METODOLOGÍA PARA LA EVALUACIÓN DE RIESGOS EN LA ADMINISTRACIÓN PÚBLICA MUNICIPAL DE TUMBISCATÍO, MICHOACÁN, EN MATERIA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES.

CONTENIDO

INTRODUCCIÓN.

Hoy en día, seguridad de la información está constantemente en las noticias con el robo de identidad, las infracciones en las empresas los registros financieros y las amenazas de terrorismo cibernético. Un sistema de gestión de seguridad de la información **(SGSI)** es un enfoque sistemático para la gestión de la información confidencial de la empresa para que siga siendo seguro. Abarca las personas, procesos y sistemas de TIC (ISO N. , s.f.).

Cada día dependemos y empleamos más a menudo las denominas TIC´s para realizar actividades fundamentales tanto en las empresas privadas como en las públicas. No es la excepción en la Administración Pública del Municipio de Tumbiscatío en donde la tecnología a pesar de ser limitada se emplea en casi todos los procesos administrativos, de ahí que surge la necesidad de establecer una metodología para el análisis de riesgos de Tecnologías de la información y comunicación, cuyo fin es minimizar y mitigar el posible impacto en caso de materialización de los riesgos previamente identificados y valorados. Tomar acciones preventivas o en su caso correctivas.

A continuación, se propone una metodología simplificada pero eficaz aplicable a la Administración Pública Municipal en materia de "Gestión de riesgos en Tecnología de la Información y la Comunicación", basada en algunas de las normas ISO sobre la administración de riesgos, como la norma ISO 31000:2018 Directrices Gestión del riesgo, ISO 27001 Gestión de la seguridad de la información, ISO 27002 Buenas prácticas para gestión de la seguridad de la información, entre otras más consultadas.

CONCEPTOS CLAVE.

Riesgo.- Efecto de la incertidumbre sobre los objetivos (ISO 3. , 2018).

Con frecuencia, el riesgo se expresa en términos de fuentes de riesgo, eventos potenciales, sus consecuencias y sus probabilidades.

El hecho de que un evento ocurra dentro de la Administración Pública Municipal de Tumbiscatío, que pueda truncar el cumplimento de los objetivos en cuanto a tecnologías de la información y la comunicación se refiere, puede ser de carácter interno o externo, su impacto puede variar en función de las probabilidades de ocurrencia y potencialidad de daño.

Gestión de Riesgo.- La norma ISO 31000:2018 define el riesgo como "las actividades coordinadas para dirigir y controlar la organización con relación al riesgo".

Uno de los objetivos principales en la Gestión del Riesgo es el establecer una metodología funcional apropiada a las necesidades del ente. Además de la implementación de un plan estratégico para la detección y mitigación oportuna de los riesgos en los que puede incurrir la empresa.

Valoración del riesgo.- Proceso en que se identifican las amenazas a los activos, se evalúan las vulnerabilidades y probabilidades de ocurrencia, y se estima el impacto potencial.

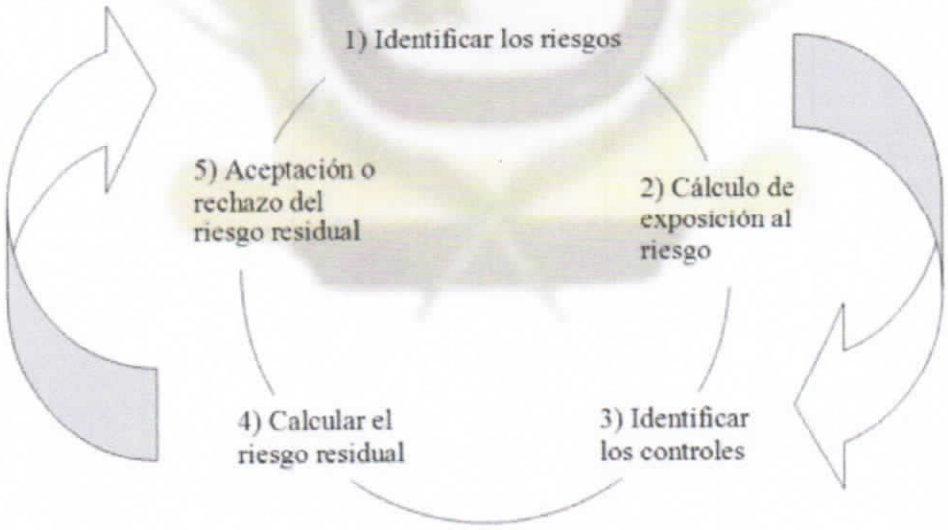
Control.- Es una medida técnica, organizativa, legal o de cualquier otro tipo que mitiga el riesgo intrínseco del escenario de riesgo, reduciéndolo y generando lo que denominamos riesgo residual, que es el riesgo que obtenemos tras la valoración de la efectividad de los controles. Cabe agregar que el riesgo residual no debe superar nunca el posible riesgo que se está tratando.

METODOLOGÍA PARA LA EVALUACIÓN DE RIESGOS.

El proceso de administración de Riesgos es continuo y no único o aislado, es un proceso cíclico enfocado en la mejora continua por lo tanto es necesario establecer una metodología que se adapte a las necesidades de la Administración Pública Municipal de Tumbiscatío en donde a pesar de que la Tecnologías de la Información y la comunicación es limitada no deja de ser menos importante para el cumplimiento de los objetivos, en este contexto una posible materialización de riesgos no dejara de afectar la evidencia y eficacia de los procesos.

La Organización Internacional de Normalización (ISO por sus siglas en inglés) a través de diferentes normas como son: ISO 31000:2018 Gestión del Riesgo-directrices, ISO 27001 Seguridad de la Información, ISO 27002. La importancia de las buenas prácticas en los Sistemas de Seguridad de la Información nos presenta las bases para la implementación de la metodología en gestión de riesgos de TIC´s.

El esquema que se muestra a continuación muestra un proceso simplificado para la detección y corrección de riesgos.



IDENTIFICACIÓN DE RIESGOS

Identificar los riesgos: Definir para cada activo, la probabilidad de que las amenazas o las vulnerabilidades propias del activo puedan causar un daño total o parcial al activo de la información, en relación a su disponibilidad, confidencialidad e integridad del mismo. (27001, s.f.)

Para realizar una adecuada identificación de riesgos tanto internos como externos de la organización en materia de Tecnologías de la Información y la comunicación, a través del análisis en las diferentes áreas usuarias de TIC´s, se emplea como herramienta el método *What If.* Que consiste básicamente en crear un equipo interdisciplinario de trabajo que mediante la técnica *brainstorming,* genera preguntas, estudia las posibles consecuencias, desarrolla y evalúa respuestas, diseña recomendaciones aplicables a cada caso.

El Método What if, es una herramienta muy sencilla y fácil de comprender, es comúnmente utilizada en las primeras etapas de la identificación de riesgos, se programan reuniones con representantes de las diferentes áreas de la administración, los riesgos se identifican a partir de la pregunta ¿Qué Pasa si…? La Siguiente tabla muestra el esquema básico que se sugiere usar.

¿Qué ocurre si?	Consecuencia	Recomendación

EXPOSICIÓN AL RIESGO

Cálculo del riesgo: Este se realiza a partir de la probabilidad de ocurrencia del riesgo y el impacto que este tiene sobre la organización (Riesgo = impacto x probabilidad de la amenaza). Con este procedimiento determinamos los riesgos que deben ser controlados con prioridad. (27001, s.f.)

Para determinar la exposición al riesgo se emplea la Matriz de Riesgo, se utilizan dos directrices principalmente la probabilidad de ocurrencia y el impacto generado en caso de materialización.

La probabilidad de que un riesgo se materialice se puede medir de forma cualitativa o cuantitativa, mediante conocimiento del impacto definimos que acciones tomar con mayor o menor urgencia.

Los identificadores se pueden tomar de acuerdo al siguiente orden.

Severidad del Daño:

- Baja
- Media
- Alta

Probabilidad de ocurrencia:

- Improbable
- Probable
- Muy probable.

Nivel de Riesgo:

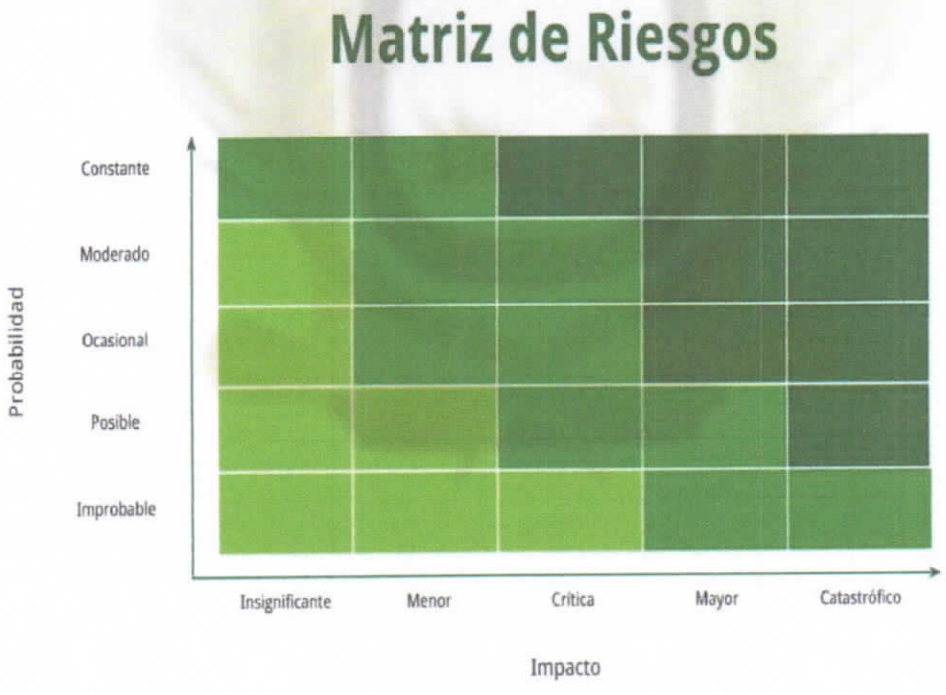
- Nulo
- Moderado
- Alto

VALORACIÓN DEL RIESGO

Una vez establecidos estos parámetros de valoración podemos generar una Matriz de Riesgos, ya sea de forma manual o mediante un software especializado.

Esta herramienta viene representada mediante tablas. Estas tablas están compuestas de los riesgos, la probabilidad de que terminen sucediendo, su gravedad, así como posibles soluciones. Esta herramienta de control y gestión permite diferenciar y clasificar los riesgos, según su tipología, nivel y factores. Puede aplicarse a cualquier tipo de empresa, independientemente de su tamaño y naturaleza. (School, 2017)

La Matriz de Riesgos está basada en dos ejes: La Probabilidad del Riesgo (eje X) y el Impacto o severidad de Daño (eje Y). A continuación se muestra una gráfica a modo de ilustración.



Fuente: (School, 2017)

TRATAMIENTO DEL RIESGO

Una de las ventajas de aplicar una Matriz de Riesgo es que permite identificar cuáles son los riesgos que tienen un mayor impacto y por la tanto se puede desarrollar e implementar un plan de tratamiento oportuno.

El resultado de una evaluación de riesgo debe ser un inventario de acciones, por orden de prioridad, para desarrollar, mantener o mejorar controles. (Trabajo, 2018)

Presentar un plan estratégico correspondiente a cada área donde se ha identificado los posibles riesgos siguiendo el orden de prioridades y midiendo los efectos colaterales, resultara efectivo para la Administración Publica, en dicho plan se dan respuesta a cuestiones básicas como: ¿qué hacer?, ¿dónde hacer? ¿Quién lo va hacer? ¿Cuándo se va hacer?

Control del Riesgo

Una vez que se han identificado los posibles riesgos en orden de prioridad se procede a desarrollar los controles para cada riesgo susceptible de materialización en tecnologías de la información y comunicación, en la siguiente tabla se muestra de forma general el riesgo y el control.

	Riesgo	Control
1	Cambios no autorizados, erróneos o fraudulentos a programas.	Políticas y procedimientos para el "manejo del cambio" a programas, asegurando que la versión autorizada se encuentra en producción.
2	Daño o robo de equipos en centros de datos.	Protocolos de seguridad con acceso físico restringido.
3	Acceso no autorizado.	Protocolos de seguridad con acceso lógico, por ejemplo: a través de claves.
4	Fallas en los sistemas que interrumpen la operación.	Planes de continuidad operativa y recuperación de la información (BCP y DRP).

Mapas de Riesgo

Los mapas de riesgos son otra herramienta muy útil a la hora de presentar de forma gráfica los riesgos y sus posibles controles, el siguiente mapa muestra algunos de los riesgos en tecnología más comunes.

RIESGO	DESCRIPCION	CAUSA	EFECTO	CLASIFICACION	ANALISIS		VALORACION	POLITICAS
					CALIFICACION	EVALUACION	Probabilidad e Impacto Vs. Controles	
Fallas Eléctricas	Cada ramal inicialmente diseñado se le han instalado mas equipos produciendo una sobrecarga en cada línea y en las Ups existentes	Cableado eléctrico sobrecargado de equipos	Daño en equipos Perdida de Información Posibilidad de Incendio	Riesgo tecnológico	20	Zona de Riesgo Moderado	Zona de Riesgo Tolerable	Evitar el riesgo. Se debe hacer nuevos diseños de la red eléctrica y cambiar la actual con protectores tanto eléctricos como contra incendios, además se debe tener una planta eléctrica para eventualidades
Desactualización de Tecnología computacional	Los sistemas ofrecen cada día herramientas mas versátiles que le permite a los usuarios obtener información mas rápida y de fácil interpretación	Software y hardware se vuelven obsoletos y no se puede apoyar la institución con tecnología de punta	Falta de credibilidad. Menos argumentos para toma de decisiones por parte de la alta gerencia	Riesgo tecnológico	20	Zona de Riesgo Moderado	Zona de Riesgo Moderado	Evitar el riesgo. Actualizar equipos de computo y de comunicaciones para ofrecer un mejor servicio a la comunidad
Inseguridad en porterías de la División de Sistemas, Central Telefónica y el Centro de Servicios de Información	La falta de seguridad en estas puertas permite el acceso a toda persona	No se tienen sistemas de seguridad en puertas	Perdida de elementos Perdida o daño de información Salida o conocimiento de información confidencial	Riesgo tecnológico	10	Zona de Riesgo Tolerable	Zona de Riesgo Tolerable	Evitar el riesgo. Se deben adquirir sistemas de seguridad que permitan verificar identidad y permisos de acceso de quien entra a estas dependencias
Perdida de información por virus informáticos	Se debe tener un antivirus con actualización en línea con la casa matriz con el fin de poder detectar cualquier virus informático	No se tiene un software actualizado que detecte Virus informáticos	Perdida de información Daño en equipos Perdida de tiempo para poder entregar información oportunamente	Riesgo tecnológico	20	Zona de Riesgo Importante	Zona de Riesgo Importante	Evitar el riesgo. Adquirir licencias de antivirus que detecten cualquier virus informático como también culturizar a los usuarios de la red como deben manejar la información que están grabando en cada equipo

RIESGO RESIDUAL.

Es aquel riesgo que subsiste, después de haber implementado controles. Es importante advertir que el nivel de riesgo al que está sometido una compañía nunca puede erradicarse totalmente. Por ello, se debe buscar un equilibrio entre el nivel de recursos y mecanismos que es preciso dedicar para minimizar o mitigar estos riesgos y un cierto nivel de confianza que se puede considerar suficiente (nivel de riesgo aceptable). El riesgo residual puede verse como aquello que separa a la compañía de la seguridad absoluta. (Rodiguez, 2014)

Llegado este punto, se puede realizar nuevamente una evaluación para el riesgo residual, este nunca deberá ser mayor que el riesgo inherente. Si el nivel de riesgo cumple con los criterios de aceptación de riesgo no es necesario poner controles y este puede ser aceptado. Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo bajo.

La evaluación de riesgos en una institución no es un proceso único o aislado, por el contrario requiere un análisis periódico y cíclico, los riesgos en tecnologías de la información y comunicación siempre estarán presentes de ahí la necesidad de tener en la mayor medida posible el control establecido para actuar de forma oportuna, y la eficiencia y eficacia de la administración no se vean comprometidas.

Bibliografía

27001, I. (s.f.). *NORMAS ISO*. Obtenido de NORMAS ISO: https://www.normas-iso.com/iso-27001/

ISO, 3. (2018). *ISO*. Obtenido de ISO: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

ISO, N. (s.f.). *NORMAS ISO*. Obtenido de https://www.normas-iso.com/iso-27001/

Rodiguez, I. (2014). *auditool*. Obtenido de auditool: https://www.auditool.org/blog/control-interno/3073-que-es-el-riesgo-riesgo-inherente-y-riesgo-residual#:~:text=Un%20riesgo%20inherente%20es%20uno,despu%C3%A9s%20de%20haber%20implementado%20controles.&text=El%20riesgo%20residual%20es%20aqu%C3%A9l,sus%20res

School, E. B. (2017). *EALDE Business School*. Obtenido de EALDE Business School: https://www.ealde.es/como-elaborar-matriz-de-riesgos/

Trabajo, S. d. (2018). *Superintendencia de Riesgos del Trabajo.* Obtenido de https://www.srt.gob.ar/wp-content/uploads/2018/08/Guia_ERL.pdf