PROYECTO DE TRABAJO DE GRADO

DIAGNÓSTICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN LA ALCALDÍA MUNICIPAL DE ICONONZO TOLIMA.

JONIER PAVA CAMACHO

JAMES SARMIENTO PEREZ

BRYAN FORERO ORJUELA

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN Y AUDITORÍA DE SISTEMAS DE INFORMACIÓN

BOGOTÁ D.C JUNIO 09 2018

TABLA DE CONTENIDO

INTRODUCCIÓN **8**

1 GENERALIDADES **10**

1.1 Línea de Investigación 10

1.2 Planteamiento del Problema 10

1.2.1 Antecedentes del problema *10*

1.2.2 Pregunta de investigación *13*

1.3 Justificación 13

1.4 Objetivos 14

1.4.1 Objetivo general *14*

1.4.2 Objetivos específicos *14*

2 MARCOS DE REFERENCIA **15**

2.1 Marco conceptual 15

2.2 Marco teórico 20

2.3 Marco jurídico o regulatorio 27

2.3.1 Marco jurídico institucional de la estrategia 28

2.3.2 Marco regulatorio de gobierno abierto 29

2.3.3 Marco regulatorio de trámites y servicios 29

2.3.4 Marco regulatorio de gestión TI 30

2.3.5 Marco regulatorio de seguridad y privacidad de la información 31

2.3.6 Marco arquitectura empresarial y lineamientos 31

2.4 Marco geográfico 33

3 DIAGNÓSTICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN **37**

3.1 Evaluación del estado actual. 38

3.1.1 Evaluación de efectividad de controles 38

3.1.2 Brecha anexo a ISO 27001:2013 40

3.1.3 Avance del ciclo PHVA (planear-hacer-verificar-actuar) 41

3.2 Nivel de madurez 44

3.3 Vulnerabilidades técnicas y administrativas....50
3.3.1 Vulnerabilidades Administrativas:....50
3.3.1.1 Políticas de Seguridad de la Información....50
3.3.1.2 Responsabilidades Y Organización Seguridad Información....51
3.3.1.3 Seguridad De Los Recursos Humanos....52
3.3.1.4 Gestión De Activos....53
3.3.1.5 Aspectos De Seguridad De La Información De La Gestión De La Continuidad Del Negocio....53
3.3.1.6 Cumplimiento....54
3.3.1.7 Relación Con Los Proveedores....55
3.3.1.8 Conclusiones Vulnerabilidades Administrativas....55
3.3.2 Vulnerabilidades Técnicas....56
3.3.2.1 Control de Acceso....56
3.3.2.2 Criptografía....57
3.3.2.3 Seguridad Física y del Entorno....57
3.3.2.4 Seguridad de las Operaciones....59
3.3.2.5 Seguridad de las Comunicaciones....60
3.3.2.6 Adquisición, Desarrollo y Mantenimiento de Sistemas....61
3.3.2.7 Gestión de Incidentes de Seguridad de la Información....62
3.3.2.8 Conclusiones Vulnerabilidades Técnicas....62
3.4 Recomendaciones de Seguridad y Privacidad de la Información....63
3.4.1 Políticas de seguridad de la información....64
3.4.2 Organización de la seguridad de la información....64
3.4.3 Seguridad de los recursos humanos....65
3.4.4 Gestión de los activos....65
3.4.5 Control de acceso....66
3.4.6 Criptografía....67
3.4.7 Seguridad física y del entorno....67
3.4.8 Seguridad de las operaciones....68
3.4.9 Seguridad de las comunicaciones....68
3.4.10 Adquisición, desarrollo y mantenimiento de los sistemas....69
3.4.11 Relaciones con los proveedores....69
3.4.12 Gestión de incidentes de la seguridad de la información....69
3.4.13 Aspectos de seguridad de la información de la gestión de la continuidad del negocio....70
3.4.14 Cumplimiento....70

4 CONCLUSIONES 72

5 ANEXOS 74

6 BIBLIOGRAFÍA 75

LISTA DE FIGURAS

Pág.

FIGURA 1 - FASES DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. MSPI..... 23
FIGURA 2 - OBJETIVOS DE LA FASE DIAGNOSTICO MSPI 25
FIGURA 3 - UBICACIÓN POBLACIÓN ICONONZO TOLIMA..... 34
FIGURA 4 - MUNICIPIO ICONONZO TOLIMA. ZONA RURAL 34
FIGURA 5 - MUNICIPIO ICONONZO TOLIMA. ZONA URBANA 35
FIGURA 6 - ALCALDÍA MUNICIPAL DE ICONONZO TOLIMA. UBICACIÓN..... 36
FIGURA 7 - BRECHA ANEXO A ISO 27001:2013 40
FIGURA 8 - AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN 43
FIGURA 9 - DESCRIPCIÓN NIVELES DE MADUREZ Y CUMPLIMIENTO..... 45

LISTA DE TABLAS

Pág.

TABLA 1-1DIEZ DEPARTAMENTOS CON MÁS AVANCE ESTRATEGIA GEL..... 12

TABLA 2-1INSTRUMENTOS DE LA FASE DIAGNOSTICO MSPI..... 24

TABLA 2-2METAS, RESULTADOS E INSTRUMENTOS DE LA FASE PREVIA A LA IMPLEMENTACIÓN (DIAGNÓSTICO)..... 26

TABLA 3-1EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A..... 39

TABLA 3-2 AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)..... 41

TABLA 3-3 FECHAS LÍMITE DE CUMPLIMIENTO PARA ENTIDADES PÚBLICAS MSPI. 42

TABLA 3-4 NIVEL DE MADUREZ. ALCALDÍA MUNICIPAL DE ICONONZO TOLIMA..... 46

INTRODUCCIÓN

La fase de diagnóstico de Seguridad y Privacidad de la información se define como la fase inicial del Modelo de Seguridad y Privacidad de la información (MSPI) establecido por el Ministerio de Tecnologías de la Información y las comunicaciones (MinTIC) para todas aquellas entidades que pertenecen al ámbito gubernamental y permite identificar el estado actual de las organizaciones con respecto a los requerimientos del MSPI. Esta fase pretende alcanzar metas tales como: Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad, determinar el nivel de madurez de los controles de seguridad de la información, identificar el avance de la implementación del ciclo de operación al interior de la entidad, identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales e identificación del uso de buenas prácticas en seguridad de la información.

La Información y los activos que la contienen son uno de los activos más importantes en cualquier organización y el buen uso de éstos y su protección marca la diferencia entre el éxito o el fracaso. Según la ISO 27001, la seguridad de la información preserva la integridad , confidencialidad y disponibilidad pero para poder considerar que si es de gran valor, la información debe poseer ciertas características tales como: el ser relevante, estar siempre actualizada, ser altamente confiable, poseer un alto nivel de calidad, siempre debe ser completa y ser aplicable entre otras; esto le permite cumplir eficientemente con el objetivo por el cual fue creada, por ello se hace necesario implementar medidas que permitan salvaguardar de la mejor manera y que al hacerlo cumpla con los tres grandes pilares de la seguridad (la confidencialidad, la integridad y la disponibilidad), evitando que sea usada para fines distintos y pueda afectar de gran manera la operación en la empresa y el cumplimiento del objetivo institucional.

De acuerdo a lo anterior, el desarrollo de este proyecto logró realizar un diagnóstico inicial en la Alcaldía Municipal de Icononzo Tolima, el cual permitió determinar el nivel de gestión y de madurez de la seguridad y privacidad e identificar las vulnerabilidades existentes tanto técnicas como administrativas; todo esto referente a la información y los medios que la

contienen y como valor agregado elaborar un documento con recomendaciones para el mejoramiento de los controles y políticas destinados a la protección de la información lo cual servirá como insumo para las restantes fases establecidas dentro del MSPI para esta entidad.

1 GENERALIDADES

1.1 LÍNEA DE INVESTIGACIÓN

Software Inteligente y Convergencia Tecnológica

1.2 PLANTEAMIENTO DEL PROBLEMA

1.2.1 Antecedentes del problema

En el mundo, las organizaciones gubernamentales han ido creciendo de manera continua y eficiente con respecto a métodos y estrategias que buscan velar por la privacidad y la seguridad de la información. Los gobiernos han estado implementando distintas estrategias para sus entidades públicas, todo esto relacionado a la protección de una manera eficiente de la información contenida en ellas y todos los procesos resultantes prestados del uso de la misma, buscando poder participar en conjunto con la ciudadanía a través de la publicación de información que estaba protegida y ahora pueda ser puesta a disposición de los ciudadanos mediante el uso de las nuevas tecnologías. Pero proteger esta información y determinar cuál puede ser publicada o cuál debe ser resguardada no ha sido una tarea sencilla, ya que ha sido vulnerada de muchas maneras buscando apropiarse de ella o afectándola para que no cumpla el objetivo por el cual fue creada.

De acuerdo al estudio Global Open Data Index – Índice Global de Datos Abiertos realizado por Open Knowledge Foundation – Fundación de Conocimiento Abierto, durante estos últimos años se ha venido evidenciando las mejoras establecidas por los gobiernos para el manejo, uso y publicación de información destinada a la población buscando crear un estado más transparente y colaborativo de la mano con la ciudadanía. Dentro de este estudio, bajo el índice internacional, se evidencia que Colombia ha sido un partícipe directo de este tipo de estrategias logrando posicionarse en el cuarto lugar a nivel Mundial refiriéndonos al índice de datos abiertos y en el puesto doce en un listado general en materia de gobierno Electrónico. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2015)

En Colombia, bajo el marco de la estrategia Gobierno en Línea (GEL), se ha implementado a nivel nacional métodos, normas, planes y políticas refiriéndonos al eje de seguridad y privacidad de la información, buscando definir y aclarar qué información puede considerarse para ser mostrada al público y velando por que el uso que le destinen sea el apropiado de acuerdo a su objetivo. De acuerdo a los resultados publicados en la página web de la estrategia GEL del año 2016, 147 organizaciones que corresponden al índice nacional reportaron a través del Formulario Único de Reporte de Avances en la Gestión (FURAG), información de su avance en la implementación de la misma y en cuanto al índice territorial (Alcaldías y Gobernaciones) esta ha sido adoptada por 1121 entidades. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2015)

Dentro del índice nacional y el reporte publicado en el 2016 en la web del Ministerio de Tecnologías de la Información y las Comunicaciones, de las 147 organizaciones las 5 que más avances han tenido son las vinculadas al área de Defensa sumando un total de 21 entidades, en segundo lugar se puede apreciar la participación de las vinculadas al área de Hacienda y Crédito Público con un total de 18 entidades, en tercer lugar las vinculadas al área de Educación correspondientes a 11 entidades, en penúltimo lugar las vinculadas a las áreas de Salud y Protección Social y por último de estas 5 encontramos las vinculadas a Comercio, Industria y Turismo. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2015)

De acuerdo al reporte publicado bajo el índice territorial en la misma web, de las 1121 entidades, los diez departamentos que más han reportado avances en cuanto a la adopción de esta estrategia y su correcta implementación son Antioquia con un total de 125 entidades correspondientes al 11.14%, Boyacá con un total de 124 entidades correspondientes al 11.05%, Cundinamarca con un total de 114 entidades correspondientes al 10.16%, Santander con un total de 88 entidades correspondientes al 7.84%, Nariño con un total de 62 entidades correspondientes al 5.53%, Tolima con un total de 48 entidades correspondientes al 4.28%, Bolívar con un total de 44 entidades correspondientes al 3.92 %, Cauca con un total de 43 entidades correspondientes al 3.83 %, Valle del Cauca con un total de 43 entidades correspondientes al 3.83% y Norte de Santander con un total de 41 entidades correspondientes al 3.65%, aclarando que las entidades

consignadas en esta información corresponden únicamente a Alcaldías y Gobernaciones. Los otros veinticuatro departamentos siendo Huila el puesto once y San Andrés el último suman en total 390 entidades correspondientes al 34.75 % de las entidades que han adoptado y reportado esta estrategia para sus instituciones. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2015) (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016)

Tabla 1-1Diez departamentos con más avance estrategia GEL.

ESTRATEGIA GEL EN COLOMBIA		
DEPARTAMENTO	**NÚMERO DE ENTIDADES**	**PORCENTAJE**
Antioquia	125	11,14%
Boyacá	124	11,05%
Cundinamarca	114	10,16%
Santander	88	7,84%
Nariño	62	5,53%
Tolima	48	4,28%
Bolívar	44	3,92%
Cauca	43	3,83%
Valle del Cauca	43	3,83%
Norte de Santander	41	3,65%
Otros Departamentos	390	34,75%
Para el Número de entidades se agrupan Alcaldías y Gobernaciones		

Fuente: Índice de Gobierno Digital - Nivel Territorial – Estrategia GEL.

1.2.2 Pregunta de investigación

¿Cómo se puede determinar el nivel actual de gestión de seguridad y privacidad de la información en la Alcaldía Municipal de Icononzo - Tolima?

1.3 JUSTIFICACIÓN

Velar por una eficiente protección de la información y de los activos que se vinculan a esta, es una ardua labor que se ha venido justificando a través de los años, pues la información ha sido valorada como un elemento de alta importancia para el cumplimiento de los objetivos institucionales en las empresas. En cuanto a las entidades públicas, el manejo de esta información, de acuerdo a las nuevas estrategias que tienen como finalidad desarrollar un Estado más transparente, resaltan el poder determinar de manera precisa cuál o qué información debe clasificarse como visible por todos y para todos, y para lograr esto siempre debe establecerse una etapa inicial que permita determinar el estado actual referente a la seguridad y privacidad de la información y de todo lo que corresponde a esto, este punto inicial es el ejecutar un diagnóstico.

Este proyecto se hace importante para la entidad porque se encaminó a diagnosticar el estado actual de la entidad, detectar vulnerabilidades, proteger los activos tecnológicos, apoyar la innovación tecnológica, apoyar la implementación de estrategias, hacer recomendaciones de uso, y concientizar a usuarios y funcionarios, e iniciar en el proceso de adopción de estrategias a la Alcaldía Municipal de Icononzo Tolima, todo esto dirigido a cumplir con los principios de seguridad y privacidad de la información establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones bajo el Modelo de Seguridad y Privacidad de la Información contenido dentro del marco de la estrategia Gobierno en Línea (GEL). Así mismo, en el ámbito legal, el proyecto permite de gran manera cumplir con lo solicitado por entidades de control, las cuales proponen adoptar métodos y estrategias para los mismos principios. En la parte académica permite aplicar de manera precisa los conocimientos adquiridos buscando cumplir con el perfil de especialista requerido por la Universidad.

1.4 OBJETIVOS

1.4.1 Objetivo general

Diagnosticar el estado actual de la Alcaldía Municipal de Icononzo Tolima con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información propuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones.

1.4.2 Objetivos específicos

- Evaluar el estado actual de la gestión de seguridad y privacidad de la información en la entidad.
- Determinar el nivel de madurez de seguridad y privacidad de la información en la Alcaldía Municipal de Icononzo Tolima.
- Identificar vulnerabilidades técnicas y administrativas referentes a la privacidad y seguridad de la información.
- Plantear recomendaciones para el mejoramiento de los aspectos correspondientes a la seguridad y privacidad de la información.

2 MARCOS DE REFERENCIA

2.1 MARCO CONCEPTUAL

Para poder entender de manera precisa cada aspecto obtenido y tratado mediante este proyecto, se hace necesario definir los conceptos más importantes que se identifican en el desarrollo y cumplimiento de los objetivos establecidos como metas mediante esta investigación.

De acuerdo con esto:

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)

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 auditoria. (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)

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 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).

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)

ISO/IEC 27000: Parte de una familia en crecimiento de estándares sobre Sistemas de Gestión de la Seguridad de la Información (SGSI) de ISO/IEC, el ISO 27000 series. ISO/IEC 27000 es un grupo de estándares internacionales titulados: Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Visión de conjunto y vocabulario. Tiene como fin ayudar a organizaciones de todo tipo y tamaño a implementar y operar un Sistema de Gestión de la Seguridad de la Información (SGSI).

ISO/IEC 27001: Estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for

Standardization y por la comisión International Electrotechnical Commission. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como "Ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 27002, anteriormente conocida como ISO/IEC 17799, con orígenes en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

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)

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**.**

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.

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)

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 (Stakeholders): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

(Ministerio de Tecnologías de la Información y las Comunicaciones, 2016, pág. 11)

2.2 MARCO TEÓRICO

*"*Colombia es el próximo país que se instalará, definitivamente, en las tecnologías del futuro para construir una mejor realidad*"*

Presidente Juan Manuel Santos

En el mundo se han evidenciado bastantes cambios haciendo referencia a la manera en que los gobiernos operan frente a su responsabilidad con la ciudadanía; de la misma forma, los ciudadanos se han transformado ya que tienen un conocimiento importante que puede ser aprovechado en beneficio de las sociedades y han basado sus necesidades en mecanismos más directos y más poderosos, la mayoría apoyados en el uso de las tecnologías de la información y las comunicaciones. Esto ha hecho que se busquen estrategias más eficientes asociadas a la actividad gubernamental para la satisfacción y mejora en la atención con los ciudadanos, siendo estos los beneficiarios directos de las políticas públicas y de la toma de decisiones, lo que hace cada vez más imperante involucrarse activamente en la construcción y validación de estas estrategias.

Este proyecto se enfocó en participar de manera directa en este gran cambio, estableciendo su eje en diagnosticar cada aspecto correspondiente a la seguridad y privacidad de la información, convirtiéndose en una parte de la línea base o de apoyo para la estrategia difundida por el gobierno que es destinada para las entidades públicas haciendo referencia a la materia de datos abiertos y uso de tecnologías y la protección de los mismos; todo esto aplicado en la Alcaldía Municipal de Icononzo – Tolima y así mismo en un enfoque más técnico, este proyecto permitió determinar el nivel de madurez e identificar vulnerabilidades de acuerdo a los requerimientos establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI). Para poder ejecutar un diagnóstico en esta entidad, por ser pública, se encaminó cada tarea respondiendo directamente a lo que el Ministerio de Tecnologías de la Información y las

Comunicaciones (MinTIC) establece, y por ello como adicional, es necesario aclarar cada concepto de manera que permita entender de forma precisa los parámetros definidos para la ejecución del mismo.

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), según la Ley 1341 o Ley de TIC, es la entidad que se encarga de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones. Dentro de sus funciones está incrementar y facilitar el acceso de todos los habitantes del territorio nacional a las Tecnologías de la Información y las Comunicaciones y a sus beneficios. (Ministerio de las Tecnologías de la Información y las Comunicaciones, 2017)

La estrategia GEL es una estrategia promovida e implementada por MinTIC , instaurada como una política Nacional de Gobierno electrónico que se definió a través del Decreto 1078 de 2015 artículo 2.2.9.1.1.1 y fue estructurada en 4 ejes temáticos, (TIC para el gobierno Abierto, TIC para servicios, TIC para la gestión y por último Seguridad y privacidad de la información) y que tiene como propósito lograr que los ciudadanos cuenten con servicios en línea de alta calidad, impulsar el empoderamiento y la colaboración de los ciudadanos con el Gobierno, todo esto gracias al uso estratégico de la tecnología. Esta estrategia fue establecida para ser adoptada por las entidades públicas y que al hacerlo aporten de la mejor manera a su desarrollo, en un concepto más preciso para el cumplimiento de los objetivos institucionales y que estos contribuyan a los fines esenciales del estado. (Ministerio de las Tecnologías de la Información y las Comunicaciones, 2017)

De los 4 ejes implícitos dentro del marco de la estrategia GEL, se tomó como base para el desarrollo del proyecto el eje correspondiente a la seguridad y privacidad de la información el cual tiene como propósito garantizar la integridad, la disponibilidad y la confidencialidad de la información pública, en una definición menos técnica, este eje comprende las acciones tendientes a proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada. Para ello, ha creado un modelo que ha sido estructurado bajo normas y estándares nacionales e internacionales recalcando el uso de las

mejores prácticas relacionadas a la protección de la información.

El Modelo de Seguridad y Privacidad de la Información (MSPI) es una guía que conduce a la preservación de la confidencialidad, integridad y disponibilidad de la información, permitiendo garantizar la privacidad de los datos mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos y el cual fue estructurado recopilando las mejores prácticas nacionales e internacionales para suministrar requisitos para sus 5 fases las cuales son: el Diagnóstico, la Planificación, la Implementación, la Gestión y el Mejoramiento continuo referentes a la privacidad y seguridad de la información (Ministerio de las Tecnologías de la Información y las Comunicaciones, 2017). De estas 5 fases, en el ámbito del proyecto se estimará únicamente la fase inicial o Fase Diagnóstico con el cual se podrá determinar el estado de seguridad y privacidad de la información en la Alcaldía Municipal de Icononzo - Tolima con respecto a los requerimientos del MSPI.

El diagnóstico es el primer de cinco fases que se encuentran establecidas dentro del ciclo de operación del Modelo de Seguridad y Privacidad de la Información (MSPI). Esta fase tiene como objetivo identificar el estado actual de la organización con respecto a los requerimientos del mismo y su desarrollo debe apoyarse principalmente en el diligenciamiento del Instrumento de Evaluación, el cual contiene todos los aspectos necesarios para realizar una valoración satisfactoria que sirve como eje inicial de cualquier proceso de seguridad y privacidad de la información en las entidades públicas. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016)

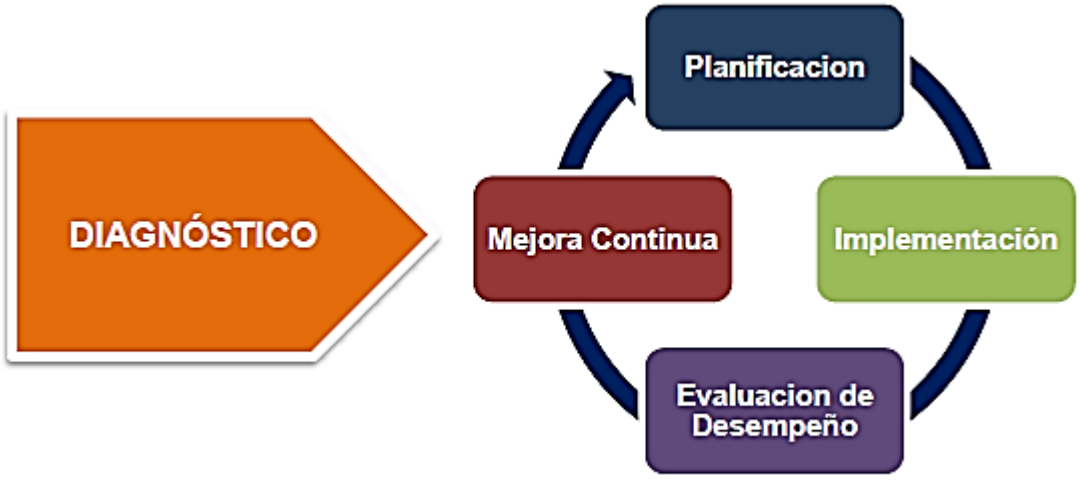

Figura 1 - Fases del Modelo de Seguridad y Privacidad de la Información. MSPI.

Fuente: Modelo de Seguridad y Privacidad de la información MSPI. Estrategia GEL.

De manera precisa la Fase de Diagnóstico pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información (MSPI), entre sus metas y para dar cumplimiento a esto están el determinar el estado actual de la gestión de seguridad y privacidad de la información, identificar el nivel de madurez de seguridad y privacidad de la información e identificar las vulnerabilidades técnicas y administrativas dentro de la entidad que sirvan como insumo para la segunda fase denominada Fase de Planeación (La Fase Planeación no está estipulada en el desarrollo del proyecto). (Ministerio de Tecnologías de la Información y las Comunicaciones, 2017). Para desarrollar el diagnóstico en la Alcaldía, se hizo uso de la Herramienta de Diagnóstico de Seguridad y Privacidad de la Información (Instrumento_de_Evaluación_MSPI) (Ver anexo: Instrumento de Evaluación MSPI), herramienta que está contenida dentro de la Fase Diagnóstico que a su misma vez esta contendía dentro del MSPI, la cual permite hacer un levantamiento de información y un proceso de evaluación siendo parte de la línea base para determinar el estado actual en la entidad con respecto a la seguridad y privacidad de la información, dicha herramienta está contenida en el marco del MSPI como parte de la primer fase del desarrollo y adopción de este modelo denominada Fase de Diagnóstico. (Ministerio de Tecnologías de la Información y las

Comunicaciones, 2016)

En esta fase es necesario que las entidades identifiquen cómo se está garantizando la privacidad sobre todo el ciclo de la información que tienen en su poder verificando la implantación o no de medidas que den cumplimiento a los requerimientos de las normas sobre protección de datos personales y que, adicionalmente contribuya a identificar la información pública sometida a reserva o clasificada en los términos de la Ley. Para ello se pone a disposición de las entidades, el instrumento de diagnóstico y seguimiento a la implementación. A través del diligenciamiento de este instrumento se podrá conocer la realidad de la información relacionada con el manejo de los activos de la información que reposen en bancos de datos o archivos y a partir de allí determinar las medidas a nivel procedimental que deben adelantar las entidades para otorgar un nivel adecuado de protección a esta información. (Ministerio de las Tecnologías de la Información y las Comunicaciones, 2017)

Tabla 2-1Instrumentos de la Fase Diagnostico MSPI.

Diagnostico			
Metas	Resultados	Instrumentos	
		MSPI	MRAE
Diagnostico	Realizar el diagnóstico de las condiciones en que se encuentran los activos de información administrados por la entidad. Diligenciamiento de la herramienta.	Herramienta de diagnóstico.	
	Documento con el resultado del diagnóstico realizado por la entidad con la clasificación y distinción de los activos de información teniendo en cuenta la información con datos personales y aquellos que no lo son identificando la criticidad de la información clasificada o reservada.		

Con el resultado del diagnóstico se puede contar con un insumo frente a la identificación de aquella información que debe ser manejada como privada (clasificada en los términos de la Ley) para a partir de allí incorporar las medidas de seguridad proporcionales a su naturaleza

como los procedimientos que lleven al cumplimiento de la normatividad de protección de datos, transparencia y acceso a la información pública soportado todo ello en la incorporación de un sistema de privacidad por diseño que responda a la realidad presupuestal, humana y técnica de cada entidad. Para construir los instrumentos de gestión de la información pública, las entidades pueden remitirse a la Guía sobre Instrumentos de Gestión de la Información Pública de la Secretaría de Transparencia de la Presidencia de la República. (Ministerio de las Tecnologías de la Información y las Comunicaciones, 2017)

Este diagnóstico tiene tres objetivos primordiales claramente definidos los cuales deben ser cubiertos en su totalidad al realizar el procedimiento y están estructurados para determinar:

1. Estado actual de la entidad con respecto a los requerimientos de seguridad y privacidad de la información.
2. Identificación del nivel de madurez correspondiente a la seguridad y privacidad de la información en la entidad.
3. Levantamiento de información.

Figura 2 - Objetivos de la Fase Diagnostico MSPI

Fuente: Modelo de Seguridad y Privacidad de la Información – MSPI.

De igual manera existen algunas metas que también deben cumplirse y que se encuentran inmersas en el desarrollo de la fase:

1. Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.
2. Determinar el nivel de madurez de los controles de seguridad de la información.
3. Identificar el avance de la implementación del ciclo de operación al interior de la entidad.
4. Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
5. Identificación del uso de buenas prácticas en ciberseguridad.

Para tener una concepción más clara, a continuación, podemos observar las metas, resultados e instrumentos que fueron utilizados para realizar este proceso, además de los lineamientos normativos que controlan el buen desarrollo de cada actividad. (Ministerio de las Tecnologías de la Información y las Comunicaciones, 2017)

Tabla 2-2Metas, resultados e instrumentos de la fase previa a la implementación (Diagnóstico)

Diagnostico			
Metas	**Resultados**	**Instrumentos MSPI**	**Alineación MRAE**
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	Diligenciamiento de la herramienta.	Herramienta de diagnóstico.	LI.ES.01 LI.ES.02 LI.GO.01 LI.GO.04 LI.GO.05 LI.GO.07 LI.ST.14
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad	Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad.	Herramienta de diagnóstico	
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.	Herramienta de diagnóstico	

Fuente: Modelo de Seguridad y Privacidad de la Información – MSPI.

La herramienta de diagnóstico (Instrumento de Evaluación MSPI) es una herramienta que fue creada con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas, según lo definido en la Estrategia de Gobierno en Línea en su cuarto componente "Seguridad y Privacidad de la Información". (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016). El diligenciamiento de esta herramienta debe consentir realizarse basándose en un Instructivo, (Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información), que se establece y que les permite a las entidades públicas de orden nacional, y entidades públicas del orden territorial, entender de una mejor manera como se debe diligenciar la herramienta de diagnóstico para poder obtener un resultado preciso, el cual le permite a cada entidad generar un plan de seguridad de la información para ser desarrollado al interior de esta, y de esta manera dar cumplimiento con lo estipulado en el manual de gobierno en línea en su cuarto componente. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016)

2.3 MARCO JURÍDICO O REGULATORIO

La Alcaldía Municipal de Icononzo Tolima es una entidad gubernamental y como tal para poder adoptar cualquier requerimiento solicitado por los entes de control debe proceder bajo las políticas y normas establecidas según los marcos regulatorios que estos determinen. El Ministerio de Tecnologías de la Información y las Comunicaciones establece políticas, normas y decretos que están contenidos dentro del marco regulatorio de la estrategia Gobierno en Línea – GEL que fue creada a través del decreto 1078 de 2015 artículo 2.2.9.1.1.1, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. El marco regulatorio para el desarrollo e implementación de la estrategia GEL el cual es base para poder desarrollar un diagnóstico de seguridad y privacidad de la información en la Alcaldía, contempla lo siguiente:

2.3.1 MARCO JURÍDICO INSTITUCIONAL DE LA ESTRATEGIA

- 1995 - Conpes 2790 de 1995, Gestión Pública orientada a resultados. Mejoramiento de la gestión pública en torno al cumplimiento de los objetivos del Plan Nacional de Desarrollo.
- 1995 - Decreto Ley 2150 de 1995, Estatuto Anti-trámites. Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública.
- 2000 - Conpes 3072 de 2000, Agenda de Conectividad. Masificar el uso de las Tecnologías de la Información y con ello aumentar la competitividad del sector productivo, modernizar las instituciones públicas y de gobierno, y socializar el acceso a la información, siguiendo los lineamientos establecidos en el Plan Nacional de Desarrollo 1998 – 2002.
- 2000 - Directiva 02 de 2000, Plan de Acción de la estrategia de Gobierno en Línea. Facilitar a los ciudadanos, empresas, funcionarios y otras entidades estatales el acceso a la información de las entidades públicas e iniciar la integración y coordinación de los esfuerzos de las entidades en este propósito.
- 2003 - Decreto 3107 de 2003, Supresión del Programa Presidencial e integración de la Agenda de Conectividad al MinTIC.
- 2008 - Decreto 1151 de 2008, Lineamientos generales de la Estrategia de Gobierno en línea.
- 2009 - Ley 1341 de 2009, Mecanismo y condiciones para garantizar la masificación del Gobierno en Línea.
- 2012 - Decreto 2693 de 2012, Lineamientos generales de la Estrategia de Gobierno en línea.
- 2014 - Decreto 2573 de 2014, Lineamientos generales de la Estrategia de Gobierno en línea.
- 2015 - Ley 1753, Plan nacional de desarrollo 2014-2018 "Todos por un nuevo país".
- 2016 - Decreto 415, Lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.

- 2016 - Resolución 2405 de 25 de noviembre 2016, Por el cual se adopta el modelo del Sello de Excelencia Gobierno en Línea y se conforma su comité.

2.3.2 MARCO REGULATORIO DE GOBIERNO ABIERTO

- 1985 - Ley 57 de 1985, Publicidad de los actos y documentos oficiales. 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.
- 2000 - Ley 594 de 2000, Ley General de Archivos. Tiene por objeto establecer las reglas y principios generales que regulan la función archivística del Estado.
- 2003 - Acto legislativo 01 de 2003, Uso de medios electrónicos e informáticos para el ejercicio del derecho al sufragio.
- 2004 - Ley 892 de 2004, Mecanismo electrónico de votación e inscripción. Por la cual se establecen nuevos mecanismos de votación e inscripción para garantizar el libre ejercicio de este derecho, en desarrollo del artículo 258 de la Constitución Nacional.
- 2014 - Ley 1712 de 2014, Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- 2015 - Ley Estatutaria 1757 de 2015, Promoción y protección del derecho a la participación democrática.
- 2015 - Decreto Reglamentario Único 1081 de 2015 Decreto 103 de 2015, Reglamento sobre la gestión de la información pública. Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- 2015 - Resolución 3564 de 2015, Reglamentaciones asociadas a la Ley de Transparencia y Acceso a la Información Pública.

2.3.3 MARCO REGULATORIO DE TRÁMITES Y SERVICIOS

- 1991 - Ley 527 de 1999, Ley de Comercio Electrónico. Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen

funciones públicas o prestan servicios públicos.

- 2000 - Decreto 1747 de 2000, Entidades de certificación, los certificados y las firmas digitales.
- 2012 - NTC 5854 de 2012, Accesibilidad a páginas web. 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.
- 2012 - Decreto 019 de 2012, Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
- 2012 - Decreto 2364 de 2012, Firma electrónica. Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
- 2015 - Decreto 1080, Decreto Único Reglamentario del Sector Cultura.

2.3.4 MARCO REGULATORIO DE GESTIÓN TI

- 2002 - Directiva Presidencial No. 10 de 2002, Programa de renovación de la Administración Pública: hacía un Estado Comunitario.
- 2002 - Ley 790 de 2002, Programa de Reforma de la Administración Pública. Por la cual se expiden disposiciones para adelantar el programa de renovación de la administración pública y se otorgan unas facultades extraordinarias al presidente de la República.
- 2003 - Conpes 3248 de 2003, Renovación de la Administración Pública
- 2003 - Decreto 3816 de 2003, Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública. Por el cual se crea la Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública.
- 2010 - Decreto 235 de 2010, Intercambio de información entre entidades para el cumplimiento de funciones públicas.

2.3.5 MARCO REGULATORIO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- 2008 - Ley 1266 de 2008, Disposiciones generales de habeas data y se regula el manejo de la información. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- 2009 - Ley 1273 de 2009, Código Penal. 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.
- 2012 - Ley Estatutaria 1581 de 2012. Protección de datos personales. Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.
- 2015 - Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.

2.3.6 MARCO ARQUITECTURA EMPRESARIAL Y LINEAMIENTOS

- Entendimiento estratégico - LI.ES.01: Las instituciones de la administración pública deben contar con una estrategia de TI que esté alineada con las estrategias sectoriales, el Plan Nacional de Desarrollo, los planes sectoriales, los planes decenales - cuando existan- y los planes estratégicos institucionales. La estrategia de TI debe estar orientada a generar valor y a contribuir al logro de los objetivos estratégicos
- Definición de la Arquitectura Empresarial - LI.ES.02: Cada sector e institución, mediante un trabajo articulado, debe contar con una Arquitectura Empresarial que

permita materializar su visión estratégica utilizando la tecnología como agente de transformación. Para ello, debe aplicar el Marco de Referencia de Arquitectura Empresarial para la gestión de TI del país, teniendo en cuenta las características específicas del sector o la institución.

- Alineación del gobierno de TI - LI.GO.01: La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir e implementar un esquema de Gobierno TI que estructure y direccione el flujo de las decisiones de TI, que garantice la integración y la alineación con la normatividad vigente, las políticas, los procesos y los servicios del Modelo Integrado de Planeación y Gestión de la institución.
- Cadena de Valor de TI - LI.GO.04: La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar el macroproceso de gestión de TI, según los lineamientos del Modelo Integrado de Planeación y Gestión de la institución, teniendo en cuenta el Modelo de gestión estratégica de TI
- Capacidades y recursos de TI - LI.GO.05: La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir, direccionar, evaluar y monitorear las capacidades disponibles y las requeridas de TI, las cuales incluyen los recursos y el talento humano necesarios para poder ofrecer los servicios de TI.
- Criterios de adopción y de compra de TI - LI.GO.07: La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir los criterios y métodos que direccionen la toma de decisiones de inversión en Tecnologías de la Información (TI), buscando el beneficio económico y de servicio de la institución. Para todos los proyectos en los que se involucren TI, se deberá realizar un análisis del costo total de propiedad de la inversión, en el que se incorporen los costos de los bienes y servicios, los costos de operación, el mantenimiento, el licenciamiento, el soporte y otros costos para la puesta en funcionamiento de los bienes y servicios por adquirir. Este estudio debe realizarse para establecer los requerimientos de financiación del proyecto. Debe contemplar los costos de capital (CAPEX) y los costos de operación (OPEX).
- Análisis de vulnerabilidades - LI.ST.14: La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar el análisis de

vulnerabilidades de la infraestructura tecnológica, a través de un plan de pruebas que permita identificar y tratar los riesgos que puedan comprometer la seguridad de la información o que puedan afectar la prestación de un servicio de TI.

Fuentes: (Ministerio de Tecnologías de la Información y las Comunicaciones, 2015) (Ministerio de las Tecnologías de la Información y las Comunicaciones, 2017)

2.4 MARCO GEOGRÁFICO

Descripción Física: El Municipio de Icononzo es uno de los 47 Municipios del departamento del Tolima, este se encuentra situado al oriente del departamento del Tolima, a una altura de 1.304 mts sobre el nivel del mar; su latitud norte es de 4:11´04" y su longitud es de 70:27´20", su temperatura media es de 21° grados centígrados. Hace parte de la subregión del Sumapaz, junto con los Municipios de melgar, Carmen de Apicalá, Villarrica y Cunday. (Alcaldía Municipal de Icononzo Tolima, 2015). (Instituto Geográfico Agustin Codazzi, 2017)

Límites y extensión del Municipio: El Municipio posee un área de 23.886 hectáreas, de las cuales corresponde a la Zona Urbana 24.2 hectáreas y al Área Rural 23.841.8 hectáreas. Este se encuentra limitado así: por el Norte con los Municipios de Fusagasugá y Pandi (Cundinamarca); por el Oriente, con los Municipio de Venecia y Cabrera (Cundinamarca), por el Sur, con los Municipio de Villarrica y Cunday y finalmente por el occidente, con el municipio de Melgar. (Instituto Geográfico Agustin Codazzi, 2017)

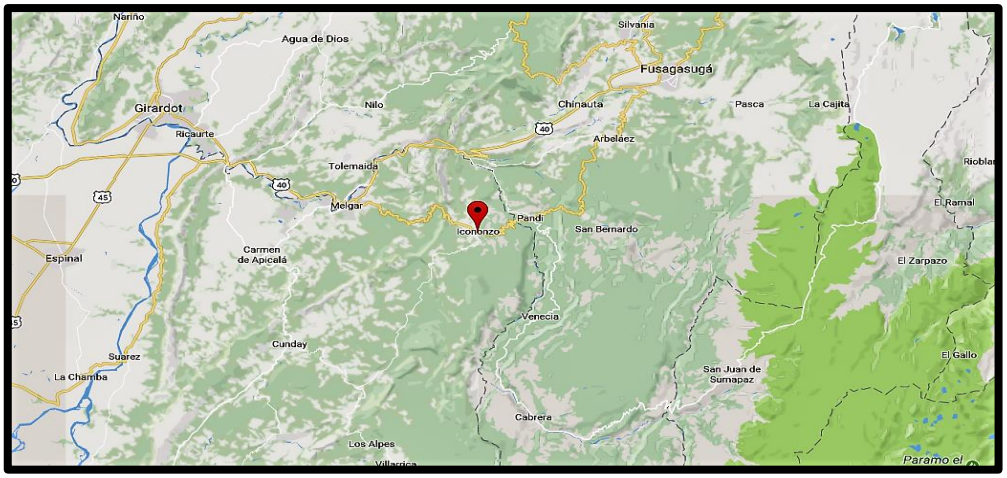

Figura 3 - Ubicación Población Icononzo Tolima

La zona rural la constituyen 30 veredas: Alto de Icononzo, Balconcitos, Basconta, Boquerón, Buenos Aires, Cafrería, Canadá – Escocia, Cuba, Chaparro, Dos Quebradas, El Mesón, El Páramo, El Santuario, El Triunfo, Guamitos, Hoya Grande, La Esperanza, La Fila, La Georgina, La Laja, La Maravilla, Montecristo, Mundo Nuevo, Paramitos, Parroquia Vieja, Paticuinde, Piedecuesta, Portachuelo, San José de Guatimbol, Yopal. (Alcaldía Municipal de Icononzo Tolima, 2015)

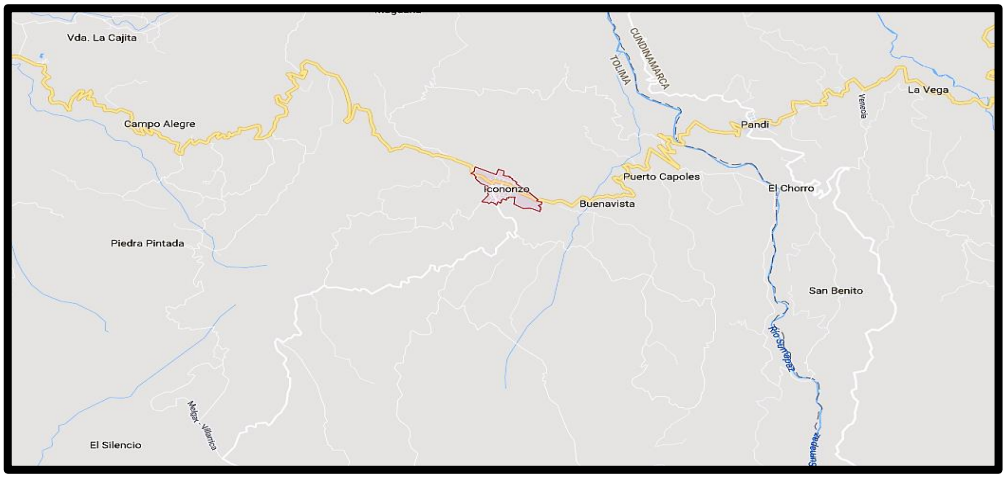

Figura 4 - Municipio Icononzo Tolima. Zona Rural

La zona urbana de Icononzo está conformada por 8 barrios: Alto de la Virgen, Alfonso Uribe, La Campiña, Los Almendros, Obrero, Pueblo Nuevo, Santofimio, Miraflores. (Alcaldía Municipal de Icononzo Tolima, 2015).

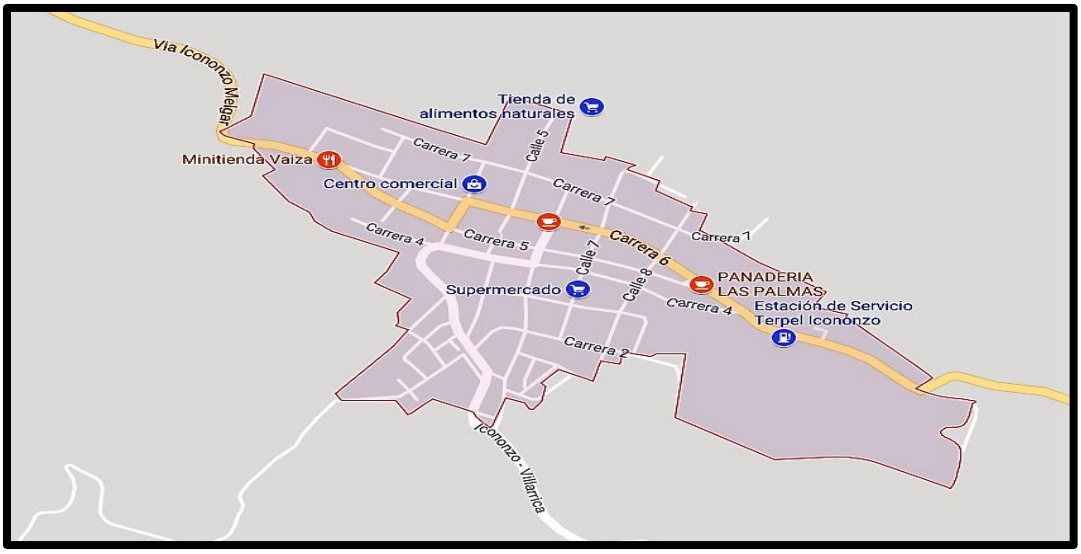

Figura 5 - Municipio Icononzo Tolima. Zona Urbana

Encontramos en el Municipio el Palacio Municipal o la Alcaldía Municipal situada en la dirección Cra 6ta N° 5 – 57 barrio Centro en la zona urbana del Municipio. (Alcaldía Municipal de Icononzo Tolima, 2015) (Instituto Geográfico Agustin Codazzi, 2017)

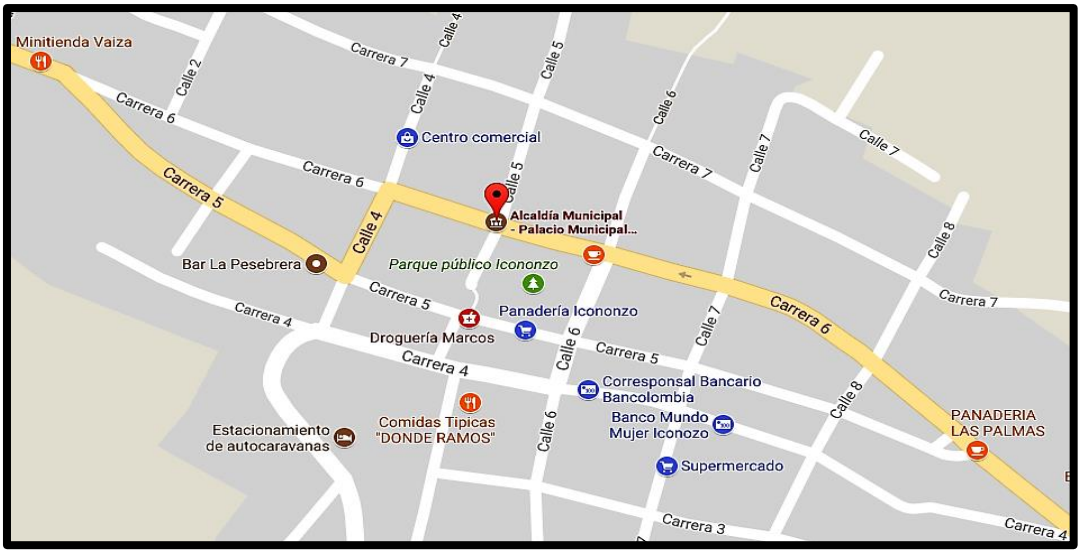

Figura 6 - Alcaldía Municipal de Icononzo Tolima. Ubicación

3 DIAGNÓSTICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En el mes de Diciembre de 2017 con el acompañamiento de un funcionario de MinTIC, la participación de los jefes de cada área o proceso en la organización y en especial el funcionario de la Alcaldía de Icononzo Tolima Edison Álvaro Díaz Gaitán con el cargo de Auxiliar Administrativo - Enlace TIC, se recolectó información mediante el diligenciamiento de un cuestionario (Elaboración Propia) y la herramienta (Ver Anexo: Instrumento Evaluación MSPI) proporcionada por MinTIC para determinar el estado actual de gestión de seguridad y privacidad de la información al interior de la entidad. Para el diligenciamiento de este instrumento (MSPI), se usó como guía el *"Instructivo para el Diligenciamiento de la herramienta de Diagnóstico de Seguridad y Privacidad de la Información"* el cual nos proporcionó de manera precisa los pasos a seguir para recolectar toda la información posible y determinar si se cumplen y en qué calificación se encuentran los objetivos que pide registrar. De acuerdo a esto:

1. Mediante el diligenciamiento del Cuestionario (Ver anexo: 3. Cuestionario Familiarización), logramos entender y familiarizarnos con la parte tecnológica de la entidad y nos proporcionó un acercamiento para saber con cuales herramientas informáticas y de seguridad cuenta la Alcaldía.

2. Con el diligenciamiento de la herramienta (Instrumento Evaluación MSPI), permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de Alcaldía Municipal de Icononzo Tolima, según lo definido en la Estrategia de Gobierno en Línea en su cuarto componente "Seguridad y Privacidad de la Información".
3. Se realizaron pruebas Técnicas y Administrativas en la organización, tomando cada una de las áreas y recolectando evidencias fotográficas y documentales de los ítems solicitados por el instrumento.
4. Se analizó de manera minuciosa cada ítem y registro diligenciado al realizar la visita en campo de acuerdo con los resultados obtenidos, se plantearon recomendaciones en pro del mejoramiento del estado actual de la seguridad y privacidad de la información.

A continuación, se desglosa de manera precisa el proceso realizado y los resultados obtenidos para cada aspecto evaluado e identificado mediante el diagnóstico de seguridad y privacidad de la información.

3.1 EVALUACIÓN DEL ESTADO ACTUAL.

Para determinar el estado actual de seguridad y privacidad de la información se empleó como herramienta de diagnóstico el Instrumento de Evaluación MSPI establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). En esta etapa fue necesario identificar cómo se está garantizando la privacidad sobre todo el ciclo de la información que se tiene en la entidad verificando la implantación o no de medidas que dan cumplimiento a los requerimientos de las normas sobre la protección de datos personales y que adicionalmente contribuya a identificar la información pública sometida a reserva o clasificada en los términos de la ley. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016)

3.1.1 EVALUACIÓN DE EFECTIVIDAD DE CONTROLES

El diligenciamiento de la herramienta permitió obtener una calificación calculada para cada dominio y está totalizada a partir del valor registrado y promediado sobre la cantidad de objetivos de control que se establecen, todo esto referenciado desde las hojas nombradas como ADMINISTRATIVAS y TÉCNICAS dentro de la Herramienta Instrumento MSPI. El resultado obtenido para la evaluación del estado actual nos refleja los controles y su efectividad según la Normatividad ISO 27001 del 2013 y lo planteado dentro del desarrollo del Modelo de seguridad y privacidad de la información que ha establecido MinTIC para las entidades públicas de orden nacional, así como el avance del ciclo PHVA (Planear-Hacer-Verificar-Actuar). Con el diligenciamiento de la herramienta MSPI, se obtuvieron los siguientes resultados de los dominios para la EVALUACIÓN Y EFECTIVIDAD DE CONTROLES:

Tabla 3-1Evaluación de efectividad de Controles - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	0	100	**INEXISTENTE**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	14	100	**INICIAL**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	22	100	**REPETIBLE**
A.8	GESTIÓN DE ACTIVOS	42	100	**EFECTIVO**
A.9	CONTROL DE ACCESO	9	100	**INICIAL**
A.10	CRIPTOGRAFÍA	10	100	**INICIAL**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	14	100	**INICIAL**
A.12	SEGURIDAD DE LAS OPERACIONES	6	100	**INICIAL**
A.13	SEGURIDAD DE LAS COMUNICACIONES	13	100	**INICIAL**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	5	100	**INICIAL**
A.15	RELACIONES CON LOS PROVEEDORES	10	100	**INICIAL**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	6	100	**INICIAL**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	4	100	**INICIAL**
A.18	CUMPLIMIENTO	8,5	100	**INICIAL**
PROMEDIO EVALUACIÓN DE CONTROLES		**12**	**100**	**INICIAL**

Fuente: Herramienta – Instrumento de Evaluación MSPI – Portada.

De acuerdo con el análisis y los resultados obtenidos, la calificación promediada de los controles dentro de la organización fue de 12, lo cual evidencia que la entidad se encuentra en un proceso inicial de implementación de medidas para la seguridad y privacidad de la información, de los responsables de la misma y los activos que la contienen.

De manera precisa los dominios que deben ser tratados de manera inmediata para su fortalecimiento son el dominio A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO, A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS, A.12 SEGURIDAD DE LAS OPERACIONES Y A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**.** En estos dominios se evidencia que la calificación obtenida está muy por debajo del promedio total de la evaluación de

controles, alcanzando un valor menor a la mitad del promedio. Para ello, en el punto 7.4 del proyecto se plantean recomendaciones que apoyaran en gran medida las mejoras necesarias para este proceso.

3.1.2 BRECHA ANEXO A ISO 27001:2013

De acuerdo con la evaluación realizada y el diagnóstico obtenido, la entidad está en un proceso inicial con respecto a los aspectos referentes a la implementación de medidas y controles destinados a la privacidad y seguridad de la información así mismo como la protección de los activos que la contienen. La brecha identificada mediante el desarrollo de esta evaluación se puede ver identificada en el siguiente gráfico.

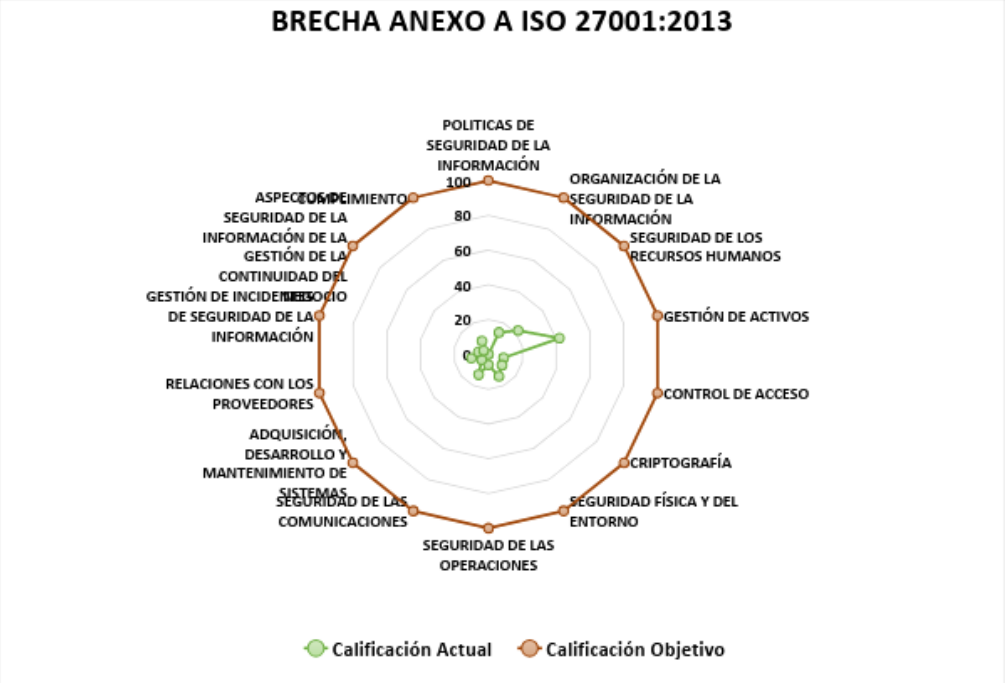

Figura 7 - Brecha Anexo a ISO 27001:2013

Fuente: Instrumento de Evaluación MSPI – Portada.

Según fechas establecidas para el desarrollo de las actividades correspondientes a la implementación del modelo de seguridad y privacidad de la información el cual se basa en

aspectos del marco 27001:2013, para el año 2018 todas las entidades a nivel nacional deberían cumplir con la meta propuesta la cual está entre el 80% y el 100% de ejecución del MSPI. Como se evidencia en el gráfico anterior, la Alcaldía Municipal de Icononzo Tolima no sobrepasa el 50% en ninguno de sus controles y esto ha enmarcado una gran deficiencia referente a la seguridad y privacidad de la información, logrando poner en riesgo en gran medida cada aspecto relacionado con la información y su valor. Este gráfico plasma los valores obtenidos en la Evaluación de efectividad de controles de la tabla 2 Evaluación de efectividad de Controles - ISO 27001:2013 ANEXO A.

3.1.3 AVANCE DEL CICLO PHVA (PLANEAR-HACER-VERIFICAR-ACTUAR)

Otro de los aspectos que deben determinarse mediante la evaluación del estado actual en la organización es el correspondiente al Ciclo del modelo de Operación PHVA el cual se encuentra alineado con los plazos para la implementación de las actividades que se establecieron para el manual de Gobierno en Línea a través del decreto 1078 de 2015. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016)

La tabla que se muestra a continuación, (Tabla 3 - 2 Avance Ciclo de Funcionamiento Del Modelo De Operación (PHVA)), permite visualizar el avance que la Alcaldía Municipal de Icononzo Tolima presenta con respecto al avance del ciclo PHVA.

Tabla 3-2 Avance Ciclo de Funcionamiento Del Modelo De Operación (PHVA)

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2015	Planificación	8%	40%
2016	Implementación	4%	20%
2017	Evaluación de desempeño	3%	20%

2018	Mejora continua	4%	20%
TOTAL		**18%**	**100%**

Fuente: Instrumento de Evaluación MSPI – Portada.

La tabla muestra el estado de avance (columna % de avance actual) frente a cada una de las etapas del ciclo (columna componente), es importante tener en cuenta que de acuerdo al tipo de entidad hay diferentes objetivos (columna % avance objetivo) de avance, así: (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016)

Tabla 3-3 Fechas Límite de Cumplimiento para Entidades Públicas MSPI.

TIPO DE ENTIDAD	2015	2016	2017	2018	2019	2020
De Orden Nacional	40%	60%	80%	100%	Mantener 100%	Mantener 100%
De Orden Territorial A	35%	50%	80%	100%	Mantener 100%	Mantener 100%
De Orden Territorial B y C	10%	30%	50%	65%	80%	100%

Fuente: Instructivo de Diligenciamiento Herramienta de Evaluación MSPI.

Según el análisis realizado para la tabla (Tabla 3 - 2 Avance Ciclo de Funcionamiento Del Modelo De Operación (PHVA)), la alcaldía se encuentra en un proceso inicial de cumplimiento con respecto al PHVA y todo lo referente a la implementación de la estrategia Gobierno en Línea mediante el MSPI. Para el ítem de planificación la entidad se encuentra en un 8% del 40% que debería presentar par el año 2018, para el ítem de Implementación la alcaldía se encuentra en un 4% de un total de un 20% que debería presentar para este mismo año, para el ítem de evaluación de desempeño la entidad se encuentra cumpliendo actualmente con un 3% de

un total del 20% que debería presentar y para el ítem de mejora continua la Alcaldía Municipal de Icononzo Tolima ha completado un 4% de un total del 20% que debería presentar para el año 2018.

Lo anterior se puede visualizar de manera precisa en la siguiente figura (Figura 8 - Avance Ciclo de Funcionamiento del Modelo de Operación) la cual representa el avance actual en la organización y lo esperado para el año 2018 mostrando las diferencias precisas de cada fase del ciclo PHVA. La gráfica presenta una comparación entre el avance logrado por la entidad, el avance objetivo y el avance total posible.

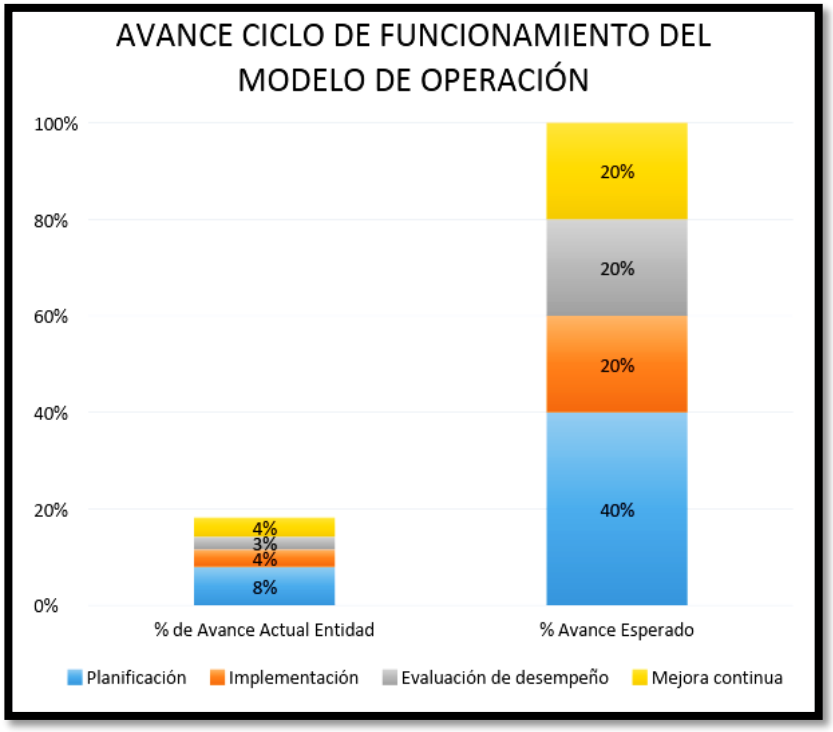

Figura 8 - Avance Ciclo de Funcionamiento del Modelo de Operación

FUENTE: Instrumento de Evaluación MSPI – Portada.

3.2 NIVEL DE MADUREZ

La madurez de la seguridad y privacidad de la información incluye los controles tanto administrativos como técnicos, la competencia técnica de los recursos informáticos, las directivas, los procesos y las prácticas sostenibles, así como la eficiencia de los controles establecidos dentro de la organización. La madurez de la seguridad se puede medir únicamente a través de la capacidad de la entidad para utilizar de forma eficaz las herramientas disponibles de forma que se cree un nivel de seguridad sostenible a lo largo de muchas disciplinas. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2015). Para ello debe establecerse una línea de partida de la madurez de la seguridad y usarse para definir las áreas en las que centra los programas de seguridad de la entidad, para el desarrollo del proyecto, el nivel de madurez se identificó mediante el diligenciamiento del Instrumento de Evaluación MSPI evidenciado en la hoja llamada madurez MSPI, que permitió identificar el estado actual y las carencias con las que cuenta la Alcaldía con respecto al Modelo de Seguridad y Privacidad de la Información y se identificaron requisitos que en su mayoría han sido previamente evaluados en las hojas Administrativas, Técnicas y PHVA. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016)

En el resultado obtenido al diligenciar la herramienta Instrumento de Evaluación MSPI, la Alcaldía Municipal de Icononzo Tolima evidencia que la entidad **NO ALCANZA EL NIVEL INICIAL** de madurez y de cumplimiento de acuerdo con la implementación del Modelo de Seguridad y Privacidad de la Información. En este nivel se encuentran las entidades, que aún no cuentan con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto, los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información. Ver Figura 9 - Descripción Niveles de Madurez y Cumplimiento.

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

Figura 9 - Descripción Niveles de Madurez y Cumplimiento

Fuente: Instrumento de Evaluación MSPI – Madurez.

La calificación obtenida durante este proceso para el nivel de madurez es de doscientos (200) e indica que el puntaje obtenido por la entidad de acuerdo con los requerimientos establecidos para este Modelo de cumplimiento **NO SUPERA** el puntaje esperado para la etapa Inicial el cual es de doscientos sesenta (260) y por ende no da cumplimiento a ninguno de los siguientes Niveles establecidos para su calificación. A continuación, se ilustra en la siguiente tabla los puntajes obtenidos para la entidad haciendo referencia al nombramiento del Nivel, los requisitos involucrados de cumplimiento, el puntaje obtenido por la entidad y el puntaje mínimo esperado. Ver Tabla 3 4 Nivel de Madurez. Alcaldía Municipal de Icononzo Tolima.

Tabla 3-4 Nivel de Madurez. Alcaldía Municipal de Icononzo Tolima.

NIVEL	ID. REQUISITO	PUNTAJE OBTENIDO	PUNTAJE ESPERADO
OPTIMIZADO	R55	-	1100
ADMINISTRADO	R41 a R53	-	880
DEFINIDO	R20 a R40	-	660
REPETIBLE	R9 a R19	-	460
INICIAL	R1 a R8	200	260

Fuente: Instrumento de Evaluación MSPI - Madurez

En el límite de madurez inicial se obtuvieron doscientos (200) puntos de calificación correspondientes a los requisitos:

R1 (Hoja: Administrativo):

1. Si Se identifican en forma general los activos de información de la Entidad, están en cuarenta (40) puntos.
2. Si se cuenta con un inventario de activos de información física y lógica de toda la entidad, documentado y firmado por la alta dirección, están en sesenta (60) puntos.
3. Si se revisa y monitorea periódicamente los activos de información de la entidad, están en ochenta (80) puntos.

Para este requisito, la entidad obtuvo una calificación de ochenta (80) puntos acumulados y corresponden al ítem AD.4.1.1. Inventario de Activos.

R2 (Hoja: Administrativo):

1. Se clasifican los activos de información lógicos y físicos de la Entidad.

Para este requisito, la entidad obtuvo una calificación de ochenta (80) puntos acumulados y corresponden al ítem AD.4.1.2. Propiedad de los Activos.

R3 (Hoja: Administrativo):

1. Si Los funcionarios de la Entidad no tienen conciencia de la seguridad y privacidad de la información y se han diseñado programas para los funcionarios de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, están en veinte (20) puntos.
2. Si se observa en los funcionarios una conciencia de seguridad y privacidad de la información y los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, están aprobados y documentados, por la alta Dirección, están en cuarenta (40) puntos.
3. Si se han ejecutado los planes de toma de conciencia, comunicación y divulgación, de las políticas de seguridad y privacidad de la información, aprobados por la alta Dirección, están en sesenta (60) puntos.

Para este requisito, la entidad obtuvo una calificación de cero (0) puntos acumulados y corresponden al ítem Administrativas AD3.2.2. Responsable de SI/Líderes de los procesos.

R4 (Hoja: Administrativo - PHVA):

1. Existe la necesidad de implementar el Modelo de Seguridad y Privacidad de la Información, para definir políticas, procesos y procedimientos claros para dar una respuesta proactiva a las amenazas que se presenten en la Entidad.

Para este requisito, la entidad obtuvo una calificación de veinte (20) puntos acumulados y corresponden PHVA P.1 Alcance MSPI (Modelo de Seguridad y Privacidad de la Información) con una calificación parcial de veinte (20) puntos, Administrativas AD1.1. Documento de la política de seguridad y privacidad de la Información con una calificación parcial de cero (0) puntos y PHVA P.4 Roles y responsabilidades para la seguridad de la información con una calificación parcial de cero (0) puntos.

R5 (Hoja: Madurez):

1. Si se tratan temas de seguridad y privacidad de la información en los comités del modelo integrado de gestión, coloque 20
2. Los temas de seguridad de la información se tratan en los comités directivos interdisciplinarios de la Entidad, con regularidad, coloque 40

Para este requisito, la entidad obtuvo una calificación de cero (0). Correspondientes al mismo requisito R5 establecido en la hoja MADUREZ.

R6 (Hoja: Administrativas):

1. Si se empiezan a definir las políticas de seguridad y privacidad de la información basada en el Modelo de Seguridad y Privacidad de la Información, están en 20.
2. Si se revisan y se aprueban las políticas de seguridad y privacidad de la información, están en 40.
3. Si se divulgan las políticas de seguridad y privacidad de la información, están en 60**.**

Para este requisito la entidad obtuvo una calificación de cero (0) puntos acumulados y corresponden al ítem Administrativas AD1.1. Documento de la política de seguridad y privacidad de la Información.

R7 (Hoja: PHVA):

1. Establecer y documentar el alcance, límites, política, procedimientos, roles y responsabilidades y del Modelo de Seguridad y Privacidad de la Información.

Para este requisito, la entidad obtuvo una calificación de veinte (20) puntos acumulados y corresponden al ítem P.1. Responsable de SI/Alcance MSPI (Modelo de Seguridad y Privacidad de la Información).

R8 (Hoja: Técnicas):

1. Determinar el impacto que generan los eventos que atenten contra la integridad, disponibilidad y confidencialidad de la información de la Entidad.

Para este requisito, la entidad obtuvo una calificación de cero (0) puntos acumulados y corresponden al ítem T.7.1.4. Responsable de SI/Evaluación de eventos de seguridad de la información y decisiones sobre ellos.

DESCRIPCIÓN ADICIONAL Tabla 3 4 Nivel de Madurez. Alcaldía Municipal de Icononzo Tolima.

El puntaje esperado para el nivel de madurez se obtiene mediante la suma de los requisitos para cada etapa**:**

Límite de Madurez Inicial: El puntaje esperado para esta etapa es de doscientos sesenta (260), este puntaje es el resultado de la suma de los requisitos (R1, R2, R3, R4, R5, R6, R7, R8). Ver anexo Instrumento de evaluación MSPI pestaña Madurez.

Límite de Madurez Repetible: El puntaje esperado para esta etapa es de cuatrocientos sesenta (460), este puntaje es el resultado de la suma de los requisitos (R9, R10, R11, R12, R13, R14, R15, R16, R17, R18, R19). Ver anexo Instrumento de evaluación MSPI pestaña Madurez

Límite de Madurez Definido: El puntaje esperado para esta etapa es de seiscientos sesenta (660), este puntaje es el resultado de la suma de los requisitos (R20, R21, R22, R23, R24, R25, R26, R27, R28, R29, R30, R31, R32, R33, R34, R35, R36, R37, R38, R39, R40). Ver anexo Instrumento de evaluación MSPI pestaña Madurez.

Límite de Madurez Administrado: El puntaje esperado para esta etapa es de ochocientos ochenta (880), este puntaje es el resultado de la suma de los requisitos (R41, R42, R43, R44, R45,

R46, R47, R48, R49, R50, R51, R52, R53). Ver anexo Instrumento de evaluación MSPI pestaña Madurez.

Límite de Madurez Optimizado: El puntaje esperado para esta etapa es de mil cien (1100), este puntaje es el resultado de la suma de los requisitos (R55). Ver anexo Instrumento de evaluación MSPI pestaña Madurez.

3.3 VULNERABILIDADES TÉCNICAS Y ADMINISTRATIVAS

Luego de recibir la colaboración del Sr. Edison Álvaro Díaz Gaitán, funcionario de la Alcaldía de Icononzo (Tolima), funcionarios del Ministerio de Tecnologías de la información y las Comunicaciones y de los Líderes de Áreas de la entidad, se procede a realizar en la instalaciones de la Alcaldía (Áreas) el estudio de vulnerabilidades técnicas y administrativas utilizando el Instrumento de Evaluación MSPI que es la herramienta que fue creada con el fin de identificar el nivel de madurez en la implementación del Modelo de Seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas.

Para este estudio se realizaron entrevistas en cada área con el personal o dueño de los procesos solicitando documentación o evidencias fotográficas requerida por el Instrumento de Evaluación MSPI en la columna de PRUEBA. También se realizó una inspección física a las áreas de la entidad para recolectar evidencias para el estudio de vulnerabilidades.

A continuación, se presenta el resultado del estudio de vulnerabilidades Administrativas y Técnicas realizadas en la entidad de acuerdo a los dominios establecidos por el MSPI:

3.3.1 VULNERABILIDADES ADMINISTRATIVAS:

3.3.1.1 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

El Dominio A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, es el

ambiente en el que trabaja la organización, se especifican los objetivos de la entidad y cómo alcanzarlos adoptando estrategias para mejorar los procesos de funcionamiento. En este dominio se pudo establecer mediante las pruebas solicitadas en la Herramienta MSPI, (Ver Anexo Instrumento de Evaluación MSPI - Hoja ADMINISTRATIVAS - ID. ITEM AD.1 - Columna Pruebas), que en la Alcaldía Municipal de Icononzo Tolima se obtuvo una calificación total de cero (0) puntos, promediando sus controles A.5.1.1 - A.5.1.2. Quiere decir que este dominio se encuentra en una etapa de evaluación de efectividad del control INEXISTENTE, en la entidad hay Total falta de cualquier proceso reconocible.

3.3.1.2 RESPONSABILIDADES Y ORGANIZACIÓN SEGURIDAD INFORMACIÓN

Para el Dominio A.6 RESPONSABILIDADES Y ORGANIZACIÓN SEGURIDAD INFORMACIÓN, se establece la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la organización. Debe existir un ámbito de gestión para efectuar tareas tales como la aprobación de las políticas de seguridad, la coordinación de la implementación de la seguridad y la asignación de funciones y responsabilidades. En este dominio se pudo establecer mediante las pruebas solicitadas en la Herramienta MSPI, (Ver Anexo Instrumento de Evaluación MSPI - Hoja ADMINISTRATIVAS - ID. ITEM AD.2 - Columna Pruebas), que la Alcaldía Municipal de Icononzo Tolima obtuvo una calificación total de catorce (14) puntos promediando sus objetivos de control A.6.1 - A.6.2. Quiere decir que este dominio se encuentra en una etapa de evaluación de efectividad del control INICIAL, en la entidad hay una evidencia 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. Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican. En este dominio se evalúan dos (2) objetivos de control que son A.6.1 qué es el Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización y el objetivo de control A.6.2. Qué es garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles. El Objetivo de control A.6.1, obtuvo una calificación de ocho (8) puntos, promediando sus controles A.6.1.2 - A.6.1.3 - A.6.1.4 - A.6.1.5, mientras que el objetivo de control A.6.2 obtuvo una calificación de veinte (20) puntos, promediando sus controles A.6.2.1 - A.6.2.2. El promedio

de esta calificación (objetivos de control) fue el total de todo el dominio anteriormente citado Dominio A.6.

3.3.1.3 SEGURIDAD DE LOS RECURSOS HUMANOS

En el Dominio A.7 SEGURIDAD DE LOS RECURSOS HUMANOS, existe la necesidad de educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de actividad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. Se solicita revisar el proceso de selección de personal (funcionarios y contratistas) verificando referencias satisfactorias, verificación de la hoja de visa, confirmación de calificaciones académicas, protección de los datos personales de los candidatos, el contratista debe especificar las responsabilidades. En este dominio se pudo establecer mediante las pruebas solicitadas en la Herramienta MSPI, (Ver Anexo Instrumento de Evaluación MSPI - Hoja ADMINISTRATIVAS - ID. ITEM AD.3 - Columna Pruebas), que la Alcaldía Municipal de Icononzo Tolima, obtuvo una calificación total de veintidós (22) puntos promediando sus objetivos de control A.7.1 - A.7.1.2 - A.7.3. Quiere decir que este dominio se encuentra en una etapa de evaluación de efectividad del control REPETIBLE, en la entidad 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. En este dominio se evalúan tres (3) objetivos de control que son A.7.1 - A.7.1.2 - A.7.3. El objetivo de control A.7.1, es asegurar que el personal y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que son considerados, el objetivo de control A.7.2, Asegurar que los funcionarios y contratistas tomen conciencia de sus responsabilidades sobre la seguridad de la información y las cumplan y el objetivo de control A.7.1.3, proteger los intereses de la Entidad como parte del proceso de cambio o terminación de empleo. El objetivo de control A.7.1, obtuvo una calificación de cuarenta (40) puntos, promediando sus controles A.7.1.1 - A.7.1.2, el objetivo de control A.7.1.2 obtuvo una calificación de siete (7) puntos promediando sus controles A.7.2.1 - A.7.2.2 – A.7.2.3, mientras que el objetivo de control A.7.3 obtuvo una calificación de veinte

(20) puntos promediando sus controles A.7.3.1. El promedio de esta calificación (objetivos de control), fue el total de todo el dominio anteriormente citado Dominio A.7.

3.3.1.4 GESTIÓN DE ACTIVOS

Para el Dominio A.8 GESTIÓN DE ACTIVOS, la organización debe tener conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos. En este dominio se pudo establecer mediante las pruebas solicitadas en la Herramienta MSPI, (Ver Anexo Instrumento de Evaluación MSPI - Hoja ADMINISTRATIVAS - ID. ITEM AD.4 - Columna Pruebas), que la Alcaldía Municipal de Icononzo Tolima, obtuvo una calificación total de cuarenta y dos (42) puntos promediando sus objetivos de control A.8.1 - A.8.2 - A.8.3. Quiere decir que este dominio se encuentra en una etapa de evaluación de efectividad del control EFECTIVO, Los procesos y los controles se 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. En este dominio se evalúan TRES (3) objetivos de control que son A.8.1 que es identificar los activos organizacionales y definir las responsabilidades de protección apropiadas, el objetivo de control A.8.2 asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la Entidad y el objetivo de control A.8.3 evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de la información almacenada en los medios. El objetivo de control A.8.1, obtuvo una calificación de sesenta (60) puntos, promediando sus controles A.8.1.1 - A.8.1.2 - A.8.1.3 - A.8.1.4, el objetivo de control A.8.2 obtuvo una calificación de cuarenta y siete (47) puntos promediando sus controles A.8.2.1 - A.8.2.2 – A.8.2.3, mientras el objetivo de control A.8.3, obtuvo una calificación de veinte (20) puntos, promediando los controles A.8.3.1 - A.8.3.2 – A.8.3.3 El promedio de esta calificación (objetivos de control), fue el total de todo el dominio anteriormente citado Dominio A.8.

3.3.1.5 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Para el Dominio A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO, preservar la seguridad de la información

durante las fases de activación, de desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad. En este dominio se pudo establecer mediante las pruebas solicitadas en la Herramienta MSPI, (Ver Anexo Instrumento de Evaluación MSPI - Hoja ADMINISTRATIVAS - ID. ITEM AD.5 - Columna Pruebas), que la Alcaldía Municipal de Icononzo Tolima, obtuvo una calificación total de tres, cinco (3,5) puntos promediando sus objetivos de control A.17.1, A.17.2. Quiere decir que este dominio se encuentra en una etapa de evaluación de efectividad del control INICIAL, en la entidad hay una evidencia 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. Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican. En este dominio se evalúan dos (2) objetivos de control que son A.17.1 que es La continuidad de la seguridad de la información debe incluir en los sistemas de gestión de la continuidad del negocio de la Entidad y el objetivo de control A.17.2 que es asegurar la disponibilidad de las instalaciones de procesamiento de la información. El objetivo de control A.17.1, obtuvo una calificación de siete (7) puntos, promediando sus controles A.17.1.1 - A.17.1.2 - A.17.1.3, mientras que el objetivo de control A.17.2 obtuvo una calificación de cero (0) puntos, promediando sus controles A.17.2.1. El promedio de esta calificación (objetivos de control) fue el total de todo el dominio anteriormente citado Dominio A.17.

3.3.1.6 CUMPLIMIENTO

Para el Dominio A.18 CUMPLIMIENTO es el diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales. En este dominio se pudo establecer mediante las pruebas solicitadas en la Herramienta MSPI, (Ver Anexo Instrumento de Evaluación MSPI - Hoja ADMINISTRATIVAS - ID. ITEM AD.6 - Columna Pruebas), que la Alcaldía Municipal de Icononzo Tolima, obtuvo una calificación total de ocho, cinco (8,5) puntos promediando sus objetivos de control A.18.1 - A.18.2. Quiere decir que este dominio se encuentra en una etapa de evaluación de efectividad del control INICIAL, en la entidad hay una evidencia 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. Se cuenta con procedimientos documentados, pero

no son conocidos y/o no se aplican. En este dominio se evalúan dos (2) objetivos de control que son A.18.1 qué es Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad y el objetivo de control A.18.2 que es revisiones de seguridad de la información. El objetivo de control A.18.1, obtuvo una calificación de diez (10) puntos, promediando sus controles A.18.1.1 - A.18.1.2 - A.18.1.3 - A.18.1.4 - A.18.1.5, mientras que el objetivo de control A.18.2 obtuvo una calificación de siete (7) puntos, promediando sus controles A.18.2.1 - A.18.2.2 - A.18.2.3. El promedio de esta calificación (objetivos de control) fue el total de todo el dominio anteriormente citado Dominio A.18.

3.3.1.7 RELACIÓN CON LOS PROVEEDORES

Para el Dominio A.15 RELACIONES CON LOS PROVEEDORES es implementar y mantener el nivel apropiado de seguridad de la información y la entrega de los servicios contratados en línea con los acuerdos de entrega de servicios de terceros. En este dominio se pudo establecer mediante las pruebas solicitadas en la Herramienta MSPI, (Ver Anexo Instrumento de Evaluación MSPI - Hoja ADMINISTRATIVAS - ID. ITEM AD.7 - Columna Pruebas), que la Alcaldía Municipal de Icononzo Tolima, obtuvo una calificación total de diez (10) promediando sus controles A.15.1. - A.15.2. Quiere decir que este dominio se encuentra en una etapa de evaluación de efectividad del control INICIAL, en la entidad 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. Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican.

3.3.1.8 CONCLUSIONES VULNERABILIDADES ADMINISTRATIVAS

Se identifica que en el Instrumento de Evaluación MSPI (Modelos de Seguridad y Privacidad de la Información) en la pestaña “Administrativas”, el dominio que obtuvo la

calificación más baja es: ID. ITEM: AD1 - POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, con una calificación actual de Cero (0) puntos y su EVALUACIÓN DE EFECTIVIDAD ES: INEXISTENTE.

También se identificó el dominio con más alta puntuación: ID. ITEM: AD8 - GESTIÓN DE ACTIVOS, con una calificación de Cuarenta y Dos (42) puntos y su EVALUACIÓN DE EFECTIVIDAD ES: EFECTIVO.

3.3.2 VULNERABILIDADES TÉCNICAS

3.3.2.1 CONTROL DE ACCESO

El dominio A.9 CONTROL DE ACCESO se basa en controlar el acceso a la información por medio de un sistema de restricciones y políticas establecidas por la entidad para impedir el acceso no autorizado a los sistemas de información. En este dominio se pudo establecer mediante las pruebas solicitadas en la Herramienta MSPI, (Ver Anexo Instrumento de Evaluación MSPI - Hoja TECNICAS - ID. ITEM T.1 - Columna Pruebas), que la Alcaldía Municipal de Icononzo Tolima obtuvo una calificación total de nueve (9) en el dominio A.9 CONTROL DE ACCESO tomando los resultados de los Objetivos de Control (A.9.1, A.9.2, A.9.3, A.9.4) promediados. En el Objetivo de Control A.9.1 REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO, se evidencia inexistencia en los controles (A.9.1.1 y A.9.1.2), no hay documentación ni procedimientos. En el Objetivo de Control A.9.2 GESTIÓN DE ACCESO DE USUARIOS. El control (A.9.2.1) tuvo una calificación de veinte (20) en el cual se evidencia que el único control de acceso que existe es el ingreso local al equipo (usuario y contraseña), pero se evidencia que el procedimiento no está documentado. Para los controles (A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6) se evidencia inexistencia, no hay documentación ni procedimientos. En el Objetivo de Control A.9.3 RESPONSABILIDADES DE LOS USUARIOS. El control (A.9.3.1) tuvo una calificación de veinte (20) en el cual se evidencia que los accesos existentes a las plataformas cumplen con las políticas de encriptación y no visualización de información confidencial, pero esto es propio de cada aplicativo y no es establecido por la entidad. En el Objetivo de Control A.9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES. Los controles (A.9.4.1,

A.9.4.2, A.9.4.3) cada uno tuvo una calificación de veinte (20) en el cual se evidencia que los accesos existentes a las plataformas cumplen con las políticas de encriptación y no visualización de información confidencial, pero esto es propio de cada aplicativo y no es establecido por la entidad. Para los controles (A.9.4.4, A.9.4.5) se evidencia inexistencia, no hay documentación ni procedimientos.

3.3.2.2 CRIPTOGRAFÍA

El dominio A.10 CRIPTOGRAFÍA se basa en el uso de sistemas y técnicas criptográficos para la protección de la información, esto con el fin de asegurar un buen manejo, buscando mantener la triada de la información (confidencialidad, disponibilidad e integridad). En este dominio se pudo establecer mediante las pruebas solicitadas en la Herramienta MSPI, (Ver Anexo Instrumento de Evaluación MSPI - Hoja TECNICAS - ID. ITEM T.2 - Columna Pruebas), que la Alcaldía Municipal de Icononzo Tolima obtuvo una calificación total de diez (10) en el dominio A.10 CRIPTOGRAFÍA tomando los resultados del Objetivo de Control (A.10.1). En el Objetivo de Control A.10.1 CONTROLES CRIPTOGRÁFICOS. Se evidencia inexistencia en el control (A.10.1.1), no hay documentación ni procedimientos. Para el control (A.10.1.2) se obtuvo una calificación de veinte (20), en el cual se evidencia la existencia de tokens para la validación de cuentas bancarias y acceso a los aplicativos de Certicámara para la firma digital del alcalde.

3.3.2.3 SEGURIDAD FÍSICA Y DEL ENTORNO

El dominio A.11 SEGURIDAD FÍSICA Y DEL ENTORNO se basa en seguridad física y perimetral, seguridad de locales y edificios, protección contra amenazas externas y del entorno, en evitar el acceso físico no autorizado, el daño o la interferencia a las instalaciones y a la información de la organización, los equipos deberán estar protegidos contra amenazas físicas y ambientales. En este dominio se pudo establecer mediante las pruebas solicitadas en la Herramienta MSPI, (Ver Anexo Instrumento de Evaluación MSPI - Hoja TECNICAS - ID. ITEM T.3 - Columna Pruebas), que la Alcaldía Municipal de Icononzo Tolima obtuvo una calificación total de catorce (14) en el dominio A.11 SEGURIDAD FÍSICA Y DEL ENTORNO

tomando los resultados de los Objetivos de Control (A.11.1, A.11.2) promediados. En el Objetivo de Control A.11.1 ÁREAS SEGURAS se evidencia inexistencia en los controles (A.11.1.1, A.11.1.2, A.11.1.4), no hay documentación ni procedimientos. En los controles (A.11.1.3, A.11.1.5, A.11.1.6) cada uno tuvo una calificación de veinte (20) en el cual se evidencia que existe nomenclatura correspondiente accesos y/o restricciones a personas no autorizadas y existe nomenclaturas correspondientes a casos de emergencia. En el Objetivo de Control A.11.2 EQUIPOS. El control (A.11.2.1) tuvo una calificación de veinte (20) en el cual se evidencia que los equipos están ubicados en el área de trabajo con las condiciones óptimas que puede establecer la estructura física o planta. El control (A.11.2.2) tuvo una calificación de veinte (20), se evidencia que alguno de los equipos maneja UPS y reguladores de voltaje para evitar fallos de energía y apagados abrupto. El control (A.11.2.3) tuvo una calificación de veinte (20), se evidencia que hay una infraestructura de red, pero esta se encuentra en un estado bastante deteriorado con el paso de los años y por hechos externos también ha dejado de funcionar en algunas áreas. El control (A.11.2.4) tuvo una calificación de cuarenta (40), se evidencia que realizan mantenimientos preventivos y correctivos, se conectan a los equipos Ups para garantizar flujo eléctrico en caso de apagado por falta de fluido, a si los funcionarios pueden guardar su información después de una falla eléctrica. El control (A.11.2.5) tuvo una calificación de veinte (20), los funcionarios reconocen que los equipos no pueden salir del recinto al menos que se presente una carta de autorización de su jefe directo. No existe documentación sobre este ítem en los repositorios de la Alcaldía, pero verbalmente al asignarle el equipo al funcionario se les hace la anotación o aviso. El control (A.11.2.6) tuvo una calificación de veinte (20), Se evidencia en el manual de inventarios de la administración, un equipo al salir de las instalaciones de la Alcaldía sin el respectivo permiso corre el riesgo de ser robado o averiado, trayendo como consecuencia el pago parcial o total del equipo. El control (A.11.2.8) tuvo una calificación de veinte (20), se evidencia fotografías de los equipos con restricción o clave de acceso, los equipos se colocan en modo bloqueo para poder ser nuevamente accedidos por medio de una credencial de tipo sistema operativo. Para los controles (A.11.2.7, A.11.2.9) se evidencia inexistencia, no hay documentación ni procedimientos.

3.3.2.4 SEGURIDAD DE LAS OPERACIONES

El dominio A.12 SEGURIDAD DE LAS OPERACIONES el objetivo es controlar los procedimientos de las operaciones y su desarrollo, manteniendo documentación actualizada al respecto, asegurando que se realicen correctamente los procesos relacionados con la información. En este dominio se pudo establecer mediante las pruebas solicitadas en la Herramienta MSPI, (Ver Anexo Instrumento de Evaluación MSPI - Hoja TECNICAS - ID. ITEM T.4 - Columna Pruebas), que la Alcaldía Municipal de Icononzo Tolima obtuvo una calificación total de seis (6) en el dominio A.12 SEGURIDAD DE LAS OPERACIONES tomando los resultados de los Objetivos de Control (A.12.1, A.12.2, A.12.3, A.12.4, A.12.5, A.12.6, A.12.7.) promediados. En el Objetivo de Control A.12.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES. El control (A.12.1.1) tuvo una calificación de veinte (20) en el cual se evidencia que los procedimientos de operación de los funcionarios de planta se encuentran documentados (Documentación de contratos) y a disposición en la Alcaldía Municipal de Icononzo Tolima. El control (A.12.1.3) tuvo una calificación de veinte (20) en el cual se evidencia un firewall configurado, este equipo es capaz de proporcionar una restricción de ancho de banda para poder monitorear el tráfico pasante, además se puede bloquear desde el software de los AP UBIQUITI los equipo a los cuales no puedan realizar descargas. Para los controles (A.12.1.2, A.12.1.4) se evidencia inexistencia, no hay documentación ni procedimientos. En el Objetivo de Control A.12.2 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS. El control (A.12.2.1) tuvo una calificación de veinte (20) en el cual se evidencia antivirus instalados en los equipos para la protección de códigos maliciosos, los equipos se le realiza la instalación del software antivirus llamado AVAST, se realizan ejecuciones de actualización por parte del mismo funcionario o el encargado del área de sistemas. No hay documentación al respecto, todo se hace en el acto. En el Objetivo de Control A.12.3 COPIAS DE RESPALDO. Para el control (A.12.3.1) se evidencia inexistencia, no hay documentación ni procedimientos. En el Objetivo de Control A.12.4 REGISTRO Y SEGUIMIENTO. El control (A.12.4.1) tuvo una calificación de veinte (20) en el cual se evidencia que no existe documentación de registros de eventos de seguridad en la alcaldía, se realiza o mitiga la falla una vez ocurre el problema y se ataca para no se maneja registro de eventos. Para los controles (A.12.4.2, A.12.4.3, A.12.4.4) se evidencia inexistencia, no hay documentación ni

procedimientos. En el Objetivo de Control A.12.5 CONTROL DE SOFTWARE OPERACIONAL. Para el control (A.12.5.1) se evidencia inexistencia, no hay documentación ni procedimientos. En el Objetivo de Control A.12.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA. Para el control (A.12.6.1) se evidencia inexistencia, no hay documentación ni procedimientos. El control (A.12.6.2) tuvo una calificación de veinte (20) en el cual se evidencia un firewall configurado, no existe documentación para establecer la implementación de las reglas, pero por medio del firewall se puede configurar reglas para restringir las descargas de las páginas o contenidos a los equipos mediante la MAC. En el Objetivo de Control A.12.7 CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN. Para el control (A.12.7.1) se evidencia inexistencia, no hay documentación ni procedimientos.

3.3.2.5 SEGURIDAD DE LAS COMUNICACIONES

El dominio A.13 SEGURIDAD DE LAS COMUNICACIONES buscar asegurar y proteger la información a través de los diferentes canales de comunicación que maneja la entidad. En este dominio se pudo establecer mediante las pruebas solicitadas en la Herramienta MSPI, (Ver Anexo Instrumento de Evaluación MSPI - Hoja TECNICAS - ID. ITEM T.5 - Columna Pruebas), que la Alcaldía Municipal de Icononzo Tolima obtuvo una calificación total de trece (13) en el dominio A.13 SEGURIDAD DE LAS COMUNICACIONES tomando los resultados de los Objetivos de Control (A.13.1, A.13.2) promediados. En el Objetivo de Control A.13.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES. El control (A.13.1.1) tuvo una calificación de cuarenta (40) en el cual se evidencia un firewall configurado, no existe documentación para establecer la implementación de las reglas, pero por medio del firewall se puede configurar reglas para restringir las descargas de las páginas o contenidos a los equipos mediante la MAC. El control (A.13.1.2) tuvo una calificación de veinte (20) en el cual se evidencia contratos que se hacen con proveedores, quedan anexos las cláusulas de contrato con los terceros para la prestación de servicios donde se evidencian los términos contractuales o ANS para cuando se presenten fallas en el servicio saber qué pasos realizar. Para el control (A.13.1.3) se evidencia inexistencia, no hay documentación ni procedimientos. En el Objetivo de Control A.13.2 TRANSFERENCIA DE INFORMACIÓN. El control (A.13.2.3) tuvo una calificación de veinte (20) en el cual se evidencia dispositivos de almacenamiento externos como USB, discos

duros, carpetas compartidas y alojamiento de información en servidores externos. La información es respaldada en carpetas compartidas a un servidor (NO todos los equipos tienen carpetas compartidas con el server), los funcionarios son responsables de guardar o realizar sus Backus en memorias flash o servidores externos como ONE drive, Dropbox, Drive etc. Para los controles (A.13.2.1, A.13.2.2, A.13.2.4) se evidencia inexistencia, no hay documentación ni procedimientos.

3.3.2.6 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

El dominio A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS se enfoca en la protección de los activos de la organización a los cuales los proveedores o terceros tienen acceso. En este dominio se pudo establecer mediante las pruebas solicitadas en la Herramienta MSPI, (Ver Anexo Instrumento de Evaluación MSPI - Hoja TECNICAS - ID. ITEM T.6 - Columna Pruebas), que la Alcaldía Municipal de Icononzo Tolima obtuvo una calificación total de diez (10) en el dominio A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS tomando los resultados de los Objetivos de Control (A.14.1, A.14.2, A.14.3) promediados. En el Objetivo de Control A.14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN. El control (A.14.1.1) tuvo una calificación de veinte (20) en el cual se evidencia que al implementar o comprar algún sistema o software, se debe incluir los requisitos en los contratos como cláusula para mejorar los sistemas de información. Para el control (A.14.1.2) se evidencia inexistencia, no hay documentación ni procedimientos. El control (A.14.1.3) tuvo una calificación de veinte (20) en el cual se evidencia que no existe documentación en los repositorios de la Alcaldía, pero todos los funcionarios de la Alcaldía manejan sus propias claves de acceso a sus plataformas de uso diario que son administradas por el proveedor. Estas contraseñas no se proporcionan a otros trabajadores. En el Objetivo de Control A.14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE. El control (A.14.2.2) tuvo una calificación de veinte (20) en el cual se evidencia que No hay documentación existente para este ítem, los cambios en los desarrollos quedan en los repositorios de los proveedores. Dentro de los contratos quedan establecidos cómo será el ciclo de vida del software. No se tiene acceso a los diferentes controles por parte del proveedor de software. El control (A.14.2.4) tuvo una calificación de veinte (20) en el cual se evidencia que

estas modificaciones las realiza el proveedor de software con autorización de la persona que solicita el cambio y posterior capacitación a los funcionarios de la entidad que utilicen este software. Para los controles (A.14.2.1, A.14.2.3, A.14.2.5, A.14.2.6, A.14.2.7, A.14.2.8, A.14.2.9) se evidencia inexistencia, no hay documentación ni procedimientos. En el Objetivo de Control A.14.3 DATOS DE PRUEBA. Para el control (A.14.3.1) se evidencia inexistencia, no hay documentación ni procedimientos.

3.3.2.7 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

El dominio A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN busca aplicar un proceso de mejora continua en la gestión de incidentes de seguridad de la información de tal forma que se aplique las acciones preventivas o correctivas en el tiempo oportuno. En este dominio se pudo establecer mediante las pruebas solicitadas en la Herramienta MSPI, (Ver Anexo Instrumento de Evaluación MSPI - Hoja TECNICAS - ID. ITEM T.7 - Columna Pruebas), que la Alcaldía Municipal de Icononzo Tolima obtuvo una calificación total de seis (6) en el dominio A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN tomando los resultados de los Objetivos de Control (A.16.1) promediando los controles. En el Objetivo de Control A.16.1 GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN. El control (A.16.1.3) tuvo una calificación de veinte (20) en el cual se evidencia que actualmente al reportar un fallo, el funcionario llama al personal de sistemas y este revisa que o como tratar el incidente de seguridad y así tomar las debidas correcciones. El control (A.16.1.6) tuvo una calificación de veinte (20) en el cual se evidencia que el personal de la entidad al adquirir conocimiento sobre un incidente, este se hace público para que otros funcionarios no repitan lo mismo. Para los controles (A.16.1.1, A.16.1.2, A.16.1.4, A.16.1.5, A.16.1.7) se evidencia inexistencia, no hay documentación ni procedimientos.

3.3.2.8 CONCLUSIONES VULNERABILIDADES TÉCNICAS

Se identifica que en el Instrumento de Evaluación MSPI (Modelos de Seguridad y Privacidad de la Información) en la pestaña “TÉCNICAS”, el dominio que obtuvo la calificación

más baja es: ID. ITEM: T.6 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS, con una calificación actual de Cero (5) puntos y su EVALUACIÓN DE EFECTIVIDAD ES: INICIAL.

También se identificó el dominio con más alta puntuación: ID. ITEM: T.3 - SEGURIDAD FÍSICA Y DEL ENTORNO, con una calificación de Catorce (14) puntos y su EVALUACIÓN DE EFECTIVIDAD ES: INICIAL.

Toda la información detallada en este capítulo se encuentra plasmada en tabla de vulnerabilidades Administrativas y Técnicas y puede evidenciarse en el Anexo Instrumento de Evaluación MSPI en las hojas denominadas Administrativas y Técnicas para un seguimiento a profundidad.

Durante la realización de este proceso, se hace recolección de evidencias fotográficas y documentos físicos de los dominios que presentaron calificación mayor a cero (0). Ver Anexo: Evidencia Fotográfica Vulnerabilidades Técnicas y Vulnerabilidades Administrativas. Y se entrega matriz de vulnerabilidades identificadas. Ver Anexo: Matriz de vulnerabilidades Técnicas y Administrativas.

3.4 RECOMENDACIONES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El diagnóstico de seguridad y privacidad de la información realizado en la Alcaldía Municipal de Icononzo Tolima se centró en la detección de falencias correspondientes a las medidas de seguridad, privacidad y protección de los activos de información y la misma información contenida en ellos, así como la verificación de cumplimiento de normatividades establecidos por organizaciones regulatorias quienes solicitan de manera precisa informar sobre el avance de las actividades estipuladas para las entidades gubernamentales.

Las recomendaciones mencionadas a continuación, son un ítem de libre elección para la entidad a los cuales la Alcaldía Municipal de Icononzo Tolima puede acogerse buscando mejorar

de gran manera cada aspecto incluido dentro del desarrollo de las actividades de protección de activos y su información, así como el mejoramiento de los ítems ya existentes que permitan dar cumplimiento con lo solicitado por las entidades regulatorias con respecto al mejoramiento organizacional, la seguridad de los datos, sus contenedores y los responsables de los mismos. Las recomendaciones registradas a continuación se establecen de acuerdo a los dominios identificados en la Herramienta MSPI descritos en la tabla de Evaluación de efectividad de controles y las matrices de vulnerabilidades técnicas y Administrativas dando prioridad a necesidades esenciales en la organización y permitirán cubrir un nivel inicial de privacidad y seguridad de la información.

3.4.1 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

- Se recomienda establecer un documento con las políticas que expresen de manera global los métodos y normatividades de protección de la información y los activos.
- Se recomienda la divulgación del documento con las políticas de seguridad y privacidad de la información a todos los usuarios.
- Se recomienda establecer métodos de actualización de las políticas de acuerdo a los cambios organizacionales y posibles actualizaciones en el desarrollo de actividades.
- Se recomienda establecer el ámbito de aplicación describiendo los departamentos, área, procesos y actividades de la organización a los que aplican las políticas de seguridad y privacidad de la información.
- Se recomienda informar las políticas a todas las partes externas involucradas con los procesos de la organización.

3.4.2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

- Se recomienda almacenar la información y archivos de registro en una base de datos que permita ser analizada de manera periódica y que permita el acceso por si se presenta algún incidente

- Se recomienda establecer cuentas separadas para las actividades administrativas o de gestión asegurando que las credenciales administrativas se revisan y cambian periódicamente.
- Se recomienda supervisar y gestionar cuentas inactivas de usuarios tanto de personal que se retiró de la entidad temporal o permanentemente
- Se recomienda establecer procesos para incluir alertas de notificación inmediata a todos los administradores del sistema para el personal que ya no está en la organización. Así mismo para usuarios que se transfieran a otro departamento dentro de la organización.
- Se recomienda definir y asignar claramente roles y responsabilidades para la privacidad y seguridad de la información.

3.4.3 SEGURIDAD DE LOS RECURSOS HUMANOS

- Se recomienda capacitar al personal de la organización buscando una eficiente respuesta ante posibles incidentes.
- Se recomienda realizar revisiones de verificación de antecedentes de los candidatos al empleo ofrecidos en la entidad permitiendo cumplir con las regulaciones de acuerdo con la clasificación de la información a la cual se le dará acceso.
- Se recomienda requerir a todos y cada uno de los empleados aplicar la seguridad en concordancia con las políticas y los procedimientos establecidos por la entidad.
- Se recomienda establecer y documentar procedimientos de entrega de responsabilidades laborales, cargos e información para cada empleado al terminar su vinculación con la entidad.

3.4.4 GESTIÓN DE LOS ACTIVOS

- Se recomienda de manera precisa hacer levantamiento de licencias para todos y cada uno de los aplicativos involucrados dentro de los procesos ejecutados en la organización.

- Se recomienda ubicar los equipos de red y principales activos de información en una habitación o armario cerrados. Ubicación de equipos a una zona más segura.
- Se recomienda hacer un levantamiento preciso del inventario de los activos de información en la entidad, el cual debe identificar y valorar cada uno de estos.
- Se recomienda implantar medidas para el uso adecuado de la información y los activos que la contienen.

3.4.5 CONTROL DE ACCESO

- Se recomienda utilizar VPN de acceso de usuarios que cuenten con tecnologías SSL.
- Se recomienda utilizar lista de accesos a redes y permisos que limiten el acceso a los recursos de la entidad.
- Se recomienda la difusión de la SSID únicamente a personal de la organización y protección del acceso mediante cifrado de contraseñas tales como la WPA.
- Se recomienda establecer restricciones de acceso a los servicios de red limitándose mediante el acceso
- Se recomienda poner en práctica directivas de contraseñas complejas para las cuentas vinculadas a los procesos en la organización que cumplan condiciones como: Deben ser contraseñas alfanuméricas, deben contener mayúsculas y minúsculas, deben contener al menos un carácter especial y que sean contraseñas con longitud mínimo de 10 caracteres. Así mismo para limitar los riesgos, es necesario implementar controles de caducidad de estas contraseñas y bloqueo de cuentas después de 3 intentos fallidos.
- Se recomienda poner en práctica métodos de autenticación tales como tokens, tarjetas inteligentes a los aplicativos misionales en la organización.
- Se recomienda segmentar la red con lo cual se busca limitar el acceso de los servicios suministrados, así como el acceso por parte de terceros tales como proveedores, fabricantes, o usuarios externos a la estructura organizacional.
- Se recomienda la implementación de mecanismos de detección de intrusos (NIDS) basados en la red o basados en el host (HIDS), asegurando la continua

actualización de firmas y tecnologías correspondientes.

- Se recomienda establecer un proceso de desactivación de cuentas para el personal que ya no esté en la organización, y una continua revisión del listado de permisos.
- Se recomienda desactivar las funciones de actualización automática de las soluciones antivirus en todos los sistemas para evitar la utilización de archivos potencialmente peligrosos antes de su comprobación
- Se recomienda utilizar cortafuegos y otro dispositivo que permita proteger los recursos de la organización en el perímetro. Este dispositivo debe mantener una configuración restrictiva para permitir solo el tráfico necesario y correspondiente al desarrollo de las labores organizacionales.

3.4.6 CRIPTOGRAFÍA

- Se recomienda utilizar algoritmos de cifrado estándar que permitan proteger la confidencialidad de la información en caso de intercepción, robo o perdida.
- Se recomienda la utilización de software o soluciones de cifrado de disco buscando no poner en riesgo la confidencialidad en caso de robo de algún equipo de la entidad.

3.4.7 SEGURIDAD FÍSICA Y DEL ENTORNO

- Se recomienda el mejoramiento de los controles físicos existentes y el uso en todos los equipos informáticos de la organización.
- Se recomienda la instalación de sistemas de alarmas buscando la detección de acceso de intrusos a las instalaciones de la entidad.
- Se recomienda establecer controles adicionales de acceso físico evitando el ingreso de personal no autorizado a las instalaciones de la entidad.
- Se recomienda evaluar de manera periódica todos y cada uno de los controles que se establezcan para la seguridad física y del entorno.
- Se recomienda evaluar todos los controles de acceso físico para garantizar que son adecuados.

3.4.8 SEGURIDAD DE LAS OPERACIONES

- Se recomienda capacitación a usuarios de acuerdo a los roles que desempeñan garantizando que estos entiendan que se espera de ellos y como deben cumplir con los aspectos de seguridad.
- Se recomienda el uso de antivirus con una estructura general que permita controlar activamente a los clientes de los servidores desde una consola administrativa.
- Se recomienda implementar configuración de cuentas separadas para usuarios administrativos y de gestión y modificación de estas cuentas de manera periódica.
- Se recomienda utilizar equilibradores de carga eléctrica tales como UPS o reguladores buscando obtener un alto nivel de disponibilidad de los servicios y la no detención de los procesos.
- Se recomienda realizar pruebas a las aplicaciones, software o soluciones adquiridas validando los datos de entrada y el procesamiento que estos realizan buscando evidenciar de manera precisa la integridad de la información.

3.4.9 SEGURIDAD DE LAS COMUNICACIONES

- Se recomienda establecer procedimientos para la creación de informes de incidentes y sus respuestas, problemas o preocupaciones sobre seguridad.
- Se recomienda definir roles y responsabilidades quienes serán acreedores de las actividades de comunicaciones dentro y fuera de la organización.
- Se recomienda establecer acuerdos documentados que permitan establecer de manera segura la transferencia de información entre la entidad y los Stakeholders o terceros.
- Se recomienda establecer métodos de protección la información correspondiente a la mensajería electrónica.

3.4.10 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS

- Se recomienda crear un plan en colaboración con el fabricante de los sistemas de información con el fin de mitigar las vulnerabilidades de seguridad.
- Se recomienda probar todas y cada una de las aplicaciones o soluciones adquiridas para la organización y el procesamiento de sus actividades.
- Se recomienda al adquirir nuevos sistemas, validar la existencia de métodos de control de autenticación y que estos sean proporcionales a las necesidades de seguridad de la organización.
- Se recomienda solicitar de manera habitual a los fabricantes información sobre actualizaciones para los sistemas implantados en la organización. Si existen estas actualizaciones, descárguelas y pruébelas antes de implantarlas de manera permanente.

3.4.11 RELACIONES CON LOS PROVEEDORES

- Se recomienda establecer cláusulas en los contratos de soluciones adquiridas con proveedores que permitan entender de manera clara el alcance de cada aspecto de y servicio prestado por estos.
- Se recomienda establecer medidas de protección tales como la no divulgación de la información para cada acuerdo que se adquiera con proveedores.
- Se recomienda monitorear de manera periódica todas y cada una de las actividades de prestación de servicios por parte del proveedor.

3.4.12 GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

- Se recomienda establecer medidas para informar incidentes buscando garantizar una respuesta inmediata y eficaz frente a estos.
- Se recomienda establecer canales de comunicación que permitan informar los

incidentes presentados.

- Se recomienda capacitar a los usuarios para dar respuesta ante los incidentes cumpliendo con políticas y normatividades establecidas por la entidad.
- Se recomienda registrar la presentación de incidentes buscando reducir la probabilidad o impacto de incidentes futuros.
- Se recomienda establecer medidas de recopilación de información que sirvan de evidencia ante la presentación de incidentes.
- Se recomienda evaluar los eventos presentados que afecten la privacidad y seguridad de la información para su posterior clasificación.

3.4.13 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

- Se recomienda implementar métodos de copias de seguridad y realizar pruebas a estos validando su buen funcionamiento y la disponibilidad de la información contenida en ellos.
- Se recomienda designar un equipo de respuesta de emergencia que incluya representantes de varias disciplinas, incluida tecnología, recursos humanos y legales para responder a todos los incidentes y problemas de seguridad.
- Se recomienda implementar planes de recuperación ante desastres y de reanudación de negocio. Estos planes deben estar documentados y deben ser actualizados periódicamente para asegurar la recuperación en un período de tiempo aceptable.
- Se recomienda establecer un proceso de creación de informes de incidentes documentado para garantizar que todos los problemas e incidentes se revisan y se evalúen de manera periódica.

3.4.14 CUMPLIMIENTO

- Se recomienda dar inicio de manera inmediata a la segunda fase del MPSI para dar cumplimiento a lo requerido por el Ministerio de Tecnologías de la Información y las Comunicaciones.

- Se recomienda contratar un especialista en el área de Seguridad de la Información quien de apoyo para realizar los procedimientos exigidos por las entidades regulatorias.
- Se recomienda identificar, documentar y actualizar para cada sistema de información y para la organización todos los requisitos estatutarios, normativos y contractuales legislativos que son exigidos por las entidades regulatorias.
- Se recomienda establecer métodos que permitan proteger contra pérdidas, destrucción, falsificación, accesos y publicación no autorizada, la información de la organización de acuerdo con los requisitos legales.
- Se recomienda establecer métodos que permitan garantizar la privacidad y la protección de la información personal según lo requiera la normatividad y legislaciones vigentes.
- Se recomienda revisar regularmente los sistemas de información para verificar su cumplimiento con las políticas y normas de seguridad dispuestas la alta gerencia.

4 CONCLUSIONES

La Alcaldía Municipal de Icononzo Tolima se encuentra en un nivel de gestión de seguridad y privacidad de la información menor a la inicial solicitado por el Ministerio de Tecnologías de la Información y las Comunicaciones. Esto conlleva a que corra un alto riesgo con respecto a la protección de su información y pueda contraer multas o penalizaciones que incurren en afectaciones económicas de alto impacto.

Se evidencia que como no se han establecido políticas siendo el inicio de los procesos de seguridad de la información, no hay concepción de la falta de controles y medidas para este aspecto.

La entidad debe acelerar la implantación del Modelo de Seguridad y Privacidad de la Información para poder cubrir los requisitos que el Ministerio de Tecnologías de la Información y las Comunicaciones ha establecido para esta entidad.

Al no contar con personal encargado de los procesos de seguridad de la información, la Alcaldía Municipal de Icononzo Tolima desconoce de gran manera como debe ejecutar los procesos establecidos para el mejoramiento de las actividades relacionadas a la protección de los activos y la información contenida en los mismos. Sin embargo, el Ministerio no exige que la persona que implemente y proceda con el MSPI tenga estos conocimientos.

Para acoplarse a la estrategia Gobierno en Línea, la Alcaldía Municipal de Icononzo Tolima debe iniciar de manera inmediata con las fases planificación e implementación del Modelo de Seguridad y Privacidad de la Información. De lo contrario, se verá afectada en el desarrollo de sus actividades por no acatar normatividades establecidas para este tipo de entidades.

La entidad se encuentra en un cambio de sede, lo cual hace que el ejecutar actividades correspondientes a la seguridad y privacidad de la información no sean de prioridad alta para el

desarrollo de los objetivos institucionales.

El desarrollar este tipo de proyectos en entidades públicas se ve limitado por las normatividades y legislaciones que restringen los accesos de los ejecutores y el acceso a la información de la organización.

Para la implementación del Modelo de Seguridad y Privacidad de la Información no es necesario que sea ejecutado por especialistas o expertos en el tema, pero debe cumplirse de manera precisa el desarrollo de este basado en estándares y normatividades establecidas por las entidades regulatorias.

5 ANEXOS

Los anexos que se involucran a continuación se encuentran en carpetas que se adjuntan con el documento del proyecto Diagnostico de Seguridad y Privacidad de la Información - Alcaldía Municipal de Icononzo Tolima, se menciona el anexo y la ruta donde podrán ser visualizados.

1. Instrumento de Evaluación MSPI. Ruta de Acceso: \Proyecto\Anexos
2. Carta Presentación y Aceptación. Ruta de Acceso: \ Proyecto\Anexos
3. Cuestionario Familiarización. Ruta de acceso: \ Proyecto\Anexos
4. Evidencia fotográfica Administrativa. Ruta de Acceso: \Proyecto\Anexos\Evidencias\Administrativas\ Evidencia Fotográfica
5. Evidencia Documental Administrativa. Ruta de Acceso: \Proyecto\Anexos\Evidencias\Administrativas\ Evidencia Documental
6. Evidencia Fotográfica Técnica. Ruta de Acceso: \Proyecto\Anexos\Evidencias\Técnicas
7. Matriz de Vulnerabilidades Técnicas y Administrativas. Ruta de Acceso: \Proyecto\Anexos
8. Informe de Hallazgos General Vulnerabilidades. Ruta de Acceso: \Proyecto\Anexos

6 BIBLIOGRAFÍA

Ministerio de las Tecnologías de la Información y las Comunicaciones. (2017). *MinTIC*. Obtenido de http://www.mintic.gov.co/portal/604/w3-propertyvalue-540.html

Ministerio de Tecnologías de la Información y las Comunicaciones. (2015). *Gobierno en Linea*. Obtenido de http://estrategia.gobiernoenlinea.gov.co/623/w3-channel.html

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Modelo de Seguridad y Privacidad de la Información. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Ministerio de las Tecnologías de la Información y las Comunicaciones. http://www.mintic.gov.co. Obtenido de http://www.mintic.gov.co/portal/604/articles3586_documento.pdf

Instituto Geográfico Agustin Codazzi. (2017). Instituto Geográfico Agustin Codazzi. Obtenido de https://www.igac.gov.co

Alcaldía Municipal de Icononzo Tolima. (2017). Nuestro Municipio. Obtenido de http://www.icononzo-tolima.gov.co/informacion_general.shtml