, mediante buenas prácticas de tratamiento de información institucional.
- ✓ Hacer de conocimiento publico los porcentajes de avances y tiempos estimados de la implementación del Sistema de Gestión de la Seguridad de la Información.

4. FUNDAMENTOS

4.1 MISION

Mejorar la calidad de vida de los habitantes del municipio de Támesis; desarrollando la ruralidad, potenciando la sostenibilidad agroambiental y turística del Municipio; orientado por los Objetivos de Desarrollo Sostenible y apoyado en alianzas estratégicas pertinentes en un escenario de recuperación socioeconómica post COVID-19.

4.2 VISION

El municipio de Támesis-Antioquia para el 2030 será reconocido como ejemplo de sostenibilidad agroambiental y ecoturístico; libre de minería metálica, promotor y defensor de sus riquezas hídricas, paisajísticas, arqueológicas, biodiversas, socioculturales; con altos estándares de calidad de vida rural; con excelentes niveles de resiliencia colectiva para afrontar las crisis; aportante significativo en la reducción del impacto del cambio climático y que colaborativamente se asocia armónicamente a su entorno natural.

4.3 PRINCIPIOS DE BUEN GOBIERNO PARA LA CONFIANZA [1]

1. El Gobierno Municipal actuará en el desempeño de sus funciones de acuerdo con la Constitución Nacional, la normatividad legal y reglamentaria; obrando conforme a los principios democráticos, participativos y pluralistas.

2. ***Las actuaciones*** del Gobierno Municipal se regirán por la eficiencia y la eficacia, defendiendo los intereses generales de la comunidad con honestidad, objetividad, imparcialidad, austeridad, responsabilidad y cercanía a la ciudadanía.

3. ***Mejoraremos*** los modelos de gestión administrativa y aseguraremos a la comunidad tamesina un buen Gobierno Municipal, que garantice la equidad y promueva la solidaridad comunitaria.

4. ***Fomentaremos*** la transparencia y la democracia promoviendo el control ciudadano, facilitando el acceso oportuno y veraz a la información y publicando y difundiendo la actuación del Gobierno Municipal.

5. ***Trabajaremos*** en favor de la inclusión social y del equilibrio territorial entre la cabecera municipal, centros poblados de los corregimientos y las veredas, acercando los servicios administrativos a la ciudadanía y la atención a la población vulnerable como niñas y niños, jóvenes, indígenas, personas de la tercera edad, población en situación de discapacidad física o mental, víctimas del conflicto armado y madres o padres cabeza de familia.

[1] Vásquez Hincapié Juan Martín, Plan de desarrollo – 2020-2023

6. ***Valoraremos*** responsablemente la voluntad de la ciudadanía y actuaremos con coherencia política para garantizar la pluralidad.

7. ***Garantizaremos*** la independencia de los poderes públicos y facilitaremos su colaboración en función del interés general.

8. ***En el Gobierno Municipal*** promoveremos y respetaremos los derechos humanos, la diversidad étnica y cultural y los valores cívicos; facilitando el ejercicio de los derechos y el cumplimiento recíproco de los deberes y obligaciones de la comunidad en general.

9. ***El Gobierno Municipal*** se abstendrá de ejercer sus funciones para favorecer intereses privados contrapuestos al interés general.

5. POLÍTICAS DE SEGURIDAD

Son el conjunto de leyes, reglas, protocolos y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de la seguridad informática. Así mismo definen los lineamientos encargados de juzgar lo permitido y lo prohibido, así como las herramientas y los procedimientos necesarios en la toma de decisiones basados o que hagan uso de las tecnologías informáticas, pero también aquellas decisiones en cuanto a la organización y el manejo de los mismos recursos informáticos y de la información.

El desarrollo e implantación de política de seguridad informativa es indicación de las buenas prácticas administrativas de la organización. Al implantarse las políticas de seguridad deben atender a los siguientes principios y garantías.

6. PRINCIPIOS Y GARANTÍAS.

Responsabilidad individual: Los miembros de la organización deben estar conscientes de sus actividades, que estas serán registradas y monitoreadas.

Autorización: Son las reglas que especifican quien, cuando, como puede acceder a la información.

Confidencialidad: La información solo puede ser accesible por aquellos miembros autorizados.

Integridad: es la salvaguarda y garantía de la exactitud y totalidad de los datos.

Disponibilidad: capacidad de acceso a la información y los recursos alusivos a su almacenamiento y procesamiento para los miembros autorizados de la organización.

Separación de obligaciones: las funciones deben estar divididas entre las personas encargadas de las mismas funciones.

Autenticidad: que se garantice la validez de la información para todos los miembros con acceso, que las copias y distribución sean concordantes entre sí.

Mínimo Privilegio: los miembros deben contar con la menor cantidad de permisos posible, necesarios para la realización de sus funciones.

Auditabilidad: las actividades del personal deben ser monitoreadas desde su inicio hasta su término.

Redundancia: la información valiosa debe disponer de copias de sí misma con fines de seguridad.

Irrenunciabilidad: garantía de la toda la comunicación que se envié o se reciba llegue al destinatario final.

Legalidad: referido al cumplimiento de las leyes, normas, reglamentos o disposiciones a las que está sujeta la organización.

Confiabilidad: que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de la misiones y funciones.

Reducción de riesgo: se debe reducir, dentro de los posible, todas las posibles amenazas a la información a un nivel aceptable.

7. METODOLOGIA

Las metodologías presentadas en este documento dentro de la óptica del ISO 27001, los métodos planteados son de fácil aplicación y permiten rápidamente que la organización se estructure de la manera correcta y más eficiente para implantar el diseño.

El modelo está basado en una indagación e investigación descriptiva que consiste en llegar a conocer las actividades, situaciones y metodologías actuales y predominantes a través de la descripción exacta de los procesos internos, la recolección de datos y el personal de la Alcaldía Municipal de Támesis.

El objetivo de estudio es realizar una investigación a profundidad en el marco de referencia de la norma internacional ISO 27001.

8. PROCESO

Con el Sistemas de Gestión de la Seguridad de la Información que actualmente tiene la Administración Municipal de Támesis, donde reconoce los riesgos que aquejan a sus sistemas de información, asumiendo de tal manera que se minimice, transfiera y controle mediante una sistemática definida, documentada y conocida por todos los miembros de la organización y evoluciones en pro de mejorar según las prioridades requeridas.

9. CICLO DE OPERACIÓN MSPI

El ciclo de operación del Modelo de Seguridad Privacidad de la Información de la política de Gobierno Digital está compuesto por 5 fases, permitiendo así que se gestione de manera progresiva en base a actividades, cronogramas y recursos. Por ende, cada fase será sujeta de estudio de manera individual, sin embargo, el avance de casa fase se reflejará como el avance global del MSPI cuyo objetivo es que se pueda gestionar de manera adecuada la seguridad y la privacidad de sus activos de información.

Figura 1. Ciclo de operación del modelo de seguridad y privacidad de la información.[2]

[2] *Figura tomada de la guía Modelo de Seguridad y Privacidad de la Información capítulo 8*

10. PORCENTAJES DETERMINADOS A CADA FASE

La imagen a continuacion denota que cada fase de la implementacion del Modelo de Seguridad y Privacidad de la Informacion tiene un porcentaje asociado que representa el avance global de la implementacion del MSPI en la Alcaldia de Támesis, dichos porcentajes se establecieron como referencia para la entidad y son de carácter interno para la evaluacion del avance, por ende este porcentaje no se debe confundir con el procentaje que arrojan los instrumentos como el diagnostico del Modelo Integrado de Planeacion y Gestion MIPG, ni el instrumento de evaluacion del MSPI o el reporte en el Formulario Unico de Reporte Avance a la Gestion FURAG.

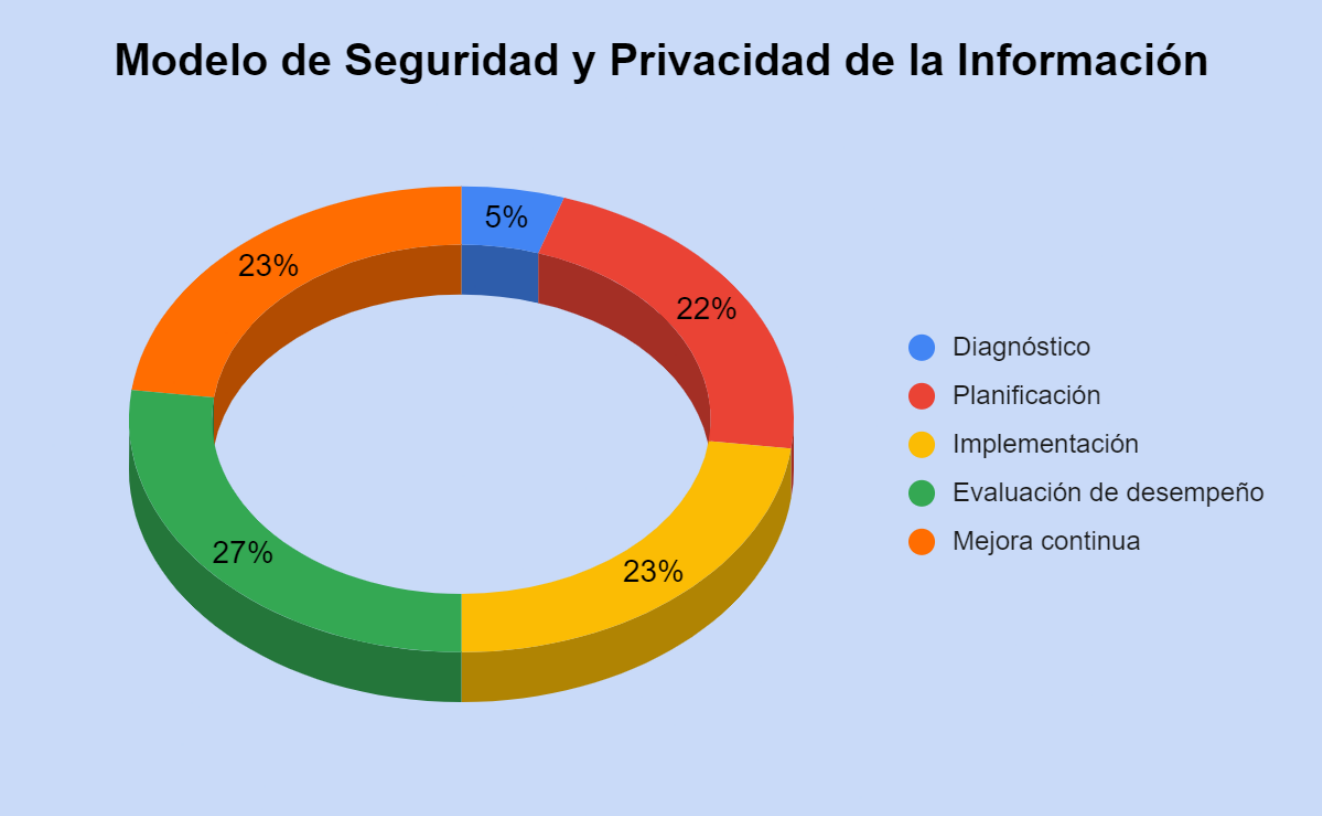


Figura 2. Porcentaje determinado para cada fase del MSPI. [3]

[3] *Fuente. Creación propia*

11. FASES

11.1 Fase de diagnóstico.

La fase diagnostica comprende actividades que se ejecutan con el fin de conocer la situación actual de la entidad en lo que se refiere a seguridad y privacidad de la información, su aplicación permite identificar el nivel de madurez, las vulnerabilidades y otros aspectos relevantes y que demuestran la situación actual en la Alcaldía Municipal de Támesis. Esta fase se convierte en un insumo de vital importancia como cimiento para la siguiente fase de planificación, entendiendo que cada fase esta en concordancia con la siguiente, dando continuidad al ciclo de operación entre fases que se muestra en la Figura 1. Ciclo de operación del Modelo de Seguridad y Privacidad de la Información.

Figura 3. Fase de diagnóstico. [4]

11.1.1 Identificación de los riesgos asociados al Sistema de Información de la Alcaldía Municipal de Támesis.

Se Identificaron los riesgos asociados al sistema de información en la Alcaldía Municipal de Támesis, mediante el Instructivo para gestión de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información según NORMA TECNICA COLOMBIANA ISO 27001.

[4] *Figura tomada de la guía Modelo de Seguridad y Privacidad de la Información capítulo 8.1*

La amplitud del alcance de la Alcaldía Municipal de Támesis se determinará dependiendo de los recursos disponibles, la experiencia y la criticidad de los procesos en relación con los riesgos de información.

11.1.2 Evaluación del nivel del cumplimiento de la norma ISO 27001

Tabla 1. Escala Nivel de Cumplimiento ISO 27001 ANEXO A		
Descripción	**Calificación**	**Criterio**
No aplica	N/A	No aplica
Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Definido	60	Los procesos y los controles s e documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas s e siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua

Tabla 1. Escala Nivel de Cumplimiento

De acuerdo con la Tabla de Escala Nivel de Cumplimiento ISO 27001 (Ver Anexo A) del instrumento Evaluación del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC. Partiendo de la toma de contacto, el análisis y la evaluación de los sistemas de información y del personal que labora en la alcaldía, se puede situar la

calificación del el Sistemas de Gestión de la Seguridad de la Información en la calificación 40 que permite tener un nivel Repetible. El fundamento es que existen protocolos y estándares conocidos para el tratamiento de la información, pero cuya no aplicación no es sancionada y no se cuenta con un documento central que reúna toda la normativa referente a los sistemas de información, como puede ser el caso del Plan Estratégico de las Tecnologías de la Información (PETI) que actualmente está en desarrollo.

11.1.3 Diagnostico del Nivel de Madurez

Modelo de seguridad y privacidad de la información.

De acuerdo con la **- Nivel de madurez Instrumento de MinTIC,** se puede establecer que el nivel de madurez de la Alcaldía Municipal de Támesis es **INTERMEDIO.**

Implementación del levantamiento de información

En esta fase se identificarán aspectos como son los activos de información, comprendidos en el alcance del diseño del SGSI; seguidamente se valorará cada activo con base en la confidencialidad, integridad y disponibilidad. Una vez efectuada la valoración la organización decidirá que activos se consideran importantes para la continuidad de los procesos.

A continuación, se debe identificar y calcular las amenazas y vulnerabilidades para dar tratamiento a los riesgos e iniciar un proceso de toma de decisiones con respecto a cómo se tratará el riesgo, es decir; si los riesgos serán aceptados, transferidos o simplemente se evitarán.

DATOS BÁSICOS	
Tipo de Entidad	Publica
Misión	Mejorar la calidad de vida de los habitantes del municipio de Támesis; desarrollando la ruralidad, potenciando la sostenibilidad agroambiental y turística del Municipio; orientado por los Objetivos de Desarrollo Sostenible y apoyado en alianzas estratégicas pertinentes en un escenario de recuperación socioeconómica post COVID-19.
Análisis de Contexto	https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf
Mapa de procesos	¿?
Organigrama	Ver Figura 4
PREGUNTAS	

Que le preocupa a la Entidad en temas de seguridad de la información?	Algunos de los temas más preocupantes tienen que ver con el historial de ataques y hackeos que tiene la organización, es evidente no solo la falta de políticas de seguridad bien estructuradas, sino lo susceptible de su infraestructura de red a las intrusiones y la relativa facilidad con la que la información institucional puede verse comprometida
¿En qué nivel de madurez considera que está?	INTERMEDIO
¿En qué componente del ciclo considera que va?	PLANIFICACION

Tabla 2. Diagnostico MPSI

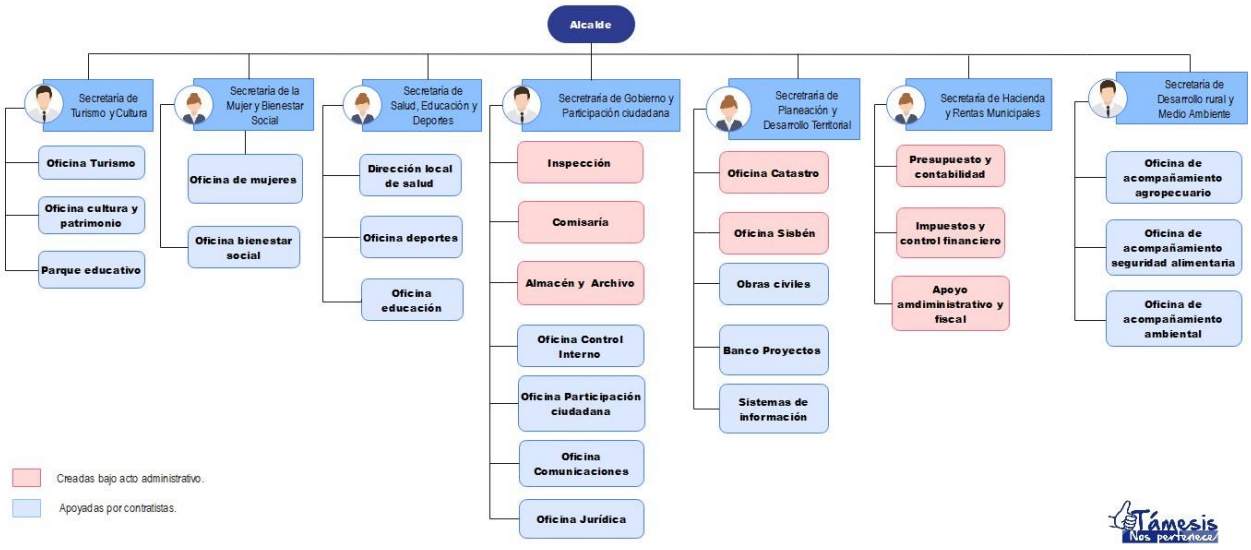


Figura 4. Organigrama Administración Municipal. [5]

[5] Extraído de http://www.tamesis-antioquia.gov.co/alcaldia/organigrama

Tabla de diagnóstico – funcionario.

RESPONSABLE/AREA	TEMA	FUNCIONARIO
Control Interno	Revisiones de seguridad de la información	Departamento de sistemas
	revisión independiente de la seguridad de la información	
	cumplimiento con las políticas y normas de seguridad	
	CUMPLIMIENTO	
	Auditoría Interna Plan	
	Auditoría interna, ejecución y subsanación de hallazgos	
Líder de proceso 1	**Administración del Servidor**	Departamento de sistemas
	Revisión semanal estado del servidor.	
Líder de proceso 2	**Actualización de los Back-up de la información**	Departamento de sistemas
	Realización de backups, cada dos meses al personal administrativo	
Líder de proceso 3	**Control y revisión de la ejecución de la política de Seguridad de la Organización.**	Departamento de sistemas
	Revisión y ejecución de los procedimientos semanales de las políticas de seguridad, donde se verifica si las políticas se están ejecutando.	
Responsable de compras y adquisiciones	Relaciones con los proveedores	Asistente de Gobierno
	Seguridad de la información en las relaciones con los proveedores	
	Gestión de la prestación de servicios de proveedores	

Tabla 3. Diagnostico – funcionario.

El departamento de sistemas está conformado por dos contratistas, Brian Leandro Bermúdez Agudelo (Tecnólogo en mantenimiento de equipos de cómputo, diseño e instalación de cableado estructurado) encargado de mantenimiento, comunicaciones y sonido, y Andres Mauricio Roman Toro (Estudiante de Ingeniería de Telecomunicaciones) Administrador de redes de datos, plataformas institucionales y políticas de Seguridad Digital y Gobierno Digital.

11.1.4 Avance

A continuación, en la Tabla 4, se muestra el avance de la fase de diagnóstico, en la que se especifica el numero de actividades realizadas en esta fase, el tiempo empleado, la dependencia encargada, la dependencia que apoya la gestión, el porcentaje de avance y la vigencia de las actividades. Ya se ha concluido la recolección de información de la fase de diagnóstico, por lo que se tiene un avance del 100%, aun así, ni los activos, ni el personal, ni las circunstancias permanecen inmutables, por lo que las actividades de recolección de información y de diagnostico de los sistemas se realizan y actualizan de forma constante.

Avance de la Fase de Diagnostico	
Tiempo estimado de ejecución	3 meses
Dependencia a cargo	Secretaria de Gobierno
Dependencias adicionales involucradas	Secretaria de Planeación
Cantidad de actividades a realizar	3
Fase en ejecución	Si
Porcentaje de avance	100%

Tabla 4. Avance de la Fase de Diagnóstico[6]

11.2 Fase de planificación.

La fase de planificación concierne en la interpretación y el procesamiento de la información obtenida en la fase anterior, con esta se planea y se ejecutan las acciones con base en las necesidades que se han podido identificar. Esta fase se planea y se ejecuta ajustando el MSPI a los objetivos, misión, visión, necesidades y demás requerimientos determinados para preservar la confidencialidad, disponibilidad, integridad y privacidad de los activos de información de la Alcaldía de Támesis, para ello se requiere la conformación de equipos interdisciplinarios para dar paulatino cumplimiento a cada una de las actividades en esta fase.

En esta fase lo más importante es entender el contexto de la entidad y así generar acciones que suplan las necesidades y que estos procesos estén razonables a la realidad de la capacidad humana y económica para dicha implementación del MSPI. También demuestra el compromiso de la alta dirección para la implementación de este mediante la Política General de Seguridad y Privacidad de la Información.

[6] Fuente. Elaboración propia

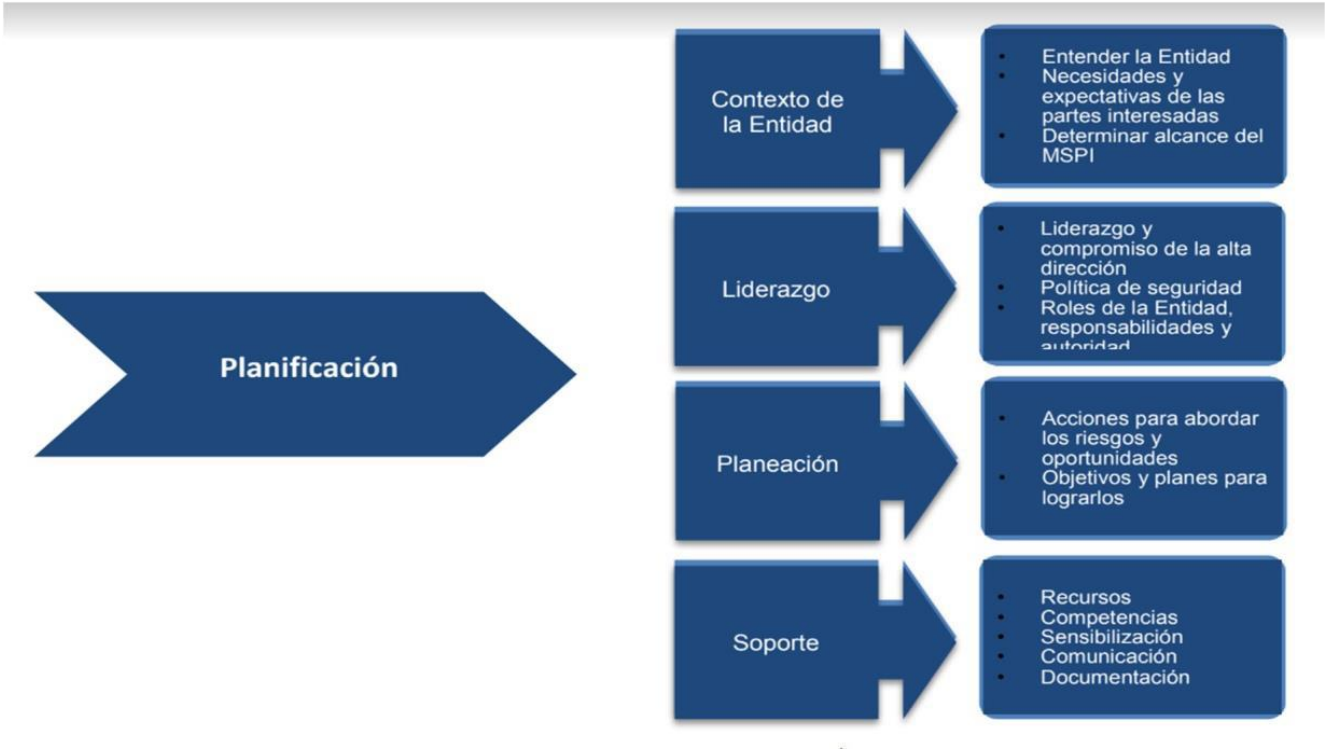


Figura 5. Fase de planificación. [7]

11.2.1 Marco Normativo

Este plan estratégico de seguridad, se desarrolla el siguiente marco legal.

NORMA	DESCRIPCION
Decreto 1151 de 2008	Lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.
Ley 1955 del 2019	Establece que las entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).
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.

[7] Figura tomada de la guía Modelo de Seguridad y Privacidad de la Información capítulo 8.2

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-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
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 1753 de 2015	Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "TODOS POR UN NUEVO PAIS" "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 962 de 2005	El artículo 14 lo siguiente "Cuando las entidades de la Administración Pública requieran comprobar la existencia de alguna circunstancia necesaria para la solución de un procedimiento o petición de los particulares, que obre en otra entidad pública, procederán a solicitar a la entidad el envío de dicha información. En tal caso, la carga de la prueba no corresponderá al usuario. Será permitido el intercambio de información entre distintas entidades oficiales, en aplicación del principio de colaboración. El envío de la información por fax o por cualquier otro medio de transmisión electrónica, proveniente de una entidad pública, prestará mérito suficiente y servirá de prueba en la actuación de que se trate, siempre y cuando se encuentre debidamente certificado digitalmente por la entidad que lo expide y haya sido solicitado por el funcionario superior de aquel a quien se atribuya el trámite".
Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establece las entidades de certificación y se dictan las dictan otras disposiciones.
Ley 734 de 2002	Por la cual se expide el *Código Disciplinario Único.*
Ley 1437 de 2011	Por la cual se expide el *Código de Procedimiento Administrativo* y de lo *Contencioso Administrativo.*
Ley 1474 de 2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión publica
Decreto 4485 de 2009	Por medio de la cual se adopta la actualización de la Norma Técnica de Calidad en la Gestión Pública.
Decreto 235 de 2010	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.
Decreto 2364 de 2012	Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
Decreto 2693 de 2012	Por el cual se establecen los lineamentos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de

	2009, 1450 de 2011, y se dictan otras disposiciones.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012" o Ley de Datos Personales.
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 2433 de 2015	Por el cual se reglamenta el registro de TIC y se subroga el título 1 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1081 de 2015	Por medio del cual se expide el *Decreto Reglamentario Único del Sector Presidencia de la Republica*
Decreto 124 de 2016	Por el cual se sustituye el Titulo 4 de la Parte 1 del Libro 2 del Decreto 1081 de 2015 relativo al *Plan Anticorrupción y Atención al Ciudadano*.
Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las Comunicaciones.
Decreto 728 de 2017	Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
Decreto 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
Decreto 612 de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 2106 del 2019	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública Cap. II Transformación Digital Para Una Gestión Pública Efectiva.
Decreto 620 de 2020	Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

Resolución 2710 de 2017	Por la cual se establecen los lineamientos para la adopción del protocolo IPv6.
Resolución 3564 de 2015	Por la cual se reglamentan aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.
Resolución 3564 2015	Reglamenta algunos artículos y parágrafos del Decreto número 1081 de 2015 (Lineamientos para publicación de la Información para discapacitados).
Norma Técnica Colombiana NTC 5854 de 2012	Accesibilidad a páginas web El objeto de la Norma Técnica Colombiana (NTC) 5854 es establecer los requisitos de accesibilidad que son aplicables a las páginas web, que se presentan agrupados en tres niveles de conformidad: A, AA, y AAA.
CONPES 3292 de 2004	Señala la necesidad de eliminar, racionalizar y estandarizar trámites a partir de asociaciones comunes sectoriales e intersectoriales (cadenas de trámites), enfatizando en el flujo de información entre los eslabones que componen la cadena de procesos administrativos y soportados en desarrollos tecnológicos que permitan mayor eficiencia y transparencia en la prestación de servicios a los ciudadanos.
CONPES 3920 de Big Data, del 17 de abril de 2018	La presente política tiene por objetivo aumentar el aprovechamiento de datos, mediante el desarrollo de las condiciones para que sean gestionados como activos para generar valor social y económico. En lo que se refiere a las actividades de las entidades públicas, esta generación de valor es entendida como la provisión de bienes públicos para brindar respuestas efectivas y útiles frente a las necesidades sociales.
CONPES 3854 Política Nacional de Seguridad Digital de Colombia, del 11 de abril de 2016	El crecimiento en el uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, reflejado en la masificación de las redes de telecomunicaciones como base para cualquier actividad socioeconómica y el incremento en la oferta de servicios disponibles en línea, evidencian un aumento significativo en la participación digital de los ciudadanos. Lo que a su vez se traduce en una economía digital con cada vez más participantes en el país. Desafortunadamente, el incremento en la participación digital de los ciudadanos trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado. Situación que debe ser atendida, tanto brindando protección en el ciberespacio para atender estas amenazas, como reduciendo la probabilidad de que estas sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo.
CONPES 3975	Define la Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los lineamientos para que las entidades públicas del orden nacional elaboren sus planes de transformación digital con el fin de que puedan enfocar sus esfuerzos en este tema.
Circular 02 de 2019	Con el propósito de avanzar en la transformación digital del Estado e impactar positivamente la calidad de vida de los ciudadanos generando valor público en cada una de las interacciones digitales entre ciudadano y Estado y mejorar la provisión de servicios digitales de confianza y calidad.

Directiva 02 2019	Moderniza el sector de las TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones.

Tabla 5. Marco Normativo

11.2.2 Políticas de seguridad y privacidad de la información

- ✓ La Política de Seguridad y Privacidad de la Información es la afirmación general que representa la posición de la Alcaldía Municipal de Támesis, con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información: incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y especificas para la gestión de la seguridad de la información.

- ✓ En la Alcaldía de Támesis, la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la administración de riesgos y la consolidación de una cultura de seguridad.

- ✓ Consciente de sus necesidades actuales, el Municipio de Támesis implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece une cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales. regulatorios vigentes.

La Seguridad de la Información en la Entidad se establece con el objetivo de:

- ✓ Minimizar el riesgo en las funciones más importantes de la entidad.
- ✓ Cumplir con los principios de seguridad de la información.
- ✓ Mantener la confianza de sus usuarios y servidores públicos.
- ✓ Apoyar la innovación tecnológica.
- ✓ Implementar el Plan de Copias de seguridad de la información.
- ✓ Proteger los activos tecnológicos.
- ✓ Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- ✓ Fortalecer la cultura de seguridad de la información en los servidores públicos, practicantes y usuarios de la administración municipal.
- ✓ Garantizar la continuidad de los procesos de la administración frente a incidentes de la plataforma tecnológica

11.2.3 Plan de transición de IPv4 a IPv6

		Diagnostico	Planeación	Implementación	Seguimiento	Lanzamiento
Recurso Humano	**Gerencia de proyecto**	Revisión políticas y plan de trabajo Revisión de manuales de procedimientos Requerimientos y necesidades	Determinación de alcance y tiempo, cronograma, obtención presupuesto y recursos Construcción plan de proyecto y planes específicos	Desarrollo del plan detallado de trabajo del proyecto. Desarrollo de planes específicos	Controles de riesgo. Informes de avance y gestión. Control de alcances, tiempo, costo y calidad. Mediciones de rendimiento, controles de cambios	Acta de cierre de proyecto y aceptación. Cierre de contratos. Entrega documentación y recomendaciones generales.
	Talento Humano	Evaluación de recurso humano equipo de trabajo	Especificación de roles, perfiles y competencias	Desarrollo del equipo de trabajo	Indicadores de gestión y rendimiento. Gestión de equipo de trabajo.	Cierre de contratos
Recurso Técnico	**Infraestructura**	Inventario de activos de información y servicios Diagramas lógicos de interrelación Ingeniería de detalle solución actual. Banco de configuraciones.	Evaluación requerimientos Ingeniería de detalle, diagramas lógicos y de componentes nueva solución Especificación equipos, plan de integración. Protocolo de pruebas. Factores de éxito y aceptación.	Ambiente de coexistencia y pruebas. Conexiones físicas. Gestión de calidad. Control de versiones. Validación de factores de éxito y aceptación.	Controles de cambio, gestión de riesgos, gestión de calidad. Validación factores de éxito y aceptación.	Puesta en producción. Entrega documentación y manuales de usuario. Entrega de configuraciones.
	Aplicaciones	Inventario de aplicaciones Evaluación estado de aplicaciones (Propietario, código fuente,	Evaluación código fuente, interfaces utilizadas. Evaluación de capacidad, estructuras de	Ambiente de coexistencia y pruebas. Modificación librerías, APIs, código fuente, etc.	Controles de cambio, gestión de riesgos, gestión de calidad.	Puesta en producción. Entrega documentación y manuales de usuario.

		derechos de autor) Mapa de comunicaciones por cada aplicación.	datos y lenguajes de programación para soporte de IPV6, convivencia con IPV4. Plan de integración, protocolo de pruebas. Factores de éxito y aceptación.	Ejecución protocolo de pruebas.	Validación factores de éxito y aceptación	
	Seguridad	Revisión de políticas de seguridad. Revisión de inventario de activos.	Plan de seguridad para la coexistencia de los dos protocolos. Protocolo de pruebas de aceptación.	Aseguramiento de servidores y de servicios. Ejecución de pruebas de seguridad.	Gestión de incidentes de seguridad. Gestión de riesgos de seguridad.	Ajustes a políticas de seguridad. Entrega documentación.

Tabla 6. Modelo del proceso de transición[8]

11.2.4 Avance

A continuación, en la Tabla 6, se muestra el avance de la fase de Planificación, en la que se especifica el número de actividades realizadas en esta fase, el tiempo empleado, la dependencia encargada, la dependencia que apoya la gestión, el porcentaje de avance y la vigencia de las actividades. En esta fase se analiza y se procesa la información consolidada en la fase de diagnóstico, actualmente se están sentando las bases de una planificación sólida para la Alcaldía de Támesis, las actividades iniciales en esta fase están orientadas hacia una comunicación interna asertiva y una atención prioritaria de los problemas más urgentes, para ello se ha desarrollado la herramienta ***intranet*** que corresponde al 20% del avance de la fase de planificación.

Avance de la Fase de Planificación	
Tiempo estimado de ejecución	10 meses
Dependencia a cargo	Secretaria de Gobierno

[8] Tomado de "Modelo de Transición hacia IPv6", Velásquez, Jairo Alberto – Cintel, IPv6 Colombia, 2012

Dependencias adicionales involucradas	Ninguna
Cantidad de actividades a realizar	8
Fase en ejecución	Si
Porcentaje de avance	20%

Tabla 7. Avance de la Fase de Planificación.[9]

11.3 Fase de implementación.

Es fundamental reconocer que la información pertenece a un activo material de la entidad pública, en ese caso el municipio de Támesis, donde la Data está al servicio de la comunidad, claro está con los protocolos necesarios del uso adecuado de las diversas fuentes, contenidos propios y exógenos para el desarrollo territorial. De esta forma se requiere un buen uso de ella, de una manera eficiente y oportuna, justamente para rendir a los entes de control, en este caso contraloría y entidades del Estado. De esta forma, "se protege, estos recursos de las amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la información y garantizar la continuidad de los procesos de la entidad, minimizando los riesgos identificados y aportando al correcto complimiento de los objetivos organizacionales. Las Políticas de Seguridad de la Información, surgen como una herramienta institucional de obligatorio cumplimiento y como parte integral de la gestión de la seguridad de la información en la aplicación del Modelo de Seguridad y Privacidad de la información definido por el Ministerio de las Tecnologías de la Información y las Comunicaciones.[10]

[9] Fuente. Elaboración propia.
[10] JUAN CARLOS GRANADOS BECERRA Contralor de Bogotá, D.C

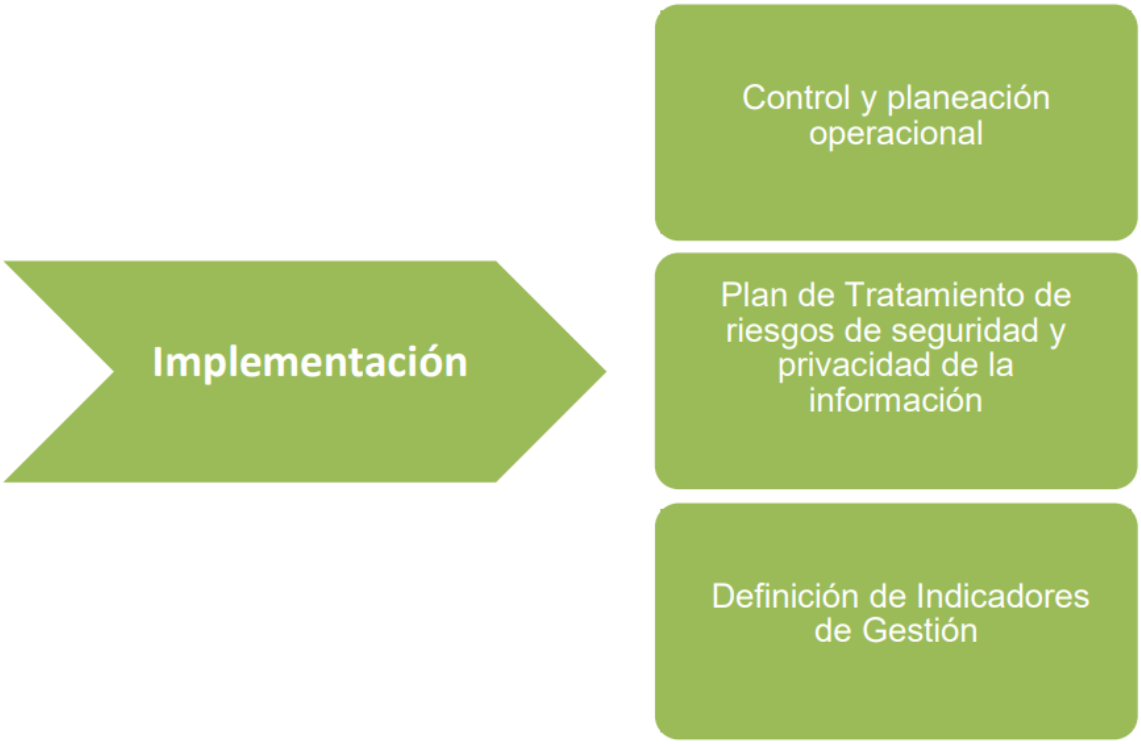


Figura 6. Fase de implementación.[11]

La fase de implementación permite instaurar lo que hasta el momento se ha planificado en la fase anterior, significando así que es la fase donde se genera el compromiso de la alta dirección con la implementación del Modelo de Seguridad y Privacidad de la Información ya que en esta fase se inician los controles y acciones necesarias para resguardar la información de la Alcaldía de Támesis. Iniciando también con todo lo concerniente a un plan trascendental para los sistemas de información y la entidad, no solo para Támesis sino para todas las entidades públicas, las cuales en aras de fortalecer el desarrollo institucional y mejorar de forma significativa la seguridad y la accesibilidad a la información, están en la obligación de crear un Plan de Transición de IPv4 a IPv6.

11.3.1 Establecimiento de políticas de Planificación y Control Operacional.

Los entes de control, reconoce la importancia de la protección de los activos de Información que soportan los procesos de la Entidad, por ello se encuentra comprometida con la implementación de medidas para asegurar su confidencialidad, integridad, disponibilidad y privacidad de acuerdo con las normas legales vigentes, para lo cual,

[11] Figura tomada de la guía Modelo de Seguridad y Privacidad de la Información capítulo 8.3

adopta políticas, procedimientos, lineamientos y asigna responsabilidades para la adecuada gestión de la seguridad de la información.

Todas las personas mencionadas dentro del alcance deberán dar cumplimiento al 100% de las políticas descritas. El incumplimiento a las Políticas de Seguridad de la Información del Municipio de Támesis Antioquia, traerá consigo, las consecuencias disciplinarias, fiscales y penales que apliquen a la Entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a Seguridad y Privacidad de la Información.[12]

Por lo anterior se establecen las siguientes políticas para la Alcaldía Municipal de Támesis.

Política de Confidencialidad de la Información

Esta Política General define los criterios y lineamientos esenciales, en cuanto a la administración, custodia y uso de la información y de los bienes asociados a su tratamiento. La Seguridad de la Información es entendida como la preservación de la confidencialidad, integridad y disponibilidad de la información y la protección de ésta, de una amplia gama de amenazas, a fin minimizar el daño, garantizar la continuidad comercial y maximizar el retorno sobre las inversiones y las oportunidades de negocios.

Para la Alcaldía Municipal de Támesis se establecen las siguientes políticas de confidencialidad de la información.

1. La Información es un bien valioso para la Institución, que debe ser administrada bajo los más altos estándares de seguridad.

2. La información es considerada como un recurso imprescindible para la gestión y operación de la institución.

3. La Seguridad de la Información, es responsabilidad de todos, independiente del cargo que se desempeñe.

4. La información de la organización solo puede ser accedida por funcionarios debidamente autorizados, según las funciones que desempeñe dentro de la alcaldía y con derechos expresamente establecidos en las normas vigentes y con controles que garanticen su protección.

5. La alcaldía declara su decisión de cumplir con la normativa y legislación vigente en relación con aspectos de reserva y privacidad de la información de sus clientes, colaboradores.

6. Todo empleado, proveedor o personal de outsourcing que preste sus servicios a la alcaldía debe acceder únicamente a la información que, de acuerdo a su clasificación, le sea autorizada para las tareas que debe cumplir.

[12] MINTIC Elaboración de la política general de seguridad y privacidad de la información.

7. Todo empleado o colaborador tiene la obligación de notificar cualquier actividad o situación que afecte la Seguridad de los activos de Información.

8. La organización reconoce que la sensibilización, capacitación y entrenamiento adecuados a su personal en las materias de Seguridad de la Información son tareas prioritarias.

9. Las Políticas de Seguridad de la Información regirán independientemente de cómo se presente o almacene la información, los sistemas que la proseen o los métodos de transporte utilizados (Base de Datos, respaldos magnéticos, información impresa, Internet, otros).

10. Las disposiciones relacionadas con las Políticas referidas a la Seguridad de la Información serán debidamente controladas en su cumplimiento por los estamentos definidos por la alcaldía.

11. El incumplimiento de esta política constituirá una falta grave y será sancionado como tal de acuerdo con lo establecido por la alcaldía.

12. Verificar el estado de los medios de almacenamiento en disco duro, cinta u otro dispositivo.

13. Verificar la correcta ejecución de los backups y la integridad de los datos contenidos en ellos.

14. Es deber de los responsables de la información de cada sistema de información verificar la integridad de la información, una vez sea restaurada.

15. Se debe garantizar la salvaguarda de la información que esté alojada en los equipos que requieran servicio de mantenimiento donde se deba reinstalar el sistema operativo, formatear el o los disco(s) duro(s) de que disponga, mediante una copia de respaldo que deberá dejar en Sistemas de Almacenamiento durante el tiempo que dure el mantenimiento y puesta a punto del equipo.

16. Antes de adelantar un mantenimiento correctivo para el caso de daño de un disco duro, el responsable del mantenimiento deberá contar con las herramientas y mecanismos técnicos y tecnológicos para buscar salvar la información almacenada en el dispositivo averiado.

17. Para los Despachos, Oficinas y la Secretarías, la Entidad ha dispuesto un recurso de ***almacenamiento en la red***, donde debe reposar la información propia de su gestión.
    El tipo de información que debe ser resguardada en el servidor de archivos de acuerdo a la Ley 1712 de 2014 es Publica Clasificada Artículo 18 y Pública Reservada. Artículo 19.

18. La información que es considera Pública de acuerdo a la Ley 1712 de 2014 en su artículo 11, debe ser guardada en el ***almacenamiento en la nube***, donde se cuenta con las medidas de aseguramiento y respaldo de la información que cada funcionario allí deposita, por tanto, la Entidad garantiza la disponibilidad de la información allí almacenada.

19. Es deber de los responsables de la información de cada sistema de información verificar la integridad de la información, una vez sea restaurada.

20. Se debe hacer backup de la información contenida en las estaciones de trabajo cuando hay retiro de un funcionario de la Entidad.

21. Por ningún motivo el usuario instalará software de promoción y/o entretenimiento.

22. La adquisición o desarrollo de software será responsabilidad del área de sistemas.

23. El usuario tiene la obligación de proteger las unidades de almacenamiento que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial

24. Es responsabilidad de los usuarios almacenar su información únicamente en la partición de disco duro destinada para ello, en el servidor, unidad extraíble, o en servicios en la nube suministradas o autorizadas por la institución, ya que otras rutas están destinadas para archivos de programa y sistema operativo.

25. Es responsabilidad del usuario evitar en todo momento la fuga de la información de la institución que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

26. El uso de los grabadores de discos externos es exclusivo para copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen.

27. Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto y además deben configurar el bloqueo de pantalla para que se active al cabo de 20 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además, el usuario debe activar manualmente la suspensión o apagado del equipo cada vez que se ausente de su oficina.

28. Si un computador tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso especial, preferiblemente por hardware.

29. A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la institución está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

30. Los usuarios no deben copiar a un medio removible, el software o los datos históricos residentes en los computadores de la Alcaldía, sin la aprobación previa del área de sistemas o del jefe inmediato

31. Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al área de sistemas y poner el computador en cuarentena hasta que el problema sea resuelto.

32. Sólo pueden descargarse archivos de redes externas de acuerdo a los procedimientos establecidos.

33. Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otras dependencias de la institución

34. No debe utilizarse software descargado de Internet y en general software que provenga de una fuente no confiable, a menos que haya sido comprobado en forma rigurosa y que esté aprobado su uso por el área de sistemas.

35. Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la Instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por el área de sistemas.

36. No deben usarse USB u otros medios de almacenamiento en cualquier computador de la institución a menos que se haya sido previamente verificado que están libres de virus u otros agentes dañinos.

37. Periódicamente debe hacerse el respaldo de los datos guardados en computadores y servidores y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación de la institución deben guardarse en otra sede, lejos del edificio.

38. El área de sistemas será responsable de la generación de las copias de seguridad de los equipos de la entidad y definirá la frecuencia del respaldo.

39. Siempre que sea posible, debe eliminarse información confidencial de los computadores y unidades de disco duro antes de que les mande a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, debe efectuarse la reparación bajo la supervisión de un representante de la institución.

40. No debe dejarse las impresoras desatendidas, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial de la institución.

41. Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuándo se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.

Políticas de uso del correo electrónico institucional.

La Alcaldía Municipal de Támesis cuenta con 65 cuentas de correo institucional de Google Workspace, las cuales cuentan con un almacenamiento estándar de 30 Gb para actividades del correo electrónico y almacenamiento en Google Drive, 7 de estas cuentas tienen un almacenamiento adicional de 50 Gb por tratarse de cuentas asignadas

a cargos con altos flujos de información. Los correos electrónicos de la administración son el medio de comunicación interna para coordinar las tareas, actividades y procesos.

Las políticas que se definen para el uso de correo electrónico son las que siguen.

1. Las cuentas de correo son asignadas por cargo y pueden ser compartidas entre empleados que trabaje o den apoyo a las mismas actividades.

2. El correo electrónico institucional es de uso exclusivo para las actividades relacionadas con la entidad y queda restringido su uso para otros fines.

3. Se prohíbe expresamente el envió de archivos, transmisión o almacenamiento de cualquier información que pudiera ser considerada de carácter pornográfico, difamatorio, racista, así mismo contenido multimedia como videos, música, etc., o que atente contra las buenas costumbres o principios.

4. Las contraseñas deben ser cambiadas como mínimo una vez cada 3 meses, de no hacerlo el sistema lo solicitará y restringirá el acceso hasta no configurar una nueva contraseña.

5. Evitar cualquier correo phishing y eliminar cualquier mensaje sospechoso si se tiene la certeza de ser malicioso.

6. Eliminar periódicamente la bandeja del spam.

7. Por ningún motivo se debe utilizar el correo institucional para temas personales, de modo que no debe almacenarse o sincronizarse información de tal índole.

8. No debe usarse la cuenta de correo institucional para realizar suscripciones a sitios web de ventas, promociones, entretenimiento y cualquier otro servicio que no provenga de plataformas institucionales.

9. En caso de recibir información con archivos adjuntos sospechosos, se deberá informar al área de sistemas para su verificación.

10. No deberá enviar información de tipo estadístico, informativo o información relevante de las acciones de la dirección, área de trabajo o del Gobierno Municipal a ningún destino no autorizado.

Elementos de TI.

Los elementos de las Tecnologías de la Información (TI) se constituyen como una herramienta fundamental para el desarrollo de las labores administrativas de la Alcaldía, ya que en ellos se crea, procesa y almacena la información de todos los procesos y actividades de la organización. Es por ello que su correcta operabilidad es

fundamental, para preservar su funcionamiento y correcto desempeño se establecen las políticas para los elementos de TI

1. El equipo de cómputo será asignado de acuerdo al puesto o función laboral en su área de trabajo. Siendo el responsable de dicha asignación el director del Área.

2. Cada equipo está preparado con el Hardware y Software básico necesario para su funcionamiento, el usuario no deberá alterar el contenido físico y/o lógico del mismo incluyendo sus periféricos.

3. En caso de presentar una falla física o lógica se deberá notificar al área de Sistemas y en el caso de ser requerido enviar el equipo para su revisión y/o reparación de acuerdo al procedimiento establecido.

4. En ningún caso el usuario intentará reparar el equipo o diagnosticarlo, únicamente debe informar de la posible falla.

5. El usuario será el único responsable del equipo de cómputo.

6. En ningún caso, el usuario tendrá cerca alimentos, bebidas u otros materiales que puedan derramarse sobre el equipo.

7. Solo se utilizará el equipo para funciones de interés del área y de ninguna manera para asuntos personales

8. El personal asignado deberá comprobar sus conocimientos o experiencia en el manejo del equipo de cómputo y periféricos básicos.

9. En caso de que el usuario no tenga conocimientos y/o experiencia, se notificará al área de sistemas para su correspondiente Capacitación.

10. La adquisición de equipo será con cargo al presupuesto de cada área o de la secretaria general, las características técnicas serán proporcionadas por el área de sistemas.

11. La solicitud del equipo de cómputo será responsabilidad de la secretaria interesada, bajo las características técnicas definidas por el área de sistemas e informando a las áreas relacionadas con la asignación de los recursos.

12. Toda recepción de equipo de cómputo por adquisición o donación se realizará a través del Almacén, con el apoyo del área de sistemas.

13. La salida de equipo de cómputo del Almacén, será total responsabilidad del almacén, el cual revisará la integridad física y el área de sistemas instalará la integridad lógica e instalará y preparará el software y hardware correspondiente a las licencias contenidas.

14. Cada equipo contiene el software de acuerdo a las necesidades del área de trabajo, El cual No deberá ser alterado.

15. El usuario deberá reportar de forma inmediata al área de Sistemas cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, contactos eléctricos con riesgo de incendio u otros.

16. Cualquier persona que tenga acceso a las instalaciones de la institución, deberá registrar al Momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la Institución, en el área de recepción, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente.

17. Los computadores personales, los computadores portátiles, y cualquier activo de tecnología de información, podrán salir de las instalaciones únicamente con la autorización de salida del área de Almacén anexando el vale de salida del equipo debidamente por el secretario de la oficina o la equivalente en las dependencias de la institución.

18. Los centros de cómputo u oficina de servidores de la Institución son áreas restringidas, por lo que sólo el personal autorizado por el área Sistemas puede acceder a ellos.

19. Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, al retirar sellos de los mismos sin la autorización del Área de Sistemas, en caso de requerir este servicio deberá solicitarlo a través de la intranet.

20. El Área de Almacén será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de consérvalos en la ubicación autorizada por el área de Sistemas.

21. El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones de la institución.

22. Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas

23. Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del computador.

24. Se debe mantener el equipo informático en un entorno limpio y sin humedad.

25. Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados con una semana de anticipación al área de Sistemas a través de un plan detallado o una solicitud para el debido acompañamiento del área de sistemas

26. Queda prohibido que el usuario abra o desarme los equipos de cómputo.

27. Únicamente el personal autorizado por el área de Sistemas podrá llevar a cabo los servicios y reparaciones al equipo informático.

28. El usuario que tenga bajo su resguardo algún equipo de cómputo será responsable de su uso y custodia en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo extravío o pérdida del mismo.

29. El usuario deberá dar aviso inmediato al Área de Sistemas y Almacén de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo

30. El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se les dé

31. El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario quien resguarda el equipo, se levantara un reporte de incumplimiento de políticas de seguridad.

32. Los equipos de la Alcaldía sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.

33. Debe respetarse y no modificar la configuración de hardware y software establecido por el Área de sistemas

34. No pueden extraerse datos fuera de la institución sin la aprobación previa de la Administración. Esta política es particularmente pertinente a aquellos que usan a computadores portátiles o están conectados a redes como Internet.

35. Los usuarios de computadores son responsables de proteger los programas y datos contra pérdida o daño.

36. El personal que utiliza un computador portátil que contenga información confidencial de la institución, no debe dejarlo desatendido, sobre todo cuando esté de viaje.

37. Todos los equipos permanecerán en el lugar registrado por el área de almacén.

Red LAN

La Red de Área Local de la Alcaldía, está pensada como una herramienta para coordinar las labores y hacer accesible la información para cualquier oficina conectada a la red. Por medio de la red LAN se hace uso el protocolo Server Message Block (SMB) de Windows, se comparten recursos como carpetas e impresoras, haciendo accesible la información para quienes la requieras. Las políticas de seguridad en este apartado están destinadas a garantizar la disponibilidad e integridad de la información compartida en la red, así como el establecimiento de las medidas que ayuden a preservar el buen funcionamiento de los equipos de impresión

Las políticas establecidas son las siguientes.

1. Por ningún motivo se deben conectar equipos diferentes a los contemplados sin la aprobación del supervisor del área, su instalación debe llevarse a cabo por el personal de sistemas o bajo su supervisión.

2. Los equipos con carpetas compartidas públicas deben habilitar la menor cantidad de permisos posibles, los archivos deben ser de solo lectura.

3. Los documentos que sean mandados a imprimir deben ser retirados inmediatamente de la impresora para evitar el acceso a personas no autorizadas a los documentos de la entidad.

4. Las consolas de impresoras y dispositivos de red deben estar protegidas con usuario y contraseña y serán de conocimiento y gestión únicamente del área de sistemas.

5. No se debe realizar ningún ataque de fuerza bruta o explotación de backdoors en las consolas de equipos conectados a la red local por parte de los empleados. Cualquier modificación en la configuración de los equipos debe ser solicitada y aprobada por el área de sistemas y el supervisor del área.

6. Los equipos como switchs y routers deben permanecer en el cuarto del rack, bajo llave y protegidos del polvo, la humedad y con acceso restringido.

7. Ninguna miembro fuera del área de sistemas está autorizado a realizar modificaciones en el sistema de cableado de la Alcaldía.

8. La red WiFi debe estar protegida con el tipo de seguridad WPA2 y su tiempo máximo de conexión debe estar limitado a 2 horas.

Contraseñas

La correcta ejecución de las funciones de los empleados demanda el uso de diversas plataformas gubernamentales e institucionales, así como cuentas de correo y sesiones en equipos de cómputos, todas ellas de uso exclusivo del funcionario o del equipo de funcionarios destinado a una tarea, la información contenida en estas plataformas es de uso exclusivo de la organización, es privada y su filtración o divulgación supone una falta grave y un agujero de seguridad. Para evitar esto se establecen las políticas de generación de claves y contraseñas seguras para las diversas plataformas.

Las políticas se enuncian a continuación.

1. Todas las contraseñas deben tener una longitud mínima de 8 caracteres y cuanto más larga, más segura es.

2. Las contraseñas deben ser cambiadas como mínimo cada 3 meses, en el caso del correo electrónico este cambio se sugiere al vencerse este plazo.

3. Cada que se cambie una contraseña, esta debe ser diferente de al menos las últimas tres anteriores.

4. Los caracteres empleados en la contraseña deben ser diversos, emplear letras mayúsculas y minúsculas, números y caracteres especiales.

5. El usuario debe almacenar su contraseña de forma segura, esta no debe estar registrada en papel en lugares de fácil acceso, ni debe ponerse como indicio de contraseña en los sistemas con esta opción.

6. No debe incluir información personal, como fechas de nacimiento, nombres propios o de allegados, números telefónicos, direcciones, ni cualquier dato que pueda facilitar que sea deducible. En lo posible no debe usarse palabras o frases con sentido.

7. Las contraseñas no deben contener secuencias de ningún tipo, ni numéricas, ni alfabéticas.

8. Las contraseñas restablecidas por el área de sistemas deben ser temporales y válidas para la primera sesión. En ese momento el usuario deberá configurar una nueva contraseña.

9. Se evitará utilizar una misma contraseña para el acceso a diversos sistemas o plataformas.

10. Los usuarios no deben intentar romper contraseñas con métodos como ataques de fuerza bruta, todos los procedimientos para el restablecimiento de alguna contraseña debe hacerse por métodos establecidos por los sistemas y plataformas, o por medios legales, con las diferentes entidades o ministerios que proporcionan los accesos a plataformas.

11. Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos computadoras, redes y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.

12. Está prohibida la divulgación de claves de acceso a sistemas y plataformas de las que haga uso la administración municipal.

11.3.2 Medidas y procedimientos

Plantear las medidas y procedimientos necesarios que permitan EL CUMPLIMIENTO de las políticas de seguridad informática en el sistema de INFORMACIÓN de la Alcaldía Municipal de Támesis.

Un aspecto importante de la política de seguridad implementada en la Alcaldía Municipal de Támesis, es asegurar que todos conozcan su propia responsabilidad para mantener la seguridad de la entidad. Es difícil que una política de seguridad se anticipe a todas las amenazas posibles. Sin embargo, las políticas se pueden asegurar que para cada tipo de problema haya un responsable de su manejo responsable. Uno de los items es que cada usuario debe ser responsable de cuidar su contraseña. El usuario que permite que su contraseña se vea comprometida incrementa la posibilidad de comprometer otras contraseñas y por ende los recursos. Por otra parte, los administradores de la red y del sistema son responsables de administrar la seguridad general de la red.

11.3.3 Avance

A continuación, en la Tabla 8, se muestra el avance de la fase de Planificación, en la que se especifica el número de actividades realizadas en esta fase, el tiempo empleado, la dependencia encargada, la dependencia que apoya la gestión, el porcentaje de avance y la vigencia de las actividades. En esta fase se establecen las políticas que servirán como guía procedimental para las actividades que se desarrollen dentro de la entidad y que requiera el uso de sistemas de información, lo que es equivalente a un manual de procedimientos que establece las normas a las que los empleados y usuarios deben acogerse para fortalecer la seguridad de la información de la organización y da la potestad de destinar sanciones a aquellos elementos que no se acojan a ellas.

Avance de la Fase de Implementación	
Tiempo estimado de ejecución	12 meses
Dependencia a cargo	Secretaria de Gobierno
Dependencias adicionales involucradas	Ninguna
Cantidad de actividades a realizar	3
Fase en ejecución	Si
Porcentaje de avance	20%

Tabla 8. Avance de la Fase de Implementación.[13]

11.4 Fase de evaluación de desempeño.

En esta fase se compilan todos los resultados elaborados en las fases anteriores y se verifica o contrasta fase por fase verificando así el cumplimiento de los objetivos propuestos y que cada fase se haya desarrollado alienada a los objetivos, visión y misión de la Alcaldía de Támesis, identificando así acciones que se deben trasladar la fase siguiente.

De esta fase corresponde realizar seguimiento a los indicadores al igual que verificación del alcance propuesto en la fase de planificación, también el resultado de las auditorías internas y externas generando un gran insumo hacia la toma de decisiones del Modelo de Seguridad y Privacidad de la Información.

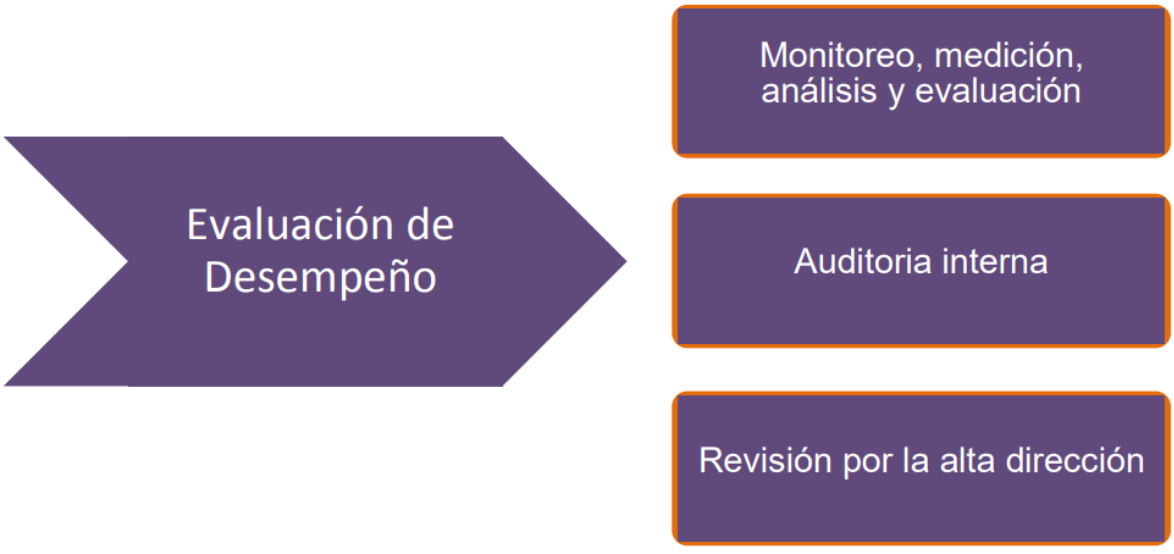


Figura 7. Fase de Evaluación de Desempeño.[14]

[13] Fuente. Elaboración propia
[14] Figura tomada de la guía Modelo de Seguridad y Privacidad de la Información capítulo 8.4

11.4.1 Plan de revisión y seguimiento a la implementación del MSPI

La implementación y operación del Sistema de Gestión de Seguridad de la Información de la Alcaldía Municipal de Támesis está cimentado en la administración del riesgo de la seguridad de la información. Por esto, en pro de garantizar la integridad, confiabilidad y disponibilidad de la información, mediante la mitigación de riesgos y amenazas para los activos de información de la entidad, la Alcaldía se compromete a implementar los controles tecnológicos, procedimentales y de talento humano que sean necesarios para minimizar los riesgos a niveles aceptables.

11.4.2 Plan de manejo de riesgos de seguridad

Entiéndase por Incidente todo aquel evento extraordinario que ocurra con los activos evaluados de la Alcaldía Municipal de Támesis: por ejemplo, Mantenimiento preventivo de uno o todos los computadores (Anual o Preventivo), Fallo de Activos, etc. El procedimiento en cualquiera de estos casos se debe registrar teniendo en cuenta los siguientes pasos:

- ✓ Aislar el equipo de la red local y cualquier conexión a internet, para evitar la propagación de la amenaza o la fuga de información privada.
- ✓ Comunicar el caso a la mesa de ayuda.

El procedimiento que debe llevar a cabo la mesa de ayuda es:

- ✓ Evaluar la criticidad de la amenaza.
- ✓ Verificar el estado de las copias de seguridad.
- ✓ Si el funcionario desarrolla sus actividades directamente en la nube, se le debe proporcionar un equipo de respaldo.
- ✓ Validar el nivel de daño y de amenaza, para tomar decisiones acerca de su correcta disposición.

11.4.3 Avance

Avance de la Fase de Evaluación de Desempeño	
Tiempo estimado de ejecución	12 meses
Dependencia a cargo	Secretaria de Gobierno
Dependencias adicionales involucradas	Ninguna
Cantidad de actividades a realizar	3
Fase en ejecución	No

Porcentaje de avance	0%

Figura 8. Avance de la Fase de Evaluación de Desempeño.[15]

11.5 Fase de mejora continua.

La fase de mejora continua nos permite entender las falencias, aciertos, ventajas y desventajas de las decisiones adoptadas en la fase de planificación e implementación del MSPI permitiendo así que ante de regresar nuevamente a la fase de panificación se entiendan las nuevas necesidades y se cubran o mejoren los aspectos que quedaron pendiente en el anterior ciclo de implementación.

Por ende, esta fase es de mucha relevancia ya que permite trazar nuevamente la hoja de ruta con unas lecciones aprendidas y así ir mejorando en conjunto la seguridad y privacidad de los activos de información en la Alcaldía de Támesis.

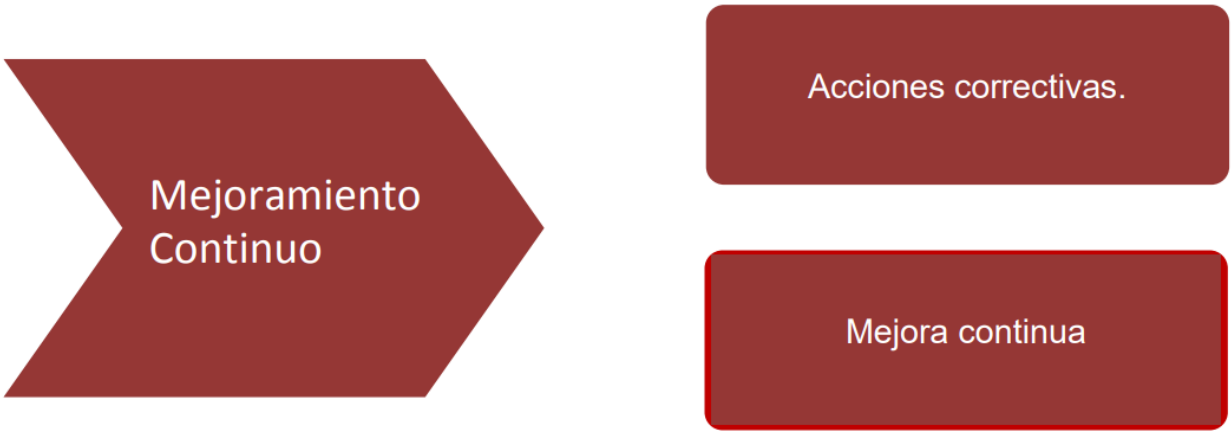


Figura 9. Fase de Mejoramiento Continuo.[16]

11.5.1 Plan de mejora continua

El objetivo de las acciones que se implementen en esta fase es la de resolver problemas asociados al diseño del Sistema de Gestión de la Seguridad de la información, con el fin de optimizar su operación y prevenir que dichos problemas sean recurrentes. Para ello se toman las siguientes medidas.

[15] Fuente. Elaboración propia
[16] Figura tomada de la guía Modelo de Seguridad y Privacidad de la Información capítulo 8.5

- ✓ Determinar por medio de la evaluación de incidentes de seguridad, los fallos del sistema de gestión y establecer sus causas para tomar medidas correctivas
- ✓ Diseño e implementación de las acciones correctivas necesarias
- ✓ Puesta a prueba de la acción correctiva empleada.

Tras haberse diseñado e implementado el Sistema de Gestión de Seguridad de la Información, se llega a la fase de mejoramiento continuo, con el que se determinan las correcciones del mismo. Para esto se diseña un plan de auditorias internas, en las que se tiene en cuenta la criticidad de la información, los recursos informáticos y el talento humano que puede gestionarlos, así como la importancia de los procesos y la concordancia con la filosofía de transparencia de la entidad. En estos planes se incluyen los métodos de auditoría, la frecuencia con la que se aplican, el alcance, las pruebas y la selección del personal encargado de su desarrollo.

La meta de la auditoria interna es determinar si los procedimientos diseñados, los procesos aplicados y los objetivos propuestos cumplen con los siguientes requerimientos.

- ✓ Están implementados y se desarrollan correctamente de acuerdo a los requisitos del estándar de ISO 27001:2013.
- ✓ Cumplen los requisitos normativos.

La retroalimentación de las auditorias debe ser efectuada por todos los participantes en el diseño e implementación del SGSI y de la institución, la revisión de los requisitos de la norma, la medición de los indicadores, las sugerencias de los implicados, pero sobre todo en el manejo de las no conformidades de la institución, de los usuarios y de los empleados.

11.5.2 Avance

Avance de la Fase de Mejoramiento Continuo	
Tiempo estimado de ejecución	4 meses
Dependencia a cargo	Secretaria de Gobierno
Dependencias adicionales involucradas	Ninguna
Cantidad de actividades a realizar	2
Fase en ejecución	No
Porcentaje de avance	0%

Tabla 9. Avance de la Fase de Mejoramiento Continuo[17]

[17] Fuente. Elaboración propia

12. MODELO DE MADUREZ

Este modelo es una herramienta que permite identificar el nivel de madurez del MSPI en el que se encuentra la entidad, mediante la identificación de las características que puedan caracterizar la implementación del Sistema de Gestión de Seguridad de la Información dentro de un determinado nivel, como se aprecia en la Figura 10.

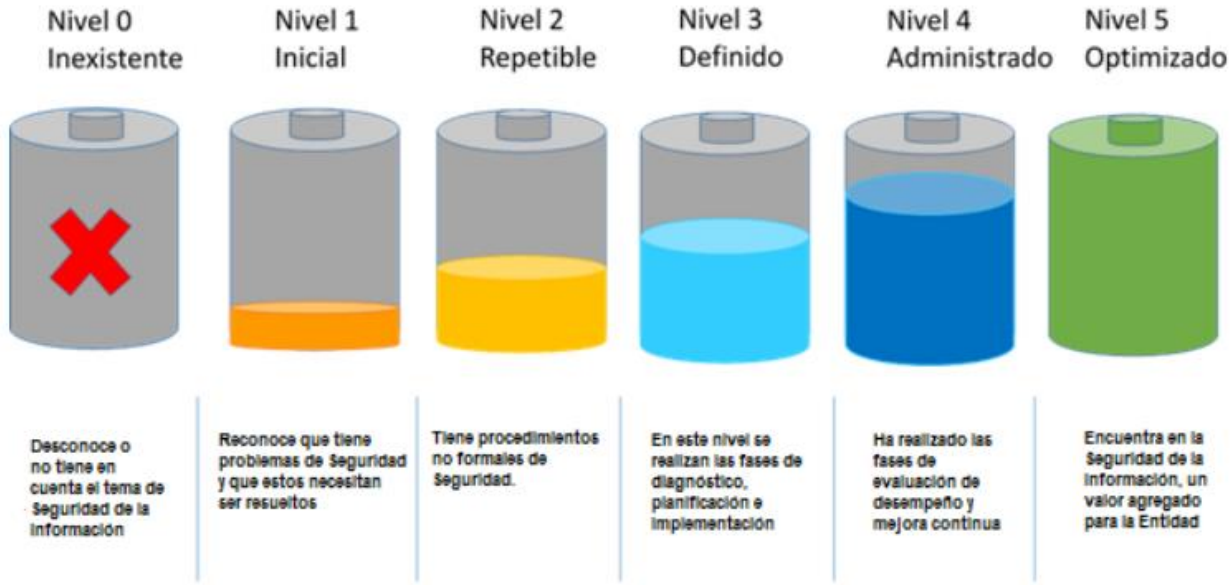


Figura 10. Nivel de Madurez.[18]

Las características se muestran en la Tabla 10 y se asocian directamente con un nivel que determina la madurez de la entidad en la que se aplica. Para el caso particular de la Alcaldía Municipal de Támesis, se tiene una identificación general de los activos de información y su clasificación, los servidores públicos están conscientes de las buenas practicas que deben asumir y ejecutar para la protección de los datos, y se establecen medidas con la mesa de apoyo para brindar soluciones a las problemáticas que puedan surgir en lo que a integridad, disponibilidad y confidencialidad de la información se refiere, pero además si tiene una fase inicial de diagnóstico de la transición de IPv4 a IPv6 en la entidad, lo que de forma global lo sitúa en el ***Nivel 2. Repetible***, lo que en pocas palabras indica que se tienen procedimientos no formales de seguridad de la información.

Nivel	Descripción
Inexistente	• Se han implementado controles en su infraestructura de TI, seguridad física, seguridad de recursos humanos entre otros, sin embargo, no están alineados a un Modelo de Seguridad.

[18] Figura tomada de la guía Modelo de Seguridad y Privacidad de la Información capítulo 9

	• No se reconoce la información como un activo importante para su misión y objetivos estratégicos. • No se tiene conciencia de la importancia de la seguridad de la información en la entidad.
Inicial	• Se han identificado las debilidades en la seguridad de la información. • Los incidentes de seguridad de la información se tratan de forma reactiva. • Se tiene la necesidad de implementar el MSPI, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que se presentan en la Entidad.
Repetible	• Se identifican en forma general los activos de información. • Se clasifican los activos de información. • Los servidores públicos de la entidad tienen conciencia sobre la seguridad de la información. • Los temas de seguridad y privacidad de la información se tratan en los comités del modelo integrado de gestión. • La entidad cuenta con un plan de diagnóstico para IPv6.
Definido	• La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información. • La Entidad ha determinado los objetivos, alcance y límites de la seguridad de la información. • La Entidad ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas. • La Entidad tiene procedimientos formales de seguridad de la Información • La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información. • La Entidad ha realizado un inventario de activos de información aplicando una metodología. • La Entidad trata riesgos de seguridad de la información a través de una metodología. • Se implementa el plan de tratamiento de riesgos. • La entidad cuenta con un plan de transición de IPv4 a IPv6
Administrado	• Se revisa y monitorea periódicamente los activos de información de la Entidad. • Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información. • Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro. • La entidad cuenta con ambientes de prueba para el uso del protocolo IPv6.
Optimizado	• En este nivel se encuentran las entidades en las cuales la seguridad es un valor agregado para la organización.

	• Se utilizan indicadores de efectividad para establecer si la entidad encuentra retorno a la inversión bajo la premisa de mejora en el cumplimiento de los objetivos misionales. • La entidad genera tráfico en IPv6.

Tabla 10. Nivel de madurez.

13. CRONOGRAMA DE IMPLEMENTACION DEL MODELO

El siguiente cronograma corresponde al periodo comprendido para la administración ***¡Támesis nos pertenece!***

AÑO	2022											
MES	1	2	3	4	5	6	7	8	9	10	11	12
FASE DE DIAGNOSTICO												
FASE DE PLANIFICACION												
FASE DE IMPLEMENTACION												
FASE DE EVALUACION DE DESEMPEÑO												
FASE DE MEJORA CONTINUA												

Tabla 11. Cronograma de implementación año 2022.

AÑO	2023											
MES	1	2	3	4	5	6	7	8	9	10	11	12
FASE DE DIAGNOSTICO												
FASE DE PLANIFICACION												
FASE DE IMPLEMENTACION												
FASE DE EVALUACION DE DESEMPEÑO												

FASE DE MEJORA CONTINUA												

Tabla 12. Cronograma de implementación año 2023.

14. GLOSARIO

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

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

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

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

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

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

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

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

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

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

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

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

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

• **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

• **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

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

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

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

• **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y

tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

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

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

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

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

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

- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.

- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.

- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

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

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

- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete

realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

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

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

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

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

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

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

- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

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

- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

- **Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

15. REFERENCIAS

- ✓ Ley 1450 de 2011, por el cual se expide el Plan Nacional de Desarrollo 2010-2014, en el artículo N° 55 sobre accesibilidad a servicios de TIC.

- ✓ 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-, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones en el artículo 38 sobre Masificación del uso de las TIC y cierre de la brecha digital.

- ✓ Decreto 2693 de 2012, por el cual se establecen los lineamientos generales de la estrategia de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

- ✓ Capítulo IV referente a la Gestión de Documentos Electrónicos de Archivo del Decreto 2609 de 2012, por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

- ✓ 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.

- ✓ Ley 1581 de 2012, reglamentada parcialmente por el Decreto 1377 de 2013, por la cual se dictan disposiciones generales para la protección de datos personales.