
**PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD**

**Y PRIVACIDAD DE LA INFORMACION**

**2020 - 2023**

**CONCEJO MUNICIPAL DE YUMBO**

## INTRODUCCION

Para el Concejo Municipal de Yumbo, al realizar funciones del Control Político a la administración Municipal, entes descentralizados, estudio y aprobación de proyectos de acuerdo se genera la necesidad de controlar y administrar la información sensible y de carácter privado, convirtiendo la seguridad y privacidad de la información se convierten en una prioridad y a través de procesos que permita minimizar y detectar alteraciones, mal uso, pérdida de la información que se general al interior de la entidad.

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.

## 1. OBJETIVOS

### 1.1 OBJETIVO GENERAL

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

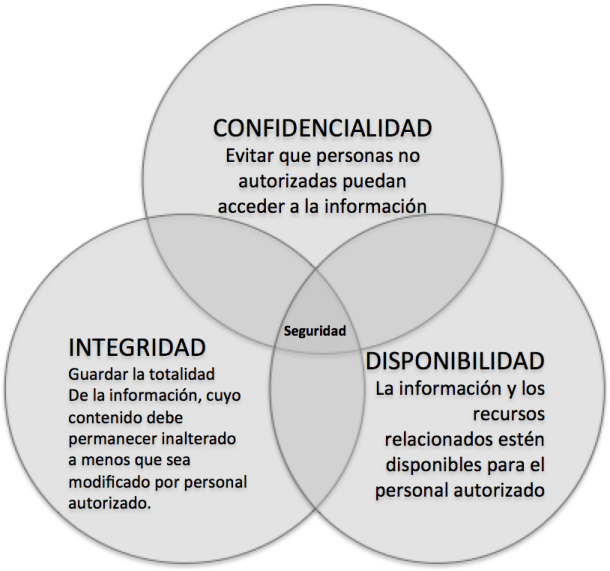
### 1.2 OBJETIVOS ESPECÍFICOS

- 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.

## 2. MARCO TEORICO

### 2.1 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.




**2.2 NORMA ISO 27001**

La norma ISO 27001 es un estándar internacional que describe cómo implementar el Sistema de gestión de seguridad de la información de una empresa. Investiga como salvaguardar la información mediante una serie de estándares, lineamientos y procesos que facilitan la identificación de los riesgos.

**2.3 NORMA ISO 27005**

La norma ISO 27005 es un soporte a la norma (ISO 27001) la cual proporciona directrices para la gestión de riesgos de seguridad de la información, es aplicable a todos los tipos de organización y no proporciona ni recomienda una metodología específica.

ISO 27001. ORIGEN E HISTORIA

1901 – Nacen en Inglaterra las Normas “BS”: La British Stand Ards Institución pública normas con el prefijo “BS” con carácter internacional.

1995- Se escribe la norma BS 7799-1:1995 por el Departamento de Comercio e Industria del Reino Unido (DTI), Mejores prácticas para la gestión de la seguridad de la información.

1998 –Se hace una revisión de la anterior norma BS 7799-2:1999 que establecía los requisitos para implantar un Sistema de Gestión de Seguridad de la Información certificable.
2000 - La Organización Internacional para la Estandarización (ISO) tomó la norma británica BS 7799-1 que dio lugar a la llamada ISO 17799, sin experimentar grandes cambios dando como resultado la norma

ISO/IEC 17799:2000:

2005 – ISO/IEC 27001:2005 e ISO/IEC17799:2005: Aparece el estándar ISO 27001.

Como norma internacional certificable y se revisa la ISO 17799 dando lugar a la ISO 27001:2005.

2006 - BS 7799-3:2006 proporciona una guía para soportar los requisitos establecidos por ISO/IEC 27001:2005 con respecto a todos los aspectos que debe cubrir el ciclo de análisis y gestión del riesgo en la construcción de un sistema de gestión de la seguridad de la información (SGSI).

2007 –Se renombra la norma ISO 17799: y pasa a ser la ISO 27002:2005 2007 – Se la publica nueva versión de la norma ISO/IEC 27001:2007:

2008 – nace la guía para la Implantación (bajo desarrollo) ISO 27003:2008.[2] 2008 -ISO 27004:2008 Métricas e Indicadores (bajo desarrollo).
2008 –se crea la norma ISO 27005:2008 para la Gestión de Riesgos (BS 7799-3:2006)
2009 – Se publica un documento adicional de modificaciones llamado ISO 27001:2007/1M:2009.
2011 – ISO 27005:2011: Se publica la nueva versión.

Este año 2013 se ha publicado ya la nueva versión de la ISO 27001 que trae cambios significativos en su estructura, evaluación y tratamiento de los riesgos.

**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**. |

## 2.4 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.


## 2.5 METODOLOGÍA MAGERIT

Esta norma establece los principios para el uso eficaz, eficiente y aceptable de las tecnologías de la información. Garantizando que sus organizaciones siguen estos principios ayudará a los directores a equilibrar riesgos y oportunidades derivados del uso de las TI Esta metodología, guía paso a paso cómo llevar a cabo el análisis de riesgos.

Magerit persigue los siguientes objetivos: Directos:

1. concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos

2. ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)

3. ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos:

4. preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso También se ha buscado la uniformidad de los informes que recogen los hallazgos y las conclusiones de las actividades de análisis y gestión de riesgos:

**Modelo de valor** Definición del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos.

**Mapa de riesgos** Relación de las amenazas a que están expuestos los activos.

**Notificación de uso** Para un conjunto de protecciones, se indica sin son de aplicación en el sistema de información bajo estudio o si, por el contrario, carecen de sentido.

**Evaluación de protección** Evaluación de la eficacia de las protecciones existentes en relación al riesgo que afrontan.

**Estado de riesgo** definir los activos por su riesgo residual; es decir, por lo que puede pasar tomando en consideración las protecciones desplegadas.

**Informe de insuficiencias** Ausencia o debilidad de las protecciones que aparecen como oportunas para reducir los riesgos sobre el sistema. Es decir, recoge las vulnerabilidades del sistema, entendidas como puntos débilmente protegidos por los que las amenazas podrían materializarse.

**Cumplimiento de normativa** Satisfacción de unos requisitos. Declaración de que se ajusta y es conforme a la normativa correspondiente.

**Plan de seguridad** Conjunto de proyectos de seguridad que permiten materializar las decisiones de tratamiento de riesgos.

La segunda parte es el inventario activo de información que puede utilizar la entidad para enfocar el análisis de riesgo**,** las características que deben tenerse en cuenta para valorar los activos identificados y además un listado con las amenazas y controles que deben tenerse en cuenta.

Por último, son las técnicas que Contiene ejemplos de análisis con tablas, algoritmos, árboles de ataque, análisis de costo beneficio, técnicas gráficas y buenas prácticas para llevar adelante sesiones de trabajo para el análisis de los riesgos.

### 2.6 OBJETIVOS DE LA METODOLOGÍA MAGERIT

- Identificar y evaluar los riesgos que enfrentan la entidad y como mitigarlos. Minimizando los riesgos para evitar se materialicen.

## 3. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO

1. **Definir alcance**
2. **Identificación de activos**
3. **Identificación de riesgos**
4. **Identificación de Amenazas**
5. **Identificación de vulnerabilidades**
6. **Identificación de controles**
7. **Evaluación de Riesgos**
8. **Valoración de Control**

**3.1 . DEFINIR EL ALCLANCE**

Establecer los objetivos, argumentar del procedimiento que se llevaran a cabo, los funcionarios implicados y el contexto de seguridad informática con el que cuenta El concejo Municipal de Yumbo.

**4.1 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.

Teniendo en cuenta estos aspectos se diseñó un formato de inventario de activos de información que contiene los siguientes campos:

**Nombre del líder del proceso** / Nombre del funcionario

**Norma, función o proceso /** Función que realiza el funcionario

**TIPO DOCUMENTAL:**

**Nombre del activo de información** / Nombre correspondiente al activo de información como Base de Datos, Actas, informes, Sistemas de información etc.
**Descripción del activo de información**

**TIPOLOGÍA:**

**Software** / el activo de información se encuentra en forma digital

**Hardware**/ el activo de información se encuentra en física.

**Servicios** / el activo de información se emplea como servicio a terceros

**Documentos físicos**

**TIPO DE SOPORTE** (medio de conservación y/o Soporte:

**Análogo** / Copia adicional del documento en forma física

**Digital** / Copia de seguridad en otro equipo, en correo electrónico o en la Nube.

**Electrónico** / Copia de seguridad en equipo electrónico como Disco Duro Externo USB.

**Presentación de la información (formato o extensión)** / en que aplicación se realiza el activo de información Ej.: .PDF, DOC, XLS etc.

**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 |

**Estado de la información /** Si la información es variable o constante

**Localización del documento o del activo de información** / Numero de Equipo o Archivador

**Publicada en (Link Web Page).** Área/Dependencia Observaciones.

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

| | | |
|---|---|---|
| **Daño en los equipos tecnológicos** | -Manejo inadecuado de los equipos<br>- Falta de mantenimiento o mala conexión de los mismos en las instalaciones eléctricas<br>Falta de equiposde potenciación<br>- Fallas por defectos de fabrica<br><br>- Derrame de líquido<br>- Falta de ambiente adecuado para los equipos<br>Falta Educación a los usuarios en el manejo de los equipos de computo | -Perdida de información<br>-Perdidas de los quipos informáticos<br>- Indisponibilidad del Servicio<br>- Traumatismos en los procesos |
| **Dumpsterdiving (buceo en la basura)** | -Desconocimiento del riesgo.<br>-Falta de capacitación y conciencia. | -Creación de perfil de ataque<br>-Captura de información privilegiada |
| **Perdida de conectividad** | -Daño externo del ISP (Internet service provider)<br><br>-Ataque DDoS o DOS (denegación de servicios distribuidos o Denegación de servicios ) | |
| **Ataques Informáticos** | -Estimulo o Reto personal<br><br>-Rebelión<br><br>-Ánimo de lucro<br><br>-Espionaje | -Daño en los equipos tecnológicos<br>-incidente en la confidencialidad, integridad y disponibilidad de la información<br>-Denegación de servicios<br><br>-Secuestro de la información<br>-Divulgación ilegal de la información<br><br>-Suplantación de identidad<br><br>-Destrucción de la información<br><br>-Soborno de la información |

### 4.3 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 forzado 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 6: Identificación de Amenazas**

### 4.4 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** | La política de escritorio limpio, es implementada para que los funcionarios no dejen expuestos: |

| | |
|---|---|
| **escritorio Limpio.** | 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 clon, no cuentan con software legal que pueden infectar la red o traer problemas legales |

**Tabla 7: Identificación de Vulnerabilidades**

### 4.5 IDENTIFICACIÓN DE CONTROLES EXISTENTES

La identificación de los controles existentes permite realizar la evaluación de riesgos. Lo controles garantizan que al momento de la materialización de un riesgo se reduzcan o mitiguen los riesgos informáticos y la organización funcionen correctamente. Pero se debe tener en cuenta que nunca se va a estar 100% seguros.

Dada la importancia de los controles, con que cuenta el Concejo Municipal de Yumbo no es adecuado exponerlos en el proyecto, por lo que se pueden crear perfiles de ataque.

### 4.6 EVALUACIÓN DE RIESGO

La evaluación de riesgo se realiza con enfrentamiento entre la probabilidad de ocurrencia y el impacto que genera el riesgo en los activos de información, dado por la matriz de calificación, evaluación y respuestas a los riesgos.

El Concejo Municipal de Yumbo cuenta con Sistema de Gestión Documental que realiza el análisis de riesgos con la información recolectada en el análisis de riesgos. La metodología que se emplea para la evaluación de riesgos es margerit.

| TABLA DE PROBABILIAD | | | |
|---|---|---|---|
| **NIVEL** | **DESCRIPTOR** | **DESCRIPCIÓN** | **FRECUENCIA** |
| 1 | Raro | El evento puede ocurrir solo en circunstancias excepcionales | No se ha presentado en los últimos 5 años |
| 2 | improbable | El evento puede ocurrir en algún momento | Al menos una vez en los últimos 5 años |
| 3 | posible | El evento podría ocurrir en algún momento | Al menos una vez en los últimos 2 años |
| 4 | probable | El evento probablemente ocurra en la mayoría de las circunstancias | Al menos una vez en el último año |
| 5 | Casi Seguro | Se espera que el evento ocurra en la mayoría de las circunstancias | Más de una vez al año |

**Tabla 8: Probabilidad de riesgo**

| TABLA DE IMPACTO | | |
|---|---|---|
| **NIVEL** | **DESCRIPTOR** | **DESCRIPCIÓN** |
| 1 | Insignificante | Si el hecho llegara a presentarse, tendría consecuencias o efecto mínimos sobre la entidad |
| 2 | Menor | Si el hecho llegara a presentarse, tendría bajo impacto o efecto mínimos sobre la entidad |
| 3 | Moderado | Si el hecho llegara a presentarse, tendría medianas consecuencias o efecto sobre la entidad |
| 4 | Mayor | Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad |
| 5 | Catastrófico | si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad |

**Tabla 9: Impacto del riesgo**

| PROBABILIDAD | IMPACTO | | | | |
|---|---|---|---|---|---|
| | Insignificante(1) | Menor(2) | Moderado(3) | Mayor(4) | Catastrófico (5) |
| Raro(1) | B | B | M | A | A |
| improbable(2) | B | B | M | A | E |
| posible(3) | B | M | A | E | E |
| probable(4) | M | A | A | E | E |
| Casi Seguro (5) | A | A | E | E | E |
| | | | | | |
| B: Zona de Riesgo Baja: Asumir el riesgo | | | | | |
| M: Zona de Riesgo Moderada: Asumir el riesgo, Reducir el riesgo | | | | | |
| A: Zona de Riesgo Alta: Reducir, Evitar, Compartir o Transferir | | | | | |
| E: Zona de Riesgo extrema: Reducir el riesgo, evitar compartir o transferir | | | | | |

**10: Matriz de calificación, evaluación y respuestas a los riesgos.**

| 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 |
| | | | | | |

**Tabla 11: Ejemplo de análisis de riesgo**

| PROBABILIDAD | IMPACTO | | | | |
|---|---|---|---|---|---|
| | Insignificante(1) | Menor(2) | Moderado(3) | Mayor(4) | Catastrófico (5) |
| Raro(1) | B | B | M | A | A |
| improbable(2) | B | B | M | A | E |
| posible(3) | B | M | A | E | E |
| probable(4) | M | A | A | E | E |
| Casi Seguro (5) | A | A | E | E | E |

B: Zona de Riesgo Baja: Asumir el riesgo

M: Zona de Riesgo Moderada: Asumir el riesgo, Reducir el riesgo

A: Zona de Riesgo Alta: Reducir, Evitar, Compartir o Transferir

E: Zona de Riesgo extrema: Reducir el riesgo, evitar compartir o transferir

Luego de identificar el riesgo se le aplica la causa y efecto que provoca.

El segundo paso para el proceso de gestión de riesgos informáticos es hacer el análisis. Para esto se emplea la matriz vista anteriormente, que relaciona le impacto con la probabilidad de ocurrencia, dando como resultado el nivel de riesgo

### 4.7 VALORACION DE CONTROLES

La valoración de controles, evalúa los controles existentes en la organización y la efectividad para mitigar la exposición al riesgo.

Se emplea una tabla para la valoración de control donde se establecen 2 parámetros con 5 criterios, dependiendo del puntaje y si el control se ejecuta con la probabilidad, con el impacto o ambos, se genera un desplazamiento del valor del riesgo

.

| VALORACIÓN DE CONTROL | | |
|---|---|---|
| **PARAMETROS** | **CRITERIOS** | **PUNTAJE** |
| **HERRAMIENTAS PARA EJERCER EL CONTROL** | Posee una herramienta para ejercer el control. | 15 |
| | Existen manuales, Instructivos o procedimientos o procedimientos | 15 |
| | En el tiempo que lleva la herramienta ha | 30 |
| **SEGUIMIENTO AL CONTROL** | Están definidos los responsables de la ejecución demostrado ser efectiva | 15 |
| | La frecuencia de ejecución del control y seguimiento es adecuada. | 25 |
| **TOTAL** | | 100 |

| | |
|---|---|
| **RANGOS DE** | **DEPENDIENDO SI EL CONTROL AFECTA PROBABILIDAD O IMPACTO, DESPLAZA EN LA MATRIZ DE CALIFICACION,EVALUACION Y RESPUESTA A LOS RIESGOS** |

| CALIFICACION DE LOS CONTROLES | CUADRANTES A DISTRIBUIR EN LA PROBABILIDAD | CUADRANTES A DISTRIBUIR EN EL IMPACTO |
|---|---|---|
| ENTRE 0-50 | 0 | 0 |
| ENTRE 51-75 | 1 | 1 |
| ENTRE 76-100 | 2 | 2 |

**Tabla 14: Evaluación de los controles**

| ANÁLISIS DE RIESGOS | | | | | | | |
|---|---|---|---|---|---|---|---|
| RIESGO | CALIFICACIÓN | | CONTROL | TIPO DE CONTROL | PUNTAJE Herramienta para ejercer el control | PUNTAJE Seguimiento al Control | PUNTAJE FINAL |
| | PROB | IMPACTO | | | | | |
| Perdida, Robo o fuga de información | 3 | 5 | Reservado | PROBABILIDAD E IMPACTO | 60 | 40 | 100 |

**Tabla 15: Ejemplo de análisis de riesgos con evaluación de controles**

De acuerdo con el análisis anterior, el riesgo reduce dos puntos en Probabilidad, y dos en impacto, de acuerdo a las calificaciones de los controles, como se muestra en la siguiente ilustración:

| PROBABILIDAD | IMPACTO | | | | |
|---|---|---|---|---|---|
| | Insignificante(1) | Menor(2) | Moderado(3) | Mayor(4) | Catastrófico (5) |
| Raro(1) | B | B | M | A | A |
| improbable(2) | B | B | M | A | E |
| posible(3) | B | M | A | E | E |
| probable(4) | M | A | A | E | E |
| Casi Seguro (5) | A | A | E | E | E |
| | | | | | |
| B: Zona de Riesgo Baja: Asumir el riesgo | | | | | |
| M: Zona de Riesgo Moderada: Asumir el riesgo, Reducir el riesgo | | | | | |
| A: Zona de Riesgo Alta: Reducir, Evitar, Compartir o transferir | | | | | |
| E: Zona de Riesgo extrema: Reducir el riesgo, evitar compartir o transferir | | | | | |

**Tabla 16: Matriz probabilidad impacto**

El Sistema de Gestión Documental establece los campos para la valoración de los controles, Se realiza la valoración de controles y se reevalúa el riesgo y se agregan las políticas y actividades a realizar.

**Ilustración 13: Valoración de Controles**

Ya con toda la información se crea el mapa de riesgos informáticos.

Dada la importancia y privacidad de la información suministrada por el Concejo Municipal de Yumbo, se presenta una muestra del mapa de riesgos.

### 4.8 SOCIALIZACIÓN DE LA IMPORTANCIA DE LA GESTIÓN DE RIESGOS INFORMÁTICOS Y SEGURIDAD DE LA INFORMACIÓN

Debido a que los funcionarios de una entidad, son el eslabón más débil de la seguridad informática, se realiza una presentación sobre seguridad informática y seguridad de la información que permite a los funcionarios, conocer la importancia de la gestión de riesgos informáticos y conocer los riesgos que enfrentan para poder mitigarlos.

## 4. RESULTADOS Y DISCUSIÓN

La gestión de Riesgos informáticos permitió conocer las vulnerabilidades, las amenazas y los riesgos informáticos del Concejo Municipal de Yumbo. Este Análisis permite a la entidad fortalecer la estructura de la seguridad de la información y prepararse para cualquier evento o incidente.

### 5.1 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 la Alcaldía en temas de seguridad informática.
- Establecer un responsable de la seguridad informática en cada secretaria o dependencia.
- Reactivar el comité de seguridad informática.

**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

| | | |
|---|---|---|
| Elaborado por:<br>Julio Potosi Guampe | Cargo:<br>Contratista | Firma: |
| Revisador por:<br>Martha Cecilia Burbano Velásquez | Cargo:<br>Auxiliar Administrativo | Firma |
| Aprobado por:<br>Guillermina Becerra Caicedo | Cargo:<br>Secretaria General | Firma |