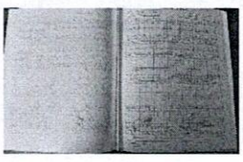
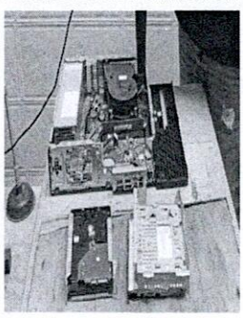
1. SEGUIMIENTO ADMINISTRATIVO

IDENTIFICACIÓN DEL CONTRATO:	100.0501.027-2025
CONTRATISTA:	JULIO POTOSI GUAMPE
OBJETO CONTRACTUAL:	PRESTAR POR SUS PROPIOS MEDIOS Y AUTONOMIA ADMINISTRATIVA LOS SERVICIOS PROFESIONALES DE APOYO A LA GESTION EN EL CONCEJO DE YUMBO
VALOR DEL CONTRATO:	VEINTI OCHO MILLONES OCHOCIENTOS MIL PESOS M/CTE ($28, 800.000)
PLAZO DE EJECUCIÓN:	El plazo para la ejecución del contrato será contado a partir de la suscripción del Acta de Inicio, previo cumplimiento del registro de perfeccionamiento y legalización del mismo y hasta el día 30 de septiembre de 2025. La vigencia del contrato no podrá extender al 31 de diciembre de 2025
FECHA DE INICIO:	DIEZ Y SIETE (17) DIAS DEL MES DE FEBRERO DE 2025
FECHA DE TERMINACION:	30 DE SEPTIEMBRE DE 2025
FORMA DE PAGO:	Para todos los efectos legales y fiscales se estima el valor del contrato de Prestación de Servicios Profesionales de Apoyo al a Gestión en la suma de VEINTI OCHO MILLONES OCHOCIENTOS MIL PESOS M/CTE (28.800.000).EL CONTRATANTE cancelará el valor del contrato previo recibo a satisfacción, de la siguiente manera :Ocho (8) cuotas por valor de T RES MILLONES SEIS CIENTOS MIL PESOS M/CTE ($3.600.000), pagaderos a partir del último día hábil de cada mes, iniciando en el mes de febrero de 2025 .incluidos todos los costos derivados de la ejecución del contrato.
NOMBRE Y CARGO SUPERVISOR (ES) DEL CONTRATO:	URIEL URBANO URBANO Secretario General
PERIODO DE SUPERVISIÓN:	**ABRIL 2025**

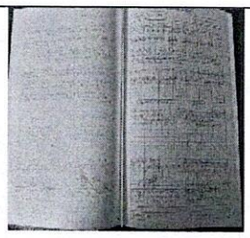
2. SEGUIMIENTO TÉCNICO

Actividades Contratadas	**Actividades Ejecutadas**	**Registro o Evidencia de la Actividad**	**Ubicación Física del registro o evidencia**
1. Apoyar la coordinación del proceso Gestión de tecnologías de la información	Se elaboro documentos sobre la propuesta de proyectos de Tecnologías de la Información (TI) que permita Mejorar la gestión de las tecnologías de la información en el Concejo Municipal de Yumbo mediante la implementación de herramientas digitales que optimicen la atención al ciudadano, fomenten la transparencia y faciliten la participación comunitaria, asegurando así una administración pública más eficiente y accesible. Se realizo asistencia al segundo comité de gestión y desempeño del año 2025.	proyecto proceso de gestión de tecnologías de la información del CMY	Esta evidencia reposa en el proceso de tecnologías de la información.

Este documento es propiedad del Concejo Municipal de Yumbo.
Prohibida su reproducción por cualquier medio, sin previa autorización de la Presidencia.

2. Brindar apoyo en la actualización del plan estratégico de tecnología de la información y hacer seguimiento a las actividades	Se realizo proceso de identificación de los activos de información del concejo Municipal de Yumbo que permita las Fortalecer la protección de la información del Concejo Municipal de Yumbo mediante la identificación y clasificación de los activos de información.	FORMALIZAR PROCESO DE IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN	Esta evidencia reposa en el proceso de tecnologías de la información.
3. Brindar apoyo en la actualización del plan de tratamientos de riesgos de seguridad de la información y hacer seguimiento a las actividades.	Se realizo la evolución la importancia de los riesgos de seguridad de la información identificados para el Concejo Municipal de Yumbo, mediante el análisis sistemático de su impacto potencial y probabilidad de ocurrencia, con el fin de establecer una base priorizada y fundamentada para la toma de decisiones sobre su tratamiento.	Evaluación y clasificación de los riesgos según su impacto y probabilidad	Esta evidencia reposa en el proceso de tecnologías de la información.
4. Bri ndar apoyo en la actualización del plan de seguridad y privacidad de la información y hacer seguimiento a las actividades.	Se elaboro documento que permita **Establecer y operar** el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) del Concejo Municipal de Yumbo, conforme a los lineamientos de este Plan, para gestionar proactivamente los riesgos, asegurar el cumplimiento normativo (ISO 27001, MSPI, Ley 1581/1712) y proteger de manera continua la confidencialidad, integridad y disponibilidad de sus activos de información.	Documentos Plan de seguridad y privacidad de la información	Esta evidencia reposa en el proceso de tecnologías de la información.
5.Brindar apoyo profesional en la atención de incidencias en los equipos del Concejo Municipal de Yumbo cuando sea solicitado.	Se realizo asistencia al llamado del a funcionaria Naomi quintero para atender requerimiento con los impresos por problemas de atasco de papel Se realizo actualización del sistema operativo del equipo del funcionario Octavio Rodríguez Se realizo revisión de la impresora por problemas de conexión al equipo de la funcionaria Martha Burbano	Bitácora del almacén 	Servidor
6. Brindar apoyo profesional en la administración y mantenimiento de equipos, servidores y Configuración de redes.	preventivo y correctivo de los 5 equipos de cómputo del recinto del Concejo Municipal de Yumbo es crucial para asegurar la continuidad y eficiencia de los servicios administrativos. Este mantenimiento no solo prolonga la vida útil de los equipos, sino que también minimiza la probabilidad de fallas técnicas que podrían interrumpir las actividades diarias del Concejo.	Bitácora del almacén 	Esta evidencia reposa en el proceso de tecnologías de la información.

Este documento es propiedad del Concejo Municipal de Yumbo.
Prohibida su reproducción por cualquier medio, sin previa autorización de la Presidencia.

	Además, al realizar limpieza externa e interna, respaldar información, actualizar software y realizar pruebas de seguridad, se garantiza que los sistemas operen óptimamente, lo que a su vez mejora la productividad del personal y reduce los costos asociados a reparaciones inesperadas.		
7. Las demás actividades inherentes al objeto del contrato.	Se realizo apoyo en la instalación de diapositivas de los computadores del recinto para las actividades de rendición de cuantas de las diferentes secretarias citadas por el honorable concejo	Plantilla informe de gestión 2025 	16 equipos del recinto
OBSERVACIONES			

Cumplimiento de Actividades Contratadas y Objeto Contractual en el Periodo	SI	X	NO		Cumple Parcialmente	

5. SEGUIMIENTO CONTABLE, FINANCIERO Y JURIDICO

	No.	Cuenta / Apropiación	Fecha	Valor
CDP	**000025**	2.1.2.02.02.008	3 FEBRERO de 2025	28,800, 000
Registro Presupuestal	00066	2.1.2.02.02.008	17 FEBRERO de 2025	28,800, 000

Valor a Pagar en el Periodo	Valor Ejecutado a la Fecha	Valor por Ejecutar
$3.600.000	S 10.800.000	S 10.800.000

Prorroga / Adiciones al Contrato: Tiempo _____ Valor: _____ Actividades: _____

Diligenciar en caso de adiciones por valor

6. PAGO DE SEGURIDAD SOCIAL

Base de Cotización	Valor pagado a			Total Pagado	No. De Planilla	Fecha de pago
	EPS	PENSIÓN	ARL			
$ 4.437.560	$554.700	$710.100	$108.100	$ 1.374.900	85561260	04/04/2025

7. CERTIFICACIÓN:

a. Por parte del Supervisor:

Certificó el cumplimiento a satisfacción de las obligaciones establecidas en el contrato por parte del contratista en desarrollo de las actividades específicas descritas en el informe de gestión correspondientes al mes de abril de 2025 según lo pactado en el contrato en mención del año avante, informe que se anexa debidamente refrendado por las partes. Igualmente se anexa pago de la seguridad social.

Este documento es propiedad del Concejo Municipal de Yumbo.
Prohibida su reproducción por cualquier medio, sin previa autorización de la Presidencia.

b. Por parte del Contratista

Manifiesto bajo la gravedad del juramento que me encuentro afiliado al Sistema de Seguridad Social Integrado, y que realizaré los aportes al mismo, de conformidad con lo dispuesto en el Art. 3.2.7.5 y en el Art. 3.2.7.6 del Decreto 1273 de 2018.

Para constancia de lo anterior se firma la presente acta por el contratista y los que en ella supervisan a los 30 días del mes de abril de año 2025.

Firma de Supervisor
Nombre: URIEL URBANO URBANO
Cargo: secretario general

Firma del Contratista
Nombre: Julio Potosí Guampe
Cedula de Ciudadanía No 4.664.604

Revisado: Angelica Aguirre – Abogada de Apoyo
Revisado: Nahomy Quintero – Apoyo Direccionamiento estratégico

Este documento es propiedad del Concejo Municipal de Yumbo.
Prohibida su reproducción por cualquier medio, sin previa autorización de la Presidencia.

Tabla de contenido

Introducción 2

Justificación 3

Alcance 4

Objetivo General: 5

Evaluación y clasificación de los riesgos según su impacto y probabilidad ... 6

Conclusiones 22

Recomendaciones 23

Introducción

La gestión proactiva de la seguridad de la información es un pilar fundamental para el funcionamiento eficiente, transparente y confiable de cualquier entidad pública, y el Concejo Municipal de Yumbo no es la excepción. En un entorno donde la información digital es un activo cada vez más valioso y, a la vez, más expuesto a diversas amenazas, resulta indispensable no solo identificar los elementos que podrían comprometerla, sino también comprender la magnitud real de dicho peligro. Este documento se centra precisamente en esa fase crítica del ciclo de gestión de riesgos: la evaluación y clasificación sistemática de los riesgos identificados que afectan a los activos de información del Concejo.

Tras una fase inicial de identificación exhaustiva de los activos de información clave desde los datos sensibles de los ciudadanos y la documentación oficial hasta los sistemas tecnológicos y el propio personal así como las amenazas y vulnerabilidades asociadas a ellos, el presente análisis da un paso adelante. Su propósito es cuantificar, de manera estructurada y metodológica, la severidad potencial de cada riesgo. Esto se logra mediante la valoración de dos dimensiones cruciales: el impacto que tendría la materialización de una amenaza sobre la confidencialidad, integridad y disponibilidad de la información, así como sobre los objetivos operativos, legales y reputacionales del Concejo; y la probabilidad de que dicho evento adverso ocurra realmente, considerando las vulnerabilidades existentes y el panorama actual de amenazas.

Aplicando principios metodológicos reconocidos (como los de MAGERIT), este documento presenta los resultados de la evaluación, combinando las estimaciones de impacto y probabilidad para determinar un nivel de riesgo inherente para cada escenario identificado. Los riesgos se clasifican en categorías (como Muy Alto, Alto, Medio, Bajo, Muy Bajo), lo que permite visualizar de forma clara cuáles representan las mayores preocupaciones y requieren atención prioritaria. Esta clasificación no es un fin en sí misma, sino una herramienta esencial para la toma de decisiones informadas.

El objetivo final de esta evaluación y clasificación es proporcionar al Concejo Municipal de Yumbo una base sólida y objetiva para la siguiente etapa: el desarrollo del Plan de Tratamiento de Riesgos. Al comprender qué riesgos son los más críticos, la entidad podrá asignar recursos de manera más eficiente, diseñar e implementar controles de seguridad más efectivos y, en última instancia, fortalecer su resiliencia operativa. Este esfuerzo es vital para garantizar la continuidad de las funciones del Concejo, cumplir con las obligaciones legales y normativas, y, sobre todo, mantener y reforzar la confianza de la comunidad de Yumbo en su institución representativa.

Justificación

La simple identificación de los activos de información, amenazas y vulnerabilidades, si bien es un primer paso esencial, resulta insuficiente para una gestión de riesgos eficaz en el Concejo Municipal de Yumbo. Ante la multitud de posibles escenarios adversos y la realidad de contar con recursos finitos (presupuestales, técnicos y humanos), se hace imperativo establecer un mecanismo que permita discernir entre aquellos riesgos que representan una amenaza trivial y aquellos que podrían tener consecuencias significativas o incluso catastróficas para la entidad. La evaluación y clasificación de riesgos según su impacto y probabilidad responde directamente a esta necesidad crítica de priorización.

Este proceso de evaluación es fundamental porque transforma una lista potencialmente extensa y abrumadora de riesgos en un panorama ordenado y jerarquizado. Al asignar valores específicos al impacto potencial sobre las operaciones, la reputación, las finanzas y el cumplimiento legal del Concejo, y al estimar la probabilidad de ocurrencia de cada amenaza, se obtiene una medida objetiva del nivel de riesgo inherente. Esta cuantificación permite a los líderes y tomadores de decisiones del Concejo Municipal de Yumbo comprender la verdadera magnitud de cada amenaza y, en consecuencia, enfocar los esfuerzos y la asignación de recursos de manera estratégica, atendiendo primero aquellos riesgos clasificados como críticos o altos.

Además, la evaluación y clasificación rigurosa de los riesgos constituye el cimiento indispensable sobre el cual se construirá un Plan de Tratamiento de Riesgos efectivo y realista. La clasificación resultante (por ejemplo, en niveles Muy Alto, Alto, Medio, Bajo) guía directamente las decisiones sobre cómo abordar cada riesgo: si requiere medidas de mitigación urgentes, si puede ser transferido, si necesita un plan de contingencia específico, o si su bajo nivel permite una aceptación informada con monitoreo continuo. Sin esta evaluación previa, cualquier intento de tratamiento sería reactivo, ineficiente y potencialmente inadecuado para proteger adecuadamente los activos de información del Concejo.

Finalmente, llevar a cabo y documentar esta evaluación demuestra un compromiso formal del Concejo Municipal de Yumbo con la seguridad de la información y la gestión responsable de los datos públicos y ciudadanos. No solo facilita el cumplimiento de marcos normativos como la Ley 1581 de 2012 y la Ley 1712 de 2014, sino que también refuerza la transparencia y la rendición de cuentas ante la ciudadanía. Es, por tanto, un ejercicio esencial de buena gobernanza que contribuye directamente a la protección de los intereses de la comunidad, la operatividad de la institución y la preservación de la confianza pública.

Alcance

El presente documento establece el alcance de la **evaluación y clasificación de los riesgos de seguridad de la información** identificados previamente para el Concejo Municipal de Yumbo. Su objetivo primordial es analizar de manera sistemática dichos riesgos, determinando su magnitud relativa en función de su impacto potencial sobre la organización y la probabilidad estimada de su ocurrencia, con el fin de establecer una base clara para la priorización y el tratamiento posterior.

Este análisis abarca todos los riesgos de seguridad de la información que pueden afectar a los activos críticos del Concejo, identificados en fases anteriores del proceso de gestión de riesgos. Esto incluye, pero no se limita a, los riesgos relacionados con: la **confidencialidad, integridad y disponibilidad** de los datos de los ciudadanos (como registros PQR y datos de participación), la documentación oficial (actas, acuerdos, contratos), los sistemas de información (software de gestión, plataformas web, correo electrónico), la infraestructura tecnológica (servidores, redes, equipos) y la actuación del personal (funcionarios, concejales, contratistas) en el manejo de la información. La evaluación considera el impacto potencial en dimensiones operativas, legales (cumplimiento de Ley 1581, Ley 1712, etc.), financieras y reputacionales para el Concejo.

La metodología empleada para la evaluación se basa en principios de análisis cualitativo de riesgos, adaptando enfoques reconocidos como MAGERIT. Se asignan valores de impacto y probabilidad utilizando escalas predefinidas (por ejemplo: Muy Bajo, Bajo, Medio, Alto, Muy Alto), y la combinación de ambos determina el nivel de riesgo inherente para cada escenario identificado. El resultado principal de este análisis es una **clasificación jerarquizada de los riesgos**, presentada típicamente en una matriz o lista priorizada, que indica claramente cuáles riesgos requieren atención inmediata (Críticos/Muy Altos, Altos) y cuáles pueden gestionarse a medio o largo plazo (Medios, Bajos).

Es importante delimitar que este documento se enfoca estrictamente en la **evaluación y clasificación del riesgo inherente**, es decir, el riesgo existente antes de la aplicación de nuevas medidas de tratamiento. Por lo tanto, el alcance **no incluye** la definición detallada del Plan de Tratamiento de Riesgos (aunque sí lo fundamenta), ni la implementación específica de los controles o salvaguardas, ni la auditoría exhaustiva de la efectividad de los controles ya existentes (aunque su presencia o ausencia se considera al evaluar la probabilidad y vulnerabilidad). El foco está en proporcionar una fotografía clara del panorama de riesgos actual para informar la toma de decisiones estratégicas en materia de seguridad de la información dentro del Concejo Municipal de Yumbo.

Objetivo General:

- **Evaluar** la importancia de los riesgos de seguridad de la información identificados para el Concejo Municipal de Yumbo, mediante el análisis sistemático de su impacto potencial y probabilidad de ocurrencia, con el fin de establecer una base priorizada y fundamentada para la toma de decisiones sobre su tratamiento.

Objetivos Específicos:

1. Establecer los criterios y escalas cualitativas para la valoración del impacto potencial (considerando dimensiones clave como confidencialidad, integridad, disponibilidad, así como consecuencias legales, reputacionales y operacionales) y la probabilidad de ocurrencia de las amenazas identificadas, adaptados al contexto específico y a la normativa aplicable al Concejo Municipal de Yumbo.
2. Analizar cada uno de los riesgos de seguridad de la información previamente identificados, descomponiéndolos en función de las dimensiones de impacto y los factores de probabilidad definidos en las escalas, considerando las vulnerabilidades asociadas y el entorno de amenazas relevante para el Concejo.
3. Clasificar los riesgos evaluados en niveles de criticidad distintos (por ejemplo: Muy Alto, Alto, Medio, Bajo, Muy Bajo), mediante la combinación estructurada de los valores de impacto y probabilidad asignados, generando una matriz o listado jerarquizado que evidencie las prioridades de actuación para la gestión de la seguridad de la información en el Concejo Municipal de Yumbo.

Evaluación y clasificación de los riesgos según su impacto y probabilidad

MAGERIT se enfoca en valorar los activos, identificar amenazas que puedan afectarlos y analizar las vulnerabilidades existentes para determinar el nivel de riesgo. Utilizaremos escalas cualitativas (Muy Bajo, Bajo, Medio, Alto, Muy Alto) para el impacto y la probabilidad, derivando de ellas el nivel de riesgo.

1. Definición de Escalas (Adaptación MAGERIT)

Para adaptar MAGERIT, utilizaremos las siguientes escalas cualitativas:

- **Impacto Potencial (Consecuencia de la materialización de la amenaza):** Mide el daño sobre las dimensiones de seguridad (Confidencialidad, Integridad, Disponibilidad - C, I, D - y potencialmente Autenticidad y Trazabilidad) y las consecuencias organizacionales (legales, financieras, reputacionales, operacionales).
    - **MA (Muy Alto):** Consecuencias catastróficas. Parálisis operativa significativa, incumplimiento legal grave con sanciones máximas, daño reputacional irreparable, pérdida financiera muy elevada, compromiso severo de C/I/D de activos críticos.
    - **A (Alto):** Consecuencias graves. Interrupción significativa de servicios, incumplimiento legal con sanciones importantes, daño reputacional considerable, pérdidas financieras altas, compromiso importante de C/I/D
    - **M (Medio):** Consecuencias moderadas. Interrupción parcial de servicios, posible incumplimiento legal con sanciones menores, daño reputacional limitado, pérdidas financieras moderadas, compromiso notable de C/I/D.
    - **B (Bajo):** Consecuencias leves. Molestias operativas menores, bajo riesgo de incumplimiento legal, impacto reputacional mínimo, pérdidas financieras bajas, compromiso leve de C/I/D.
    - **MB (Muy Bajo):** Consecuencias insignificantes. Impacto operativo casi nulo, sin implicaciones legales o reputacionales, pérdidas financieras mínimas, compromiso mínimo de C/I/D.
- **Probabilidad de Materialización:** Mide la posibilidad de que la amenaza se materialice, explotando una o más vulnerabilidades.
    - **MA (Muy Alta):** Ocurrencia casi segura o muy frecuente. La amenaza se materializa repetidamente o es inminente.
    - **A (Alta):** Ocurrencia probable. La amenaza se materializa con frecuencia o es esperable en el corto/medio plazo.
    - **M (Media):** Ocurrencia posible. La amenaza podría materializarse ocasionalmente o en el medio plazo.
    - **B (Baja):** Ocurrencia improbable. La amenaza se materializa raramente o en el largo plazo.
    - **MB (Muy Baja):** Ocurrencia muy improbable o excepcional.

2. Matriz de Evaluación de Riesgo (MAGERIT - Cualitativa 5x5)

Combinando Impacto y Probabilidad, obtenemos el Nivel de Riesgo Inherente:

	Impacto Potencial				
Probabilidad	**MB**	**B**	**M**	**A**	**MA**
MA	M	A	A	MA	MA
A	B	M	A	A	MA
M	B	M	M	A	A
B	MB	B	M	M	A
MB	MB	MB	B	B	M

Niveles de Riesgo:

- **MA (Muy Alto):** Requiere acción inmediata y prioritaria.
- **A (Alto):** Requiere acción prioritaria a corto plazo.
- **M (Medio):** Requiere acción y planificación a medio plazo.
- **B (Bajo):** Requiere monitoreo y posible acción a largo plazo. Puede ser aceptable.
- **MB (Muy Bajo):** Generalmente aceptable, requiere monitoreo mínimo.

3. Evaluación y Clasificación de Riesgos (Ejemplos basados en el documento)

A continuación, se presenta una tabla con la evaluación de algunos riesgos clave extraídos o inferido s de tu documento, aplicando la metodología descrita:

ID	Activo de Información	Dimensiones Valoradas (Ej. C,I,D)[1]	Amenaza	Vulnerabilidad Asociada	Impacto Potencial (C,I,D + Org.)	Probabilidad	Nivel de Riesgo Inherente	Justificación (Impacto/Probabilidad)
R01	Datos de Ciudadanos (PQR, Participación)	C: MA, I: A, D: M	Acceso no autorizado (interno/externo)	Contraseñas débiles, falta de controles de acceso granular, posible falta de capacitación	MA	A	MA	**Impacto:** Divulgación masiva de datos sensibles (Ley 1581), pérdida de confianza ciudadana, sanciones legales. **Prob:** Vulnerabilidades comunes, motivación interna/externa existe.
R02	Sitio Web del Concejo / Plataforma de Transparencia	C: B, I: M, D: A	Ataque de Denegación de Servicio (DDoS)	Falta de protección anti-DDoS específica, posible infraestructura subdimensionada	A	A	MA	**Impacto:** Impide acceso a información pública (Ley 1712), afecta imagen y comunicación. **Prob:** Ataques comunes a entidades públicas, relativa facilidad de ejecución.

R03	Documentación Oficial (Actas, Acuerdos, Contratos)	C: A, I: MA, D: A	Modificación o eliminación no autorizada	Falta de controles de integridad, permisos de acceso inadecuados, falta de backups	**MA**	**M**	**A**	**Impacto:** Pérdida de registros oficiales, decisiones basadas en información errónea, problemas legales/auditoría. **Prob:** Menos frecuente que el acceso, pero posible con fallos de control.
R04	Sistemas de Información (Gestión Documental, etc.)	C: A, I: A, D: MA	Infección por Malware (Ransomware)	Software desactualizado, falta de antivirus/antimalware robusto, falta de capacitación (phishing), backups insuficientes/no probados	**MA**	**A**	**MA**	**Impacto:** Parálisis operativa, pérdida/secuestro de datos críticos, costos de recuperación elevados. **Prob:** Amenaza muy prevalente y dirigida a menudo a entidades con recursos limitados.
R05	Datos de Ciudadanos	C: MA, I: A, D: M	Incumplimiento de Ley 1581	Falta de consentimiento informado claro, políticas	**A**	**A**	**MA**	**Impacto:** Sanciones económicas significativas (SIC), daño reputacional severo, pérdida de

			(Protección Datos)	desactualizadas, manejo inadecuado				confianza. **Prob:** El cumplimiento requiere procesos robustos, fácil cometer errores sin ellos.
R06	Infraestructura Tecnológica (Servidores, Red)	C: M, I: M, D: A	Fallo de hardware / Desastre Natural (Incendio, Inundación)	Falta de redundancia, plan de continuidad de negocio (BCP/DRP) inexistente o no probado, ubicación física vulnerable	**MA**	**B**	**A**	**Impacto:** Interrupción prolongada de todos los servicios dependientes, pérdida de datos si los backups fallan. **Prob:** Baja probabilidad de desastres mayores, pero fallos de hardware ocurren.
R07	Personal (Funcionarios, Concejales)	C: A, I: B, D: B	Error humano (envío erróneo, eliminación accidental)	Falta de capacitación continua, falta de procedimientos claros, ausencia de controles de doble verificación	**A**	**MA**	**MA**	**Impacto:** Divulgación accidental de información confidencial, pérdida de datos, interrupciones menores. **Prob:** Errores humanos son muy frecuentes en ausencia de controles y conciencia.

R08	Información Confidencial (Estrategias, Contratos)	C: MA, I: M, D: M	Fuga de información (intencional o accidental)	Controles de acceso insuficientes, falta de monitoreo, falta de políticas de clasificación de información, uso de canales inseguros	**MA**	**M**	**A**	**Impacto:** Pérdida de ventaja competitiva (si aplica), daño reputacional, incumplimiento contractual/legal. **Prob:** De pende de controles y cultura, pero la oportunidad existe.
R09	Equipos de Cómputo / Dispositivos Móviles	C: A, I: A, D: A	Pérdida o Robo de dispositivos	Falta de cifrado de disco, contraseñas débiles, falta de políticas BYOD (si aplica), no inventario/control	**A**	**M**	**A**	**Impacto:** Acceso no autorizado a datos almacenados/cache, posible acceso a sistemas corporativos. **Prob:** Ocurre con cierta frecuencia, especialmente con dispositivos móviles.

Habiendo identificado y evaluado los riesgos de seguridad de la información que enfrenta el Concejo Municipal de Yumbo, el siguiente paso lógico y absolutamente crucial es la definición de controles específicos. Este proceso representa el puente entre la comprensión teórica de las amenazas y vulnerabilidades y la implementación práctica de defensas efectivas. Sin controles claramente definidos, el mapa de riesgos permanece como un diagnóstico sin tratamiento; es en la selección y diseño de estas salvaguardas donde la estrategia de seguridad cobra vida y se traduce en acciones concretas que protegen activamente los activos de información de la entidad.

La definición detallada de controles es fundamental porque aborda directamente las vulnerabilidades previamente identificadas en los sistemas, procesos y recursos humanos del Concejo. Para cada riesgo significativo, como el acceso no autorizado a datos ciudadanos, la interrupción del sitio web o la pérdida de documentación oficial, los controles propuestos – ya sean técnicos como firewalls y cifrado, organizacionales como políticas y capacitación, o físicos como el control de acceso – actúan como barreras y mecanismos de mitigación. Esta especificidad asegura que los esfuerzos y recursos se enfoquen precisamente donde más se necesitan, maximizando la efectividad de las inversiones en seguridad y reduciendo la probabilidad o el impacto de incidentes perjudiciales.

En última instancia, este paso no solo fortalece la postura de seguridad del Concejo de Yumbo, sino que también demuestra un compromiso tangible con la protección de la información y el cumplimiento normativo, como lo exigen la Ley 1581 de Protección de Datos Personales y la Ley 1712 de Transparencia. Al implementar controles adecuados y bien definidos, el Concejo no solo reduce su exposición a sanciones legales y daños reputacionales, sino que, lo más importante, construye y mantiene la confianza de los ciudadanos a los que sirve, asegurando que su información está siendo gestionada con la diligencia y seguridad que merece. Es, por tanto, una fase indispensable para materializar la seguridad de la información en la operación diaria del Concejo.

Definir controles específicos para las vulnerabilidades identificadas es el corazón del Plan de Tratamiento de Riesgos. A continuación, te propongo controles (salvaguardas según MAGERIT) para cada uno de los riesgos evaluados, enfocándonos en las vulnerabilidades que mencionamos y buscando reducir el impacto (y a veces la pro

babilidad) del riesgo:

Tabla de Controles Sugeridos por Riesgo y Vulnerabilidad

ID	Activo de Información	Vulnerabilidad Asociada	Controles Sugeridos para Reducir Impacto/Probabilidad	Tipo de Control (Ej: O, T, F, L)[1]
R01	Datos de Ciudadanos (PQR, Participación)	Contraseñas débiles, falta de controles de acceso granular, posible falta de capacitación	1. Política de Contraseñas Robustas: Implementar y exigir contraseñas complejas, con cambio periódico y no reutilización. (T/O) 2. Control de Acceso Basado en Roles (RBAC): Definir roles y asignar permisos mínimos necesarios (principio de menor privilegio) para acceder/modificar datos de ciudadanos. (T/O) 3. Auditoría de Accesos: Habilitar y revisar logs de acceso a datos sensibles. (T) 4. Capacitación Específica (Ley 1581): Formar al personal sobre manejo seguro de datos personales, riesgos de ingeniería social y políticas internas. (O) 5. Cifrado: Cifrar la base de datos o campos sensibles (at rest) y las comunicaciones (in transit). (T)	T, O

R02	Sitio Web del Concejo / Plataforma de Transparencia	Falta de protección anti-DDoS específica, posible infraestructura subdimensionada	1. Servicio Anti-DDoS: Contratar o configurar un servicio de mitigación de DDoS (puede ser a nivel de ISP, CDN o especializado). (T/Servicio) 2. Web Application Firewall (WAF): Implementar un WAF para filtrar tráfico malicioso, incluyendo algunos tipos de ataques DDoS a nivel de aplicación. (T) 3. Monitoreo de Rendimiento y Disponibilidad: Establecer alertas para detectar picos inusuales de tráfico o caídas del servicio. (T) 4. Plan de Respuesta a Incidentes (IRP): Incluir escenarios de DDoS con pasos de actuación definidos. (O) 5. Revisión de Capacidad: Evaluar si la infraestructura actual soporta picos de carga esperados y planificar escalabilidad si es necesario. (T/O)	T, O, Servicio
R03	Documentación Oficial (Actas, Acuerdos, Contratos)	Falta de controles de integridad, permisos de acceso inadecuados, falta de backups	1. Sistema de Gestión Documental (SGD) con Control de Versiones: Utilizar un SGD que registre cambios y permita revertir a versiones anteriores. (T) 2. Controles de Integridad: Usar checksums o firmas digitales para verificar la integridad de documentos críticos. (T)	T, O

			3. Permisos Granulares en SGD: Aplicar permisos estrictos de lectura/escritura/eliminación basados en roles. (T/O) 4. Política de Backup y Recuperación: Realizar backups frecuentes (ej. diarios), verificar su integridad y probar restauraciones periódicamente. Almacenar copias offline/offsite. (T/O) 5. Auditoría de Acciones: Registrar quién accede, modifica o elimina documentos oficiales. (T)	
R04	Sistemas de Información (Gestión Documental, etc.)	Software desactualizado, falta de antivirus/antimalware robusto, falta de capacitación (phishing), backups insuficientes/no probados	1. Gestión de Vulnerabilidades y Parches: Proceso formal para actualizar S.O., aplicaciones y firmware regularmente. (O/T) 2. Solución de Seguridad Endpoint (EDR/Antivirus): Instalar y mantener actualizada una solución robusta y centralizada en todos los equipos. (T) 3. Campañas de Concienciación y Simulación de Phishing: Entrenar al personal para identificar correos/mensajes sospechosos. Realizar simulacros. (O) 4. Backup 3-2-1: Implementar estrategia (3 copias, 2 medios distintos, 1 offsite). Asegurar que los backups estén aislados (contra ransomware) y probados. (T/O)	T, O

			5. Filtro Antispam y Antiphishing: Utilizar soluciones a nivel de correo electrónico para bloquear amenazas. (T)	
R05	Datos de Ciudadanos (Incumplimiento Ley 1581)	Falta de consentimiento informado claro, políticas desactualizadas, manejo inadecuado	1. Revisión y Actualización de Políticas de Privacidad: Asegurar que sean claras, completas y conformes a Ley 1581. (O/L) 2. Mecanismos de Consentimiento Explícito: Implementar casillas de verificación (no pre-marcadas), formularios claros, y registro del consentimiento. (T/O) 3. Procedimientos de Atención a Derechos ARCO: Definir y comunicar cómo los ciudadanos pueden ejercer sus derechos (Acceso, Rectificación, Cancelación, Oposición). (O) 4. Designación de Responsable de Protección de Datos: Nombrar un encargado (interno o externo) para supervisar el cumplimiento. (O) 5. Minimización de Datos: Recolectar y retener solo los datos estrictamente necesarios para la finalidad informada. (O)	O, L, T

R06	Infraestructura Tecnológica (Servidores, Red)	Falta de redundancia, plan de continuidad (BCP/DRP) inexistente/no probado, ubicación física vulnerable	1. Implementar Redundancia: Servidores en clúster, fuentes de poder redundantes, múltiples enlaces de red, RAID para discos. (T) 2. Desarrollar y Probar Plan de Continuidad/Recuperación (BCP/DRP): Documentar procedimientos y realizar simulacros anuales. (O) 3. Mejorar Seguridad Física del Centro de Datos/Servidores: Control de acceso físico estricto, sistemas de detección/extinción de incendios, control ambiental (temperatura, humedad), SAI/UPS. (F) 4. Backups Offsite: Asegurar que una copia de los backups críticos esté en una ubicación geográfica distinta. (T/F/O)	T, O, F
R07	Personal (Funcionarios, Concejales)	Falta de capacitación continua, falta de procedimientos claros, ausencia de controles de doble verificación	1. Programa de Formación Continua en Seguridad: Sesiones periódicas (anuales/semestrales) y boletines informativos sobre nuevas amenazas y buenas prácticas. (O) 2. Documentación de Procedimientos (SOPs): Crear y difundir guías claras para tareas sensibles (manejo de información, comunicaciones oficiales, etc.). (O) 3. Controles de Doble Verificación: Implementar para acciones críticas (ej. transferencias, publicación de	O, T

			acuerdos, cambios de configuración importantes) donde sea viable. (O/T) 4. Clasificación de Información: Entrenar al personal sobre cómo identificar y manejar información según su sensibilidad. (O) 5. Reporte de Incidentes Simplificado: Facilitar que el personal reporte errores o incidentes de seguridad sin temor a represalias excesivas. (O)	
R08	Información Confidencial (Estrategias, Contratos)	Controles de acceso insuficientes, falta de monitoreo, falta de políticas de clasificación, uso de canales inseguros	1. Política de Clasificación de la Información: Definir niveles (Público, interno, Confidencial, etc.) y reglas de manejo para cada uno. (O) 2. Controles de Acceso Reforzados: Aplicar permisos estrictos (need-to-know) en sistemas donde reside información confidencial. (T/O) 3. Herramientas de Prevención de Fuga de Datos (DLP): Considerar implementar DLP en endpoints o red para monitorear/bloquear la salida no autorizada de datos clasificados. (T) 4. Política de Comunicación Segura: Exigir uso de correo electrónico corporativo cifrado, VPN para acceso remoto, prohibir uso de apps de mensajería no seguras para info. sensible. (O/T)	O, T, L

			5. Acuerdos de Confidencialidad (NDA): Para personal y terceros con acceso a información sensible. (O/L)	
R09	Equipos de Cómputo / Dispositivos Móviles	Falta de cifrado de disco, contraseñas débiles, falta de políticas BYOD, no inventario/control	1. Cifrado de Disco Completo (FDE): Obligatorio en todos los portátiles corporativos (ej. BitLocker/FileVault). (T) 2. Autenticación Fuerte en Dispositivos: Exigir contraseñas/PIN complejos o biometría. Bloqueo automático por inactividad. (T/O) 3. Gestión de Dispositivos Móviles (MDM): Implementar MDM para aplicar políticas de seguridad, inventariar y permitir borrado remoto en dispositivos corporativos y/o BYOD aprobados. (T) 4. Política de Uso de Dispositivos (Incluyendo BYOD): Definir claramente qué se permite, requisitos de seguridad para BYOD (si se aceptan), y responsabilidades. (O) 5. Inventario de Activos TI: Mantener un registro actualizado de todos los dispositivos. (O) 6. Borrado Remoto: Asegurar la capacidad de borrar datos de dispositivos perdidos/robados gestionados. (T)	T, O

Notas:

1. **Tipo de Control (¹):**
    - **O:** Organizacional (Políticas, Procedimientos, Roles, Capacitación)
    - **T:** Técnico/Lógico (Software, Hardware, Configuraciones)
    - **F:** Físico (Controles de acceso físico, ambientales)
    - **L:** Legal/Cumplimiento (Contratos, Adecuación a normativas)
    - **Servicio:** Contratación de un servicio externo.
2. **Priorización**: No todos los controles pueden implementarse de inmediato. Deberás priorizarlos basándote en:
    - El Nivel de Riesgo que mitigan (empezar por los MA y A).
    - El coste y la complejidad de implementación.
    - Los recursos disponibles (presupuesto, personal).
3. **Combinación de Controles**: A menudo, se necesita una combinación de controles para abordar eficazmente una vulnerabilidad.
4. **Control Residual:** Después de implementar los controles, deberás re-evaluar el riesgo (riesgo residual) para ver si ha bajado a un nivel aceptable.

Esta lista te proporciona un punto de partida robusto para definir las acciones concretas en tu Plan de Tratamiento de Riesgos. Cada control debería detallarse más en el plan, incluyendo responsable, plazo de implementación y métricas para evaluar su eficacia.

Notas Importantes:

1. **Valoración de Dimensiones (¹):** La valoración (C, I, D) asignada es una estimación basada en la naturaleza general del activo en un contexto municipal. Debe ser validada y refinada por el personal del Concejo de Yumbo que conoce el valor específico de cada activo para la organización.
2. **Riesgo Inherente:** Esta tabla refleja el riesgo *antes* de considerar la efectividad total de los controles existentes (riesgo inherente). El siguiente paso, el Plan de Tratamiento, se basará en este nivel de riesgo para decidir cómo gestionarlo (mitigar, aceptar, transferir, evitar).
3. **Subjetividad:** La evaluación cualitativa siempre tiene un grado de subjetividad. Es crucial que esta evaluación sea consensuada por un equipo multidisciplinario dentro del Concejo (TI, Jurídico, Administrativo, Directivos).
4. **Contexto Específico:** La probabilidad y el impacto pueden variar según el contexto específico del Concejo de Yumbo (presupuesto, cultura organizacional, infraestructura actual, amenazas específicas del entorno local).

5. **Actualización:** Este análisis debe ser revisado y actualizado periódicamente (al menos anualmente) o cuando ocurran cambios significativos.

Próximos Pasos:

Con esta evaluación y clasificación de riesgos basada en MAGERIT, ahora puedes proceder a:

1. **Validar y Refinar:** Discutir esta tabla con los responsables del Concejo de Yumbo para ajustar las valoraciones de activos, impacto y probabilidad según su conocimiento detallado.
2. **Priorizar:** Enfocarse en los riesgos con nivel **MA (Muy Alto)** y **A (Alto)** para el desarrollo del Plan de Tratamiento.
3. **Desarrollar el Plan de Tratamiento:** Para cada riesgo priorizado, definir las acciones específicas (controles o salvaguardas según MAGERIT) que se implementarán para mitigar, transferir, evitar o decidir aceptar el riesgo residual.

Esta evaluación te proporciona una base sólida y estructurada, alineada con una metodología reconocida como MAGERIT, para continuar con la gestión de la seguridad de la información en el Concejo Municipal de Yumbo.

Conclusiones

1. La evaluación y clasificación de riesgos según impacto y probabilidad se confirma como un ejercicio indispensable para el Concejo Municipal de Yumbo, trascendiendo la mera identificación de amenazas para proporcionar una comprensión profunda de la severidad real que cada una representa para la organización y sus activos de información.

2. El proceso ha permitido obtener una visión clara y jerarquizada del panorama de riesgos de seguridad de la información que enfrenta el Concejo, identificando aquellos que, por su alta probabilidad de ocurrencia o por la magnitud de su impacto potencial (operacional, legal, reputacional), demandan atención prioritaria y urgente.

3. La aplicación de una metodología estructurada, basada en principios como los de MAGERIT y adaptada al contexto del Concejo, ha proporcionado un marco objetivo y consistente para la valoración, permitiendo comparar riesgos de naturaleza diversa y facilitando una toma de decisiones más informada y estratégica.

4. Los resultados de esta evaluación constituyen la base fundamental e informada sobre la cual se debe desarrollar el Plan de Tratamiento de Riesgos. La clasificación obtenida (en niveles como Muy Alto, Alto, Medio, etc.) es la guía esencial para asignar recursos y esfuerzos de mitigación de manera eficiente y efectiva.

5. Se evidencia que áreas críticas como la protección de datos personales (en cumplimiento de la Ley 1581), la garantía de la disponibilidad de servicios clave (como la plataforma de transparencia bajo la Ley 1712) y la mitigación de factores internos como el error humano, emergen como puntos focales que concentran riesgos de nivel significativo para el Concejo Municipal de Yumbo.

Recomendaciones

1. Utilizar la clasificación de riesgos obtenida en este documento como guía principal para priorizar las acciones a incluir en el Plan de Tratamiento de Riesgos, enfocando los esfuerzos iniciales y los recursos más significativos en la mitigación de aquellos riesgos catalogados como Muy Altos (MA) y Altos (A).

2. Proceder sin demora a la elaboración detallada del Plan de Tratamiento de Riesgos, definiendo para cada riesgo priorizado los controles específicos (técnicos, organizacionales, físicos, legales) a implementar, los responsables de su ejecución, los plazos estimados y las métricas para evaluar su eficacia posterior.

3. Gestionar activamente la asignación de los recursos presupuestarios, técnicos y humanos necesarios para la implementación efectiva de las medidas de tratamiento priorizadas, reconociendo que la seguridad de la información es una inversión estratégica para la continuidad y reputación del Concejo.

4. Involucrar activamente a las diferentes áreas del Concejo (Tecnologías de la Información, Jurídico, Administrativo, Comunicaciones, y a los propios Concejales y directivos) tanto en la validación final de esta evaluación como en la definición e implementación de los controles del Plan de Tratamiento, asegurando una visión integral y el compromiso organizacional.

5. Implementar un proceso formal y periódico (al menos anual, o ante cambios significativos en el entorno tecnológico, operativo o normativo) para la revisión y actualización tanto de esta evaluación de riesgos como del subsiguiente Plan de Tratamiento, garantizando que la estrategia de seguridad del Concejo permanezca relevante y efectiva a lo largo del tiempo.

Tabla de contenido

Introducción 2

Justificación 3

Alcance 4

Objetivo General: 5

Objetivos Específicos: 5

Actividades para Coordinar el Proceso de Gestión de Tecnologías de la Información del Concejo Municipal de Yumbo 6

1) **Implementación de un Módulo de Atención al Ciudadano en Orfeo** 6

2) **Desarrollo de un Portal de Transparencia y Participación Ciudadana con WordPress** 7

3) **Capacitación en Herramientas TIC para Funcionarios** 9

4) **Evaluación y Mejora de la Infraestructura Tecnológica** 10

5) **Promoción de Plataformas Digitales entre Ciudadanos** 12

Recomendaciones 15

Conclusiones 15

Introducción

En la era digital, las tecnologías de la información desempeñan un papel crucial en la optimización de la gestión pública. En particular, la interacción directa entre las instituciones y los ciudadanos es vital para garantizar un gobierno transparente y efectivo. Por ello, el Concejo Municipal de Yumbo ha decidido implementar un plan de acción orientado a mejorar la atención al ciudadano y fortalecer la participación social, con el objetivo de crear un entorno más accesible y participativo.

Una de las principales iniciativas que se desarrollarán es la implementación de un módulo de atención al ciudadano en el sistema de gestión documental Orfeo. Este módulo buscará mejorar la calidad de la atención recibida por el público, permitiendo gestionar de manera eficiente las solicitudes, quejas y sugerencias. Asimismo, se asegurará de cumplir con los estándares de accesibilidad y seguridad, alineándose a las normativas establecidas por la Ley 1712 de 2014. Esta herramienta no solo facilitará la comunicación entre los ciudadanos y el Concejo, sino que también pretende reducir los tiempos de respuesta y aumentar la satisfacción del usuario.

Simultáneamente, se establecerá un portal de transparencia utilizando WordPress como base tecnológica. Este portal será un espacio dinámico y accesible donde se publicarán documentos importantes, como acuerdos y actas, y se habilitarán herramientas de participación ciudadana, como encuestas y foros. La meta es promover una cultura de transparencia que fortalezca la confianza pública, así como incentivar la participación activa de los ciudadanos en los procesos de toma de decisiones y en el seguimiento de las acciones del Concejo.

A través de estas iniciativas, el Concejo Municipal de Yumbo busca no solo modernizar su infraestructura tecnológica, sino también fomentar un diálogo abierto con la ciudadanía. Con la implementación de estas herramientas, se espera un impacto significativo en la gestión pública, cuantificable a través de indicadores de éxito que permitirán evaluar la efectividad de las acciones emprendidas. Así, el Concejo dará un paso decidido hacia una administración más inclusiva y eficiente.

Justificación

La implementación de un módulo de atención al ciudadano en el sistema Orfeo y el desarrollo de un portal de transparencia son esenciales para garantizar una gestión pública moderna y efectiva en el Concejo Municipal de Yumbo. En un contexto en el que los ciudadanos demandan cada vez más un acceso ágil y transparente a la información, es crítico que las instituciones públicas adopten soluciones tecnológicas que permitan interactuar de manera más eficiente con la comunidad. Estas iniciativas no solo buscan mejorar la calidad del servicio ofrecido, sino también promover un cambio cultural hacia una administración más abierta y receptiva.

La Ley 1712 de 2014 establece las bases para la transparencia y el acceso a la información pública, principios que son fundamentales para una democracia saludable. Al crear un módulo de atención al ciudadano, se responden directamente a estos requerimientos legales, asegurando que las solicitudes, quejas y sugerencias sean procesadas de manera eficiente y organizada. Esto fomentará un ambiente de confianza entre los ciudadanos y la administración, ya que los ciudadanos podrán verificar cómo se manejan sus inquietudes y recibir respuestas en tiempos reducidos, lo que se traduce en una mayor satisfacción y una mejor percepción institucional.

Asimismo, el desarrollo del portal de transparencia utilizando WordPress permitirá que la información relevante esté disponible al público de forma accesible y organizada. La integración de herramientas participativas, como encuestas y foros, fortalecerá la voz de los ciudadanos en la toma de decisiones, promoviendo un sentido de pertenencia y responsabilidad compartida en la gestión pública. A medida que los ciudadanos se sientan más involucrados e informados, se incrementará su disposición a participar en los procesos democráticos, lo cual es crucial para la salud de cualquier comunidad.

Por último, la capacitación en herramientas TIC para los funcionarios no solo es un paso hacia la modernización de los procesos, sino también una inversión en el capital humano de la administración pública. Dotar a los empleados de las habilidades necesarias para utilizar eficazmente estas herramientas contribuirá a una mayor eficiencia y seguridad en la gestión de información. Al fomentar una cultura de aprendizaje continuo y adaptación a nuevas tecnologías, el Concejo Municipal de Yumbo estará mejor preparado para enfrentar los desafíos futuros y atender eficazmente las necesidades de su comunidad.

Alcance

El alcance del proyecto para coordinar el proceso de gestión de tecnologías de la información del Concejo Municipal de Yumbo se centra en la implementación de soluciones digitales que mejoren la atención al ciudadano y fomenten la participación activa de la comunidad. La primera fase del proyecto incluye el desarrollo de un módulo de atención al ciudadano en el sistema de gestión documental Orfeo. Este módulo permitirá gestionar de manera efectiva las solicitudes, quejas y sugerencias, asegurando que se cumplan los requerimientos de accesibilidad y seguridad estipulados en la Ley 1712 de 2014. Esta herramienta será fundamental para optimizar los tiempos de respuesta y aumentar la satisfacción de los usuarios.

Adicionalmente, se contempla la creación de un portal de transparencia basado en WordPress, el cual servirá como un espacio centralizado para la publicación de información relevante, como acuerdos y actas. Este portal no solo facilitará el acceso a la información pública, sino que también incluirá herramientas de participación, como encuestas y foros, permitiendo a los ciudadanos interactuar con sus representantes y expresar sus opiniones sobre asuntos de interés comunitario. De esta manera, el portal contribuirá a construir relaciones de confianza entre el Concejo y los ciudadanos, promoviendo una cultura de transparencia y rendición de cuentas.

El alcance del proyecto también abarca un programa de capacitación dirigido a los funcionarios del Concejo, con el fin de equiparlos con las habilidades necesarias para utilizar eficientemente las herramientas implementadas. Se llevarán a cabo talleres en los que se abordarán temas como el manejo de Orfeo, buenas prácticas de seguridad y el uso adecuado del portal de transparencia. Esta capacitación es vital para garantizar que los funcionarios puedan aprovechar al máximo las soluciones digitales y así mejorar el desempeño institucional en la atención al ciudadano.

Finalmente, el proyecto incluye la evaluación y mejora de la infraestructura tecnológica del Concejo, asegurando que los sistemas implementados operen de manera óptima y segura. Esto implica realizar un diagnóstico de la infraestructura existente, implementar un sistema de copias de seguridad automáticas y establecer un plan de mantenimiento continuo. Durante el ciclo de vida del proyecto, se buscará recopilar y analizar métricas de impacto que permitan medir el éxito de las iniciativas, contribuyendo así a un proceso de gestión más ágil y eficaz en el Concejo Municipal de Yumbo

Objetivo General:

Mejorar la gestión de las tecnologías de la información en el Concejo Municipal de Yumbo mediante la implementación de herramientas digitales que optimicen la atención al ciudadano, fomenten la transparencia y faciliten la participación comunitaria, asegurando así una administración pública más eficiente y accesible.

Objetivos Específicos:

1. Conocer y aplicar las normativas y estándares de accesibilidad y seguridad requeridos para el desarrollo del módulo de atención al ciudadano en Orfeo, a fin de garantizar el cumplimiento de la Ley 1712 de 2014 y mejorar la calidad del servicio al ciudadano.
2. Desarrollar y evaluar un portal de transparencia utilizando WordPress, que integre al menos tres herramientas participativas (encuestas, foros y publicación de documentos), con el propósito de promover la participación activa de los ciudadanos y fortalecer la relación entre el Concejo y la comunidad.
3. Capacitar y practicar con los funcionarios del Concejo en el uso efectivo de las nuevas herramientas y plataformas digitales implementadas, para asegurarse de que al menos el 90% de ellos puedan utilizar correctamente estas tecnologías, mejorando así el desempeño institucional en la atención a los ciudadanos.

Actividades para Coordinar el Proceso de Gestión de Tecnologías de la Información del Concejo Municipal de Yumbo

1) **Implementación de un Módulo de Atención al Ciudadano en Orfeo**

Objetivo del Plan de Acción Impactado: Mejorar la calidad de la atención al ciudadano (Objetivo Estratégico 3 y Meta de Atención al Ciudadano).

Objetivo del Documento de Alineación: Desarrollar un módulo de atención al ciudadano dentro del sistema de gestión documental Orfeo que cumpla con los estándares de accesibilidad y seguridad, contribuyendo así a una mayor transparencia y eficiencia en la gestión de solicitudes.

Descripción: La integración de un módulo de atención al ciudadano en Orfeo representa una respuesta integral a la necesidad de optimizar la comunicación entre la administración pública y la ciudadanía. Este módulo permitirá gestionar de manera adecuada solicitudes, quejas y sugerencias de los ciudadanos, alineándose con la Ley 1712 de 2014 y fortaleciendo la cultura de participación.

Importancia

1. Fortalecimiento de la Relación con la Ciudadanía: La implementación del módulo facilitará un contacto más fluido y directo entre los ciudadanos y la administración. Al permitir a los ciudadanos presentar sus inquietudes y recibir respuestas en un formato estructurado, se fortalecerá la confianza en las instituciones y se promoverá una cultura de transparencia.
2. Optimización del Proceso de Atención: Integrar este módulo al software Orfeo existente, que ya está en producción, maximiza las inversiones previas en tecnología y recursos. Facilita la continuidad y mejora de procesos, ya que se opera dentro de una plataforma conocida, eliminando la necesidad de reentrenar al personal en un nuevo sistema.
3. Cumplimiento Normativo: La creación de este módulo se alinea con las normativas que exigen una gestión pública transparente y accesible. Esto no solo garantiza un servicio de calidad a los ciudadanos, sino que también minimiza riesgos legales y fortalece la imagen institucional.

Ventajas

1. Accesibilidad y Usabilidad: Al desarrollar un módulo de atención al ciudadano en Orfeo, se facilita el acceso a servicios públicos, permitiendo a los ciudadanos realizar consultas y seguimiento de sus trámites desde cualquier lugar, en cualquier momento. El módulo también incluirá características de accesibilidad para personas con discapacidad, asegurando que todos los ciudadanos puedan interactuar con la administración sin barreras.
2. Eficiencia en la Gestión de Solicitudes: La digitalización de solicitudes, quejas y sugerencias mediante este módulo permitirá a la administración gestionar estos casos de manera más eficiente. Automatizando procesos como el seguimiento y la notificación de estados, se reducirá el tiempo de respuesta y se aumentará la satisfacción del ciudadano.

3. Mejor Toma de Decisiones: La recolección sistemática de datos y retroalimentación a través del módulo proporcionará información valiosa sobre las necesidades y expectativas de los ciudadanos. Esta información puede ser utilizada para desarrollar políticas más efectivas y para ajustar los servicios ofrecidos, alineándolos con las demandas reales de la comunidad.
4. Indicadores de Impacto: Se establecerán métricas para medir el éxito del módulo, tales como el porcentaje de solicitudes gestionadas, tiempos de respuesta y niveles de satisfacción. Estos indicadores permitirán evaluar el rendimiento del módulo de atención al ciudadano y realizar ajustes para mejorar continuamente el servicio.

En resumen, la implementación del módulo de atención al ciudadano en Orfeo no solo permitirá una atención más eficiente y accesible, sino que también fortalecerá la gestión pública, impulsando una cultura de transparencia y participación que beneficiará tanto a la ciudadanía como a la administración. A través de este esfuerzo, el Concejo Municipal de Yumbo demuestra su compromiso con la mejora continua y el servicio de calidad, alineándose con los principios de la gestión pública moderna.

2) Desarrollo de un Portal de Transparencia y Participación Ciudadana con WordPress

Objetivo del Plan de Acción Impactado: Promover la participación ciudadana y fortalecer la imagen corporativa (Objetivo Estratégico 1 y Meta de Comunicación).

Objetivo del Documento de Alineación: Mejorar el portal de transparencia y participación ciudadana existente en WordPress para optimizar la comunicación con los ciudadanos y asegurar el cumplimiento de las normativas actuales.

Descripción: La actualización del Portal de Transparencia y Participación Ciudadana, ya creado en WordPress, es un paso clave para garantizar que la información disponible sea accesible, relevante y fácil de utilizar. Este portal sirve como una plataforma vital para la publicación de datos y documentos oficiales, así como para la promoción de la participación activa de los ciudadanos en los procesos del Concejo Municipal de Yumbo.

Importancia

1. Transparencia y Rendición de Cuentas: Un portal optimizado permite a los ciudadanos acceder fácilmente a información sobre decisiones, acuerdos y proyectos del Concejo. Esto no solo mejora la transparencia, sino que también fortalece la rendición de cuentas por parte de las autoridades.
2. Fomento de la Participación Ciudadana: Al ofrecer herramientas interactivas como encuestas y foros, el portal incentivará a los ciudadanos a participar en la toma de decisiones. Esto fomenta una ciudadanía activa y comprometida con los asuntos públicos.
3. Cumplimiento Normativo: Mantener el portal actualizado garantiza que se cumplan las obligaciones legales, conforme a la Ley 1712 de 2014, que establece el derecho a la información pública en Colombia.

Ventajas

1. Mejora de la Usabilidad: Al actualizar el diseño y la estructura del portal, se puede mejorar la navegación y la experiencia del usuario. Esto incluye simplificar menús, crear secciones claramente diferenciadas y utilizar un diseño responsivo que facilite el acceso desde dispositivos móviles.
2. Integración de Herramientas Interactivas: Introducir herramientas de consulta, encuestas y foros de discusión permitirá recoger opiniones y sugerencias de la ciudadanía, garantizando que el portal no solo sea informativo, sino también un espacio para el diálogo.
3. Actualización de Contenido: Asegurar que la información publicada esté actualizada y sea relevante es crucial. La implementación de sistemas de publicación automática, como la integración con Orfeo, reducirá la carga administrativa y garantizará que los documentos sean accesibles tan pronto como se generen.
4. Aumentar la Visibilidad del Portal: Para lograr un mayor uso del portal, es esencial implementar campañas de promoción en redes sociales y otros medios locales. Esto ayudará a aumentar el tráfico del portal y a asegurar que más ciudadanos conozcan las herramientas de participación disponibles.

Recomendaciones de Mejora

1. Evaluación de Plugin y Herramientas: Revisar y actualizar los plugins utilizados en el portal para asegurarse de que estén actualizados y sean compatibles con las últimas versiones de WordPress. Considerar la implementación de nuevos plugins que mejoren la funcionalidad, como aquellos que optimizan la accesibilidad.
2. Análisis de Datos y Métricas: Integrar herramientas de análisis, como Google Analytics, para monitorear el tráfico del portal y entender qué secciones son más populares. Esto permitirá hacer ajustes basados en datos reales sobre el comportamiento de los usuarios.
3. Capacitación Continua del Personal: Ofrecer formación regular para los funcionarios encargados de gestionar el contenido del portal. Esto no solo mejorará la calidad de la información publicada, sino que también fomentará la innovación y la creatividad en la difusión de contenido.
4. Implementación de Medidas de Seguridad: Fortalecer la seguridad del portal mediante la instalación de plugins de seguridad actualizados y la realización de copias de seguridad regulares para proteger contra posibles ataques o pérdidas de datos.
5. Retroalimentación Ciudadana: Establecer mecanismos para que los ciudadanos puedan proporcionar retroalimentación sobre la funcionalidad y el contenido del portal, lo que permitirá realizar mejoras continua y adaptadas a las necesidades de los usuarios.

En conclusión, la actualización del Portal de Transparencia y Participación Ciudadana en WordPress no solo mejorará la calidad de la información y la interacción con los ciudadanos, sino que también fortalecerá la confianza en la gestión pública. Al implementar estas recomendaciones, el Concejo Municipal de

Yumbo podrá seguir avanzando hacia una administración más transparente, accesible y participativa.

3) Capacitación en Herramientas TIC para Funcionarios

Objetivo del Documento de Alineación: Capacitar al personal en herramientas de Tecnologías de la Información y la Comunicación (TIC) para asegurar la adopción efectiva de las soluciones implementadas.

Descripción: Este programa de capacitación está diseñado para empoderar a los funcionarios del Concejo Municipal de Yumbo mediante el uso de herramientas TIC, incluidas plataformas como Orfeo y prácticas de seguridad en el manejo de datos. Una capacitación adecuada permitirá que el personal maximize el uso de las tecnologías en sus funciones diarias, mejorando la eficiencia y la calidad del servicio a los ciudadanos.

Importancia

1. Aumento de la Eficiencia: La capacitación en herramientas TIC permite automatizar procesos, optimizando tiempos y recursos en el desempeño de las tareas administrativas.
2. Mejora en la Seguridad de la Información: Los funcionarios capacitados en buenas prácticas de seguridad contribuyen a proteger la información sensible y asegurar el cumplimiento de normativas legales relacionadas con la gestión de datos.
3. Adopción de Innovaciones Tecnológicas: A medida que surgen nuevas herramientas y tecnologías, la capacitación continua asegura que los funcionarios estén actualizados y puedan aprovechar al máximo las innovaciones.

Beneficios

1. Desempeño Aumentado: Mejores habilidades en TIC reflejan directamente en un aumento en la productividad y eficacia a la hora de atender las solicitudes y necesidades de los ciudadanos.
2. Confianza en el Uso de Tecnología: La capacitación proporciona a los funcionarios la confianza necesaria para utilizar herramientas digitales, lo cual es crucial en un entorno cada vez más digitalizado.
3. Integración Efectiva de Nuevas Soluciones: Un personal capacitado facilita la implementación y el uso de nuevos módulos y software, asegurando que se aprovechen todas sus funcionalidades.
4. Mejora en la Satisfacción del Ciudadano: Funcionario capacitado en TIC puede ofrecer un mejor servicio, lo que resulta en mayor satisfacción y confianza por parte de los ciudadanos.

Recomendaciones de Mejora

1. Análisis de Necesidades de Capacitación: Realizar encuestas y entrevistas con el personal para identificar áreas específicas donde se requiere capacitación, asegurando que el programa aborde las necesidades reales del equipo.

2. Diversificación de Métodos de Enseñanza: Utilizar una combinación de talleres presenciales, módulos en línea y materiales autodidactas para abarcar diferentes estilos de aprendizaje y horarios disponibles de los funcionarios.
3. Desarrollo de Materiales de Apoyo: Crear manuales de usuario, guías rápidas y tutoriales en video que los funcionarios puedan consultar posteriormente, facilitando así el aprendizaje continuo.
4. Evaluación Continua del Programa: Implementar evaluaciones periódicas al finalizar cada taller para medir la efectividad del programa y realizar ajustes basados en la retroalimentación recibida.
5. Formación de Capacitadores Internos: Identificar funcionarios con habilidades destacadas en TIC y capacitarlos para que se conviertan en formadores de sus compañeros, lo que también fomentará una cultura de colaboración y conocimiento compartido.
6. Incorporar Temas de Seguridad en la Formación: Incluir módulos específicos sobre ciberseguridad y la gestión de datos personales en la capacitación para que los funcionarios sean conscientes de las normativas y prácticas de protección necesarias.
7. Establecer una Línea de Soporte: Crear un canal de comunicación donde los funcionarios puedan hacer preguntas y resolver dudas relacionadas con el uso de herramientas TIC, promoviendo un entorno de aprendizaje continuo.
8. Programas de Reforzamiento Continuo: Organizar talleres de actualización y actualizaciones periódicas en nuevas herramientas y tecnologías, asegurando que el personal esté al día con las últimas innovaciones y mejores prácticas.

La capacitación en herramientas TIC es esencial para fortalecer la capacidad del personal del Concejo Municipal de Yumbo. Mediante una formación adecuada y persistente, se busca empoderar a los funcionarios para que ofrezcan un servicio de calidad, adaptándose a un entorno digital y cumpliendo con los requerimientos normativos de transparencia y seguridad. Este enfoque no solo beneficia al personal, sino que también fortalece la conexión con la ciudadanía, mejorando la gestión pública.

4) Evaluación y Mejora de la Infraestructura Tecnológica

Objetivo del Plan de Acción Impactado: Reducir el riesgo de pérdida de datos y optimizar procesos (Objetivo Estratégico 3).

Objetivo del Documento de Alineación: Realizar una evaluación exhaustiva y mejorar la infraestructura tecnológica existente, garantizando su capacidad para soportar las operaciones del Concejo Municipal de Yumbo de manera efectiva y segura.

Descripción: La infraestructura tecnológica es fundamental para el funcionamiento eficiente de las operaciones administrativas y la prestación de servicios al ciudadano. La evaluación y mejora de esta infraestructura permitirá no solo reducir

los riesgos asociados a la pérdida de datos, sino también mejorar la eficacia y la resiliencia organizacional.

Importancia

1. Seguridad de la Información: Una infraestructura tecnológica robusta reduce el riesgo de pérdida de datos críticos, garantizando que la información sensible esté protegida contra ataques cibernéticos y fallas técnicas.
2. Eficiencia Operativa: Al optimizar la infraestructura, los procesos internos pueden volverse más ágiles y eficientes, permitiendo al personal desempeñar sus funciones de manera más efectiva, lo que se traduce en una mejor atención al ciudadano.
3. Escalabilidad: Evaluar la infraestructura permite identificar oportunidades de mejora y asegurarse de que esté preparada para escalar según las necesidades futuras del Concejo, especialmente en un entorno tecnológico en constante evolución.

Ventajas

1. Reducción de Costos: Implementar soluciones de backup y almacenamiento más eficientes puede disminuir costos a largo plazo relacionados con la pérdida de datos o con el mantenimiento de hardware obsoleto.
2. Mejora de la Conectividad: Fortalecer la conectividad y el rendimiento de la red mejora la colaboración entre departamentos y facilita el acceso a servicios en línea tanto para funcionarios como para ciudadanos.
3. Implementación de Soluciones Innovadoras: Una infraestructura mejorada puede facilitar la adopción de nuevas tecnologías, como la inteligencia artificial o el análisis de datos, que optimizan la toma de decisiones y el servicio al ciudadano.

Recomendaciones de Mejora

1. Diagnóstico Integral de la Infraestructura: Realizar una auditoría detallada de todos los componentes de la infraestructura tecnológica, incluidas redes, servidores, dispositivos de almacenamiento y sistemas en uso. Esto ayudará a identificar puntos débiles y áreas de mejora.
2. Actualización de Hardware y Software: Sustituir o actualizar el hardware anticuado y asegurarse de que el software utilizado esté en sus versiones más recientes. Esto no solo mejorará el rendimiento, sino que también reforzará la seguridad de la infraestructura.
3. Establecimiento de un Plan de Backup Sólido: Implementar un sistema de copias de seguridad automatizadas utilizando software como Proxmox Backup Server, asegurando que haya copias de seguridad regulares y probadas a través de simulaciones de recuperación de datos.
4. Capacitación del Personal en Seguridad Cibernética: Proporcionar capacitación continua al personal sobre mejores prácticas de seguridad cibernética para minimizar riesgos y construir una cultura organizacional centrada en la seguridad de la información.

5. Plan de Mantenimiento Proactivo: Establecer un cronograma de mantenimiento regular para revisar y actualizar todos los componentes de la infraestructura. Esto puede incluir revisiones de seguridad, actualizaciones de software y pruebas de recuperación de datos.
6. Incorporación de Hardware y Software de Virtualización: Evaluar la posibilidad de usar soluciones de virtualización para consolidar servidores y mejorar la eficiencia del uso de recursos, permitiendo una mayor flexibilidad y escalabilidad.
7. Implementación de un Sistema de Monitoreo en Tiempo Real: Desarrollar e implementar un sistema que supervise el estado de la infraestructura tecnológica en tiempo real para detectar problemas antes de que afecten las operaciones.
8. Evaluación de Proveedores de Servicios de Tecnología: Revisar regularmente los contratos y el servicio proporcionado por los proveedores de tecnología para asegurarse de que cumplen con los estándares necesarios y ofrecen soluciones valiosas para el Concejo.

En conclusión, la evaluación y mejora de la infraestructura tecnológica del Concejo Municipal de Yumbo son esenciales para garantizar que los servicios ofrecidos a los ciudadanos sean eficientes y seguros. Con la implementación de estas recomendaciones, se podrá construir un entorno tecnológico resiliente, preparado para enfrentar los desafíos actuales y futuros.

5) Promoción de Plataformas Digitales entre Ciudadanos

Objetivo del Plan de Acción Impactado: Fortalecer los canales de comunicación y fomentar la participación ciudadana (Objetivo Estratégico 1).

Objetivo del Documento de Alineación: Involucrar a la ciudadanía en el uso de plataformas digitales, promoviendo la transparencia y la participación activa en la gestión pública.

Descripción: La promoción de plataformas digitales, como el portal de transparencia y el módulo de atención al ciudadano, busca mejorar la interacción entre el Concejo Municipal de Yumbo y sus ciudadanos. Esto no solo facilitará el acceso a información clave, sino que también estimulará la participación activa de los ciudadanos en temas que afectan su comunidad.

Importancia

1. Facilitación del Acceso a la Información: Las plataformas digitales permiten que los ciudadanos accedan fácilmente a información sobre actividades, proyectos y resultados del Concejo, generando confianza y transparencia en la gestión pública.
2. Fomento de la Participación Ciudadana: La promoción de herramientas digitales motiva a los ciudadanos a expresar sus opiniones, hacer consultas y participar en la toma de decisiones que afectan su entorno.
3. Mejora en la Comunicación: Estas plataformas sirven como un canal directo de comunicación entre el Concejo y los ciudadanos, permitiendo una retroalimentación más efectiva y oportuna.

Beneficios

1. Incremento en la Satisfacción Ciudadana: Al ofrecer canales de atención eficaces y accesibles, se mejora la experiencia del ciudadano al interactuar con la administración pública, lo que puede resultar en mayores niveles de satisfacción.
2. Generación de Compromiso Cívico: Promover plataformas digitales fomenta un sentido de pertenencia y responsabilidad entre los ciudadanos respecto a su comunidad y sus instituciones, impulsando un mayor compromiso cívico.
3. Optimización de Recursos: La digitalización de procesos y la interacción en línea ayudan a optimizar recursos, permitiendo que el Concejo gestione mejor su tiempo y personal en actividades de atención al ciudadano.

Recomendaciones

1. Estrategia de Comunicación Clara: Desarrollar un plan de comunicación que detalle los objetivos, los beneficios de las plataformas y las formas de uso. Utilizar mensajes claros y accesibles para todos los ciudadanos.
2. Uso de Múltiples Canales de Promoción: Implementar una estrategia que combine redes sociales, correo electrónico, talleres comunitarios y medios locales para asegurar que la información llegue a un público diverso, incluyendo aquellos que tienen menos acceso a tecnología.
3. Creación de Contenidos Atractivos: Diseñar materiales visuales e interactivos que expliquen el uso de las plataformas digitales. Videos cortos, infografías y guías paso a paso pueden ser herramientas efectivas.
4. Colaboración con Organizaciones Locales: Asociarse con organizaciones comunitarias y grupos ciudadanos para promover las plataformas digitales y organizar eventos conjuntos que fomenten la participación pública.
5. Capacitación y Soporte al Usuario: Ofrecer talleres prácticos y sesiones de capacitación que enseñen a los ciudadanos cómo usar las plataformas digitales, brindando soporte técnico a quienes lo necesiten.
6. Recopilación de Retroalimentación: Implementar mecanismos para que los ciudadanos compartan su experiencia con las plataformas digitales. Utilizar encuestas y grupos focales para evaluar la efectividad de la promoción y hacer ajustes según sea necesario.
7. Monitoreo y Evaluación de Impacto: Establecer indicadores de éxito claros, como el número de usuarios activos en las plataformas o la calidad de la retroalimentación recibida. Esto permitirá evaluar la efectividad de las acciones promocionales y realizar mejoras continuas.
8. Creación de un Espacio Virtual de Participación: Promover la creación de foros virtuales y encuestas en línea donde los ciudadanos puedan discutir temas relevantes y participar activamente en la elaboración de políticas y proyectos.

En conclusión, la promoción de plataformas digitales es fundamental para mantener una relación abierta y efectiva entre el Concejo Municipal de Yumbo y sus ciudadanos. A través de estas acciones, se puede impulsar una cultura de participación y transparencia, fortaleciendo la democracia local.

Recomendaciones

1. Formar un comité en el que participen representantes de cada área del Concejo Municipal y del equipo de tecnologías de la información. Este comité debe supervisar y coordinar las actividades relacionadas con la gestión de tecnologías, asegurando que todos los proyectos estén alineados con las necesidades institucionales y cityanas.

2. Implementar revisiones programadas del cumplimiento de la Ley 1712 de 2014 y la Ley 1581 de 2012. Estas auditorías deben ser realizadas con la colaboración de asesores legales y expertos en áreas tecnológicas para garantizar la adecuada protección de datos y la transparencia en la gestión de la información.

3. Crear un repositorio digital utilizando herramientas como Nextcloud para almacenar y documentar todos los procesos, capacitaciones y buenas prácticas en el uso de herramientas TIC. Esta documentación facilitará la transferencia de conocimientos y la formación de nuevos funcionarios, asegurando la sostenibilidad de los proyectos a largo plazo.

4. Desarrollar campañas de comunicación efectivas para informar a la ciudadanía sobre las nuevas herramientas y plataformas digitales disponibles. Esto puede incluir talleres comunitarios y el uso de redes sociales, con el objetivo de aumentar la participación ciudadana y fomentar el uso del portal de transparencia y el módulo de atención al ciudadano.

5. Establecer mecanismos de evaluación continua que permitan recolectar retroalimentación de los ciudadanos y funcionarios sobre la efectividad de las herramientas implementadas. Esto permitirá realizar ajustes necesarios y optimizar la experiencia del usuario en la utilización de las plataformas digitales.

6. Promover un ambiente dentro del Concejo que valore la innovación y la adopción de nuevas tecnologías. Esto podría incluir la creación de espacios para la formación continua en TIC y la exploración de nuevas soluciones que beneficien la gestión pública y la interacción con la comunidad.

Conclusiones

1. La implementación del módulo de atención al ciudadano en el sistema Orfeo representa un avance significativo en la calidad del servicio ofrecido por el Concejo Municipal de Yumbo. Al digitalizar y estructurar la gestión de solicitudes, quejas y sugerencias, se podrá garantizar una atención más rápida y accesible, alineada con las normativas vigentes que promueven la transparencia y la participación ciudadana.

2. El desarrollo del portal de transparencia y participación ciudadana utilizando WordPress no solo facilitará la difusión de información relevante, como

acuerdos y proyectos, sino que también incentivará la participación activa de los ciudadanos. Al ofrecer herramientas interactivas como encuestas y foros, se promueve un diálogo más cercano entre la administración y la comunidad, contribuyendo a una gestión pública más inclusiva y colaborativa.

3. La formación de los funcionarios en el uso de herramientas TIC y la gestión de contenidos es crucial para el éxito de las iniciativas implementadas. A medida que los funcionarios se familiaricen con estas tecnologías, se incrementará su confianza y competencia en la utilización de las mismas, garantizando así la sostenibilidad y efectividad de las soluciones digitales a largo plazo.

4. La creación de un comité TIC y la implementación de auditorías de cumplimiento normativo constituyen pasos esenciales para fomentar una cultura de responsabilidad y mejora continua en la gestión de tecnologías. Este enfoque no solo asegura que las iniciativas se alineen con las regulaciones actuales, sino que también impulsa la innovación constante dentro del Concejo.

5. Establecer indicadores de impacto permitirá al Concejo medir el éxito de las iniciativas implementadas, evaluar la satisfacción de los ciudadanos y realizar ajustes necesarios. La recolección continua de retroalimentación será vital para adaptar las plataformas digitales a las necesidades cambiantes de la comunidad, asegurando siempre un servicio de calidad y accesibilidad.

Contenido

1. Introducción 2

Alcance 3

Objetivos Específicos: 4

1. Gobernanza, Roles y Responsabilidades 5

Conclusiones 21

Recomendaciones 22

1. Introducción

En el ejercicio de sus funciones públicas y su compromiso con la comunidad de Yumbo, el Concejo Municipal maneja un volumen significativo de información que resulta vital para su operación diaria, la toma de decisiones y la prestación de servicios a la ciudadanía. La protección adecuada de esta información, en todas sus formas, no es solo una necesidad operativa, sino una responsabilidad fundamental para garantizar la confianza pública, la transparencia y el cumplimiento normativo. Este Plan de Seguridad y Privacidad de la Información (PSPI) se constituye como el documento rector que establece el marco operativo y las directrices concretas para gestionar proactivamente los riesgos y salvaguardar los activos de información del Concejo.

El presente PSPI ha sido desarrollado en estricta alineación con estándares internacionales de mejores prácticas, como la norma ISO/IEC 27001, y los lineamientos nacionales establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) a través del Modelo de Seguridad y Privacidad de la Información (MSPI). Esta doble alineación asegura un enfoque robusto, integral y adaptado al contexto colombiano, permitiendo al Concejo abordar de manera sistemática tanto los aspectos de seguridad (confidencialidad, integridad, disponibilidad) como los de privacidad (cumplimiento de la Ley 1581 de 2012 y normativas asociadas). Su propósito es traducir la estrategia y las políticas de seguridad y privacidad en acciones tangibles, procesos definidos y responsabilidades claras.

Este plan representa la continuación lógica y la operacionalización de los esfuerzos previos de identificación y evaluación de riesgos. Detalla cómo se implementarán, gestionarán y mantendrán los controles seleccionados en el Plan de Tratamiento de Riesgos (PTR) y la Declaración de Aplicabilidad (SoA), proporcionando la hoja de ruta necesaria para que las actividades programadas en materia de seguridad y privacidad tengan continuidad y coherencia. Define la estructura de gobernanza, los roles esenciales y los procesos clave para el monitoreo, la gestión de incidentes, la formación del personal y la mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI).

Conscientes de que cada organización es única, este PSPI ha sido concebido teniendo en cuenta la realidad específica, el tamaño y los recursos del Concejo Municipal de Yumbo, buscando ser una herramienta práctica y aplicable. Se ha priorizado un lenguaje claro y accesible, con el fin de que todos los funcionarios, concejales y personal relacionado comprendan su rol y responsabilidad en la protección de la información. Además, se reconoce que la seguridad y la privacidad son disciplinas dinámicas; por ello, este plan es un documento vivo, destinado a ser revisado y actualizado periódicamente para adaptarse a nuevos desafíos tecnológicos, amenazas emergentes y cambios normativos, asegurando así la protección sostenida e integrada de la información que el Concejo custodia y gestiona.

Alcance

Base en ISO 27001 (Cláusula 4.3): La norma ISO 27001 requiere explícitamente que la organización determine los **límites y la aplicabilidad** del sistema de gestión para establecer su alcance. Esto implica considerar:

- Cuestiones externas e internas relevantes.
- Requisitos de las partes interesadas.
- Interfaces y dependencias entre las actividades realizadas por la organización y aquellas realizadas por otras organizaciones. La estructura propuesta (Límites Organizacionales, Físicos, Lógicos) es una forma práctica y estándar en la industria para definir estos límites de manera clara y sin ambigüedades.

Base en MSPI: El MSPI, aunque tiene su propia estructura de ejes y dominios, se fundamenta en gran medida en ISO 27001. Requiere que las entidades públicas identifiquen claramente los procesos, la información y la tecnología que soportan sus funciones, lo cual está directamente relacionado con la definición del alcance. Además, el MSPI pone un fuerte énfasis en el cumplimiento del marco legal colombiano (Ley 1581, Ley 1712), por lo que definir el alcance ayuda a determinar qué datos y procesos específicos están sujetos a estas regulaciones dentro del sistema de gestión.

2.1. Límites Organizacionales, Físicos y Lógicos: Responde directamente a la necesidad de definir los **límites** del SGSPI (ISO 4.3). Es crucial saber qué departamentos, edificios y sistemas están incluidos para poder aplicar controles de manera coherente.

2.2. Activos de Información Críticos Cubiertos: Aunque el inventario detallado está en otro documento, mencionar los tipos de activos clave dentro del alcance conecta con el enfoque basado en riesgos (fundamental en ISO 27001 y MSPI), ya que el objetivo es proteger estos activos.

2.3. Partes Interesadas Relevantes: Aborda el requisito de ISO 27001 (Cláusula 4.2) de comprender las necesidades y expectativas de las partes interesadas. Para el MSPI y el contexto público colombiano, identificar a la ciudadanía, entes de control, etc., es vital para enfocar los esfuerzos de seguridad y privacidad en satisfacer sus requisitos (protección de datos, transparencia, cumplimiento).

2.4. Exclusiones Justificadas: Es una buena práctica (y requerida por ISO 27001 si se excluyen controles del Anexo A) ser explícito sobre lo que *no* está incluido, para evitar malentendidos y asegurar que cualquier exclusión sea deliberada y documentada.

En resumen, la estructura establece directrices y requisitos fundamentales de ISO 27001 y es totalmente compatible con el enfoque del MSPI de MinTIC. Te proporciona el marco correcto según los estándares solicitados. Lo que necesitas hacer es completar la información específica del Concejo Municipal de Yumbo (direcciones, nombres exactos de sistemas, etc.) dentro de esa estructura.

Objetivo General:

Establecer y operar sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) del Concejo Municipal de Yumbo, conforme a los lineamientos de este Plan, para gestionar proactivamente los riesgos, asegurar el cumplimiento normativo (ISO 27001, MSPI, Ley 1581/1712) y proteger de manera continua la confidencialidad, integridad y disponibilidad de sus activos de información.

Objetivos Específicos:

1. **Ejecutar** el Plan de Tratamiento de Riesgos (PTR) documentado, implementando los controles de seguridad y privacidad priorizados para mitigar los riesgos identificados a un nivel aceptable para el Concejo Municipal de Yumbo.
2. **Aplicar** la estructura de gobernanza, los roles, las responsabilidades y los procedimientos operativos definidos en este PSPI para asegurar la gestión coherente y sistemática de las actividades de seguridad y privacidad en las operaciones diarias del Concejo.
3. **Evaluar** periódicamente la eficacia y el desempeño del SGSPI mediante el seguimiento de indicadores clave, la realización de auditorías internas y las revisiones por la dirección, con el fin de identificar no conformidades y oportunidades para la mejora continua de la seguridad y privacidad en el Concejo.

1. Gobernanza, Roles y Responsabilidades

1.1. Estructura de Gobernanza del SGSPI

Se establece el Comité de Seguridad y Privacidad de la Información (CSPI) como la instancia formal de más alto nivel responsable de la supervisión, orientación estratégica y toma de decisiones clave relacionadas con el SGSPI del Concejo Municipal de Yumbo. Este Comité asegura la alineación del SGSPI con los objetivos estratégicos de la entidad y el cumplimiento de los requisitos legales y normativos (ISO 27001, MSPI, Ley 1581, Ley 1712, etc.).

Objetivos del CSPI:

- Aprobar la Política General y las políticas específicas de Seguridad y Privacidad de la Información.
- Supervisar la implementación y el desempeño general del SGSPI.
- Revisar y aprobar los resultados de la evaluación de riesgos y el Plan de Tratamiento de Riesgos (PTR).
- Asegurar la asignación de recursos adecuados para la implementación y mantenimiento del SGSPI.
- Tomar decisiones sobre la gestión de riesgos residuales significativos.
- Promover una cultura de seguridad y privacidad en toda la entidad.
- Realizar la Revisión por la Dirección del SGSPI (según Cláusula 9.3 de ISO 27001).

- Composición del CSPI (Sugerida - Ajustar a estructura real de Yumbo):
- Presidente del Concejo Municipal (o su delegado con autoridad): Preside el Comité.
- Secretario(a) General del Concejo.
- El Oficial/Responsable de Seguridad de la Información (actúa como Secretario Técnico del Comité).
- El Oficial/Responsable de Protección de Datos Personales (si es una figura distinta).
- Un representante del área de Tecnologías de la Información (TI) (si existe formalmente) o quien desempeñe esas funciones.
  - ✓ Un representante del área Jurídica.
  - ✓ Un representante del área Administrativa/Financiera.
  - ✓ Un representante del área de Archivo y Gestión Documental.
  - ✓ *(Opcional: Un Concejal delegado para temas de tecnología/transparencia)*

Frecuencia de Reuniones: El CSPI se reunirá de forma ordinaria al menos una vez cada trimestre y de forma extraordinaria cuando las circunstancias lo requieran (ej. incidente grave, cambio normativo significativo). Se levantarán actas de cada reunión.

1.2. Roles Clave y Responsabilidades

Se definen los siguientes roles y responsabilidades específicas dentro del SGSPI:

Alta Dirección (Mesa Directiva / Presidente del Concejo):

- Demostrar liderazgo y compromiso visible con la seguridad y privacidad de la información.
- Asegurar que la Política y los objetivos del SGSPI sean compatibles con la dirección estratégica del Concejo.
- Aprobar formalmente la Política General del SGSPI.
- Asegurar la disponibilidad de los recursos necesarios para el SGSPI.
- Promover la mejora continua del SGSPI.
- Presidir el Comité de Seguridad y Privacidad de la Información.

Oficial / Responsable de Seguridad de la Información (OSI): *(Puede ser una persona designada o un rol asignado)*

- Coordinar el diseño, implementación, mantenimiento y mejora del SGSPI en alineación con ISO 27001 y MSPI.
- Supervisar la implementación y eficacia de los controles de seguridad definidos en el PTR y el SoA.
- Coordinar la gestión de incidentes de *seguridad* de la información.
- Mantener actualizada la documentación del SGSPI (incluyendo evaluación de riesgos y PTR).
- Promover la conciencia y capacitación en *seguridad* de la información.
- Reportar sobre el desempeño del SGSPI al CSPI y a la Alta Dirección.
- Actuar como punto de contacto principal para asuntos de seguridad de la información.
- Coordinar las auditorías internas y externas del SGSPI.

Oficial / Responsable de Protección de Datos Personales (OPDP): *(Puede ser la misma persona que el OSI o una figura distinta, según Ley 1581 y capacidad del Concejo)*

- Velar por la implementación efectiva de la normativa de protección de datos personales (Ley 1581 y decretos reglamentarios) dentro del Concejo.
- Asesorar a todas las áreas sobre sus obligaciones en materia de privacidad.
- Gestionar y dar trámite a las consultas y reclamos de los titulares de datos (Derechos ARCO).
- Coordinar y supervisar el inventario de bases de datos personales y el Registro Nacional de Bases de Datos (RNBD).
- Promover una cultura de privacidad y protección de datos en la entidad.
- Actuar como enlace con la Superintendencia de Industria y Comercio (SIC) para asuntos de protección de datos.
- Supervisar la implementación de controles específicos de privacidad.

Responsables de Activos de Información: *(Ej. Jefe de Archivo, Administrador de Sistema X, Secretario General para ciertos documentos)*

- Identificar, clasificar y documentar los activos de información bajo su responsabilidad.
- Implementar y mantener los controles de seguridad y privacidad asignados a sus activos.
- Gestionar los permisos de acceso a sus activos según las políticas definidas.
- * Reportar incidentes o debilidades relacionadas con sus activos.

Área de Tecnologías de la Información (TI) (o rol equivalente):

- Implementar, configurar y mantener los controles *técnicos* de seguridad (firewalls, antivirus, sistemas de detección, backups, etc.).
- Administrar la infraestructura tecnológica (redes, servidores, sistemas operativos).
- Gestionar las cuentas de usuario y los accesos lógicos según las directrices de Control de Acceso.
- Apoyar en la investigación técnica de incidentes de seguridad.
- Aplicar parches y actualizaciones de seguridad.

Área Jurídica:

- Proporcionar asesoramiento legal sobre el cumplimiento normativo (seguridad, privacidad, contratación, etc.).
- Revisar la conformidad legal de políticas, procedimientos y contratos con terceros.
- Apoyar en la gestión de incidentes con implicaciones legales.

Área de Talento Humano (o rol equivalente):

- Integrar las responsabilidades de seguridad y privacidad en las descripciones de cargos y contratos.
- Incluir la formación en seguridad y privacidad en los procesos de inducción.
- Gestionar los acuerdos de confidencialidad.
- Aplicar procedimientos seguros en los procesos de vinculación, traslado y desvinculación del personal.

* Todos los Funcionarios, Concejales y Contratistas:

- Conocer y cumplir la Política General y las políticas específicas de seguridad y privacidad que les apliquen.
- Manejar de forma segura la información y los activos a los que tienen acceso.
- Utilizar las contraseñas y mecanismos de autenticación de forma responsable.
- Reportar oportunamente cualquier incidente, debilidad o sospecha de violación de seguridad o privacidad.

- Participar activamente en las actividades de formación y concienciación.
- Proteger los activos de información de la entidad contra acceso, divulgación o daño no autorizado.

1.3. Matriz de Responsabilidades (RACI)

Para clarificar aún más las responsabilidades en procesos clave del SGSPI, se podrá desarrollar y mantener (posiblemente como un anexo a este plan o documento separado) una Matriz RACI (Responsable, Aprueba, Consultado, Informado). Esta matriz detallará la participación de los diferentes roles en actividades críticas como:

- Gestión de Incidentes de Seguridad.
- Respuesta a Solicitudes de Derechos ARCO.
- Realización de Auditorías Internas.
- Gestión de Cambios Tecnológicos.
- Revisión por la Dirección.
- Actualización de Políticas.

2. **Gestión de Riesgos de Seguridad y Privacidad (Operacionalización)**

2.1. Referencia a la Metodología y Resultados de la Evaluación de Riesgos

El proceso de tratamiento de riesgos se basa directamente en los hallazgos documentados en el informe "Evaluación y clasificación de los riesgos según su impacto y probabilidad" del Concejo Municipal de Yumbo. Dicho documento detalla:

- La metodología empleada para la identificación y evaluación de riesgos (basada en MAGERIT y adaptada al contexto del Concejo).
- El inventario de activos de información críticos evaluados.
- La identificación de amenazas y vulnerabilidades relevantes.
- La valoración del impacto potencial y la probabilidad de ocurrencia para cada riesgo.
- La clasificación final de los riesgos inherentes en niveles (ej. Muy Alto, Alto, Medio, Bajo, Muy Bajo).

Los riesgos clasificados como Muy Altos (MA), Altos (A) y aquellos de nivel Medio (M) que superen el umbral de apetito de riesgo definido por el Concejo (determinado por el CSPI), son la entrada principal para el Plan de Tratamiento de Riesgos descrito a continuación.

2.2. Plan de Tratamiento de Riesgos (PTR)

El Plan de Tratamiento de Riesgos (PTR) es el documento operativo central que detalla las acciones específicas que el Concejo Municipal de Yumbo implementará para gestionar los riesgos identificados y priorizados. Su propósito es asegurar que cada riesgo significativo sea abordado de manera planificada, asignando responsabilidades y plazos claros.

Para cada riesgo incluido en el PTR, se documentará la siguiente información mínima:

- ID del Riesgo: Identificador único que vincula el riesgo con la evaluación previa.
- Descripción del Riesgo: Breve descripción del escenario de riesgo.
- Nivel de Riesgo Inherente: Clasificación obtenida de la evaluación (MA, A, M).
- Opción de Tratamiento Seleccionada: Decisión sobre cómo gestionar el riesgo:
- Mitigar/Modificar: Implementar controles para reducir la probabilidad y/o el impacto. (Opción más común).
- Transferir/Compartir: Trasladar parte del riesgo a un tercero (ej. seguro cibernético, cláusulas contractuales).
- Aceptar/Retener: Decisión informada y documentada (generalmente por el CSPI) de aceptar el riesgo (típicamente para riesgos bajos o medios donde el costo del tratamiento supera el beneficio).
- Evitar/Eliminar: Decidir no realizar la actividad que genera el riesgo o eliminar el activo/proceso asociado.
- Control(es) Propuesto(s): Identificación del control o controles específicos seleccionados para implementar la opción de tratamiento (haciendo referencia, siempre que sea posible, al número de control del Anexo A de ISO 27001 y/o al dominio/práctica relevante del MSPI).
- Descripción Detallada de la Acción de Tratamiento: Explicación clara de las tareas concretas a realizar para implementar el control.
- Responsable de la Implementación: Cargo o rol específico responsable de ejecutar la acción de tratamiento.
- Fecha de Inicio Estimada: Cuándo se prevé comenzar la implementación.
- Fecha de Finalización Estimada / Plazo: Fecha límite para completar la implementación del control.
- Recursos Requeridos (Estimación): Indicación de los recursos necesarios (presupuesto, personal, tecnología).
- Indicador de Seguimiento/Eficacia: Métrica o criterio para verificar que el control se implementó correctamente y está siendo efectivo.
- Nivel de Riesgo Residual Esperado: Estimación del nivel de riesgo que permanecerá después de la implementación exitosa del tratamiento.

El PTR detallado se mantendrá como un documento dinámico, gestionado por el Oficial/Responsable de Seguridad de la Información y revisado periódicamente por el CSPI. *(Indicar aquí si el PTR detallado forma parte de este PSPI como un anexo o si es un documento separado referenciado. Se recomienda que sea fácilmente actualizable, por lo que un documento separado o un anexo manejable es preferible).

2.3. Declaración de Aplicabilidad (SoA / DdA)

La Declaración de Aplicabilidad (SoA), requisito explícito de ISO 27001 (Cláusula 6.1.3.d) y alineado con las buenas prácticas del MSPI, es el documento que justifica la selección e implementación de los controles de seguridad y privacidad. Vincula los resultados de la evaluación de riesgos y las decisiones del Plan de Tratamiento con el conjunto de controles definidos en el Anexo A de la norma ISO 27001 (y por extensión, con los dominios y prácticas del MSPI).

La SoA del Concejo Municipal de Yumbo contendrá, como mínimo:

- La lista de todos los controles del Anexo A de ISO 27001 (versión aplicable).
- Una indicación clara de si cada control ha sido seleccionado (es aplicable y se implementará o ya está implementado) o excluido (no es aplicable).
- La justificación para la inclusión de cada control seleccionado (generalmente, vinculándolo a los riesgos que ayuda a mitigar, a requisitos legales/normativos, obligaciones contractuales o necesidades del negocio/operación del Concejo).
- La justificación para la exclusión de cualquier control considerado no aplicable al alcance del SGSPI del Concejo.
- Una referencia al estado actual de implementación de los controles seleccionados (ej. Implementado, En proceso, Pendiente).

La Declaración de Aplicabilidad es un documento fundamental que demuestra la cobertura y la idoneidad de los controles implementados. Será mantenida y actualizada por el Oficial/Responsable de Seguridad de la Información y aprobada por el CSPI. *(Indicar aquí si la SoA forma parte de este PSPI como un anexo o si es un documento separado referenciado).

3. Implementación de Controles de Seguridad y Privacidad

Esta sección describe el enfoque operativo y las prácticas implementadas por el Concejo Municipal de Yumbo para dar cumplimiento a los controles de seguridad y privacidad seleccionados en la Declaración de Aplicabilidad (SoA) y detallados, cuando corresponde a riesgos priorizados, en el Plan de Tratamiento de Riesgos (PTR). El objetivo es asegurar que los controles sean aplicados de manera

consistente y efectiva en toda la organización, dentro del alcance definido para el SGSPI.

La implementación se basa en una combinación de políticas definidas, procedimientos documentados, configuraciones técnicas, medidas físicas y actividades de concienciación, gestionados por los roles y responsabilidades asignados en la Sección 4. A continuación, se describe el enfoque general para los principales dominios de control (alineados con ISO 27001 Anexo A y considerando las prácticas del MSPI):

3.1. Políticas de Seguridad de la Información (Ref. ISO A.5 / MSPI)

- Se ha establecido y comunicado la Política General de Seguridad y Privacidad de la Información, aprobada por la Alta Dirección.
- Se desarrollan, aprueban, comunican y revisan periódicamente políticas específicas que detallan las reglas para áreas clave (ej. Uso Aceptable de Activos, Control de Acceso, Teletrabajo, Clasificación de la Información, etc.).
- La responsabilidad de revisar y mantener actualizadas las políticas recae en el Oficial/Responsable de Seguridad de la Información, con la aprobación del CSPI.

3.2. Organización de la Seguridad de la Información (Ref. ISO A.6 / MSPI)

- La estructura de roles y responsabilidades definida en la Sección 4 asegura la asignación clara de tareas de seguridad y privacidad.
- Se implementan medidas de seguridad para el uso de dispositivos móviles (corporativos y/o personales - BYOD si aplica) y para el teletrabajo, conforme a las políticas específicas.
- Se gestiona la segregación de funciones donde sea necesario y factible para reducir riesgos de fraude o error.

3.3. Seguridad de los Recursos Humanos (Ref. ISO A.7 / MSPI)

- Se integran consideraciones de seguridad y privacidad durante todo el ciclo de vida del personal (vinculación, durante el empleo, terminación o cambio de funciones).
- Se incluyen cláusulas de confidencialidad en los contratos laborales y de prestación de servicios.
- Los procesos de inducción incluyen formación básica en seguridad y privacidad.
- Se aplica un proceso disciplinario definido en caso de incumplimiento de las políticas.
- Se realizan actividades continuas de concienciación y formación (detalladas en Sección 7).

3.4. Gestión de Activos (Ref. ISO A.8 / MSPI)

- Se mantiene un inventario de los activos de información críticos dentro del alcance del SGSPI.
- Se aplica una metodología de clasificación de la información basada en su sensibilidad y criticidad (ej. Pública, Interna, Confidencial), con reglas de manejo asociadas.
- Se establecen normas para el uso aceptable de los activos de información.
- Se implementan procedimientos para el manejo seguro de medios extraíbles y para la eliminación o reutilización segura de equipos y medios de almacenamiento.

3.5.. Control de Acceso (Ref. ISO A.9 / MSPI)

- Se aplica una política de control de acceso basada en los principios de negocio y seguridad (ej. necesidad de conocer, menor privilegio).
- Se sigue un proceso formal para la gestión del ciclo de vida de los usuarios (alta, baja, modificación de permisos) en sistemas y aplicaciones críticas.
- Se implementan controles para la gestión de contraseñas robustas (complejidad, cambio periódico) y otros mecanismos de autenticación.
- Se gestionan los privilegios de acceso de forma restringida y controlada.
- Se aplican controles de acceso a nivel de red (ej. segmentación básica, firewalls perimetrales) y a nivel de sistemas operativos y aplicaciones.

3.6.. Criptografía (Ref. ISO A.10 / MSPI)

- Se utiliza el cifrado para proteger la confidencialidad e integridad de la información sensible, conforme a la política definida. Esto incluye, donde sea aplicable y necesario:
- Cifrado de disco completo en equipos portátiles.
- Cifrado de comunicaciones sensibles (ej. a través de HTTPS para sitios web, VPN para acceso remoto).
- Cifrado de bases de datos o campos específicos que contengan información personal altamente sensible.
- Se establecen prácticas básicas para la gestión de claves criptográficas (cuando aplica).

3.7. Seguridad Física y Ambiental (Ref. ISO A.11 / MSPI)

- Se definen y protegen perímetros de seguridad física (ej. oficinas del Concejo).
- Se aplican controles de acceso físico a las instalaciones y áreas sensibles (ej. recepción, archivo, sala de servidores/comunicaciones).
- Se implementan medidas de protección contra amenazas ambientales (ej. detectores de humo, extintores, protección básica contra fluctuaciones eléctricas para equipos críticos - UPS).
- Se promueve la política de escritorio y pantalla limpios.
- Se asegura la protección física de los equipos contra robo o daño.

3.8.. Seguridad de las Operaciones (Ref. ISO A.12 / MSPI)

- Se documentan procedimientos operativos básicos para tareas críticas de TI.
- Se aplica un proceso de gestión de cambios para modificaciones en la infraestructura o sistemas.
- Se gestiona la capacidad de los sistemas clave para asegurar su rendimiento.
- Se implementan controles robustos contra código malicioso (antivirus/antimalware actualizado en servidores y estaciones de trabajo).
- Se realiza y verifica periódicamente la ejecución de copias de seguridad (backups) de la información crítica, conforme a la política de backup y recuperación.
- Se implementa el registro (logging) de eventos relevantes para la seguridad en sistemas críticos y se establecen mecanismos básicos de monitoreo.
- Se gestionan las vulnerabilidades técnicas mediante la aplicación de parches y actualizaciones de seguridad de forma oportuna.

3.9. Seguridad de las Comunicaciones (Ref. ISO A.13 / MSPI)

- Se implementan controles de seguridad en la red (ej. firewalls, configuración segura de routers y switches) para proteger el flujo de información.
- Se establecen mecanismos para la transferencia segura de información sensible (ej. uso de correo electrónico institucional cifrado cuando sea necesario, protocolos seguros como SFTP si aplica).
- Se utilizan acuerdos de confidencialidad (NDA) con terceros que manejan información sensible del Concejo.

3.10. Adquisición, Desarrollo y Mantenimiento de Sistemas (Ref. ISO A.14 / MSPI)

- Se incluyen requisitos de seguridad en la adquisición de nuevos sistemas o servicios tecnológicos.
- Si se realiza desarrollo interno (poco común en Concejos), se aplican prácticas básicas de desarrollo seguro.
- Se gestiona de forma segura la información utilizada en entornos de prueba.
- Se aplican procedimientos de configuración segura para sistemas nuevos o actualizados.

3.11. Relaciones con Proveedores (Ref. ISO A.15 / MSPI)

- Se incluyen requisitos de seguridad y privacidad de la información en los acuerdos y contratos con proveedores que acceden, procesan o almacenan información del Concejo (especialmente proveedores de TI, nube, o manejo de datos personales).
- Se realiza un seguimiento básico del cumplimiento de estos requisitos por parte de los proveedores críticos.

3.12. Gestión de Incidentes de Seguridad de la Información (Ref. ISO A.16 / MSPI)

- Se ha establecido un proceso formal para la gestión de incidentes de seguridad y privacidad, que incluye:
- Canales y responsabilidades para el reporte de eventos e incidentes.
- Procedimientos para la evaluación, clasificación y respuesta a incidentes.
- Contención, erradicación y recuperación.
- Análisis post-incidente y lecciones aprendidas para la mejora.
- Se registran y documentan los incidentes gestionados.

3.13. Aspectos de Seguridad de la Información para la Continuidad del Negocio (Ref. ISO A.17 / MSPI)

- Se identifican los requisitos de continuidad para los sistemas y la información críticos.
- Se implementan mecanismos de redundancia donde es factible (ej. backups robustos).
- Se desarrolla y mantiene un Plan de Recuperación ante Desastres (DRP) básico, enfocado en la restauración de la información y los servicios tecnológicos esenciales.
- Se realizan pruebas periódicas de los planes de recuperación (especialmente la restauración de backups).

3.14. . Cumplimiento (Ref. ISO A.18 / MSPI)

- Se identifican y documentan los requisitos legales, regulatorios y contractuales aplicables en materia de seguridad y privacidad (Ley 1581, Ley 1712, Archivo General de la Nación, etc.).
- Se implementan controles para proteger los derechos de propiedad intelectual (licenciamiento de software).
- Se realizan revisiones periódicas de cumplimiento y auditorías internas del SGSPI (detalladas en Sección 10).
- Se implementan controles específicos para el cumplimiento de la Ley 1581 de Protección de Datos Personales (ver sección siguiente).

3.15. Implementación Especifica de Controles de Privacidad (Ley 1581 / MSPI)

- Se aplican los procedimientos definidos para obtener y gestionar el consentimiento informado de los titulares para el tratamiento de sus datos personales.
- Se ejecuta el procedimiento documentado para la atención oportuna y completa de las consultas y reclamos (Derechos ARCO) presentados por los titulares de datos.
- Se implementan medidas para asegurar la calidad, veracidad y actualización de los datos personales tratados.
- Se siguen los lineamientos para la transferencia y transmisión segura de datos personales a terceros (si aplica), asegurando el cumplimiento legal.

- Se mantiene actualizado el Registro Nacional de Bases de Datos (RNBD) ante la SIC, conforme a la normativa vigente.
- Se promueve la aplicación de principios de Privacidad desde el Diseño y por Defecto en nuevos proyectos o sistemas que involucren tratamiento de datos personales.

4. Conciencia, Formación y Competencia

Un pilar fundamental para la efectividad del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) en el Concejo Municipal de Yumbo es asegurar que todo el personal involucrado posea la conciencia, la formación y la competencia necesarias para cumplir con sus responsabilidades individuales y colectivas en la protección de la información. Esta sección describe el programa y las actividades diseñadas para lograr este objetivo, fomentando una cultura organizacional donde la seguridad y la privacidad sean una responsabilidad compartida.

4.1. Programa Anual de Capacitación y Concienciación

El Concejo Municipal de Yumbo implementa un Programa Anual de Capacitación y Concienciación en Seguridad y Privacidad de la Información, coordinado conjuntamente por el Oficial/Responsable de Seguridad de la Información y el Oficial/Responsable de Protección de Datos Personales, con el apoyo del área de Talento Humano y la aprobación del CSPI.

Objetivos del Programa:

- Garantizar que todo el personal comprenda la Política General de Seguridad y Privacidad y las políticas específicas que le son aplicables.
- Asegurar que el personal sea consciente de las principales amenazas y riesgos de seguridad y privacidad (ej. ingeniería social, malware, fugas de datos).
- Promover la comprensión de la importancia de su contribución individual a la eficacia del SGSPI.
- Dotar al personal de los conocimientos básicos necesarios para manejar la información y los activos de forma segura y conforme a la normativa (especialmente Ley 1581 y Ley 1712).
- Informar sobre los procedimientos clave (ej. reporte de incidentes, solicitud de soporte, manejo de datos personales).
- Reforzar las implicaciones del incumplimiento de las políticas y procedimientos.

Temáticas Clave a Cubrir (Adaptadas a la audiencia):

- Política General y Políticas Específicas (Uso Aceptable, Contraseñas, etc.).
- Principios básicos de Seguridad de la Información (Confidencialidad, Integridad, Disponibilidad).
- Identificación y reporte de amenazas (Phishing, Vishing, Smishing, Malware).

- Buenas prácticas de contraseñas y autenticación.
- Seguridad física (escritorio y pantalla limpios, control de acceso físico).
- Uso seguro del correo electrónico e internet.
- Manejo seguro de información clasificada.
- Protección de Datos Personales (Ley 1581): Principios, consentimiento, derechos ARCO, manejo de datos sensibles, RNBD.

Transparencia y Acceso a la Información (Ley 1712): Responsabilidades en la publicación y acceso.

- Procedimiento de reporte y gestión de incidentes de seguridad y privacidad.
- Seguridad en el teletrabajo y uso de dispositivos móviles (si aplica).

4.2. Audiencias Objetivo y Frecuencia

El programa se diseña considerando las diferentes audiencias dentro del Concejo.

- Nuevos Ingresos (Funcionarios y Contratistas): Formación obligatoria durante el proceso de inducción, cubriendo los aspectos fundamentales de seguridad y privacidad.
- Todo el Personal (Funcionarios, Concejales, Contratistas): Sesión de concienciación y actualización general al menos una vez al año. Comunicaciones periódicas (boletines, recordatorios) sobre temas relevantes.
- Roles con Responsabilidades Específicas: (Ej. Personal de TI, Responsables de Activos, Personal de PQRSD, Archivo, Contratación, Oficiales SI/PDP): Formación más detallada y específica sobre sus funciones, procedimientos y herramientas relevantes, según sea necesario.
- Concejales: Sesiones específicas adaptadas a su rol, enfocadas en el manejo seguro de información sensible, comunicaciones oficiales y riesgos asociados a su función pública.
- Alta Dirección / CSPI: Información estratégica sobre el estado del SGSPI, riesgos emergentes y su rol en el liderazgo de la seguridad y privacidad.

4.3. Metodologías de Formación y Concienciación

Se utilizarán diversas metodologías para maximizar el alcance y la efectividad:

- Sesiones presenciales o virtuales interactivas.
- Talleres prácticos (ej. identificación de correos phishing).
- Materiales de lectura y consulta (guías rápidas, folletos).
- Módulos de e-learning (si se dispone de plataforma).
- Comunicados internos, carteleras informativas, intranet.

Campañas periódicas de simulación de phishing para evaluar y reforzar la concienciación.

4.4. Gestión de la Competencia

Para roles con responsabilidades significativas en seguridad y privacidad (definidos en Sección 4), el Concejo asegurará la competencia necesaria mediante:

- Definición de los requisitos de conocimiento y habilidad en los perfiles de cargo o términos de referencia contractual.
- Consideración de la experiencia y formación previa durante los procesos de selección o asignación de roles.
- Provisión de formación especializada adicional cuando sea necesario.
- Evaluación del desempeño en el cumplimiento de las responsabilidades de seguridad y privacidad asignadas.

4.5. Evaluación de la Eficacia del Programa

La efectividad del programa de capacitación y concienciación se evaluará periódicamente a través de:

- Pruebas cortas o cuestionarios después de las sesiones de formación.
- Resultados de las campañas de simulación de phishing (tasa de clics, tasa de reportes).
- Análisis de tendencias en los incidentes de seguridad y privacidad (buscando reducción de errores humanos).
- Retroalimentación directa de los participantes.
- Observaciones durante las auditorías internas del SGSPI.
- Los resultados de la evaluación se utilizarán para identificar áreas de mejora y ajustar el contenido y las metodologías del programa para el siguiente ciclo.

4.6. Responsabilidades

- La coordinación general y diseño del programa recae en el OSI y el OPDP.
- La ejecución de las capacitaciones puede ser realizada por personal interno competente o por expertos externos contratados.
- El área de Talento Humano apoya en la logística, registro de asistencia y gestión de la formación en la inducción.
- Los Jefes de Área y Supervisores son responsables de asegurar la participación de su personal en las actividades programadas.
- La Alta Dirección/CSPI aprueba el plan anual y asigna los recursos necesarios

5. Medición, Análisis y Evaluación (Ciclo CHECK)

Para asegurar la eficacia continua, la adecuación y la idoneidad del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), el Concejo Municipal de Yumbo implementa un proceso sistemático de monitoreo, medición, análisis y evaluación. Este proceso corresponde a la fase "Verificar" (Check) del ciclo Planificar-Hacer-Verificar-Actuar (PHVA), fundamental en ISO 27001 y MSPI, y proporciona la información necesaria para la toma de decisiones y la mejora continua.

5.1.. Monitoreo, Medición, Análisis y Evaluación del Desempeño

El Concejo determinará y aplicará métodos apropiados para el monitoreo y la medición del desempeño del SGSPI y la eficacia de los controles implementados.

- Qué se Monitoreará y Medirá: Se definirán indicadores clave de rendimiento (KPIs) y métricas específicas para evaluar aspectos como:
- Eficacia de Controles Técnicos: Tasas de detección/bloqueo de malware, intentos de acceso no autorizado detectados, resultados de escaneos de vulnerabilidad, éxito de backups.
- Gestión de Incidentes: Número y tipo de incidentes reportados, tiempo medio de detección (MTTD), tiempo medio de respuesta (MTTR), tiempo medio de recuperación (MTR), impacto de los incidentes.
- Cumplimiento de Políticas: Nivel de cumplimiento de políticas clave (ej. contraseñas, escritorio limpio), resultados de auditorías internas.
- Gestión de la Privacidad: Número de solicitudes ARCO recibidas y tiempo de respuesta, cumplimiento en la gestión del consentimiento, estado del RNBD.
- Conciencia y Formación: Tasas de finalización de capacitaciones, resultados de simulacros de phishing.
- Disponibilidad: Tiempo de actividad (uptime) de servicios críticos (sitio web, sistemas internos).
- Progreso del Plan de Tratamiento: Estado de implementación de los controles definidos en el PTR.

Métodos de Monitoreo y Medición: Se utilizarán diversas fuentes y técnicas, incluyendo:

- Revisión de registros (logs) de sistemas, seguridad y aplicaciones.
- Herramientas de monitoreo de red y sistemas.
- Resultados de escaneos de vulnerabilidades y pruebas de penetración (si aplica).
- Informes de herramientas de seguridad (antivirus, firewall, DLP si existe).
- Revisión manual y listas de chequeo.
- Encuestas de satisfacción o percepción de seguridad (opcional).
- Análisis de los registros de incidentes y solicitudes ARCO.

*Análisis y Evaluación: Los datos recolectados serán analizados periódicamente (ej. mensual o trimestralmente) por el OSI y el OPDP para:

- Evaluar si se están alcanzando los objetivos de seguridad y privacidad.

- Identificar tendencias y patrones (ej. aumento de un tipo específico de incidente).
- Determinar la eficacia real de los controles implementados.
- Identificar áreas donde los controles son débiles o inexistentes.
- Proporcionar información objetiva para las auditorías internas y las revisiones por la dirección.

Responsabilidades: El OSI y el OPDP son responsables de definir las métricas específicas, coordinar la recolección de datos y realizar el análisis inicial. Los resultados consolidados se presentarán al CSPI.

5.2. Auditorías Internas del SGSPI

El Concejo Municipal de Yumbo realizará auditorías internas a intervalos planificados para proporcionar información acerca de si el SGSPI:

- Cumple con los requisitos propios de la organización para su SGSPI (políticas, procedimientos).
- Cumple con los requisitos de la norma ISO/IEC 27001 y los lineamientos del MSPI.
- Cumple con los requisitos legales y regulatorios aplicables (Ley 1581, Ley 1712, etc.).
- Se implementa y mantiene eficazmente.

- Programa de Auditoría: Se establecerá un programa anual de auditorías, gestionado por el OSI y aprobado por el CSPI. El programa definirá el alcance, la frecuencia y los métodos, considerando la importancia de los procesos, los riesgos identificados y los resultados de auditorías previas.
- Criterios y Alcance: Cada auditoría definirá claramente los criterios (contra qué se audita) y el alcance (qué procesos, áreas o controles se auditan).
- Selección de Auditores y Realización: Las auditorías serán realizadas por personal interno competente (que haya recibido formación básica en auditoría ISO 27001 si es posible) o por auditores externos contratados. Se asegurará la objetividad e imparcialidad de los auditores (no auditarán su propio trabajo).
- Resultados: Los hallazgos de la auditoría (conformidades, no conformidades, oportunidades de mejora) se documentarán en un informe formal que será comunicado a la dirección pertinente y al CSPI.
- Seguimiento: Se realizará seguimiento a las no conformidades detectadas para asegurar que se tomen las acciones correctivas adecuadas (ver Sección 11).

5.3. Revisiones por la Dirección

La Alta Dirección del Concejo (representada principalmente por el CSPI) revisará el SGSPI a intervalos planificados (al menos una vez al año) para asegurar su continua idoneidad, adecuación y eficacia.

Entradas para la Revisión: La revisión considerará obligatoriamente información sobre:

- El estado de las acciones de las revisiones por la dirección previas.
- Cambios en cuestiones externas e internas relevantes para el SGSPI.
- Retroalimentación sobre el desempeño de la seguridad y privacidad, incluyendo tendencias en:

✓ No conformidades y acciones correctivas.
✓ Resultados del monitoreo y medición (KPIs).
✓ Resultados de auditorías (internas y externas).
✓ Cumplimiento de los objetivos de seguridad y privacidad.
✓ Retroalimentación de las partes interesadas.

- Resultados de la evaluación de riesgos y estado del Plan de Tratamiento de Riesgos.
- Oportunidades de mejora continua.
- Adecuación de recursos.

Salidas de la Revisión: Las decisiones y acciones resultantes de la revisión incluirán, como mínimo:

- Decisiones relacionadas con oportunidades de mejora continua.
- Cualquier necesidad de cambio en el SGSPI (incluyendo políticas, objetivos, alcance, controles, recursos).

Documentación: Se conservará información documentada (actas de reunión) como evidencia de los resultados de las revisiones por la dirección.

Conclusiones

1. El presente Plan de Seguridad y Privacidad de la Información (PSPI) constituye el marco formal y estructurado mediante el cual el Concejo Municipal de Yumbo aborda de manera integral la protección de sus activos de información, estableciendo un Sistema de Gestión (SGSPI) alineado con las mejores prácticas internacionales (ISO 27001) y los requerimientos nacionales (MSPI de MinTIC).
2. Este PSPI operacionaliza la estrategia definida en la Política General, traduciendo los resultados de la evaluación de riesgos en un Plan de Tratamiento de Riesgos (PTR) concreto y una Declaración de Aplicabilidad (SoA) justificada, asegurando así un enfoque basado en riesgos para la selección e implementación de controles.
3. La definición explícita de una estructura de gobernanza (Comité CSPI) y la asignación detallada de roles y responsabilidades a todos los niveles (desde la Alta Dirección hasta cada funcionario y concejal) son elementos clave establecidos en este plan para asegurar la rendición de cuentas y la gestión efectiva del SGSPI.
4. El Plan proporciona la metodología para la implementación sistemática de controles técnicos, organizacionales, físicos y legales, incluyendo aquellos específicos para garantizar el cumplimiento de la normativa de protección de datos personales (Ley 1581), y enfatiza la importancia crítica de la concienciación, formación y competencia del personal como pilar fundamental de la seguridad.
5. La incorporación de ciclos de monitoreo, medición, auditoría interna y revisión por la dirección dentro de este PSPI establece el mecanismo formal para la verificación de la eficacia del SGSPI y sienta las bases para su mejora continua, asegurando su adaptación a los cambios del entorno y la evolución de las amenazas.

Recomendaciones

Se recomienda la aprobación formal de este Plan de Seguridad y Privacidad de la Información (PSPI) por parte de la Alta Dirección (Mesa Directiva/Presidencia) y su posterior comunicación efectiva a todos los funcionarios, concejales y personal relevante del Concejo Municipal de Yumbo para asegurar su conocimiento y adopción.

Es crucial asegurar el compromiso continuo de la Alta Dirección y la asignación de los recursos (presupuestarios, tecnológicos y humanos) necesarios para la implementación exitosa y el mantenimiento a largo plazo de las medidas y procesos definidos en este PSPI, incluyendo los roles clave del OSI y el OPDP.

Enfocar los esfuerzos iniciales en la implementación diligente de los controles definidos en el PTR para los riesgos clasificados como Muy Altos (MA) y Altos (A), realizando un seguimiento riguroso de los plazos y responsabilidades asignadas.

Implementar de manera prioritaria y sostenida el Programa Anual de Capacitación y Concienciación, adaptando los contenidos y metodologías para asegurar que todo el personal comprenda su rol y contribuya activamente a la protección de la información.

Ejecutar disciplinadamente las actividades de monitoreo de indicadores (KPIs), las auditorías internas planificadas y las revisiones por la dirección, utilizando sus resultados como base objetiva para identificar debilidades, tomar acciones correctivas y mejorar continuamente la eficacia del SGSPI.

Mantener actualizada toda la información documentada del SGSPI (políticas, procedimientos, registros, PTR, SoA), asegurando su accesibilidad controlada y su conformidad con los requisitos establecidos.

Fomentar la integración de las consideraciones de seguridad y privacidad ("desde el diseño y por defecto") en todos los nuevos proyectos, adquisiciones tecnológicas y cambios operativos que implemente el Concejo Municipal de Yumbo.

Tabla de contenido

INTRODUCCIÓN 2
JUSTIFICACION 3
ALCANCE 4
OBJETIVO GENERAL 5
OBJETIVOS ESPECIFICOS 5
ENFOQUE METODOLÓGICO 6
Estrategias, técnicas y herramientas: 6
RECOMENDACIONES 15
CONCLUSIONES 16
REFERENCIA BIBLIOGRAFICA 17

INTRODUCCIÓN

En la era digital, la información se ha convertido en un activo fundamental para las organizaciones. El Concejo Municipal de Yumbo, como entidad pública, no es ajeno a esta realidad. La gestión y protección de la información personal y sensible es crucial para garantizar la transparencia, la rendición de cuentas y el cumplimiento de las normas de privacidad y protección de datos.

La importancia de la información para en la entidad radica en su papel central en la gestión de una amplia gama de datos sensibles, incluyendo información personal de ciudadanos, empleados y proveedores. Esta información es crucial para la toma de decisiones, la prestación de servicios públicos, así como para la eficiente gestión administrativa y financiera. Además, la protección adecuada de esta información es esencial para mantener la confianza de la ciudadanía, asegurar el correcto funcionamiento del Concejo Municipal y garantizar el cumplimiento de las regulaciones legales pertinentes.

La ausencia de un proceso formal para la identificación de activos de información en el Concejo Municipal de Yumbo conlleva riesgos significativos. Estos incluyen la posibilidad de pérdida o filtración de información sensible, el incumplimiento de normativas de privacidad y protección de datos, así como el potencial daño a la reputación del Concejo Municipal. Además, la falta de un sistema estructurado para identificar activos de información puede resultar en decisiones erróneas debido a la falta de información precisa y oportuna. Es imperativo establecer un proceso robusto para abordar estos riesgos y proteger eficazmente los activos de información del Concejo Municipal.

La propuesta de solución para el Concejo Municipal de Yumbo consiste en la implementación de un proceso formal de identificación de activos de información dentro del Plan de Privacidad. Este enfoque busca fortalecer la protección de datos sensibles, reducir los riesgos de pérdida o filtración de información, garantizar el cumplimiento de normativas de privacidad y mejorar la toma de decisiones administrativas. Se espera que esta iniciativa genere beneficios tangibles como una mayor seguridad y confianza en la gestión del Concejo Municipal, así como mejoras significativas en la transparencia, rendición de cuentas y cumplimiento normativo.

JUSTIFICACION

La falta de un proceso formal para la identificación de activos de información en el Concejo Municipal de Yumbo conlleva riesgos sustanciales que pueden tener repercusiones negativas en múltiples áreas. Estos riesgos incluyen la exposición de datos sensibles a terceros no autorizados, el riesgo de enfrentar sanciones por incumplimiento de normativas, la pérdida de confianza por parte de la ciudadanía y la posibilidad de tomar decisiones erróneas debido a la falta de información precisa. Por lo tanto, la formalización de un proceso de identificación de activos de información dentro del plan de privacidad es crucial para mitigar estos riesgos y garantizar la protección adecuada de los datos, así como para fortalecer la confianza pública y el cumplimiento normativo del Concejo Municipal de Yumbo.

ALCANCE

El presente documento propone formalizar un proceso exhaustivo para identificar los activos de información relevantes para el Plan de Privacidad del Concejo Municipal de Yumbo. Este proceso incluirá:

- Identificación de Activos de Información: Se llevará a cabo la identificación de los diferentes tipos de activos de información, incluyendo su tipo, formato, ubicación y nivel de criticidad para las operaciones del Concejo Municipal.
- Clasificación de Activos de Información: Los activos de información serán clasificados según su nivel de sensibilidad, incluyendo categorías como pública, interna, confidencial, reservada y altamente sensible, lo que permitirá una gestión diferenciada y adecuada.
- Documentación y Registro de Activos de Información: Se establecerá un proceso para documentar y registrar todos los activos de información identificados, creando un inventario completo que incluya descripciones detalladas, ubicación, propietario, clasificación y las medidas de seguridad correspondientes.
- Revisión y Actualización del Inventario: Se realizarán revisiones periódicas del inventario de activos de información, al menos una vez al año, con el fin de garantizar su relevancia y precisión en todo momento.

OBJETIVO GENERAL

Fortalecer la protección de la información del Concejo Municipal de Yumbo mediante la identificación y clasificación de los activos de información.

OBJETIVOS ESPECIFICOS

- Identificar y clasificar la información personal y sensible que se encuentra en poder del Concejo Municipal.
- Determinar la ubicación y el responsable de cada activo de información.
- Evaluar el impacto potencial de una pérdida o fuga de información.

ENFOQUE METODOLÓGICO

- Selección de la metodología: Se recomienda la adopción de la metodología ISO/IEC 27001:2013 como marco de referencia para la identificación y clasificación de activos de información.
- Adaptación de la metodología: Ajustar la metodología seleccionada a las necesidades y características del Concejo Municipal.

Estrategias, técnicas y herramientas:

1. **Estrategias:**

a) **Compromiso de la Alta Dirección:**

- Asegurar el apoyo y la participación activa de la alta dirección en el proceso de identificación de activos de información.
- Comunicar la importancia del proceso a todo el personal.

b) **Enfoque basado en riesgos:**

- Identificar y evaluar los riesgos asociados a la pérdida o fuga de información.
- Priorizar la identificación de activos de información con mayor riesgo.
-

c) **Gestión del cambio:**

- Implementar un plan de gestión del cambio para facilitar la adopción del nuevo proceso.
- Capacitar al personal sobre la metodología y las herramientas utilizadas.

2. **Técnicas:**

a) **Entrevistas:**
- Realizar entrevistas con personal clave de diferentes áreas del Concejo Municipal.
- Identificar los tipos de información que manejan, su ubicación, criticidad y medidas de seguridad.

b) **Análisis de documentación:**

- Revisar políticas, procedimientos, manuales y otros documentos que contengan información sobre los activos de información.
- Identificar la ubicación, clasificación y medidas de seguridad de la información.

c) **Observación directa:**

- Observar el flujo de información en diferentes áreas del Concejo Municipal.
- Identificar los activos de información en diferentes formatos (físicos, digitales, etc.).

d) **Inventario de sistemas de información:**

- Identificar y documentar los sistemas de información que contienen activos de información.
- Evaluar la seguridad de los sistemas de información.

e) Análisis de flujos de información:

- Identificar el origen, destino y uso de la información dentro del Concejo Municipal.
- Evaluar los riesgos asociados a los flujos de información.

3. Herramientas:

a) Plantillas de entrevistas:

- Diseñar plantillas para guiar las entrevistas con el personal.
- Facilitar la recolección de información relevante sobre los activos de información.

b) Herramientas de análisis de documentación:

- Utilizar herramientas para analizar documentos y extraer información sobre los activos de información.
- Agilizar el proceso de identificación y clasificación.

c) Software de inventario de activos:

- Utilizar software para crear y gestionar un inventario de activos de información.
- Centralizar la información y facilitar su análisis.

d) Herramientas de análisis de riesgos:

- Utilizar herramientas para evaluar los riesgos asociados a la pérdida o fuga de información.
- Priorizar la implementación de medidas de seguridad.

IMPLEMENTACIÓN EN EL CONCEJO MUNICIPAL DE YUMBO:

1. Adaptación de la metodología:

- Ajustar la metodología ISO/IEC 27001:2013 a las necesidades y características del Concejo Municipal.
- Considerar el tamaño, la complejidad y los recursos disponibles.

2. Definición de roles y responsabilidades:

- Designar un responsable del proceso de identificación de activos de información.
- Definir las responsabilidades de cada área y persona involucrada.

3. Capacitación del personal:

- Brindar capacitación al personal sobre la metodología, las técnicas y las herramientas utilizadas.

- Asegurar la comprensión y el compromiso del personal.

4. **Ejecución del proceso:**

- Implementar las estrategias, técnicas y herramientas de la metodología.
- Documentar el proceso y los resultados obtenidos.

5. **Revisión y actualización:**

- Revisar y actualizar el inventario de activos de información de manera regular.
- Asegurar que la información se mantenga actualizada y precisa.

Identificación de activos de información:

1. **Definición de Criterios de Identificación:**

a) **Tipo de información:**

- **Información personal:** Datos relacionados con personas identificables o identificables (persona natural, como nombres, apellidos, números de identificación, etc.)
- **Información sensible:** Información confidencial, estratégica o de alto valor para la organización Información confidencial (como datos financieros, información médica, etc.).
- **Información financiera:** Datos relacionados con las finanzas del Concejo Municipal (transacciones financieras, como cuentas bancarias, tarjetas de crédito, etc.).
- **Información legal:** Documentos y contratos legales.
- **Información técnica:** Datos relacionados con los sistemas de información y la infraestructura tecnológica.
- **Estratégica:** Información que proporciona una ventaja competitiva a la organización.

b) **Formato de la información:**

- **Información física:** Documentos en papel, libros, CD, DVD , etc.
- **Información digital:** Archivos electrónicos, correos electrónicos, bases de datos, etc.
- **Información oral:** Conversaciones, reuniones, etc.

c) **Ubicación de la información:**

- **Sistemas de información:** Almacenamiento en servidores, bases de datos, aplicaciones, etc.
- **Dispositivos de almacenamiento:** Discos duros, memorias USB, etc.
- **Dispositivos electrónicos:** Computadoras, laptops, tablets, smartphones, etc.
- **Medios físicos:** Archivos físicos, documentos en papel, etc.

d) **Criticidad de la información:**

- **Crítica:** Información indispensable para el funcionamiento Y la operación del Concejo Municipal.
- **Importante:** Información que tiene un impacto significativo en las operaciones.
- **Normal:** Información de uso regular, pero no crítica ni importante.

2. **Aplicación de Técnicas de Identificación:**

a) **Entrevistas:**

- **Preparación:** Diseñar una plantilla de entrevista con preguntas sobre los tipos de información que manejan, su ubicación, criticidad y medidas de seguridad.
- **Ejecución:** Entrevistar a personal clave de diferentes áreas del Concejo Municipal.
- **Análisis:** Registrar y analizar la información recolectada para identificar los activos de información.

Realizar entrevistas con personal clave:

- Jefes de área procesos de gestión.
- Encargados de la gestión de la información.
- Personal que maneja información sensible.

Utilizar preguntas como:

- ¿Qué tipo de información maneja en su trabajo?
- ¿En qué formato se encuentra la información?
- ¿Dónde se almacena la información?
- ¿Cuál es el nivel de criticidad de la información?
- ¿Quién tiene acceso a la información?

b) Análisis de documentación:

- **Selección:** Identificar documentos relevantes como políticas, procedimientos, manuales, informes, etc.
- **Revisión:** Buscar información sobre los activos de información, como su ubicación, clasificación y medidas de seguridad.
- **Extracción**: Extraer la información relevante y documentarla en un inventario de activos de información.

Revisar documentos como:

- Políticas de seguridad de la información.
- Procedimientos de gestión de la información.
- Manuales de usuario.
- Contratos con proveedores de servicios.

Identificar:

- Tipos de información que se manejan.
- Ubicación de la información.
- Responsabilidades de acceso y manejo de la información.
- Medidas de seguridad implementadas.

c) **Observación directa:**

- **Planificación:** Definir áreas clave para la observación, como oficinas, archivos, centros de datos, etc.
- **Observación:** Observar el flujo de información y la forma en que se maneja en diferentes áreas.
- **Registro:** Registrar las observaciones y documentar los activos de información identificados.

Observar el flujo de información en diferentes áreas del Concejo Municipal:

- Cómo se recibe, procesa y almacena la información.
- Quién tiene acceso a la información.
- Qué medidas de seguridad se aplican.

d) **Inventario de sistemas de información:**

- **Identificación**: Identificar todos los sistemas de información utilizados en el Concejo Municipal.
- **Análisis:** Evaluar la seguridad de cada sistema de información.
- **Documentación:** Registrar la información sobre los sistemas de información en el inventario de activos de información.

Identificar y documentar los sistemas de información que contienen activos de información:

- Nombre del sistema.
- Función del sistema.
- Tipo de información que almacena.
- Medidas de seguridad implementadas.

e) **Análisis de flujos de información:**

- **Mapeo:** Identificar el origen, destino y uso de la información dentro del Concejo Municipal.
- **Evaluación**: Evaluar los riesgos asociados a los flujos de información.
- **Documentación**: Documentar los flujos de información y los riesgos asociados en el inventario de activos de información.

Identificar el origen, destino y uso de la información dentro del Concejo Municipal:

- Diagramas de flujo de información.
- Matrices de acceso a la información.

3. **Paso a Paso para la Identificación de Activos de Información:**

a) **Definición del equipo de trabajo:**

- Designar un responsable del proceso.
- Seleccionar miembros del equipo con diferentes habilidades y conocimientos.

b) Definición de los criterios de identificación:

- Seleccionar los criterios relevantes para el Concejo Municipal.
- Definir los indicadores para cada criterio.

c) Recolección de información:

- Aplicar las técnicas de identificación: entrevistas, análisis de documentación, observación directa, inventario de sistemas de información y análisis de flujos de información.
- Documentar la información recolectada.

d) Clasificación de activos de información:

- Aplicar los criterios de clasificación para determinar la criticidad de la información.
- Categorizar la información en diferentes niveles (pública, interna, confidencial, reservada, altamente sensible).

e) Documentación y registro: Crear un inventario de activos de información que incluya:

- Descripción del activo.
- Ubicación del activo.
- Propietario del activo.
- Categoría de clasificación.
- Nivel de criticidad.
- Medidas de seguridad aplicables.

f) Revisión y actualización:

- Revisar y actualizar el inventario de activos de información de manera regular.
- Asegurar que la información se mantenga actualizada y precisa.

Herramientas:

- Plantillas de entrevistas.
- Herramientas de análisis de documentación.
- Software de inventario de activos.
- Herramientas de análisis de riesgos.

4. Clasificación de activos de información

a) Categorías de Clasificación:

- **Pública:** Información accesible a cualquier persona sin restricciones.
- **Interna:** Información de uso exclusivo del Concejo Municipal y sus empleados.
- **Confidencial:** Información que no debe ser compartida con personas no autorizadas.
- **Reservada:** Información que solo debe ser compartida con personas que tengan un autorización.

- **Altamente sensible:** Información crítica para el Concejo Municipal que debe ser protegida con las más altas medidas de seguridad.

b) Definición de Criterios de Clasificación:

Impacto en la organización:

- **Alto:** Si la pérdida o fuga de información causa un daño significativo a la reputación, operaciones o finanzas del Concejo Municipal.
- **Medio:** Si la pérdida o fuga de información causa un daño moderado a la reputación, operaciones o finanzas del Concejo Municipal.
- **Bajo:** Si la pérdida o fuga de información causa un daño leve a la reputación, operaciones o finanzas del Concejo Municipal.

Legalidad:

- **Información legal:** Información sujeta a requisitos legales específicos.
- **Información no legal:** Información no sujeta a requisitos legales específicos.

Sensibilidad:

- **Información personal:** Datos personales de los ciudadanos, empleados.
- **Información financiera:** Datos financieros, contables, presupuestarios.
- **Información comercial:** Información confidencial sobre estrategias, planes.
- **Información técnica:** Datos técnicos, diseños, especificaciones.

c) Identificación de Fuentes de Información:

- **Sistemas de información**: Bases de datos, aplicaciones, servidores, etc.
- **Dispositivos de almacenamiento:** Discos duros, memorias USB, CD/DVD, etc.
- **Archivos físicos**: Archivos, carpetas, documentos en papel, etc.
- **Correo electrónico**: Mensajes de correo electrónico y archivos adjuntos.
- **Sitios web:** Páginas web y contenido web.
- **Redes sociales:** Perfiles de redes sociales y publicaciones.

d) Identificación de Clases de Información:

- **Información personal:** Nombres, direcciones, teléfonos, correos electrónicos, datos financieros. etc.
- **Información sensible:** Información confidencial, estratégica o de alto valor para la organización.
- **Información financiera:** Datos financieros, contables, presupuestarios, etc.
- **Información técnica:** Datos técnicos, diseños, especificaciones, etc.
- **Información legal:** Contratos, acuerdos, licencias, etc.

e) Relación de Medidas de Protección con Clases de Información:

- **Información pública:** Medidas básicas de seguridad como control de acceso y antivirus.
- **Información interna:** Medidas de seguridad adicionales como encriptación y control de acceso granular.
- **Información confidencial:** Medidas de seguridad avanzadas como monitoreo de seguridad y análisis de comportamiento de usuarios.

- **Información reservada:** Medidas de seguridad excepcionales como acceso restringido y autorización especial.
- **Información altamente sensible:** Medidas de seguridad extremas como aislamiento de red y almacenamiento en frío.

f) Calificación de la Información:

- **Análisis de riesgos:** Evaluar los riesgos asociados a la pérdida o fuga de información.
- **Determinación del impacto:** Evaluar el impacto potencial en la organización.
- **Asignación de la categoría de clasificación:** Asignar la categoría de clasificación adecuada a la información.

g) Identificación de Medidas de Protección:

- **Medidas de seguridad físicas:** Control de acceso, seguridad perimetral, etc.
- **Medidas de seguridad técnicas:** Encriptación, firewalls, antivirus, etc.
- **Medidas de seguridad administrativas:** Políticas de seguridad, procedimientos, capacitación, etc.

h) Implementación de Controles:

- Implementar las medidas de protección adecuadas para cada categoría de clasificación.
- Monitorear y revisar las medidas de protección de forma regular.
- Actualizar las medidas de protección según sea necesario.

5. Documentación y Registro de Activos de Información:

a) Importancia de la Documentación y Registro:

- Facilita la gestión y protección de la información.
- Permite la identificación y clasificación de los activos de información.
- Asegura la trazabilidad de la información.
- Demuestra el cumplimiento de las normas y regulaciones.

b) Recomendaciones para la Documentación y Registro:

Completitud:

- Documentar todos los activos de información del Concejo Municipal.
- Incluir información completa y precisa sobre cada activo.

Claridad:

- Utilizar un lenguaje claro y conciso.
- Evitar tecnicismos innecesarios.

Actualización:

- Mantener la documentación actualizada en caso de cambios en la información o en las medidas de protección.

Accesibilidad:

- Asegurar que la documentación sea accesible para las personas que la necesitan.

Seguridad:

- Proteger la documentación contra el acceso no autorizado.

c) Contenido de la Documentación:

1) Inventario de activos de información:

- Descripción del activo.
- Ubicación del activo.
- Propietario del activo.
- Categoría de clasificación.
- Nivel de criticidad.
- Medidas de seguridad aplicables.

2) Políticas y procedimientos:

- Políticas de seguridad de la información.
- Procedimientos para la identificación, clasificación, protección y gestión de activos de información.

3) Registros de actividades:

- Registros de acceso a la información.
- Registros de cambios en la información.
- Registros de incidentes de seguridad.

4) Informes:

- Informes sobre el estado de la seguridad de la información.
- Informes sobre el cumplimiento de las normas y regulaciones.

d) Herramientas para la Documentación y Registro:

- Software de inventario de activos.
- Sistemas de gestión documental.
- Plantillas de documento

6. Revisión y actualización:

Establecimiento de un proceso periódico de revisión y actualización del inventario de activos de información:

- Al menos una vez al año.
- En caso de cambios significativos en la organización o en la información que posee.

RECOMENDACIONES

- Involucrar a las partes interesadas en el proceso.
- Capacitar al personal sobre la importancia de la identificación y protección de la información.
- Comunicar el proceso a toda la organización.
- Utilizar herramientas y recursos disponibles para la gestión de la información.

CONCLUSIONES

1. Involucramiento de las Partes Interesadas: La participación activa de todas las partes interesadas, incluyendo la Alta Dirección, el personal de diferentes áreas y los usuarios de la información, es esencial para garantizar que el proceso de identificación de activos de información se adapte a las necesidades y realidades del Concejo Municipal de Yumbo.

2. Capacitación y Sensibilización: La capacitación del personal sobre la importancia de la identificación y protección de la información, así como la sensibilización sobre la seguridad de la información, son fundamentales para crear una cultura organizacional enfocada en la seguridad y protección de los activos de información.

3. Comunicación y Difusión: La comunicación efectiva del proceso de identificación de activos de información a través de diversos canales garantiza que todos los miembros del Concejo Municipal estén informados sobre el proceso y comprendan su importancia en la protección de la información.

4. Utilización de Herramientas y Recursos: La selección y utilización de herramientas y recursos adecuados facilitan el proceso de identificación de activos de información, permitiendo una gestión más eficiente y efectiva de la información en el Concejo Municipal.

5. Revisión y Actualización Periódica: La revisión y actualización periódica del proceso de identificación de activos de información garantiza su relevancia y adaptación a las necesidades cambiantes del Concejo Municipal, asegurando así una gestión continua y efectiva de la información.

6. Implementación de Medidas de Seguridad: La implementación de medidas de seguridad proporcionales al nivel de riesgo de los activos de información identificados es esencial para proteger la información sensible y cumplir con las normativas de privacidad y protección de datos, garantizando la confianza de la ciudadanía en la gestión del Concejo Municipal de Yumbo

REFERENCIA BIBLIOGRAFICA

- Norma ISO/IEC 27001:2013: https://www.iso.org/standard/27001
- Guía para la identificación y clasificación de activos de información: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf