MODELO DE SEGURIDAD YPRIVACIDAD DE LAINFORMACION

INDICADORES

ALCALDIA MUNICIPAL DE CHIA

Oficina de Tecnologías de la Información y las Comunicaciones

Chía, 28 de septiembre 2023

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El modelo de seguridad y privacidad de la información MSPI, mantiene la importancia de perseverar en la seguridad de los datos y contribuye a la minimización de riesgos relacionados con pérdidas, hace más eficiente la gestión y asegura el cumplimiento de las labores de Contexto del Instituto de Cultura y Turismo de Bolívar, apoyando el uso adecuado de las TIC.

El nivel de seguridad y privacidad de la información ha sido establecido por el Gobierno Nacional en cabeza del Ministerio de Tecnologías de Información y las Comunicaciones – MinTIC para las entidades públicas a través de la Resolución 746 del 11 de marzo de 2022, "por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021". *"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el Modelo de Seguridad y Privacidad de la Información como habilitador de la política de Gobierno Digital"*. Es por eso que el MinTIC establece lineamientos con el objetivo de generar confianza en el uso del entorno digital, garantizando el máximo aprovechamiento de las tecnologías de la información y las comunicaciones en las Entidades Públicas.

2. JUSTIFICACIÓN

El presente documento "Modelo de seguridad y privacidad de la información - MSPI" es importante pues establece la confidencialidad, integridad y disponibilidad de los datos, lo que permite asegurar la privacidad de estos a través del proceso de gestión de riesgos y da confianza a las partes interesadas de la correcta gestión de riesgos.

3. OBJETIVO GENERAL.

Implementar la norma NTC/IEC ISO 27001:2022, estrategia de gestión digital, política nacional de seguridad digital, CONPES 3854 seguridad de datos y actividades de planificación de privacidad de acuerdo con las leyes disponibles vigentes.

3.1 Objetivos Específicos

- Mantener instrucciones para el manejo de la información digital como parte de la seguridad y privacidad de la información.
- Utilizar la implementación del sistema de gestión de seguridad de la información del Instituto de Cultura y Turismo de Bolívar de acuerdo a los requisitos estipulados en el modelo de seguridad y privacidad de la información de acuerdo con los estándares requeridos en la estrategia de gobierno digital.
- Gestionar los riesgos de seguridad y privacidad de la información, seguridad digital y continuidad del negocio.
- Reducir las interrupciones en la seguridad y privacidad de los datos, seguridad digital de manera efectiva, eficiente y eficaz.
- Crear conciencia sobre los cambios organizacionales necesarios para implementar la seguridad y privacidad de los datos como un enfoque central para el Instituto de Cultura y Turismo de Bolívar.
- Cumplir los requisitos derivados de la ley sobre seguridad y privacidad de la

información, seguridad digital y protección de datos personales.

4. MODELO DE SEGURIDAD MSPI

El modelo de seguridad y privacidad de MSPI de la estrategia de gobierno digital explora los siguientes ciclos de acción, que incluyen cinco (5) pasos para permitir que las entidades gestionen adecuadamente la seguridad y la privacidad de sus activos de información.

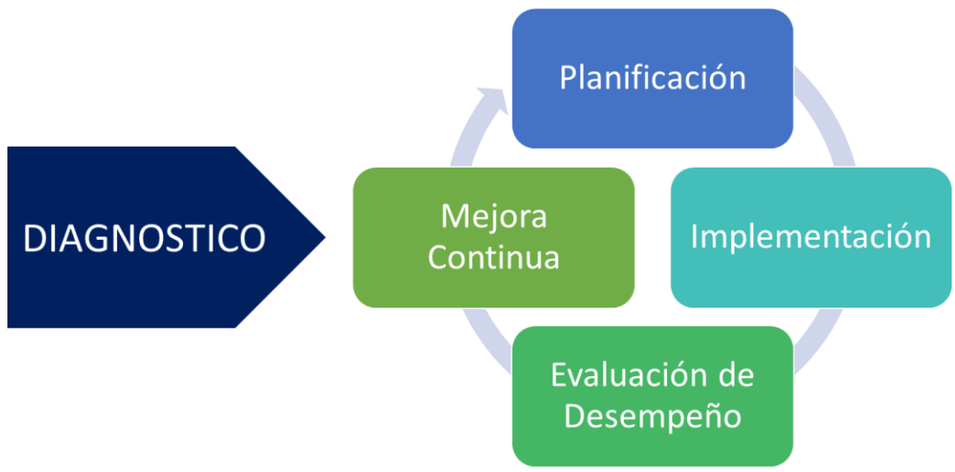


Figura 1 Ciclo de operación Modelo de Seguridad y Privacidad de la Información Fuente: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

Figura 2. Fases MSPI http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

5. FASE DE DIAGNOSTICO

Esta etapa de DIAGNÓSTICO según ISO 27001:2022 en el Capítulo 4 - Contexto Organizacional determina la necesidad de analizar los problemas externos e internos del Instituto de Cultura y Turismo de Bolívar y su contexto, incluye los requisitos y expectativasde las partes interesadas de la organización para lograr el alcance del SGSI.

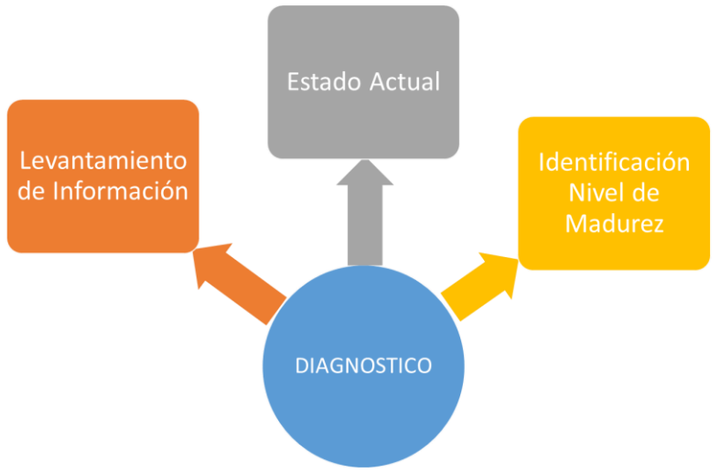


Figura 3 Etapas previas a la implementación Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pd

5.1 ESTADO ACTUAL DEL INSTITUTO DE CULTURA Y TURISMO DE BOLÍVAR

5.1.1 Conocimiento del Instituto

5.1.1.1 Misión

Garantizar a sus habitantes una oportuna y efectiva prestación de los servicios con calidad en materia de salud, educación, seguridad, construcción de obras de infraestructura, ordenamiento territorial, medio ambiente, crecimiento socio – cultural, deportivo y erradicación de la pobreza, promoviendo la participación comunitaria en aras de mejorar la calidad de vida de nuestros ciudadanos y de quienes visitan nuestro territorio.

5.1.1.2 Visión

En el año 2027 el Instituto de Cultura y Turismo de Bolívar será líder en desarrollo sostenible caracterizada por una cultura emprendedora, empoderada del medio ambiente, participativa, solidaria yorgullosa de su patrimonio e historia.

5.1.1.3 Valores Éticos

Son formas de ser y actuar de las personas que son altamente deseables como atributos o cualidades nuestras y de los demás, por cuanto posibilitan la construcción de una convivencia gratificante en el marco de la dignidad humana.

Responsabilidad: Obligación de responder por los propios actos. Capacidad para reconocer y hacerse cargo de las consecuencias de las propias acciones.

Respeto: Miramiento, consideración, deferencia del otro. Reconocimiento de la legitimidad del otro para ser distinto de uno.

Honestidad: Moderación en la persona, las acciones o las palabras. Honradez, decencia. Actitud para actuar con honradez y decencia.

Transparencia: Se refiere al comportamiento claro, evidente, que no deja dudas y que no presenta ambigüedad. Es lo contrario de la opacidad, que no deja ver, que esconde. Se sitúa en el ámbito de la comunicación, del suministro de información, de la rendición de cuentas a la sociedad.

5.1.1.4 Organización del Instituto de Cultura y Turismo de Bolívar

5.2 IDENTIFICACION DEL NIVEL DE MADUREZ

Se utilizó la herramienta de evaluación MINTIC MSPI para identificar el nivel de madurez en seguridad y privacidad de la información del Instituto de Cultura y Turismo de Bolívar , la cualarrojó el siguiente resultado:

Figura 4- Nivel de madurez en seguridad y privacidad de la información.

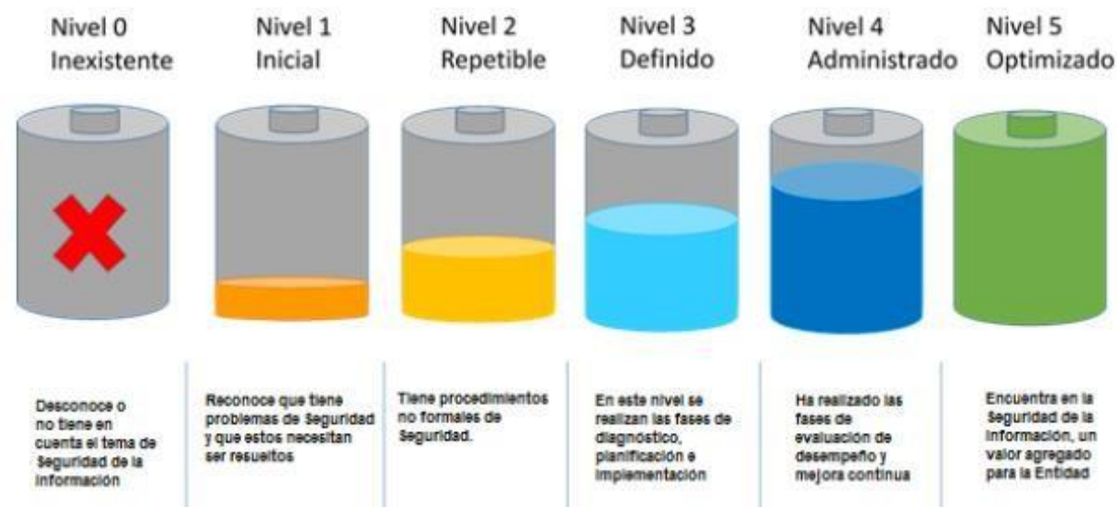


Figura 5- Niveles de madurez Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

5.3 LEVANTAMIENTO DE INFORMACIÓN

Son partes interesadas del Instituto de Cultura y Turismo de Bolívar, las entidades públicas yprivadas legalmente constituidas, que interactúan con la misma; teniendo presente los requisitos normativos internos, legales o reglamentarios y las obligaciones contractuales.

PARTES INTERESADAS	DEFINICION
GOBIERNO	**MINISTERIO DE LAS TIC**
	Órganos de control, Ministerio de las Tic, Función Pública, Contraloría General de la Republica entre otras.
FUNCIONARIOS	**Funcionarios de Planta o Provisionales**: Personas vinculadas a la entidad bajo una relación legal y reglamentaria para el cumplimiento de funciones administrativas u otras en el marco de personal aprobada.
	Contratistas: Personas naturales que apoyan a las que trabajan en la Alcaldía de actividades del que hacer propio y misional de la Institución (Alcaldía) mediante la modalidad de prestación de servicio.
PROVEEDORES	Persona Natural, jurídica u organización que tiene vínculo contractual con el Instituto, para suministrar bienes, obras o servicios.
COMUNIDAD	Ciudadanos que están interesados en la misión propia de la institución.

Tabla 1 Partes Interesadas

Figura 6. Mapa de procesos

https://icultur.gov.co/Documentos/Transp_estructura-organica/D4762996-BEDB-45A9-87C5-F484BDA96B8F.jpeg

5.3.1 Clasificación de Activos de Información

6. FASE DE PLANIFICACIÓN

Esta fase de PLANIFICACIÓN que cumple con ISO 27001:2022 en el Capítulo 5 - Liderazgo, define las responsabilidades y obligaciones de la alta dirección en relación con el sistema de gestión de seguridad de la información, incluida la necesidad de que la alta dirección prepare una política de seguridad de la información adecuada a la alcaldía, que asegura la distribución de los recursos del SGSI, la distribución, comunicación de responsabilidades y roles importantes desde el punto de vista de la seguridad de la información.

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

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

Figura 7. Fase de planificación Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

6.1 Contexto del Instituto de Cultura y Turismo de Bolívar.

6.1.1 Generalidades

El Instituto de Cultura y Turismo de Bolivar es una entidad territorial que forma parte de la organización territorial de la República y tiene autonomía política, fiscal y administrativa para gestionar sus intereses dentro de los límites de la Constitución y la ley y con base enla política TIC de la República. ámbito relacionado con la política de gobierno digital del Gobierno Nacional, establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTic) y normativa de planificación del sector TIC.

A través del Modelo de Seguridad y Privacidad de la información - MSPI, mediante su implementación se crea una estrategia integral de seguridad de la información, la cual se implementa de manera integrada con el sistema de gestión de seguridad de la información, debido a que la norma ISO/IEC 27001:2013 se basa en ambos sistemas y los lineamientos técnicos desarrollados por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, que brindan apoyo integral a otras áreas de la estrategia de gobierno digital: TIC para el Estado y TIC para la sociedad.

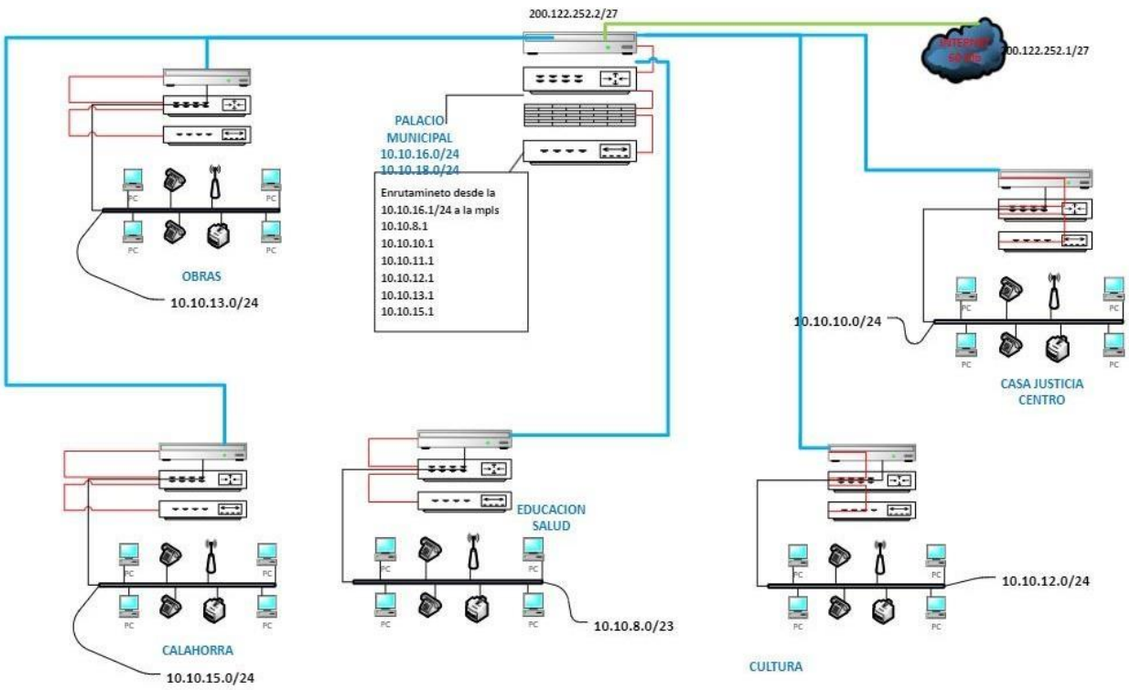
6.1.2 Contexto Tecnológico

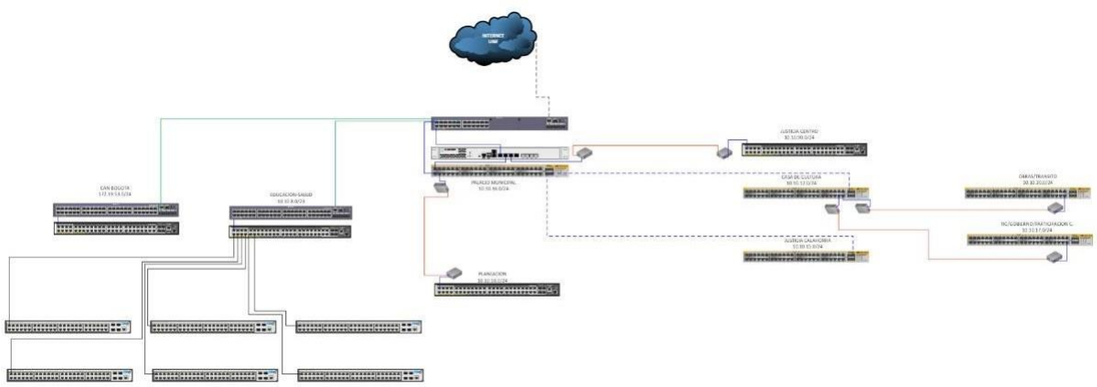
Conexiones: La conectividad del conjunto está asegurada mediante un canal propio de fibra óptica, que posibilita la conexión con diversas instituciones del municipio. De esta forma, el canal de comunicación puede soportar las necesidades del conjunto. El Instituto, considerando la infraestructura física, la cantidad de oficinas y personal que allí trabaja, así como la planta y los contratistas, requiere una arquitectura de conectividad híbrida para operar, es decir. debe tener conectividad por cable e inalámbrica, también se deben definir los tipos de perfiles de uso de la red Wi-Fi.

Red local: La red local (LAN) debe garantizar que la red de fibra óptica llegue a la red troncal y pueda distribuirse con al menos cableado categoría 5e en cada

ubicación. El análisis de segmentos se realizó según el número de oficinas administrativas. LAN inalámbrica: Se realizará una revisión para optimizar la calidad del diseño actual de la red Wi-Fi, la cual deberá incluir el perfilamiento de los usuarios para su uso y gestión. Los cambios de contraseña también se producen periódicamente.

Canal Internet: El servicio está diseñado para brindar tráfico de Internet saliente y entrante para toda la unidad, oficinas y áreas Wi-Fi.





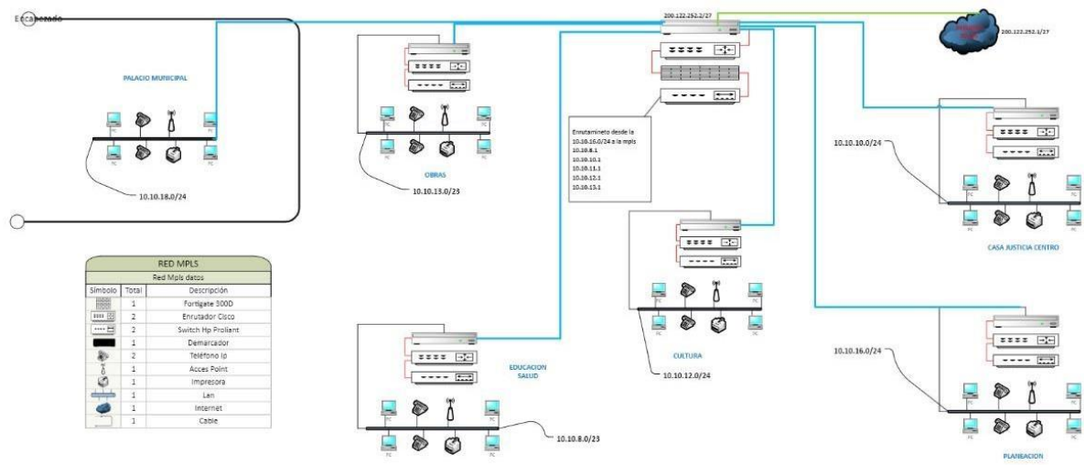


Figura 7 Arquitectura Red Servidores imagen propia

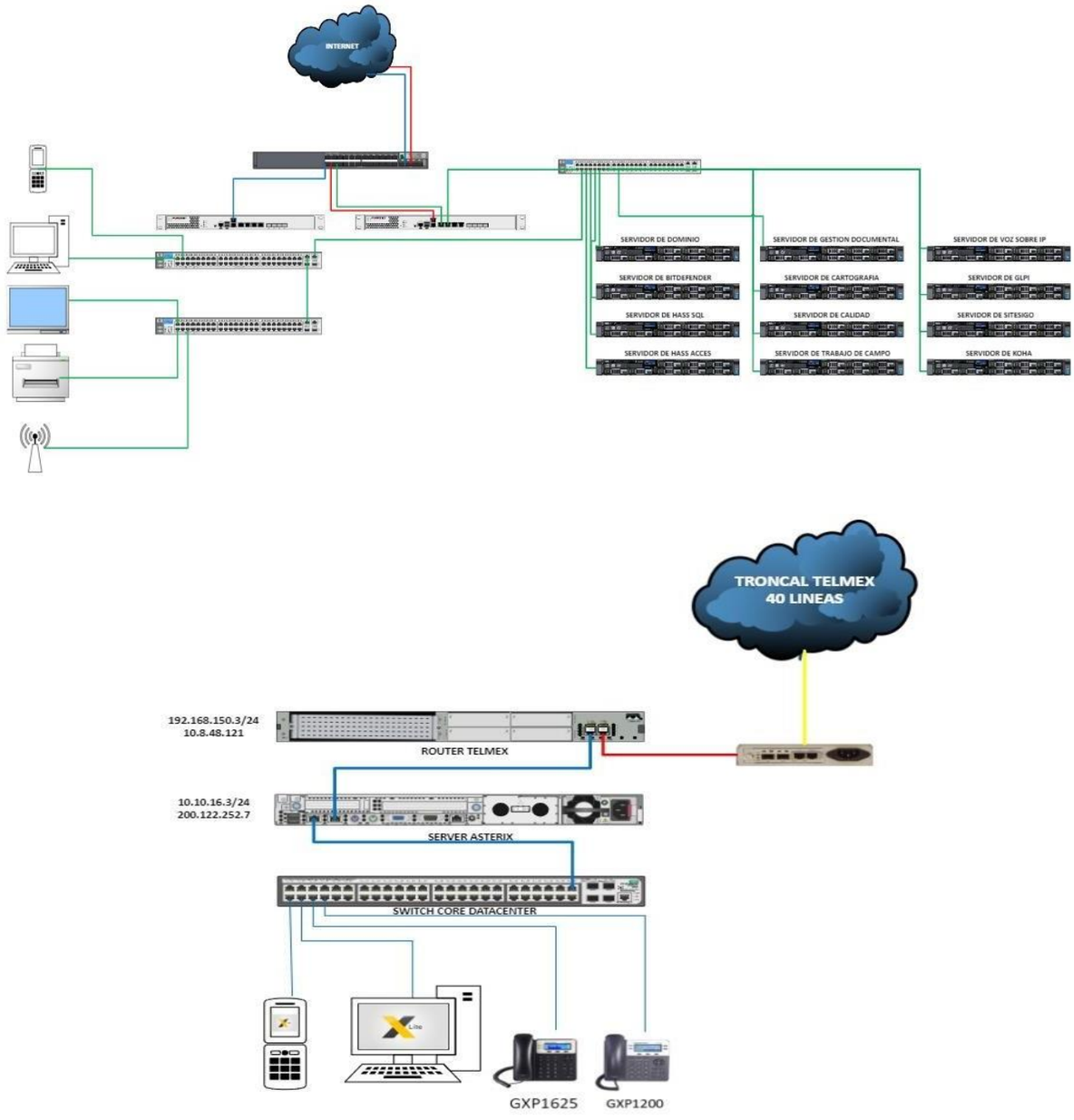


Figura 8. Arquitectura Red Telefonía imagen propia

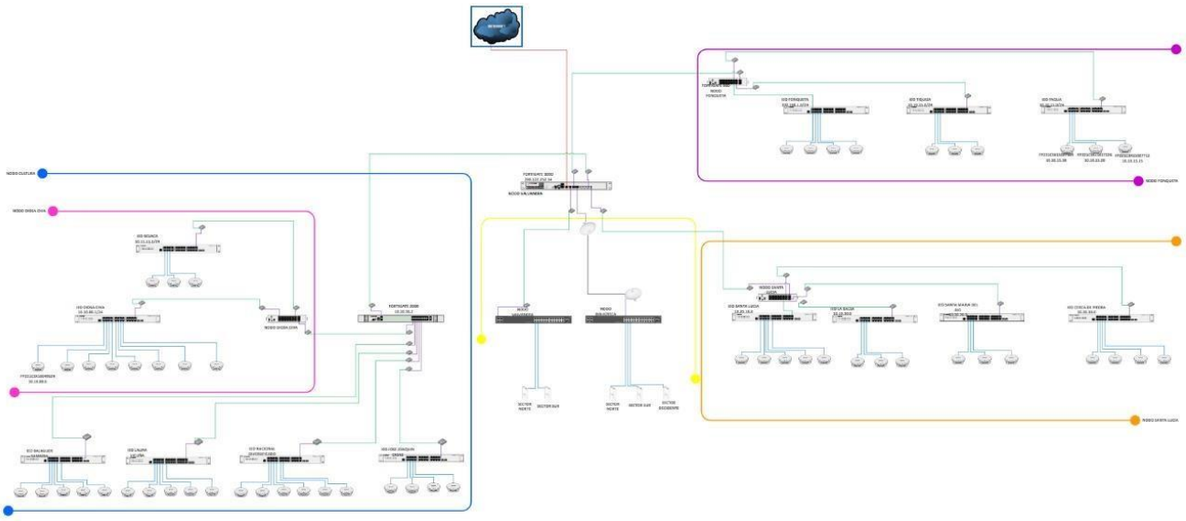


Figura 9. Arquitectura Red Colegios imagen propia

6.1.3 Expectativas de las Partes Interesadas

Partes Interesadas	Necesidades	Requisitos	Solicitud	Expectativas
Administraci Municipal GOBIERNO	Contar con la información en los plazos establecidos	Disposición de recursos financieros para la implementación del MSPI Cumplir con la normatividad aplicable Definir directrices y políticas ajustadas a las condiciones operacionales de la Alcaldía	Determinar las normas aplicables para el MSPI	Cumplir con los requerimientos y las directrices establecidas por los diferentes entes Gubernamentales.
				Mejorar la imagen de la institucionalidad e incrementar el nivel de competitividad
FUNCIONARIOS	Contar con herramientas tecnologías aprobadas	Apoyo tecnológico que permita seguir las directrices establecidas del SGSI	Políticas de Seguridad	Aprobación del SGSI, a través de aplicación de la políticas.
		Disponibilidad del servicio	Acuerdo de confidencialidad	Obtener Integridad y confidencialidad de la información

		Disponibilidad del servicio	Documentos del MSPII	Obtener una disponibilidad de los servicio Cumplimento de los acuerdos de nivel de servicio
PROVEEDORES	Especificaciones técnicas de lo requerido, acorde a las políticas de seguimientos del SGSI.	Cumplimiento en tiempos de entrega pactados.	Acuerdo de confidencialidad con terceros	Minimizar el riesgo del uso. inadecuado de la información
			Política de seguridad actualizada	Proteger con todo los controles de seguridad
COMUNIDAD	Información	Transparencia en el desarrollo de los procesos institucionales del Instituto	Aplicar las directrices establecidas por gobierno digital	Facilitar el acceso a la información pública de manera permanente (transparencia y acceso a la información) ley 1712
		Consistencia y veracidad de la información suministrada por la institución		

Tabla 2 Expectativas Partes Interesadas

6.1.4 Alcance del MSPI

Alcance del Modelo de Seguridad y Privacidad de la Información - Instituto de Cultura y Turismo MSPI aplica a todos los procesos, funcionarios, proveedores, contratistas, comunidad y quienes comparten, usan, recaudan, procesan de acuerdo a sus funciones, intercambiar o consultar información y monitorear entidades o sujetos que tengan acceso interno o externo a cualquier tipo de información sin importar su ubicación; De esta manera, nuestro objetivo es proteger y preservar la integridad ydisponibilidad de los activos de información.

6.2 Liderazgo

6.2.1 Liderazgo y Compromiso de la Alta Dirección

El Instituto de Cultura y Turismo de Bolivar se compromete a liderar la implementación del MSPI, y a gestionar la asignación de los recursos necesarios para garantizar la seguridad de la información del Instituto, delegando en la Oficina TIC, la responsabilidad de la elaboración, implementación, seguimiento y a los planes, para mejorar el modelo de seguridad y privacidad de la información.

6.2.2 Política de Seguridad

El Instituto de Cultura y Turismo de Bolívar entendió la importancia de una adecuada gestión de la información y apuesta por la implementación de un sistema de gestión de seguridadde la información que tenga como objetivo crear un marco confidencial para el cumplimiento de sus deberes con el Estado y la ciudadanía, estrictamente de acuerdo con la ley y de acuerdo con la misión y visión de la unidad. Para el instituto, el objetivo de la protección de la información es reducir sistemáticamenteel impacto de los riesgos identificados en nuestros activos para mantener un nivel deexposición que nos permita ser responsables de la integridad, confidencialidad ydisponibilidad de la información, seguridad de información, según las necesidadesde los distintos grupos de interés.

Como se indicó anteriormente, este modelo de seguridad y privacidad de la información, aplica a la Administración, sus empleados, terceros, pasantes, practicantes, proveedores y ciudadanía en general, siempre que los principios por los cuales las acciones o decisiones relacionadas con el SGSI estén determinadas por lo siguiente:

- Cumplimiento de los principios de seguridad de la información.
- Mantener la confianza de la ciudadanía, aliados y empleados.
- Apoyar la innovación tecnológica.
- Protege los activos tecnológicos.
- Preparar principios, procedimientos e instrucciones sobre seguridad de la información.
- Fortalecer la cultura de seguridad de la información del instituto.
- Asegurar la continuidad del negocio ante eventos e incidencias.
- El instituto decidió definir, implementar, utilizar y mejorar continuamente un sistema de gestión de seguridad de la información sustentado en lineamientos claros de acuerdo a las metas planteadas en el Plan de Desarrollo Municipal y la normatividad. (MinTIC, 2022)

6.2.3 Roles y Responsabilidades (Anexo. 2 Documento de Gestión de Roles y responsabilidades MSPI)

RECURSO HUMANO	Funcionarios responsables	ROL	RESPONSABILIDADES
COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO	JEFES DE AREA (Secretarios, Directores, Jefes de Oficina)	Alta Dirección	Aprobación del MSPI y de la Gestión de roles y responsabilidades. Apoyo implementación MSPI Gestión Estratégica
COMITÉ DE SEGURIDAD DE LA INFORMACION	CONTROL INTERNO DISCIPLINARIO, AREA JURIDICA, PLANEACION, GESTION DE CALIDAD, CONTRATACION, OFICINA ASESORA DE COMUNICACIÓN, PRENSA Y PROTOCOLO, OFICINA TIC.	Toma de decisiones.	Toma de decisiones frente a la seguridad de la Información

LIDER DE TECNOLOGÍA	JEFE DE OFICINA TIC	Responsable MSPI.	Liderazgo y responsabilidad del MSPI Gestión estratégica y táctica
PARTES INTERESADAS.	TODAS LAS SECRETARIAS/DEPENDENCIAS DE LA ADMINISTRACION MUNICIPAL	Cumplimiento MSPI.	Dar estricto cumplimiento a lo estipulado en el MSPI.
FUNCIONARIOS SOPORTE TECNICO Y ESPECILIZADO.	MESA DE AYUDA	Apoyo operativo de las actividades requeridas del MSPI	Gestión operativa y apoyo al Oficial de Seguridad de la Información o quien haga sus veces y Especialista de Seguridad Informática.
ESPECIALISTA SEGURIDAD INFORMATICA.	OPS o Funcionario de Planta OFICINA TIC	Apoyo operativo de las actividades requeridas del MSPI	Gestión operativa y apoyo al Oficial de Seguridad de la Información o quien haga sus veces.
GRUPO DE INFRAESTRUCTURA TECNOLOGICA	OPS o Funcionario de planta OFICINA TIC	Gestión de la transición y migración IPv4 a IPv6 Ejecución de actividades del MSPI	Implementar las estrategias de apropiación de los servicios tecnológicos
GRUPO DE DESARROLLO DE SISTEMAS DE INFORMACIÓN	Líder del área de desarrollo y OPS	Ejecución de actividades del MSPI	Implementar estrategias de seguridad en los sistemas de información desarrollados por la Oficina TIC

Tabla 3. Roles y responsabilidades

Responsabilidades:

- ✓ Generar análisis y evaluación de riesgos TIC.
- ✓ Identificación de riesgos TIC.
- ✓ Incorporación de la gestión de riesgos TIC.
- ✓ Evaluación de tratamiento de riesgos TIC.
- ✓ Validar la implementación y operación del SGSI y MSPI.
- ✓ Implementación del plan de tratamiento de riesgos TIC para lograr los objetivos de control identificados.

6.3 PLANEACIÓN

6.3.1 Acciones para abordar Los Riesgos y Oportunidades
6.3.1.1 Identificación Valoración y Tratamiento de los Riesgos.

El Instituto de Cultura y Turismo de Bolívar realiza la identificación y evaluación de las amenazasde las vulnerabilidades relativas a los activos de información, ya sea sistemas deinformación, infraestructura y recurso humano, la probabilidad de ocurrencia y suimpacto. Documento reservado por características de su naturaleza.

N°	RIESGOS	CODIGO	PESO GB
1	Divulgacion de informacion	R-02	23,5163
2	Perdida de informacion	R-15, R-16, R-17, R-18, R-44	11,0951
3	Alteracion de copias de seguridad	R-03, R-28, R-29, R-30	25,7588
4	Compromiso de la informacion	R-25, R-33, R-34	0,40356
5	Denegacion de los Servicios	R-53, R-54	0,3457
6	Robo de informacion	R-05, R-06, R-07, R-65, R-67	0,54605
7	Alteracion de la informacion	R-08, R-09, R-10, R-11, R-49, R-50	2472,60362
8	Manipulacion de la informacion	R-12, R-13, R-14	10,10016
9	Fuga de informacion	R-19, R-20, R-21, R-22	4,25562
10	Permisos de roles mal gestionados	R-27, R-66	39,1155
11	Destruccion de la informacion	R-39, R-40, R-41	98,99783223
12	perdida de bases de datos	R-32	2,6729
13	Acceso a la informacion confidencial	R-36, R-37, R-38	211,6766
14	Conexión de red a la base de datos	R-23, R-24, R-25	6,495
15	Alteracion de base de datos	R-26, R-42	25,0558
16	destruccion de equipos	R-61	0,3434
17	Acceso no autorizado	R-46, R-62	114,55154
18	No disponibilidad de la informacion fallas de medio de transmision	R-63	260,39783
19	Falla de seguridad	R-43	4,56117
20	Alteracion de usuarios y contraseñas	R-45	0,3887
21	Perdida economica	R-47, R-48	0,04783
22	Daños del sistema	R-51, R-52	0,5383
23	Codigo malicioso	R-55, R-56	12,0346
24	Caida de los sistemas	R-57, R-58	38,827964
25	Indisponibilidad de los sistemas	R-59, R-60	26,38059623
26	Daño fisico	R-64	0,7743
		Total	**3391,484772**

Tabla 4. Identificación de riesgos vs peso

CODIG	INFORMACION	RIESGO	DEPENDENCIA/SECRETARIA					
R-01	GDRC-03 - BACKUP	Divulgación de información	Gestión de Derechos y Resolución de Conflictos	R-01 Divulgación de información			PROBABILI	IMPACTO
R-01	GGS-02 - BACKUP Saray	Perdida de información	Gestión de gobierno y seguridad	R-01 Perdida de información	R-02	Divulgación de información	2	3

R-01	GGS-05 - BACKUP	Perdida de información	Gestión de gobierno y seguridad	R-01 Perdida de información	R-03	Alteración de copias de seguridad	4	3

R-02	GGS-06 - BACKUP Sisben	Divulgación de información	Gestión de gobierno y seguridad	R-02 Divulgación de información	R-04	Robo de información	4	4
R-02	GGS-08 - BACKUP EMERGENCIAS	Divulgación de información	Gestión de gobierno y seguridad	R-02 Divulgación de información	R-05	Robo de información	2	4
R-03	GTH-01 - BACKUP FUNCIÓN PÚBLICA	Alteración de copias de seguridad	Gestión de contratación	R-03 Alteración de copias de seguridad	R-06	Robo de información	3	4
R-03	GM-08 - PLANES MANEJO MOVILIDAD	Manipulación de la información	Planificación estratégica	R-03 Manipulación de la información	R-07	Robo de información	3	4
R-03	GE-18 - BACKUP	Manipulación de la información	Gestión educativa	R-03 Manipulación de la información	R-08	Alteración de la información	4	5
R-03	GC-01 - BACKUP	Alteración de copias de seguridad	Gestión de contratación	R-03 Alteración de copias de seguridad	R-09	Alteración de la información	4	4
R-03	GF-03 - BACKUP	Compromiso de la información	Gestión financiera	R-03 Compromiso de la información	R-10	Alteración de la información	2	5
R-03	GF-06 - BACKUP	Compromiso de la información	Gestión financiera	R-03 Compromiso de la información	R-11	Alteración de la información	2	5
R-04	GF-031 - BACKUP	Compromiso de la información	Gestión financiera	R-04 Compromiso de la información	R-12	Manipulación de la información	4	5
R-04	TIC-54 - LICENCIAS OFFICE	Denegación de los servicios	TIC	R-04 Denegación de los servicios	R-02	Pérdida económica	2	4
R-04	GMA-01 - COMFIS	Robo de información	Gestión de medio ambiente	R-04 Robo de información	R-13	Manipulación de la información	3	2

R-05	GGS-02 - INFORMES	Robo de información	Gestión de medio ambiente	R-05 Robo de información	R-14	Manipulación de la información	4	4
R-05	GGS-02 - REGISTRO DE VENTAS INFORMALES	Robo de información	Gestión de medio ambiente	R-05 Robo de información	R-15	Perdida de información	4	4
R-06	GSD-02 - PLATAFORMA JUVENTUDES	Robo de información	Gestión social para el desarrollo	R-06 Robo de información	R-17	Perdida de información	4	5
R-07	GSA-01 - SEGUROS Y POLIZAS	Robo de información	Comunicación estratégica	R-07 Robo de información	R-18	Perdida de información	3	4
R-07	GSA-02 - BACKUP	Robo de información	Comunicación estratégica	R-07 Robo de información	R-19	Fuga de información	3	3
R-08	GE-03 - VARIOS 2022-2023	Alteración de la información	Comunicación estratégica	R-08 Alteración de la información	R-20	Fuga de información	3	3
R-09	GGS-04 - VARIOS	Alteración de la información	Gestión de Gobierno y seguridad	R-09 Alteración de la información	R-21	Fuga de información	3	4
R-10	GE-05 - MATRICULAS - COBERTURA	Alteración de la información	Gestión educativa	R-10 Alteración de la información	R-22	Fuga de información	3	4
R-11	GC-06 - CONTRATOS AÑO 2023	Alteración de la información	Gestión contratación	R-11 Alteración de la información	R-23	Conexión de red a la base de datos	4	3
R-15	GSA-03 - RESOLUCIONES Y DECRETOS	Perdida de información	Gestión de servicios administrativos	R-15 Perdida de información	R-24	Conexión de red a la base de datos	2	4
R-11	GDI-01 - EXPEDIENTES 2022,2023	Perdida de información	Gestión disciplinaria	R-11 Perdida de información	R-25	Compromiso de la información	3	5
R-12	GDI-03 - EXPED Y DILIG AÑO 2016	Manipulación de la información	Gestión disciplinaria	R-12 Manipulación de la información	R-26	Alteración de base de datos	4	5

R-12	GDI-04 - DOCUMENTOS DE SUPERVISION	Manipulación de la información	Gestión disciplinaria	R-12 Manipulación de la información	R-27	Permisos de roles mal gestionados	3	4
R-13	GDS-01 - DERECHOS DE PETICION	Manipulación de la información	Gestión urbanística	R-13 Manipulación de la información	R-28	Alteración en copias de seguridad	4	5
R-13	GDS-01 - VARIOS DIR. CULTURA	Manipulación de la información	Gestión urbanística	R-13 Manipulación de la información	R-29	Alteración en copias de seguridad	4	4
R-14	GU-01 - INVENTARIO EXPEDIENTES	Manipulación de la información	Gestión urbanística	R-14 Manipulación de la información	R-30	Alteración en copias de seguridad	3	5
R-14	GAC-01 - DERECHOS DE PETICIÓN	Manipulación de la información	Gestión de atención a la ciudadanía	R-14 Manipulación de la información	R-31	Perdida de base de datos	4	5
R-15	GU-01 - DATOS CARTOGRAFICOS	Perdida de información	Gestión urbanística	R-15 Perdida de información	R-32	Perdida de base de datos	3	4
R-15	GU-02 - NORMA URBANISTICA	Perdida de información	Gestión urbanística	R-15 Perdida de información	R-33	Compromiso de la información	4	4
R-15	GU-03 - LEGALIZACION ASENTAMIENTO HUMANO	Fuga de información	Gestión urbanística	R-15 Fuga de información	R-34	Compromiso de la información	2	5
R-15	GU-04 - SHAPEFILE 2022	Fuga de información	Gestión urbanística	R-15 Fuga de información	R-36	Acceso a la información confidencial	4	4
R-15	GU-05 - DOTP	Fuga de información	Gestión urbanística	R-15 Fuga de información	R-37	Acceso a la información confidencial	3	5

R-16	GC-01 - RESPUESTAS ENTES DE CONTROL	Perdida de información	Gestión de contratación	R-16 Perdida de	R-38	Acceso a la información	2	4

				información		confidencial		
R-16	GC-02 - CONTRATOS	Perdida de información	Gestión de contratación	R-16 Perdida de información	R-39	Destrucción de la información	3	4
R-16	GC-03- PLAN ANUAL DE INVERSION	Perdida de información	Gestión de contratación	R-16 Perdida de información	R-40	Destrucción de la información	4	4
R-16	GS-07 - DANÉS -2022	Perdida de información	Gestión de salud	R-16 Perdida de información	R-41	Destrucción de la información	2	4
R-16	GDRC-01 - VARIOS	Divulgación de información	Gestión de Derechos y Resolución de Conflictos	R-16 Divulgación de información	R-42	Alteración de base de datos	4	5
R-17	GDRC-02 - CONCILIACIONES	Perdida de información	Gestión de Derechos y Resolución de Conflictos	R-17 Perdida de información	R-43	Falla de seguridad	2	4
R-17	GDRC-04 - SARAY CASTRO	Perdida de información	Gestión de Derechos y Resolución de Conflictos	R-17 Perdida de información	R-44	Perdida de información	3	5
R-17	GDRC-05 - CONCILIACION CASA DE JUSTICIA	Perdida de información	Gestión de Derechos y Resolución de Conflictos	R-17 Perdida de información	R-45	Alteración de usuarios y contraseñas	4	5
R-17	GDRC-06 - ARCHIVO INSPECCIÓN I	Perdida de información	Gestión de Derechos y Resolución de Conflictos	R-17 Perdida de información	R-46	Acceso no autorizado a los sistemas	2	4
R-18	GDRC-07 - ARCHIVO CALAHORRA	Perdida de información	Gestión de Derechos y Resolución de Conflictos	R-18 Perdida de información	R-47	Pérdida económica	3	5
R-18	GGS-01 - CONTRATACIÓN	Divulgación de información	Gestión de gobierno y seguridad	R-18 Divulgación de información	R-48	Pérdida económica	4	5

R-18	GGS-03 - ACTAS	Divulgación de información	Gestión de gobierno y seguridad	R-18 Divulgación de información	R-49	Alteración de la información	3	5
R-18	GGS-04 - DOCUMENTOS	Divulgación de información	Gestión de gobierno y seguridad	R-18 Divulgación de información	R-50	Alteración de la información	3	5
R-18	GGS-07 - CARPETA ARCHIVOS 2022	Divulgación de información	Gestión de gobierno y seguridad	R-18 Divulgación de información	R-51	Daños del sistema	4	5
R-19	GGS-09 - CONTRATOS SUPERVISIONES 2016-2022	Fuga de información	Gestión de gobierno y seguridad	R-19 Fuga de información	R-52	Daños del sistema	4	5
R-19	GGS-10 - HASNET	Fuga de información	Gestión de gobierno y seguridad	R-19 Fuga de información	R-53	Denegación de servicios	3	4
R-19	GGS-11 - DRIVE	Fuga de información	Gestión de gobierno y seguridad	R-19 Fuga de información	R-54	Denegación de servicios	2	4
R-20	GM-02 - ARCHIVO FÍSICO	Fuga de información	Gestión de movilidad	R-20 Fuga de información	R-55	Código malicioso	2	4
R-20	TIC-01 - DOCUMENTOS	Permisos de roles mal gestionados	Tecnologías de la información y las comunicaciones	R-20 Permisos de roles mal gestionados	R-65	Robo de información	3	5
R-20	TIC-022 - DESARROLLOS	Permisos de roles mal gestionados	Tecnologías de la información y las comunicaciones	R-20 Permisos de roles mal gestionados	R-66	Permisos de roles mal gestionados	3	4
R-20	TIC-02 - PUNTO VIVE DIGITAL	Destrucción de la información	Tecnologías de la información y las comunicaciones	R-20 Destrucción de la información	R-58	Robo de información	3	4
R-21	GSD-03 - INFORMACIÒN DESARROLLO SOCIAL	Fuga de información	Gestión social para el desarrollo	R-21 Fuga de información	R-59	Indisponibilidad de los sistemas	4	4

R-21	GSD-04 - SEGUIMIENTO LEY DE ESPECTÁCULOS PÚBLICOS	Fuga de información	Gestión social para el desarrollo	R-21 Fuga de información	R-60	Indisponibilidad de los sistemas	4	5
R-21	GSD-05 - INVENTARIO ACTIVO	Fuga de información	Gestión social para el desarrollo	R-21 Fuga de información	R-61	Destrucción de equipos	4	5
R-21	GTH-02 - CUOTAS PARTES PENSIONALES Y PENSIONADOS	Alteración de copias de seguridad	Gestión de contratación	R-21 Alteración de copias de seguridad	R-62	Acceso no autorizado	3	4
R-21	TIC-03 - REDES CHIA 2020-2023	Alteración de copias de seguridad	Tecnologías de la información y las comunicaciones	R-21 Alteración de copias de seguridad	R-63	No disponibilidad de la información fallas de medio de transmisión	3	5
R-22	GTH-04 - ARCHIVO FÍSICO FUNCIÓN PÚBLICA	Fuga de información	Gestión de contratación	R-22 Fuga de información	R-64	Daño físico	3	5
R-22	GF-01 - COMFIS	Permisos de roles mal gestionados	Tecnologías de la información y las comunicaciones	R-22 Permisos de roles mal gestionados	R-65	Robo de información	3	5
R-22	TIC-022 - DESARROLLOS	Permisos de roles mal gestionados	Tecnologías de la información y las comunicaciones	R-22 Permisos de roles mal gestionados	R-66	Permisos de roles mal gestionados	3	4
R-34	GC-02 - CONTRATACIÓN	Fuga de información	Gestión de contratación	R-34 Fuga de información	R-67	Robo de información	4	5

Tabla 5. Riesgo probabilidad, impacto

Anexo 3: Valoración del riesgo en los activos de información
Documento Reservado

6.3.1.2 Plan de Comunicaciones MSPI

Objetivo	Que se comunica	Frecuencia	Responsable	Estrategia de	A quien se Comunica

				Comunicación	
Dar a conocerla ley 1712 de 2014 transparencia y acceso a la información pública con el fin de generar la cultura de transparencia, legalidad e integridad en la administración	ley 1712 de 2014 transparencia y acceso a la información pública y su decreto reglamentario 1081 de 2015	Semestralmente	Funcionario asignado Jefe de Oficina TIC	Página web, redes sociales, correo institucional Banner portal web	Comunidad Chiense y ciudadanía en general
Dar a conocer el uso y los beneficios que plantea el Gobierno Nacional con la iniciativa de datos abiertos	Información relevante para la comunidad Chiense del uso y apropiación de datos abiertos	Semestralmente	Funcionarios asignados Oficina TIC	Página Web, redes sociales, correo institucional Banner portal web, datos.gov.co	Comunidad Chiense y ciudadanía en general
Fortalecer los conocimientos en los usuarios finales en el uso de los recursos informáticos	uso y apropiación de recursos informáticos	anualmente / cuando se requiera	Funcionario designado por el Jefe de Oficina TIC	Inducciones funcionarios - prestadores de servicio - wallpaper pantallas institucionales - correo institucional	Personal administrativo - prestadores de servicio
Socializar información relevante relacionada con MSPI y SGSI	Tip de seguridad - seguimiento a la mejora continua	Trimestralmente - cuando se requiere	secretarios y funcionario asignado de por el Jefe de Oficina TIC	Correo inducción reinducción redes sociales institucionales talleres de gestión - wallpaper pantallas institucionales - correo institucional	Personal administrativo - prestadores de servicio

Tabla 6. Plan de Comunicaciones

6.3.1.3 PLAN DE TRANSICIÓN DE IPV4 A IPV6

De acuerdo al Modelo de Seguridad y Privacidad de la Información del Ministerio de las tecnologías, para realizar la adopción del protocolo de seguridad IPv6, se deben realizar las siguientes etapas así:

Fases de Transición a IPv6

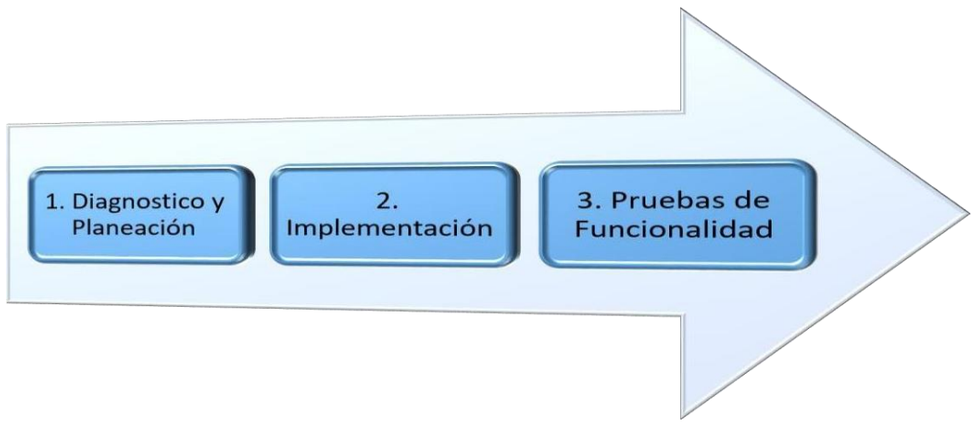


Figura 10. Lineamiento MinTIC Guía N°20, de transición IPv4 a IPv6
Fases del proceso de transición del protocolo IPv4 al IPv6

El plan estratégico consiste en realizar un análisis de la plataforma tecnológica en la infraestructura de red con el fin de ir identificando todos los elementos de red necesarios para la conexión a través de IPv6 en sus plataformas, también cabe resaltar que el plan está sujeto a una constante mejora a medida del avance en las diferentes etapas del desarrollo, su alcance es poder llevar a cabo una migración controlada en la medida que se vaya activando IPv6, esto con la finalidad de generar el menor riesgo posible de perdida de servicios existentes o algún comportamiento inesperado frente a su activación.

Figura 11. Fases del plan de migración IPv4 a IPv6 - Lineamiento MinTIC

Para el desarrollo del plan de direccionamiento se tuvo en cuenta las necesidades actuales que tiene la entidad y para poder cubrirlas se realizó de la siguiente manera:

Se tomó un bloque /44 este podrá ser subdividido en 16 redes /48 asumiendo que la entidad actualmente tiene en promedio 15 sedes, cubriría la necesidad actual y cada una de estas tiene su propio enlace a internet, todas las sedes, convergen a la sede principal para la salida a internet y consumo de recursos local.

Por otra parte, se debe mencionar que cada /48 será utilizado para cada una de las sedes actuales y futuras recordando que el ISP solo puede publicar un /48 menor o igual a un bloqué 48 para la salida a internet, se debe mencionar que la administración y supervisión del recurso IP será supervisado desde la sede principal de la Alcaldía Municipal De Chía.

De acuerdo a la estrategia del plan de direccionamiento se toma una de las redes /48 y esta a su vez se puede subdividir en /52 dieciséis (16 redes), prefijo/52, en la siguiente imagen se puede dar un bosquejo de cómo quedo.

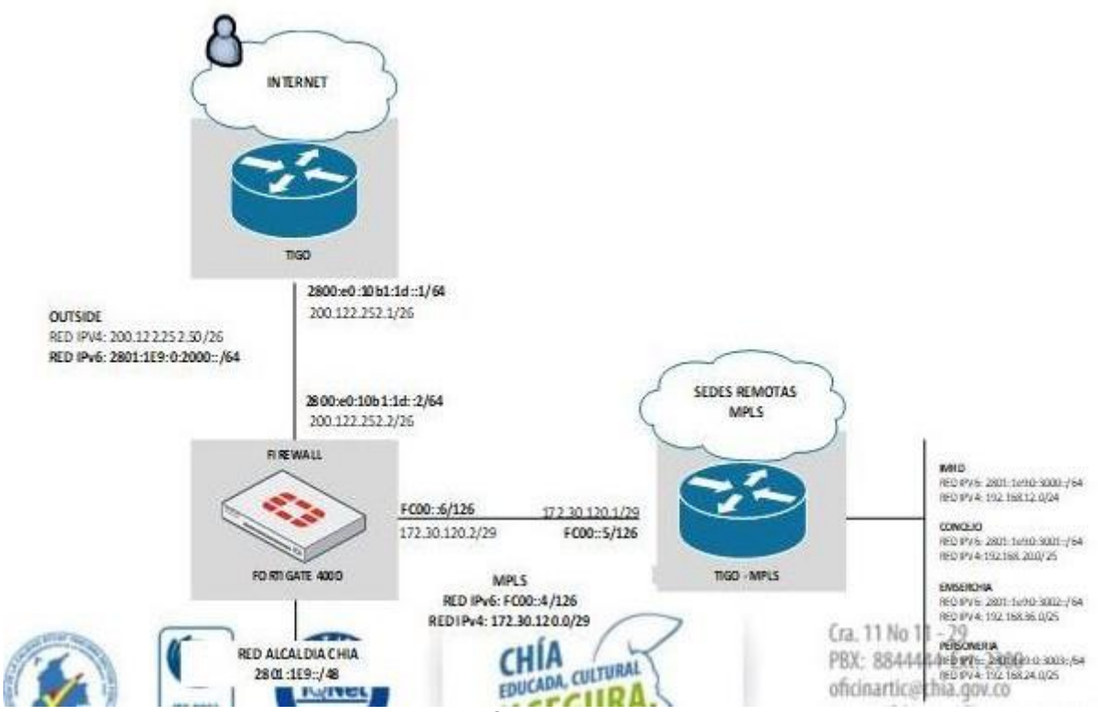
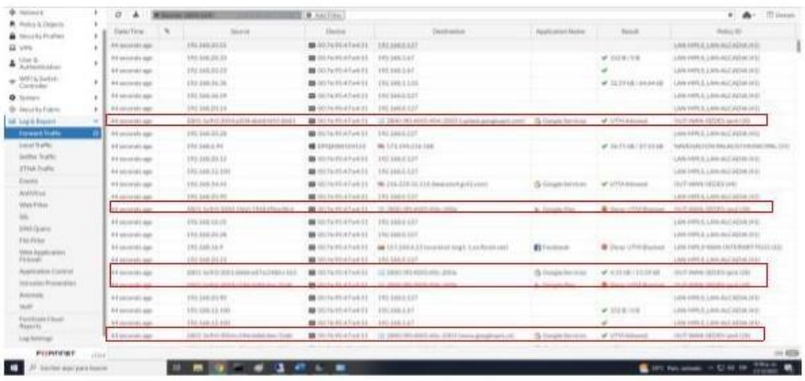
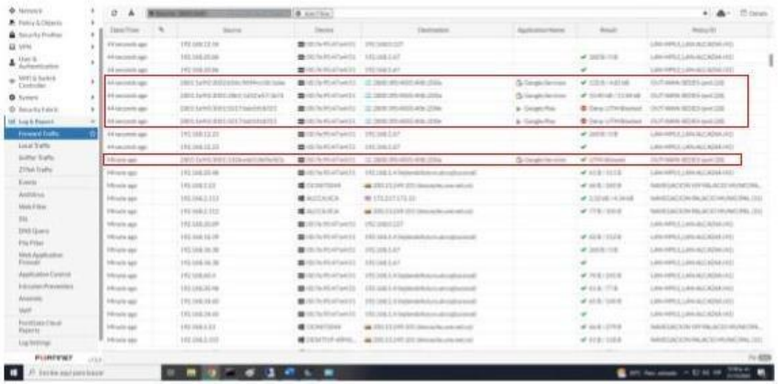


Figura. 12 Diagrama de red lógico, plan de direccionamiento (Dual Stack)

6.3.1.4 Plataforma de Seguridad

Se realizan diferentes pruebas desde el equipo de seguridad perimetral con la que cuenta la entidad de marca Fortinet, con el fin de validar el funcionamiento de IPv6. En la siguiente imagen se puede observar las peticiones que se han originado de los diferentes hosts que hacen parte de la red de datos de la entidad bajo IPv6 a páginas web.





6.4 SOPORTE

6.4.1 Recursos

Dada la importancia del Sistema de Gestión de Seguridad de la información – SGSI que hace parte del Sistema Integrado de Gestión del instituto, para mantenerlo en operación, hacerle seguimiento y mejora, es necesario contar conrecursos económicos y humanos con las competencias específicas, la infraestructura tecnológica actualizada y el apoyo de la Alta Dirección, asignando los recursos anuales, para la adquisición y sostenimiento del mismo. En cuanto al seguimiento y mejora continua se realiza de conformidad con el procedimiento que hace parte MIPG

6.4.2 Competencias, Sensibilización y Comunicación

Competente en la elaboración, sensibilización y comunicación por la estrategia de comunicación.

7. IMPLEMENTACIÓN

Esta Fase IMPLEMENTACION en la norma ISO 27001:2022, capítulo 8 - Operación, indica que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.

7.1 Control y Planeación Operacional

En la fase 5 de diagnóstico del MSPI se pretende alcanzar las siguientes metas:

- Determinar el estado actual de la gestión de seguridad y privacidad de la

información al interior de la Entidad. Estado actual de la entidad, identificando el

nivel de madurez de la misma, levantamiento de la información y emisión del diagnóstico.
• 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.
• Identificación del uso de buenas prácticas en ciberseguridad.

Para ello se recomienda utilizar los siguientes instrumentos, disponibles a través de la página web del Ministerio de Tecnologías de la Información y las Comunicaciones:
• Herramienta de diagnostico
• Instructivo para el diligenciamiento de la herramienta
• Guía No 1 - Metodología de Pruebas de Efectividad
Para realizar dicha fase las entidades deben efectuar la recolección de la información con la ayuda de la herramienta de diagnóstico y la metodología de pruebas de efectividad. Una vez se tenga el resultado del diagnóstico inicial y se haya determinado el nivel de madurez de la entidad, se procede al desarrollo de la fase de Planificación. Los resultados asociados a la fase de Diagnostico previas a la implementación deben ser revisados y socializados por las partes interesadas.

7.2 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información.

El plan de tratamiento de riesgos del Instituto de Cultura y Turismo de Bolívar comoanexo, se encuentra en proceso de aprobación.

7.3 Definición de indicadores de gestión

Según los lineamientos de MinTIC en seguridad y privacidad de la información, los indicadores de gestión están orientados principalmente en la medición de efectividad, eficiencia y eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicadores que servirán como insumo para el componente de mejora continúa permitiendo adoptar decisiones de mejora.

Tiene como objetivo:
- Evaluar la efectividad de la implementación de los controles de seguridad.
- Evaluar la eficiencia del Modelo de Seguridad y Privacidad de la Información al interior de la entidad.
- Proveer estados de seguridad que sirvan de guía en las revisiones del Modelo de Seguridad y Privacidad de la Información, facilitando mejoras en seguridad de la información y nuevas entradas a auditar.
- Comunicar valores de seguridad al interior de la entidad.
- Servir como insumos al plan de análisis y tratamiento de riesgos.

INDICADORES PROPUESTOS

- ✓ **INDICADOR 01**- ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN.

IDENTIFICADOR: SGIN01

DEFINICIÓN: El indicador permite determinar y hacer seguimiento, al compromiso de la dirección, en cuanto a seguridad de la información, en lo relacionado con la asignación de personas y responsabilidades relacionadas a la seguridad de la información al interior de la entidad.
OBJETIVO: Hacer un seguimiento a la asignación de recursos y responsabilidades en gestión de seguridad de la información, por parte de la alta dirección.

TIPO DE INDICADOR: Indicador de Gestión
DESCRIPCIÓN DE VARIABLES FORMULA FUENTE DE INFORMACIÓN
VSI01: Número de personas con su respectivo rol definido según documento Gestión de roles y responsabilidades.
Fuente de información: Plan de tratamiento de riesgos en el marco de seguridad y privacidad de la información.
Formula: (VSI01/VSI02) *100
VSI02: Número de personas con su respectivo rol definió después de un año.
Fuente de información: Actas de asignación de personal.

METAS
MÍNIMA 75-80% **SATISFACTORIA** 80- 90% **SOBRESALIENTE** 91-100%

OBSERVACIONES
De acuerdo a lo establecido en el documento Gestión de roles y responsabilidades, es necesario crear nuevos cargos y/o reingeniería y/o re-estructuración de funciones, según perfiles establecidos.

- ✓ **INDICADOR 02** - TRATAMIENTOS DE EVENTOS RELACIONADOS EN MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

IDENTIFICADOR: SGIN02
DEFINICIÓN: El indicador permite determinar la eficiencia en el tratamiento de eventos relacionados a la seguridad de la información. Los eventos serán reportados por los usuarios o determinadas en las auditorías planeadas para el sistema.
OBJETIVO: El objetivo del indicador es reflejar la gestión y evolución del modelo de seguridad y privacidad de la información al interior de la entidad.

TIPO DE INDICADOR: Indicador de Gestión
DESCRIPCIÓN DE VARIABLES FORMULA FUENTE DE INFORMACIÓN
VSI03: Número de anomalías cerradas.
Formula: (VSI03/VSI04) *100
Fuente de información: Auditorías internas, herramientas de monitoreo.
VSI04: Número total de anomalías encontradas.
Fuente de información: Firewall UTM de última generación fortigate 400E

METAS
MÍNIMA 75-80% **SATISFACTORIA** 81- 90% **SOBRESALIENTE** 91- 100%

- ✓ **INDICADOR 03** – PLAN DE SENSIBILIZACIÓN

IDENTIFICADOR: SGIN03
DEFINICIÓN: El indicador permite medir la aplicación de los temas sensibilizados en seguridad de la información por parte de los usuarios finales. Estas mediciones se podrán realizar por medio de auditorías especializadas en el tema o de forma aislada por parte de los responsables de la capacitación y sensibilización.
OBJETIVO: El objetivo del indicador es establecer la efectividad de un plan de capacitación y sensibilización previamente definido como medio para el control de incidentes de seguridad.

TIPO INDICADOR: Indicador de Gestión
DESCRIPCIÓN DE VARIABLES FORMULA FUENTE DE INFORMACIÓN
VSI05: Número de fallas o no cumplimientos encontrados en las sensibilizaciones programadas o eventos realizados para evaluar el tema.
Formula: (VSI05/VSI06) *100
Fuente de información: listas de asistencia.
VSI06: Total de personal a capacitar.
Fuente de información: Total de funcionarios de la entidad.

METAS
MÍNIMA 75-80% **SATISFACTORIA** 80- 90% **SOBRESALIENTE** 91-100%
OBSERVACIONES: Para el levantamiento de la información que permita obtener datos para la medición el responsable debe idear planes, laboratorios o actividades periódicas que permitan medir lo capacitado o divulgado.

- ✓ **INDICADOR 04** – ESTABLECER POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA ENTIDAD

IDENTIFICADOR: SGIN04
DEFINICIÓN: Establecimiento de políticas de seguridad de la información en la entidad.
OBJETIVO: Busca identificar el nivel de estructuración de los procesos de la entidad orientados a la seguridad de la información.

TIPO INDICADOR: Indicador de Cumplimiento
DESCRIPCIÓN DE VARIABLES FORMULA FUENTE DE INFORMACIÓN
VSI07: ¿La entidad ha definido una política general de seguridad de la información?
Formula: VSI0X = 1(SÍ se evidencia)
VSIOX = 0(NO se evidencia)
Fuente de información: Políticas establecidas y publicadas.

METAS
CUMPLE 1 **NO CUMPLE** 0

- ✓ **INDICADOR 05** – IDENTIFICACIÓN DE LINEAMIENTOS DE SEGURIDAD DE LA ENTIDAD

IDENTIFICADOR: SGIN05
DEFINICIÓN: Grado de la seguridad de la información y los equipos de cómputo.

OBJETIVO: Busca medir el nivel de preparación del recurso humano y su apropiación en cuanto a la seguridad de la información y los equipos de cómputo.

TIPO INDICADOR: Indicador de Cumplimiento
DESCRIPCIÓN DE VARIABLES FORMULA FUENTE DE INFORMACIÓN
VSI10: ¿La entidad ha definido lineamientos de trabajo a través del comité o responsable de seguridad para que sus funcionarios cumplan las políticas de seguridad y evalúa periódicamente su pertinencia?
Formula: VSI0X = 1 (SÍ se evidencia)
VSIOX = 0 (NO se evidencia)
Fuente de información: Usuarios Internos.
VSI11: ¿La entidad ha definido lineamientos en cuanto a la protección de las instalaciones físicas, equipos de cómputo y su entorno para evitar accesos no autorizados y minimizar riesgos de lainformación de la entidad?
Fuente de información: Usuarios Internos.
METAS
CUMPLE 1 **NO CUMPLE** 0

- ✓ **INDICADOR 06** – VERIFICACIÓN DEL CONTROL DE ACCESO

IDENTIFICADOR: SGIN06
DEFINICIÓN: Grado control de acceso en la entidad.
OBJETIVO: Busca identificar la existencia de lineamientos, normas o estándares en cuanto al control de acceso en la entidad.

TIPO INDICADOR: Indicador de Cumplimiento
DESCRIPCIÓN DE VARIABLES FORMULA FUENTE DE INFORMACIÓN
VSI12: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar el acceso de los usuarios a sus servicios de Gobierno en línea y a sus redes de comunicaciones?
Formula: VSI0X = 1 (SÍ se evidencia)
VSIOX = 0 (NO se evidencia)
Fuente de información: Usuarios Internos.
VSI13: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar el uso y el acceso a los sistemas de información, las aplicaciones y los depósitos de información con las que cuenta la entidad?
VSI14: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar las terminales móviles y accesos remotos a los recursos de la entidad?
Fuente de información: Usuarios Internos.
METAS
CUMPLE 1 **NO CUMPLE** 0

- ✓ **INDICADOR 07** – ASEGURAMIENTO EN LA ADQUISICIÓN Y MANTENIMIENTO DE SOFTWARE

IDENTIFICADOR: SGIN07
DEFINICIÓN: Grado de protección de los servicios de la entidad.
OBJETIVO: Busca identificar la existencia de lineamientos, normas o estándares en cuanto a la adquisición o desarrollo de aplicaciones.

TIPO INDICADOR: Indicador de Cumplimiento
DESCRIPCIÓN DE VARIABLES FORMULA FUENTE DE INFORMACIÓN
VSI15: ¿La entidad ha definido lineamientos, normas y/o estándares para el desarrollo o adquisición de software, sistemas y aplicaciones?
Fuente de información: Usuarios Internos.
VSI16: ¿La entidad ha definido lineamientos, normas y/o estándares para la gestión de incidentes relacionados con el servicio?
Formula: VSI0X = 1 (SÍ se evidencia)
VSIOX = 0 (NO se evidencia)
Fuente de información: Usuarios Internos.
METAS
CUMPLE 1 **NO CUMPLE** 0

- ✓ **INDICADOR 08** – IMPLEMENTACIÓN DE LOS PROCESOS DE REGISTRO Y AUDITORÍA

IDENTIFICADOR: SGIN08
DEFINICIÓN: Grado de existencia de lineamientos, normas o estándares en cuanto registro y auditoría para la seguridad de la información.
OBJETIVO: Busca identificar la existencia de lineamientos, normas o estándares en cuanto registro y auditoría para la seguridad de la información.

TIPO INDICADOR: Indicador de Cumplimiento
DESCRIPCIÓN DE VARIABLES FORMULA FUENTE DE INFORMACIÓN
VSI17: ¿La entidad ha definido lineamientos, normas y/o estándares para el registro y control de eventos que sucedan sobre sus sistemas, redes y servicios?
Formula: VSI0X = 1 (SÍ se evidencia)
VSIOX = 0 (NO se evidencia)
Fuente de información: Usuarios Internos.
VSI18: ¿La entidad verifica de manera interna y/o a través de terceros, periódicamente sus procesos de seguridad de la información y sistemas para asegurar el cumplimiento del modelo?
Fuente de información: Usuarios Internos.
METAS
CUMPLE 1 **NO CUMPLE** 0

- ✓ **INDICADOR 09** – IMPLEMENTACIÓN DE LOS PROCESOS DE REGISTRO Y AUDITORÍA

IDENTIFICADOR: SGIN09
DEFINICION: Grado de implementación de los mecanismos encaminados a la detección de anomalías e irregularidades.
OBJETIVO: Busca medir el nivel de mecanismos encaminados a la detección de anomalías e irregularidades.

TIPO INDICADOR: Indicador de Cumplimiento
DESCRIPCIÓN DE VARIABLES
VSI19: VAPRSG005: ¿La entidad ha implementado mecanismos para detectar periódicamente vulnerabilidades de seguridad en el funcionamiento de:
a) su infraestructura,
b) redes,
c) sistemas de información,

d) aplicaciones y/o
e) uso de los servicios?

Formula: VSI0X = 1 (SÍ se evidencia)
VSIOX = 0 (NO se evidencia)

Fuente de información: Usuarios Internos, No Conformidades

METAS

CUMPLE 1 **NO CUMPLE** 0

✓ **INDICADOR 10** – POLÍTICAS DE PRIVACIDAD Y CONFIDENCIALIDAD

IDENTIFICADOR: SGIN10

DEFINICIÓN: Grado de implementación de políticas privacidad y confidencialidad de la entidad.

OBJETIVO: Busca identificar el nivel de implementación de políticas privacidad y confidencialidad en la entidad.

TIPO INDICADOR: Indicador de Cumplimiento

DESCRIPCIÓN DE VARIABLES FORMULA FUENTE DE INFORMACIÓN

VSI20: ¿La entidad ha implementado lineamientos, normas y/o estándares para proteger la información personal y privada de los ciudadanos que utilicen sus servicios?

Formula: VSI0X = 1 (SÍ se evidencia)
VSIOX = 0 (NO se evidencia)

Fuente de información: Usuarios Internos.

VSI21: ¿La entidad ha implementado lineamientos, normas y/o estándares para proteger la información privada de las entidades que utilicen sus servicios?

Fuente de información: Usuarios Internos.

METAS

CUMPLE 1 **NO CUMPLE** 0

✓ **INDICADOR 11** – VERIFICACIÓN DE LAS POLÍTICAS DE INTEGRIDAD DE LA INFORMACIÓN

IDENTIFICADOR: SGIN11

DEFINICIÓN: Grado de implementación de mecanismos para la integridad de la información de la entidad.

OBJETIVO: Busca identificar el nivel de implementación de políticas de privacidad y confidencialidad de la entidad.

TIPO INDICADOR: Indicador de Cumplimiento

DESCRIPCIÓN DE VARIABLES FORMULA FUENTE DE INFORMACIÓN

VSI22: ¿La entidad ha implementado lineamientos contra modificación o pérdida accidental de información?

Formula: VSI0X = 1 (SÍ se evidencia)
VSIOX = 0 (NO se evidencia)

Fuente de información: Usuarios Internos.

VSI23: ¿La entidad ha implementado lineamientos, normas y/o estándares para recuperar información en caso de modificación o pérdida intencional o accidental?

Fuente de información: Usuarios Internos.

METAS

CUMPLE 1 **NO CUMPLE** 0

- ✓ **INDICADOR 12** – POLÍTICAS DE DISPONIBILIDAD DEL SERVICIO Y LA INFORMACIÓN

IDENTIFICADOR: SGIN12
DEFINICIÓN: Grado de cumplimiento de las políticas de disponibilidad del servicio y la información.
OBJETIVO: Busca identificar el nivel de implementación de políticas de disponibilidad del servicio y la información.

TIPO INDICADOR: Indicador de Cumplimiento
DESCRIPCIÓN DE VARIABLES FORMULA FUENTE DE INFORMACIÓN
VSI24: ¿La entidad verifica que los lineamientos, normas y/o estándares orientados a la continuidad en la prestación de los servicios se cumplan?
Formula: VSI0X = 1 (SÍ se evidencia)
VSIOX = 0 (NO se evidencia)
Fuente de información: Usuarios Internos.
VSI25: ¿La entidad ha implementado mecanismos para que los servicios de Gobierno en línea tengan altos índices de disponibilidad?
Fuente de información: Usuarios Internos.
METAS
CUMPLE 1 **NO CUMPLE** 0

- ✓ **INDICADOR 13** – ATAQUES INFORMÁTICOS A LA ENTIDAD.

IDENTIFICADOR: SGIN13
DEFINICIÓN: Porcentaje de ataques informáticos recibidos en la entidad que impidieron la prestación de alguno de sus servicios.
OBJETIVO: Busca conocer el número de ataques informáticos que recibe la entidad.

TIPO INDICADOR: Indicador de Cumplimiento
DESCRIPCIÓN DE VARIABLES FORMULA FUENTE DE INFORMACIÓN
VSI25: ¿Cuántos ataques informáticos recibió la entidad en el último año?
Formula: VSI0X = 1 (SÍ se evidencia)
VSIOX = 0 (NO se evidencia)
Fuente de información: Herramientas de Monitoreo/Usuarios Internos.
VSI26: ¿Cuántos ataques recibió la entidad en el último año que impidieron la prestación de algunos de los servicios que la entidad ofrece a los ciudadanos y empresas?
Fuente de información: Herramientas de Monitoreo/Usuarios Internos.
METAS
CUMPLE 1 **NO CUMPLE** 0

- ✓ **INDICADOR 14** – PORCENTAJE DE DISPONIBILIDAD DE LOS SERVICIO DE GOBIERNO DIGITAL QUE PRESTA LA ENTIDAD

IDENTIFICADOR: SGIN14
DEFINICIÓN: Porcentaje de disponibilidad de los servicios que presta la entidad.
OBJETIVO: Busca identificar el nivel de disponibilidad del servicio y la información.

TIPO INDICADOR: Indicador de Cumplimiento
DESCRIPCIÓN DE VARIABLES FORMULA FUENTE DE INFORMACIÓN
VSI27: La entidad tiene definidos ANS para los servicios de Gobierno en Línea que presta.
Formula: VSI0X = 1 (SÍ se evidencia)
VSIOX = 0 (NO se evidencia)
Fuentes de información: Usuarios Internos.
VSI28: Porcentaje de disponibilidad del servicio de Gobierno en línea que presta la entidad en base a los ANS del punto anterior.
Fuente de información: Usuarios Internos.
METAS
CUMPLE 1 **NO CUMPLE** 0

✓ **INDICADOR 15** – PORCENTAJE DE IMPLEMENTACIÓN DE CONTROLES
IDENTIFICADOR: SGIN15
DEFINICIÓN: Grado de avance en la implementación de controles de seguridad.
OBJETIVO: Busca identificar el grado de avance en la implementación de controles de seguridad.

TIPO INDICADOR: Indicador de Gestión
DESCRIPCIÓN DE VARIABLES FORMULA FUENTE DE INFORMACIÓN
VSI29: Número de Controles Implementados
Formula: (VSI032/VSI33) *100
Fuente de información: Plan de tratamiento de riesgos
VSI30: Número de Controles que se planearon implementar
Fuente de información: Plan de Tratamiento de riesgos.
METAS
MÍNIMA 75-80% **SATISFACTORIA** 80- 90% **SOBRESALIENTE** 91-100%

8. Fase de evaluación

La Fase EVALUACION DEL DESEMPEÑO en la norma ISO 27001:2022 descrita en el capítulo 9 - Evaluación del desempeño, define los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia del sistema de gestión de seguridad de la información.

Figura 13. Fase de evaluación Fuente Fase de Evaluación de Monitoreo: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

8.1 Monitoreo, Medición, análisis y evaluación

Se deben llevar a cabo actividades para realizar seguimiento a:

- La programación y ejecución de las actividades de auditorías internas del SGSI a través de la Oficina de Control Interno de la Administración Municipal.
- La programación y ejecución de las revisiones por parte del Líder del proceso al alcance del sistema de gestión y las mejoras del mismo.
- Los Planes de seguridad tanto para el establecimiento como la ejecución y actualización de los mismos, como respuesta a los aspectos identificados a nivel de las revisiones y seguimientos realizados en esta fase del SGSI
- A los registros de incidentes de seguridad que podrían tener impacto en la eficacia o el desempeño del SGSI.

8.2 Revisión por la alta dirección

La revisión por la Alta Dirección se realiza una vez al año o cuando la alta dirección lo considere pertinente, con el fin de asegurar la conveniencia, adecuación, eficacia, eficiencia y efectividad del Sistema de Gestión de Seguridad de la Información. La información presentada incluye aspectos de gestión del servicio, basados en las buenas prácticas del Estándar ISO 20000- 1:2018 e ISO 270001:2022, Decreto 1581 de 2012 (por la cual se dictan disposiciones generales para la protección de datos personales. Aquellas actividades que se inscriben en el marco de la vida privada o familiar de las personas naturales.) y Decreto 1377 de 2013 (Por el cual se reglamenta parcialmente la Ley 1581 de 2012).

9. FASE DE MEJORA CONTINUA

Esta Fase mejora continua en la norma ISO 27001:2022. En el capítulo 10 Mejora, se establece para el proceso de mejorar el sistema de gestión de seguridad y privacidad de la información, la inconformidad que ocurra en la entidad debe establecer las acciones más efectivas para solucionar y evaluar la necesidad de acción para eliminar el error y lograr el objetivo de que no se repita.

Figura 14. Mejora continua de MinTIC/Modelo de seguridad y privacidad de la información

9.1 Acciones preventivas

El objetivo es determinar acciones para eliminar la causa de no conformidades potenciales con los requisitos del MSPI y evitar que acurran. Las acciones preventivas tomadas deben ser apropiadas al impacto de los problemas potenciales.

- Determinar no conformidades potenciales y sus causas.
- Evaluar la necesidad de acciones para impedir que las no conformidades ocurran
- Determinar e implementar las acciones preventivas necesarias
- Registrar los resultados de la acción tomada
- Revisar la acción preventiva tomada

9.2 Acciones correctivas

El objetivo de estas acciones es eliminar la causa de problemas asociados con los requisitos del SGSI, con el fin de prevenir que ocurran nuevamente.

- Determinar y evaluar las causas de los problemas del SGSI e incidentes de seguridad de la información.
- Diseñar e implementar la acción correctiva necesaria.
- Revisar la acción correctiva tomada.

9.3 Mejora Continua

Una vez el Sistema de Gestión de Seguridad de la Información se haya diseñado e implementado se hace necesario cerrar el ciclo con el mejoramiento continuo del mismo.

Para esto se diseña un plan de auditorías internas programadas por la Oficina de Control interno, teniendo en cuenta el estado e importancia de los procesos y la criticidad de la información y recursos informáticos. Estos planes incluirán el alcance,

frecuencia de realización, métodos de la auditoria, pruebas y selección de los auditores.

El objetivo de la auditoría interna es determinar si los objetivos de control, procesos, y procedimientos del MSPI:

- Están implementados y se desarrollan correctamente de acuerdo a los requisitos del Estándar de ISO 27001:2022.
- Cumplen los requisitos normativos.

Estas auditorías se encuentran enmarcadas dentro del procedimiento, que define las responsabilidades y requisitos para la planificación y realización de las mismas, la presentación de resultados y mantenimiento de los registros.
Además de los resultados de las auditorias, como entrada a este procedimiento se prevé también la retroalimentación de todos los participantes del SGSI y de la Alcaldía Municipal, la revisión de los requisitos de la norma, el manejo de no conformidades, medición de los indicadores y sugerencias.

Dentro de la fase de mantenimiento y mejora se definen las acciones y se deben tener en cuenta algunas consideraciones especiales cuando se refiera a Auditorias especificas a los Sistemas de Información.

10. GLOSARIO

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, etc.) que tenga valor para la organización.

Amenaza: causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.

Amenaza informática: la aparición de una situación potencial o actual donde una persona tiene la capacidad de generar una agresión cibernética contra la población, el territorio, la organización política del Estado (Ministerio de Defensa de Colombia).

Análisis de riesgos: proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.

Anonimización del dato: eliminar o sustituir algunos nombres de personas (físicas o jurídicas); direcciones y demás información de contacto, como números identificativos, apodos o cargo.

Autenticidad: propiedad de que una entidad es lo que afirma ser. (ISO 27000.es, 2012).

Ciberseguridad: capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Ciberespacio: ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701).

Confidencialidad: propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

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

Custodio de activo de información: identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la Veeduría Distrital, que tiene la responsabilidad de administrar y hacer efectivo los controles que el propietario del activo haya definido, con base en los controles de seguridad disponibles en la entidad. Datos abiertos: son datos primarios o sin procesar puestos a disposición de cualquier ciudadano, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

Datos biométricos: parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema (huella digital o voz).

Dato privado: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

Dato semiprivado: es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

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.

Dato público: es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

Dato semiprivado: es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

Disponibilidad: propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Backbone: troncal (en inglés *backbone*), red troncal o troncal de internet, es una de las principales conexiones de internet.

DVD: Disco Versátil (video) Digital. En la actualidad constituye el natural sucesor del CD para la reproducción de sonido e imagen de calidad.

Disco duro: disco de metal cubierto con una superficie de grabación ferro magnético. Haciendo una analogía con los discos musicales, los lados planos de la placa son la superficie de grabación, el brazo acústico es el brazo de acceso y la púa (aguja) es la cabeza lectora/grabadora. Los discos magnéticos pueden ser grabados, borrados y regrabados como una cinta de audio.

Evento de seguridad de la información: ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.

Gestión de claves: son controles que realizan mediante la gestión de claves criptográficas.

Gestión de riesgos: actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Impacto: el coste para la empresa de un incidente -de la escala que sea, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

Gestión de incidentes de seguridad de la información: procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Habeas data: derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.

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

Incidente de seguridad de la información: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: la propiedad de salvaguardar la exactitud y complejidad de la información.

Información: La información está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.

Inventario de activos: lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser

protegidos de potenciales riesgos. (ISO 27000.es, 2012)

Integridad: la propiedad de salvaguardar la exactitud y complejidad de la información.

No repudio: servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido). (ISO-7498-2).

Parte interesada (Stakeholder): persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

Plan de tratamiento de riesgos: documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Plan de continuidad del negocio: plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Proceso: conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas. (ISO 27000.es, 2012)

Propietario de activo de información: identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.

Responsable del tratamiento: persona natural o jurídica, pública o privada. Que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información.

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, basando en un enfoque de gestión y de mejora a un individuo o entidad.

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.

Vulnerabilidad: debilidad de un activo o control que pueda ser explotado por una o más amenazas. (ISO 27000.es, 2012).

Política de Firewall: Una Política de Firewall es una de las herramientas más importantes a la hora de configurar un firewall, ya que a través de ciertas configuraciones que el administrador realice, según la necesidad de la empresa, se puede determinar el comportamiento del dispositivo en la red.

11. REFERENCIAS

Mintic. (25 de 04 de 2022). *mintic.gov.co*. Obtenido de mintic.gov.co: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-162621_Modelo_de_Seguridad_y_Privacidad____MS

https://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf