AUTODIAGNÓSTICO

Seguridad Digital

2024 - 2027



MUNICIPIO
DE YONDÓ ANTIOQUIA

pdet
PROGRAMAS DE DESARROLLO CON ENFOQUE TERRITORIAL

1. INTRODUCCIÓN

En la actualidad, la transformación digital ha sido un proceso acelerado y extendido en diversas instituciones públicas, particularmente en gobiernos locales como el Municipio de Yondó. Las tecnologías de la información y la comunicación (TIC) están siendo implementadas en múltiples niveles de la administración pública para mejorar la eficiencia, accesibilidad y transparencia de los servicios ofrecidos a la ciudadanía. Sin embargo, con el crecimiento del uso de tecnologías digitales, también emergen riesgos asociados a la seguridad de la información, los cuales deben ser gestionados adecuadamente para prevenir posibles amenazas cibernéticas que puedan afectar tanto a la infraestructura pública como a la privacidad de los ciudadanos.

En este contexto, la seguridad digital se ha convertido en un pilar fundamental para garantizar la protección de los sistemas de información, los datos sensibles y la continuidad de los servicios públicos digitales. El Municipio de Yondó, al igual que otras entidades públicas, enfrenta el reto de desarrollar y mantener políticas de seguridad digital efectivas que permitan mitigar los riesgos cibernéticos y mejorar la gestión de la información en sus diversas plataformas.

Este autodiagnóstico tiene como propósito evaluar el estado actual de la política de seguridad digital en el Municipio de Yondó, con el fin de identificar las fortalezas, debilidades, oportunidades y amenazas que afectan la seguridad de los sistemas de información y servicios digitales municipales. A través de este diagnóstico, se busca contar con un análisis detallado de las prácticas, normativas y tecnologías implementadas en la administración pública local, permitiendo establecer una base sólida para la toma de decisiones orientadas a fortalecer la ciberseguridad en la institución.

La creciente digitalización de los servicios públicos, como la implementación de plataformas para la gestión de trámites, el uso de herramientas de comunicación electrónica y el almacenamiento de información personal, pone de manifiesto la necesidad de contar con una política robusta que regule la seguridad digital. Sin una adecuada estrategia de protección de la información y sistemas, la administración local podría verse expuesta a una variedad de riesgos, entre ellos, el robo de datos, el acceso no autorizado a información sensible, ataques de ransomware o la pérdida de disponibilidad de los servicios públicos esenciales. De ahí la relevancia de realizar este autodiagnóstico, con el objetivo de evaluar la situación actual y proponer soluciones prácticas para una mejor gestión de la seguridad digital.

2. ALCANCE

Este autodiagnóstico tiene un alcance que abarca todos los aspectos relacionados con la seguridad digital en el Municipio de Yondó, incluyendo tanto las políticas y normativas internas como la infraestructura tecnológica, los procesos operativos y la capacitación del personal encargado de gestionar la información y los sistemas digitales. Se pretende realizar un análisis exhaustivo de los siguientes componentes clave:

1. Políticas y normativas de seguridad digital: Se evaluarán las políticas existentes dentro del Municipio de Yondó relacionadas con la seguridad informática, la protección de datos personales y la gestión de incidentes de seguridad. Se analizará si estas políticas están alineadas con las mejores prácticas y las normativas nacionales e internacionales en materia de ciberseguridad.

2. Infraestructura tecnológica: Se examinará la infraestructura tecnológica utilizada por el municipio, incluyendo servidores, redes de comunicación, dispositivos y sistemas de almacenamiento. Este análisis se enfocará en identificar vulnerabilidades de seguridad que puedan ser explotadas por atacantes cibernéticos.

3. Gestión de datos y protección de la privacidad: Dado el creciente volumen de datos personales gestionados por la administración municipal, se llevará a cabo un estudio sobre las prácticas y protocolos de protección de la privacidad de los ciudadanos, así como de la gestión adecuada de los datos en conformidad con las leyes de protección de datos personales.

4. Interacción digital con la ciudadanía: Se evaluarán los canales y plataformas de interacción digital entre el municipio y los ciudadanos, asegurando que estos sean seguros y que los datos de los usuarios estén adecuadamente protegidos.

El alcance del diagnóstico también incluirá un análisis de los riesgos cibernéticos actuales que afectan a las instituciones públicas y la administración local, con el fin de ofrecer un diagnóstico que contemple todos los posibles puntos de mejora y desarrollo en términos de seguridad digital.

3. OBJETIVOS

El autodiagnóstico de la política de seguridad digital del Municipio de Yondó tiene los siguientes objetivos generales y específicos:

Objetivo General:

- Evaluar el estado actual de la política de seguridad digital en el Municipio de Yondó, identificando vulnerabilidades y proponer recomendaciones para mejorar la protección de los sistemas de información, la gestión de riesgos cibernéticos y la seguridad en la interacción digital con la ciudadanía.

Objetivos Específicos:

1. Diagnosticar el nivel de madurez y efectividad de la política de seguridad digital del Municipio de Yondó, mediante la revisión de las normativas y estrategias implementadas, en comparación con las mejores prácticas nacionales e internacionales.
2. Identificar las principales vulnerabilidades y riesgos cibernéticos presentes en la infraestructura tecnológica del municipio, incluyendo sus redes de comunicaciones, servidores, sistemas de almacenamiento y bases de datos.
3. Evaluar la capacitación y sensibilización del personal público en cuanto a las mejores prácticas de ciberseguridad, y proponer acciones para fortalecer la cultura de seguridad digital en la institución.
4. Analizar las medidas de protección de datos personales implementadas por la administración municipal, asegurando el cumplimiento de la legislación vigente sobre privacidad y la adecuada gestión de la información sensible.
5. Fomentar una mayor confianza entre la ciudadanía y la administración pública mediante la implementación de medidas que garanticen la seguridad y protección de los datos personales de los usuarios de los servicios públicos digitales.

4. METODOLOGÍA

La metodología adoptada para este autodiagnóstico será de carácter mixto, combinando técnicas cualitativas y cuantitativas para obtener un análisis completo y detallado de la situación actual de la seguridad digital en el Municipio de Yondó. A continuación se describen las etapas y actividades clave de la metodología:

1. Revisión documental

Se llevó a cabo un análisis de los documentos oficiales del municipio relacionados con la seguridad digital, tales como políticas internas, procedimientos operativos estándar (SOP), normativas sobre protección de datos personales y cualquier otra directriz pertinente. Esta revisión permitió entender el marco normativo y las estrategias implementadas en el ámbito de la seguridad de la información.

2. Entrevistas con responsables clave

Se realizaron entrevistas semiestructuradas con los responsables de las áreas de tecnología de la información, seguridad informática, protección de datos y gestión de riesgos. El objetivo de estas entrevistas fue conocer de primera mano las prácticas actuales, los desafíos que enfrentan y las percepciones sobre la seguridad digital dentro de la administración pública local.

3. Evaluación técnica de la infraestructura tecnológica

Se llevó a cabo una revisión técnica de la infraestructura tecnológica utilizada por el municipio, incluyendo redes, servidores, bases de datos y sistemas de almacenamiento de información. Este análisis permitió identificar vulnerabilidades en los sistemas y determinar si se están utilizando las tecnologías adecuadas para proteger los datos y prevenir incidentes de seguridad.

4. Análisis de riesgos cibernéticos

Se desarrolló un análisis de riesgos, utilizando herramientas de evaluación de riesgos y metodologías reconocidas, como el análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas), para identificar los principales riesgos cibernéticos que enfrenta la administración municipal. Esto incluyó la identificación de amenazas internas y externas, así como las vulnerabilidades de los sistemas tecnológicos utilizados por el municipio.

7. Elaboración del informe y diligenciamiento del instrumento de medición

Una vez recopilada y analizada toda la información, se diligenció el instrumento detallado con los hallazgos del diagnóstico, incluyendo una evaluación de la madurez de la política de seguridad digital, las vulnerabilidades identificadas, los riesgos asociados y un conjunto de recomendaciones específicas para mejorar la seguridad digital en el Municipio de Yondó. Este informe servirá como base para la toma de decisiones estratégicas en el ámbito de la ciberseguridad dentro de la administración pública.

5. INSTRUMENTO DE AUTODIAGNÓSTICO DE LA POLÍTICA DE SEGURIDAD DIGITAL

5.1. Evaluación general del autodiagnóstico

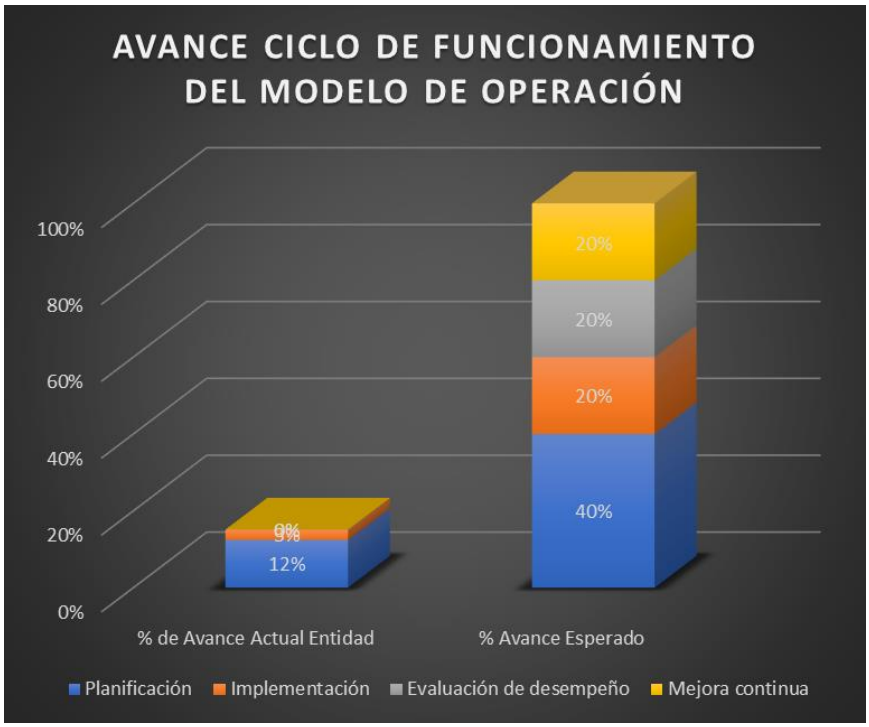
No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	83	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	32	100	REPETIBLE
A.9	CONTROL DE ACCESO	62	100	GESTIONADO
A.10	CRIPTOGRAFÍA	100	100	OPTIMIZADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	58	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	34	100	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	33	100	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	36	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	50	100	EFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	5	100	INICIAL
A.18	CUMPLIMIENTO	51.5	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		**53**	**100**	EFECTIVO

5.2. Brecha con respecto a la norma ISO 27001:2013



5.3. Avance ciclo PHVA del autodiagnóstico

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2024	Planificación	12%	40%
	Implementación	3%	20%
	Evaluación de desempeño	0%	20%
	Mejora continua	0%	20%
TOTAL		15%	100%



ANEXO

Instrumento diligenciado del autodiagnóstico de seguridad digital