CONCEJO MUNICIPAL DE YUMBO

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÒN 2024 -2027

Sistema Integrado de Gestión - SIG

Proceso Gestión Tecnologías de la Información (GTI)
1-10-2024

Contenido

1. INTRODUCCION

Para el Concejo Municipal de Yumbo, en la necesidad de controlar y administrar la información sensible y de carácter privado. El plan de Tratamiento de Riesgos se busca establecer medidas para mitigar los riesgos presentes en su análisis (perdida de confidencialidad, perdida de integridad y perdida de disponibilidad de los activos de información),

Por tal motivo se toma como referencia el Marco de Seguridad del Modelo de Seguridad y Privacidad de la información –MSPI-, y norma ISO 27005:2011 estándar internacional diseñado para la gestión del riesgo en la seguridad de la información dentro de un sistema de gestión de seguridad de la información. Contiene diferentes procedimientos y directrices, que permiten establecer los riesgos que enfrenta una organización y poder mitigarlos de la mejor manera. Se realiza la identificación, el análisis, la evaluación de los riesgos, las políticas y controles que permiten reaccionar ante una posible materialización del riesgo mediante el plan de tratamiento de riesgos.

Al elaborar la guía se busca la aplicación de controles necesarios para evitar, reducir, compartir, transferir o asumir el riesgo con medidas preventivas o correctivas que deberá generar como resultado minimizar pérdidas, rendimientos y cuidar la seguridad de la información que se genera interna como externamente en la entidad.

2. MARCO REGULATORIO Y NORMATIVO

El Concejo Municipal de Yumbo, como entidad pública, está sujeta a un marco normativo y regulatorio relacionado con la seguridad de la información y a las buenas prácticas en la seguridad de la información definidas por entidades entes regulatorio en la emisión y normalización de metodologías y buenas prácticas a nivel mundial.

A continuación, se tienen las normas, decretos y disposiciones legales que aplican al Concejo municipal de Yumbo en lo establecido del Modelo de Seguridad y Privacidad de la Información (MSPI):

- Ley 1266 de 2008 “Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”

- Ley 1273 de 2009 “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”.

- Decreto 1712 de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.
- Decreto 1078 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.

- Decreto 415 de 2016 “en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones”.

- Ordenanza departamental 430 de 2016 “Política TIC que busca convertir al departamento en un territorio inteligente e innovador”.

- Decreto 1008 de 2018 “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones”.

- Norma Técnica Colombiana NTC-ISO/IEC 27001:2013 “Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos”

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Identificar y minimizar los riesgos informáticos mediante el diagnóstico y valoración del estado y situación actual en materia de riesgos

3.2. OBJETIVOS ESPECÍFICOS

- Identificar y ubicar los activos de la entidad a través del levantamiento de inventarios.

- Clasificar y escalar los activos de información.

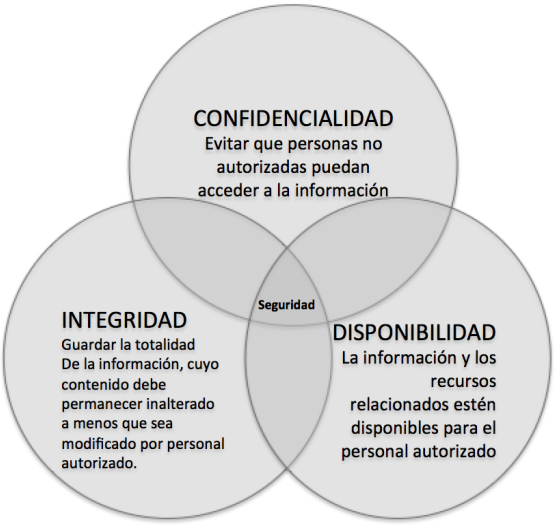
- Establecer los controles y políticas de la seguridad de la información que garantice la confidencialidad integridad y disponibilidad de la información.

- Elaborar mapa de riesgos informáticos internos y externos del concejo Municipal de Yumbo.

4. MARCO TEORICO

4.1. SEGURIDAD INFORMÁTICA

La gestión de la información se fundamenta en tres pilares fundamentales que son, confidencialidad, integridad y disponibilidad. La seguridad de la información aplica barreras y procedimientos que resguardan el acceso a los datos y sólo permite acceder a las personas autorizadas para realizarlo.

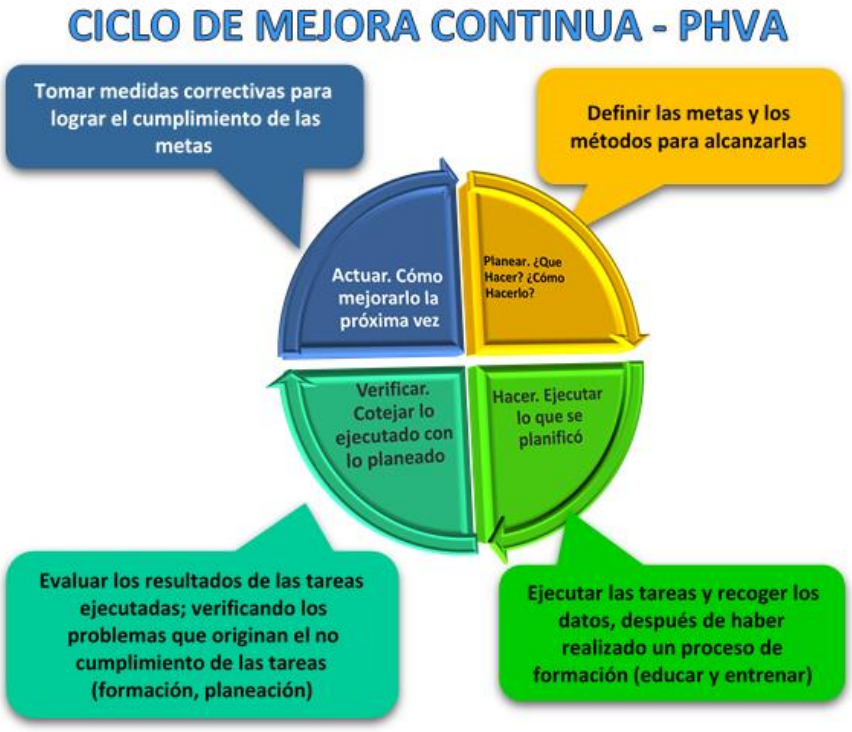


A continuación, se referencia las familias de las normas iso 2700

Cuadro. Familia de normas 27000	
Norma ISO/IEC	**Título**
ISO 27000	Gestión de la Seguridad de la Información: Fundamentos y vocabulario.
ISO 27001	Especificaciones para un **SGSI**.
ISO 27002	Código de Buenas Prácticas.
ISO 27003	Guía de Implantación de un **SGSI**.
ISO 27004	Sistema de Métricas e Indicadores.
ISO 27005	Guía de Análisis y Gestión de Riesgos.
ISO 27006	Especificaciones para Organismos Certificadores de **SGSI**.
ISO 27007	Guía para auditar un **SGSI**.

5. MODELO PHVA PARA EL SGSI

Un SGSI establece una serie de procesos y lineamientos que se deben seguir mediante la estandarización de la norma ISO 27001 para asegurar los activos de información como Bases de datos, oficios, actas etc. de una organización. El objetivo es mantener siempre la confidencialidad, integridad y disponibilidad de la información.



6. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO

- Definir alcance
- Identificación de activos
- identificación de riesgos identificación de Amenazas
- Identificación de vulnerabilidades
- Identificación de controles
- Evaluación de Riesgos
- Valoración de Control

7. DEFINIR EL ALCANCE

La gestión de riesgos de Seguridad y Privacidad de la información, da a la entidad tener buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que afectan el poder lograr los objetivos y poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información.

8. IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACION

Los activos de la entidad es la información la cual genera un valor, representada en forma física como documentos impresos o escritos a mano, en medios electrónicos almacenados en Discos Duros Externos,

Memorias USB o en forma digital, en los equipos de cómputo o en la Nube. Información requiere ser analizada para la aplicación de controles para su protección.

9. CLASIFICACIÓN DEL ACTIVO DE INFORMACIÓN:

Nivel del Criterio

Confidencialidad / Se evalúa con los siguientes valores

Nivel	Descripción Criterio de Confidencialidad	Denominación
0	Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado, contratista o tercero del concejo municipal de Yumbo	Publico
1	Información que puede ser conocida y utilizada por todos los empleados, contratistas y terceros la entidad y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas	Reservada – Uso Interno
2	Información que sólo puede ser conocida y utilizada por un grupo de empleados, contratistas y terceros que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas.	Reservada - Confidencial
3	Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados y contratistas asociados a los procesos misionales cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo o a terceros.	Reservada Secreta

Integridad / / Se evalúa con los siguientes valores

Nivel	Descripción Criterio de Integridad
0	Información cuya modificación no autorizada puede repararse fácilmente, o no afecta las operaciones del concejo municipal de yumbo.
1	Información cuya modificación no autorizada puede repararse, aunque podría ocasionar pérdidas leves para del concejo municipal de yumbo
2	Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para del concejo municipal de yumbo
3	Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves al del concejo municipal de yumbo.

Disponibilidad/ Se evalúa con los siguientes valores

Nivel	Descripción Criterio de Disponibilidad
0	Información cuya inaccesibilidad no afecta la operatoria del concejo municipal de yumbo.
1	Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas para el concejo municipal de yumbo.

2	Información cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas al concejo municipal de yumbo
3	Información cuya inaccesibilidad permanente durante una hora podría ocasionar pérdidas significativas del concejo municipal de yumbo

10. IDENTIFICACIÓN DEL RIESGO

El objetivo de la identificación de riesgos es conocer lo incidentes o eventos que pueden causar pérdidas o alteración en el funcionamiento del Concejo Municipal de Yumbo y pueden afectar la confidencialidad, integridad y disponibilidad de la información.

La identificación de los riegos se realiza con observación directa, ingeniería social y con el análisis a los equipos de seguridad perimetral. Por confidencialidad del Concejo Municipal de Yumbo se presenta la identificación de riesgos general.

RIESGOS INFORMÁTICOS	CAUSAS	EFECTO
Perdida Robo o Fuga de Información	● Fallas en el proceso de copia de respaldo o de restauración de la información, o pérdida de la misma. ● Fallas en los análisis y socialización de las vulnerabilidades de la infraestructura de IT ● No contar con acuerdos de confidencialidad con los Empleados, contratistas y terceros ● Falta controles de autorización para la extracción de información generadas por requerimientos. ● Ingreso a la red y acceso a los activos de TI por parte de máquinas ajenas a la entidad ● Habilitación de puertos USB en modo lectura y escritura para medios de almacenamiento ● Ataques cibernéticos internos o externos ● Empleados no capacitados en los temas de riesgos informáticos. ● Desconocimiento del riesgo. ● Prestar los equipos informáticos a personal no autorizado. ● No cerrar sesión cuando se desplaza del puesto. ● Acceso no autorizado a las dependencias. ● Conectar dispositivos externos a los equipos. ● Falta de implementación de la política escritorio limpio	● Afectación parcial o total de la continuidad de las operaciones de los servicios del Incumplimiento normativo ● Vulneración de los sistemas de seguridad ● Operando actualmente Mala imagen, multas, sanciones y pérdidas económicas ● Generación de consultas, funcionalidades o reportes con información sensible de los clientes ● Pérdida o fuga de información

Daño en los equipos tecnológicos	• Manejo inadecuado de los equipos • Falta de mantenimiento o mala conexión de los mismos en las instalaciones eléctricas • Derrame de líquido • Falta de ambiente adecuado para los equipos • Falta Educación a los usuarios en el manejo de los equipos de computo	• Perdida de información • Perdidas de los quipos informáticos • Indisponibilidad del Servicio • Traumatismos en los procesos
Perdida de conectividad	• Daño externo del ISP (Internet service provider) • Ataque DDoS o DOS (denegación de servicios distribuidos o Denegación de servicios)	
Ataques Informáticos	• Estimulo o Reto personal • Rebelión • Ánimo de lucro • Espionaje	• Daño en los equipos tecnológicos • Incidente en la confidencialidad, integridad y disponibilidad de la información • Denegación de servicios • Secuestro de la información • Divulgación ilegal de la información • Suplantación de identidad • Destrucción de la información • Soborno de la información

11. IDENTIFICACIÓN DE LAS AMENAZAS

Una amenaza se identifica como un evento, persona, situación o fenómeno que pueda causar daño a los activos de la organización. Las amenazas pueden ser de origen Humano o Ambientales.

AMENAZA	TIPO
Polvo, Corrosión	Evento Naturales
Inundación	Evento Naturales
Incendios	Evento Naturales
Fenómenos Sísmicos	Evento Naturales
Fenómenos Térmicos	Evento Naturales y Daños físicos
Perdida en el suministro de energía	Daño Físico
Espionaje remoto	Acciones no autorizadas
Ingeniería Social	Acciones no autorizadas
Intrusión	Acciones no autorizadas

Accesos forzados al sistema	Acciones no autorizadas
Manipulación del Hardware	Acciones no autorizadas
Manipulación con Software	Acciones no autorizadas
Fallas del equipo	Fallas técnicas
Saturación del sistema de información	Fallas técnicas

Tabla: Identificación de Amenazas

11.1. IDENTIFICACIÓN DE LAS VULNERABILIDADES

Las vulnerabilidades son las Fallas o debilidades en un sistema, que puede ser explotada por quien la conozca. Cuando la amenaza encuentra la vulnerabilidad es cuando se crea el riesgo. Por eso es necesario conocer la lista de amenazas y el inventario de activos de información.

VULNERABILIDADES	DESCRIPCIÓN
Fácil acceso a las dependencias o Secretarías.	No existe un control para el acceso de las personas no autorizadas a las secretarías.
Falta de dispositivos de seguridad biométrica para acceso a las secretarias de alto riesgo.	El dispositivo de seguridad biométrica reduce el riesgo de robo de información o equipos electrónicos por fácil acceso.
Falta de Aplicación de la Política de escritorio Limpio.	La política de escritorio limpio, es implementada para que los funcionarios no dejen expuestos: documentos, equipos electrónicos u objetos de valor, sobre los escritorios, que pueden ser robados fácilmente.
Falta de máquina trituradora de papel	La máquina trituradora de papel, evita que las personas arrojen documentos importantes con información personal a la basura, que puedan ser usados para crear perfiles de ataque.
Falta de Capacitación de los funcionarios en temas de seguridad Informática.	El eslabón más débil en términos de seguridad informática en una organización son los funcionarios, dado que no tienen conocimiento sobre las amenazas y riesgos que enfrentan y como poder mitigarlos.
Falta de equipos electrónicos para copias de respaldo.	El no contar con un HDD externo, impide a los funcionarios realizar copias de respaldo o Back ups
Falta de equipos institucionales.	El no contar con suficientes equipos institucionales, lleva a los funcionarios a traer equipo personal que pueden afectar el funcionamiento de la red o infectarla. Adicionalmente promueve el compartir cuentas de usuarios y calves que pueden afectar al prestador
Equipo clon.	Los equipos clones, no cuentan con software legal que pueden infectar la red o traer problemas legales

Tabla: Identificación de Vulnerabilidades

ANÁLISIS DE RIESGOS					
RIESGO	CALIFICACIÓN		TIPO DE IMPACTO	EVALUACIÓN	MEDIDAS DE RESPUESTAS
	PROBABILIDAD	IMPACTO		ZONA DE RIESGO	
Perdida, Robo o fuga de información	3	5	Disponibilidad integridad y confidencialidad de la información	Extrema	Reducir el riesgo, Evitar o Transferir

12. RECOMENDACIONES

- Concientizar constantemente a los secretarios, jefes y funcionarios del Concejo Municipal de Yumbo, sobre la importancia de cumplir con la política de seguridad de la información.
- Aplicar correctivos o Sanciones a los funcionarios que no cumplan con la política de seguridad de la información establecida.
- Mantener actualizada la política de seguridad de la información
- Realizar Auditorías periódicas de Seguridad Informática.
- Capacitar frecuentemente a los funcionarios de concejo Municipal de Yumbo en temas de seguridad informática.
- Establecer un responsable de la seguridad informática en cada secretaria o dependencia.

13. GLOSARIO

- **Seguridad informática:** Se ocupa de la implementación técnica y de la operación para la protección de la información.
- **Seguridad de la información:** Se Ocupa de evaluar el riesgo y las amenazas, traza el plan de acción y esquemas normativos. Es la línea estratégica de las Seguridad.
- **Amenazas:** Cualquier evento, persona, situación o fenómeno que pueda causar daño.
- **Vulnerabilidades:** Falla o debilidad en un sistema que puede ser explotada por quien la conozca.
- **Riesgo:** Probabilidad de ocurrencia de una amenaza.
- **Controles:** Conjunto de mecanismos que regulan el funcionamiento de un sistema.
- **ISO:** Organización Internacional de Normalización es una organización para la creación de estándares internacionales.
- **Activo:** Bienes, recursos o derechos que tenga valor para una organización.

- **Activo de Información:** Toda la información que maneja con la que cuenta una organización para un correcto funcionamiento.
- **Análisis de brechas:** es una herramienta de análisis para comparar el estado y desempeño real de una organización, estado o situación en un momento dado.
- **Análisis de Riesgo:** Método empleado para evaluar los riesgos informáticos y obtener respuesta de peligro.
- **Gestión del Riesgo Informáticos:** Actividades empleadas para mitigar los riesgos informáticos.
- **Incidente de seguridad informática:** daño que puede comprometer las operaciones de la alcaldía municipal.
- **Evento:** Acción que puedo haber causado daño, pero fue controlado**.**
- **Información:** Conjunto de datos que tienen un significado.
- **Probabilidad:** Posibilidad de que una amenaza se materialice
- **Impacto:** Daño que provoca la materialización de una amenaza.
- **SGSI:** Sistema de Gestión de seguridad de la Información
- **MSPI:** Modelo de seguridad y privacidad de la información
- **PHVA:** Planear, hacer, verificar, actuar

14. CONTROL DE CAMBIOS

El concejo municipal de yumbo establece como única documentación vigente la ubicada en el sistema integrado de gestión - SIG en el drive establecido por la corporación, la cual entra en vigencia a partir de su aprobación, toda copia de este se considera COPIA NO CONTROLADA.
Los documentos obsoletos se les da de baja del Sistema Integrado de Gestión – SIG activo.

Versión	Fecha edición (dd/mm/aa)	Naturaleza del cambio
1	30/01/2024	Elaboración del Plan (Versión 1) 2024.
2	01/10/2024	Actualización del mapa de procesos de la corporación, ajuste del proceso de gestión de bienes y servicios, creando de manera independiente el nuevo proceso gestión tecnologías de la información, actualización del formato de caracterizaciones de procesos, estructuración del nuevo sistema integrado de gestión y actualización de la codificación para normalizar procesos, procedimientos y documentos relacionados.

15. RUTA DE APROBACION

Versión 2					
Elaboró o actualizó		**Revisión metodológica**		**Aprobó**	
Nombre	Diego Fernando Amaya M.	Nombre	Ana L. Lenis Zuluaga	Nombre	Uriel Urbano Urbano
Cargo	Profesional apoyo a la gestión - Proceso GTI (contratista)	Cargo	Auxiliar Administrativo	Cargo	Secretario General