



**UNIVERSIDAD CÉSAR VALLEJO**

FACULTAD DE INGENIERIA

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

**FACTORES DE RIESGO DE LAS TECNOLOGÍAS DE  
INFORMACIÓN Y EL DESEMPEÑO DE WEBCAST EN LAS  
EMPRESAS ATOGAPAN S.A. Y GRUPO HCM  
COMUNICACIONES SAC**

**TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE  
INGENIERO DE SISTEMAS**

AUTOR:

Romero Camones, Jamie Evelyn

ASESOR:

Dr. Adilio Christian Ordoñez Pérez

LÍNEA DE INVESTIGACIÓN:

Auditoría de sistemas y seguridad de la información

LIMA – PERÚ

2018

El Jurado encargado de evaluar la tesis presentada por don (a):

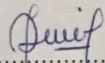
**ROMERO CAMONES JAMIE EVELYN**

cuyo título es:

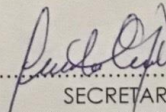
**FACTORES DE RIESGO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y EL DESEMPEÑO DE WEBCAST EN LAS EMPRESAS ATOGAPAN S.A. Y GRUPO HCM COMUNICACIONES SAC**

Reunido en la fecha, escuchó la sustentación y la resolución de preguntas por el estudiante, otorgándole el calificativo de: **15** (números) **QUINCE**(letras).

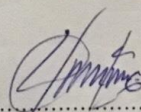
Lima, Jueves 6 de Diciembre del 2018



.....  
PRESIDENTE  
Mgtr. GALVEZ TAPIA ORLEANS MOISÉS



.....  
SECRETARIO  
Mgtr. CUEVA VILLAVICENCIO JUANITA ISABEL



.....  
VOCAL  
Dr. ORDOÑEZ PEREZ ADILIO CHRISTIAN

Elaboró	Dirección de Investigación	Revisó	Representante de la Dirección / Vicerrectorado de Investigación y Calidad	Aprobó	Rectorado
---------	----------------------------	--------	---	--------	-----------

## **Dedicatoria**

El presente proyecto va dedicado a mi familia, quien me apoyó en todo momento desde el día que decidí estudiar la carrera, por su amor y apoyo incondicional.

## **Agradecimiento**

Le agradezco a Dios, porque la sabiduría viene de lo alto, y a mi familia por brindarme la fortaleza y apoyo necesario en todo momento.

Al Dr. Adilio Christian Ordoñez Pérez, por su paciencia, apoyo y asesoría incondicional en todo momento.

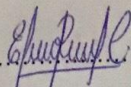
### Declaratoria de autenticidad

Yo, Jamie Evelyn Romero Camones, estudiante del programa de Ingeniería de Sistemas de la Escuela de Pregrado de la Universidad César Vallejo, identificado con DNI 43710298, con la tesis titulada "Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC" declaro bajo juramento que:

1. La tesis es de mi autoría
2. He respetado las normas internacionales de citas y referencias para las fuentes consultadas. Por tanto, la tesina no ha sido plagiada ni total ni parcialmente.
3. La tesina no ha sido auto plagiada; es decir, no ha sido publicada ni presentada anteriormente para obtener algún grado académico previo o título profesional.
4. Los datos presentados en los resultados son reales, no han sido falseados, ni duplicados, ni copiados y por tanto los resultados que se presenten en la tesis se constituirán en aportes a la realidad investigada.

De identificarse la falta de fraude (datos falsos), plagio (información sin citar a autores), auto plagio (presentar como nuevo algún trabajo de investigación propio que ya ha sido publicado), piratería (uso ilegal de información ajena) o falsificación (representar falsamente las ideas de otros), asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a la normatividad vigente de la Universidad César Vallejo.

Los Olivos, 15 de noviembre del 2018

.....  


Jamie Evelyn Romero Camones

DNI: 43710298

## **Presentación**

Señores miembros del Jurado:

Dando cumplimiento a las normas establecidas en el Reglamento de Grados y Títulos sección de Pregrado de la Universidad César Vallejo para la experiencia curricular de Metodología de la Investigación Científica, presento el siguiente proyecto de investigación titulado: "Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC".

La investigación, tiene como propósito fundamental: Determinar la relación entre los factores de riesgo en tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

La presente investigación está dividida en cinco capítulos:

En el primer capítulo se expone el planteamiento del problema: incluye formulación del problema, los objetivos, la hipótesis, la justificación, los antecedentes y la fundamentación científica. En el segundo capítulo, que contiene el marco metodológico sobre la investigación en la que se desarrolla el trabajo de campo de la variable de estudio, diseño, población y muestra, las técnicas e instrumentos de recolección de datos y los métodos de análisis. En el tercer capítulo corresponde a la interpretación de los resultados, recursos y presupuesto. En el cuarto capítulo se construye las conclusiones, y finalmente en el séptimo capítulo están las referencias bibliográficas.

Señores miembros del jurado espero que esta investigación sea evaluada y merezca su aprobación.

# Índice

	Página
<b>Carátula</b>	
<b>Páginas preliminares</b>	iii
<b>Generalidades</b>	iv
Dedicatoria	v
Agradecimiento	vi
Declaratoria de autenticidad	vii
Presentación	viii
Índice	ix
Índice de tablas	x
Índice de figuras	xi
Resumen	x
<b>I. INTRODUCCIÓN</b>	
1.1 Realidad Problemática	1
1.2 Trabajos previos	9
1.3 Teorías relacionadas al tema	17
1.4 Formulación del problema	41
1.5 Justificación del estudio	41
1.6 Hipótesis	43
1.7 Objetivos	44
<b>II. MÉTODO</b>	
2.1 Diseño de investigación	46
2.2 Variables, operacionalización	48
2.3 Población y muestra	51
2.4 Técnicas e instrumentos de recolección de datos, validez y confiabilidad	53
2.5 Métodos de análisis de datos	60
2.6 Aspectos éticos	63
<b>III. RESULTADOS</b>	
<b>IV. DISCUSIÓN</b>	
<b>V. CONCLUSIÓN</b>	
<b>VI. RECOMENDACIONES</b>	72
<b>VII. REFERENCIAS</b>	
<b>ANEXOS</b>	
Anexo N° 1: Matriz de consistencia	83
Anexo N° 2: Ficha técnica. Instrumento de recolección de datos	84
Anexo N° 3: Instrumento de investigación	85

Anexo N° 4: Base de datos experimental	89
Anexo N° 5: Resultados de la confiabilidad del instrumento	91
Anexo N° 6: Validación de la metodología y del instrumento	94
Anexo N° 7: Entrevista para la realidad problemática	115
Anexo N° 8: Carta de aprobación de la empresa	117
Anexo N° 9: Acta de implementación	118
Anexo N° 10: Diagrama de procesos	120
Anexo N° 11: Desarrollo de la metodología MAGERIT V.3	121
Anexo N° 12: Plan de capacitación	176
Anexo N° 13: Informe del plan de capacitación	184



## Índice de tablas

	Página
Tabla N°1: Programas emitidos	7
Tabla N°2: Análisis pérdidas y fallas	8
Tabla N°3. Cuadro comparativo de metodologías	29
Tabla N°4: Validación de la selección de la metodología por expertos.	30
Tabla N°5: Operacionalización de las variables.	49
Tabla N°6: Dimensiones	50
Tabla N°7: Distribución de la población	51
Tabla N°8: Validez por evaluación de expertos	54
Tabla N°9: Niveles de confiabilidad	55
Tabla N°10: Recursos humanos	66
Tabla N°11: Recursos materiales	66
Tabla N°12: Requerimiento de hardware	67
Tabla N°13: Requerimiento de software	64
Tabla N°14: Presupuesto	64
Tabla N°15: Financiamiento	65
Tabla N°16 Frecuencia valores estadísticos de la dimensión de la Eficiencia	68
Tabla N°17 Frecuencia valores estadísticos de la dimensión de la Eficacia	69
Tabla N°18 Frecuencia valores estadísticos de la dimensión de la calidad de servicio	70
Tabla N°19 Resultados de los niveles de la variable: Desempeño del webcast	71
Tabla N°20 Frecuencia valores estadísticos de la dimensión del método de análisis de riesgo	72
Tabla N°21 frecuencia valores estadísticos de la dimensión proyecto de análisis de riesgo	73
Tabla N°22 Frecuencia valores estadísticos de la dimensión de plan de seguridad	74
Tabla N°19 Resultados de los niveles de la variable: Factores de riesgo de TI	75
Tabla N°24. Prueba de Normalidad	76
Tabla N°25 Coeficiente de Correlación Rho Spearman	77
Tabla N°26 Correlación de Spearman entre las variables	78
Tabla N°27 Correlación de Spearman entre la variable 1 y la dimensión 1	79
Tabla N°28 Correlación de Spearman entre la variable 1 y la dimensión 2	80
Tabla N°29 Correlación de Spearman entre la variable 1 y la dimensión 3	81

## Índice de figuras

### Página

Figura 1. Nivel de eficiencia	4
Figura 2. Nivel de eficacia	5
Figura 3. Nivel de calidad de servicio	6
Figura 4. Nivel de las dimensiones del desempeño	6
Figura 5. N° de auspiciadores por epicentro	7
Figura 6. Entradas y salidas (Directrices generales)	23
Figura.7: Marco de Trabajo para la gestión de riesgos	30
Figura.8: Actividades formalizadas	34
Figura.9: Gestión de riesgos	38
Figura.10: Proceso de Gestión de riesgos	39
Figura 11. Diseño cuasi experimental	48
Figura 12. Resumen de procesamiento de la eficiencia	56
Figura 13. Resumen de procesamiento de la eficacia	56
Figura 14. Resumen de procesamiento de la calidad de servicio	57
Figura 15. Resumen de procesamiento de datos general de la V.D	57
Figura 16. Resumen de procesamiento del método de análisis de riesgo	58
Figura 17. Resumen de procesamiento de proyecto de análisis de riesgo	58
Figura 18. Resumen de procesamiento de la calidad de servicio	59
Figura 19. Resumen de procesamiento de datos general de la V.I	59
Figura 20. Gráfico de la frecuencia de los valores estadísticos de la dimensión de la Eficiencia	66
Figura 21. Gráfico de la frecuencia de los valores estadísticos de la dimensión de la Eficacia	67
Figura 22. Gráfico de la frecuencia de los valores estadísticos de la calidad de servicio	68
Figura 24. Resultados de las dimensiones de la variable 2: Desempeño del webcast	69
Figura 25. Gráfico de la frecuencia de los valores estadísticos del método de análisis de riesgo	70
Figura 26. Gráfico de la frecuencia de los valores estadísticos del proyecto de análisis de riesgo	71
Figura 27. Gráfico de la frecuencia de los valores estadísticos del plan de seguridad	72
Figura 28. Resultados de las dimensiones de la variable 1: Factores de riesgo de las TI	73

## Resumen

La presente tesis detalla el desarrollo de la metodología MAGERIT V.3 para probar la relación que existe entre los factores de riesgos de las tecnologías de información y el desempeño del webcast en las empresas Atogapan S.A y el grupo HCM Comunicaciones SAC, debido a que la situación empresarial previa a la implementación de la metodología presentaba deficiencias en cuanto al desempeño del webcast, en sus dimensiones de eficiencia, eficacia y calidad de servicio. El objetivo de esta investigación fue determinar la relación entre los factores de riesgo en tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

Por ello, se describe previamente aspectos teóricos de lo que es el desempeño y el proceso de webcast, así como la metodología que se implementó la cual es MAGERIT V.3, por ser la que más se acomodaba a las necesidades del proyecto, además por ser una metodología que se acoplaba a su proceso. El tipo de investigación es explicativa-correlacional-básica, el diseño de la investigación es cuasi experimental y el enfoque es cualitativo. La población fue de 32 trabajadores involucrados en el proceso de webcast, en donde se empleó el instrumento del cuestionario para medir el nivel de las dimensiones y la relación de ambas variables. El tamaño de la muestra estuvo conformado por 30 trabajadores. El muestreo es el aleatorio probabilístico simple. La técnica de recolección de datos fue la entrevista y el instrumento fue el cuestionario, los cuales fueron validados por expertos.

La implementación de la metodología MAGERIT V.3 permitió incrementar el nivel de eficiencia en un 37.2%, de eficacia en un 36.8%, y en la calidad de servicio en un 40.8%. Los resultados mencionados anteriormente, permitieron llegar a la conclusión de los factores de riesgo de las tecnologías de información tienen una relación positiva con el desempeño el webcast en las empresas Atogapan S.A y el grupo HCM Comunicaciones SAC.

Palabras clave: E-MARKETING, WEBCAST, MAGERIT V.3

## **I. INTRODUCCIÓN**

## 1.1 Realidad Problemática

En el escenario internacional, según una publicación de la revista Expansión en alianza con CNN (2014) nos dice que: “Al ver series online como Netflix y demás plataformas de entretenimiento en video, estamos haciendo que los medios de TV dejen de determinar que podemos ver, ya que desde hace 5 años la mayoría de los usuarios descargan contenido de video de la red o simplemente lo visualizan mediante el streaming, prueba de ello es que actualmente el tráfico de datos de internet en México es debido a la visualización de videos. En la encuesta nacional de consumo de contenidos audiovisuales elaborada por el IFT (Instituto Federal de Telecomunicaciones), y presentada en agosto de 2014 arrojó como resultados que el 25.8% de los entrevistados consume contenidos audiovisuales por este medio siendo YouTube (92%) la plataforma más popular para acceder a ellos y Netflix ocupa el segundo lugar (20%). Ante ello Víctor Méndez representante de desarrollo de negocios de Cisco en América Latina manifiesta que ya se está notando en el mercado, una gran competencia sobre el contenido visual ofrecido a los consumidores.”

En el escenario nacional, según una publicación de la revista Semana económica.com (2013) nos dice que: “Un tipo de servicios de *streaming* viene de las empresas u organismos que desean transmitir eventos en vivo sin hacer uso de la televisión. Es el caso de encuentros anuales, como Perumin o CADE. Una ventaja adicional es que, además de la transmisión, se puede interactuar: Si los organizadores del evento lo permiten, se puede hacer preguntas desde cualquier región o país donde esté la audiencia. No obstante, a pesar de que en los casos mencionados la señal en vivo es importante, el mayor consumo de video en las plataformas virtuales es por demanda. Es decir, el usuario decide qué ver y en qué momento. “Si una empresa tiene mil visitas por día en su página web, eso no significa que todos van a ver una señal de *streaming*; quizá sea el 10% o menos”, afirma Rivadeneira. En ese sentido, la audiencia mayor se logra luego de que la transmisión en vivo se grabe, edite y se suba a la plataforma. Con respecto al

Perú la oferta y el consumo de vídeo en vivo a través de la Internet crece alrededor de 50% al año, afirma Jean Carlo Rivadeneira, gerente de marketing de Optical Networks. La empresa, que opera la transmisión de Willax TV y algunas universidades, tiene además clientes corporativos, tales como compañías de seguros, bancos, o diversos ministerios en el sector público.”

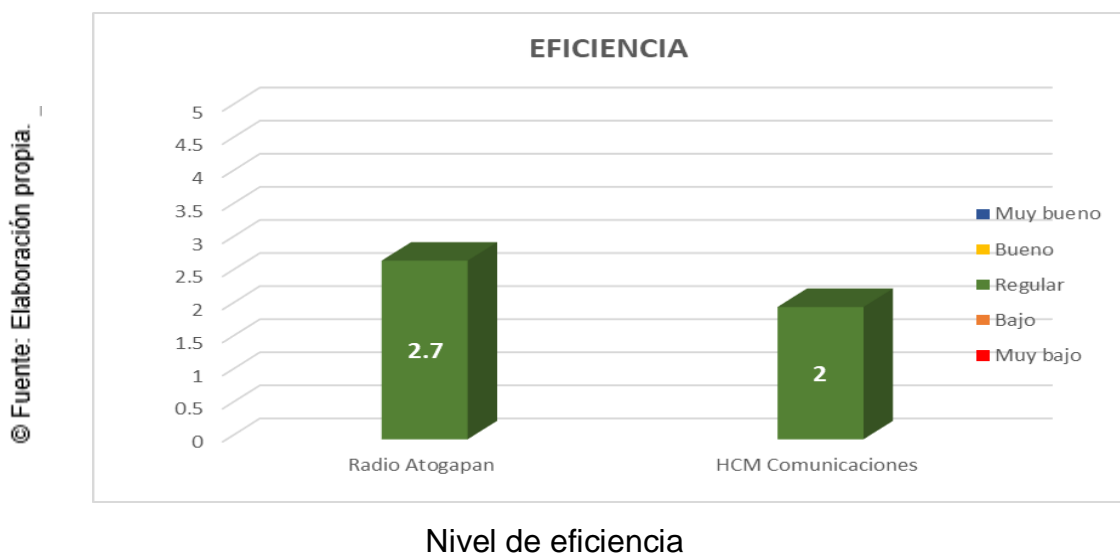
La empresa ATOGAPAN S.A. no es ajena a ello, esta empresa decidió optar por realizar webcast viendo en ello una manera accesible de transmitir programas de radio emitiendo videos en vivo sobre charlas dedicadas a la protección civil abriendo epicentros de transmisión en diferentes estados del país entre los cuales figuran 8 epicentros contando con uno en el exterior, específicamente en el país de Colombia, y es así como esta empresa se inicia en el mundo del webcast en donde su proceso para realizarlo inicia con las pruebas de conexión a internet, asegurándose de que sea estable para la transmisión, seguido de ello viene la prueba de sus equipos a utilizar, entre ellos destacan una laptop o pc de escritorio, una webcam o cámara de video profesional, un micrófono o en algunos casos un dispositivo móvil que es con lo que se realizará la transmisión en vivo, posterior a ello se debe tomar la decisión de a través de que plataforma se realizará, en donde se manejan dos opciones, las cuales son Facebook o YouTube, una vez decidido ello inicia la transmisión. Para aquellos epicentros que transmiten con dispositivo móvil simplemente colocan un trípode frente al escenario en donde se transmitirá el programa, algunos epicentros transmiten usando una laptop o pc, en ese caso se utiliza un software llamado OBS Studio el cual permite configurar y programar la emisión del programa, siendo uno de las opciones que brinda el escoger a través de que plataforma se realizará, permitiendo también que se puedan conectar dispositivos de audio y video para la transmisión. Una vez iniciado el proceso de webcast paralelo a ello se utiliza un programa llamado Sam broadcaster el cual permite que su programa transmita su radio en directo y se escuche en su página web, además se utiliza un dispositivo móvil o la misma laptop o pc para la interacción con los usuarios, respondiendo a sus comentarios mientras se está transmitiendo en vivo, cuando el programa

emitido concluye se procede a extraer el audio del programa para que este pase a ser un podcast y sea publicado en su página web para que pueda estar disponible para los usuarios que no escucharon la emisión en directo y así es como finaliza la emisión del día de cada programa emitido por los epicentros. Hasta el día de hoy esa es la forma en que se maneja el proceso de webcast, y aunque inicialmente funcionaba bien, y de alguna forma le dio un giro nuevo y ganó audiencia, con el pasar de los meses se empezaron a volver un problema, ya que se empezó a tener dificultades durante sus transmisiones en vivo, es así como jefe de T.I no los relata en la entrevista que se le realizó, en donde señala que al emitirse programas en diferentes estados dentro del país, no existe el control adecuado en cuanto a infraestructura de tecnologías de información refiere, ya que cada uno lo realiza con lo que cuenta, lo cual ha generado muchas incidencias dentro de las cuales podemos mencionar las siguientes: Tomando en cuenta el orden en el que el proceso de webcast se realiza se detalla que uno de los principales problemas es la conexión a internet que tienen, ya que en muchos de los epicentros no cuentan con el ancho de banda suficiente para evitar problemas como cortes e interrupciones durante la transmisión, lo cual ocasiona que la calidad del mismo sea deficiente, presentando además problemas de audio, otra de las grandes incidencias que se presentan es la cancelación a última hora por parte de los epicentros ya que sus equipos fallan de un momento a otro, ocasionando ello que el programa no se transmita, generando malestar entre los usuarios que esperan dicha transmisión, y todo ello se presenta porque precisamente , los factores de riesgo de TI no son tomados en cuenta, ya que cada epicentro trabaja con el equipo que cuenta, y no se toman en cuenta estándares ni los requerimientos mínimos que se necesitan para lograr un desempeño óptimo a la hora de la realización del webcast. Este tipo de problemática no solo refiere a la empresa mencionada, sino que es algo que acontece en muchas empresas como los es el del grupo HCM comunicaciones entre otras que optan por la opción de realizar webcast al verlo accesible y viable para la difusión del contenido que desean compartir, sin tener conocimientos previos de los requerimientos que se necesitan.

Para determinar la eficiencia, eficacia y calidad de servicio en cuanto al desempeño del webcast, se realizó un cuestionario (Ver anexo 3) para así determinar la situación actual de la empresa.

El primero fue para determinar la eficiencia, el cuestionario contó con 7 preguntas, aplicándose 5 opciones de respuesta en dónde el equivalente es: 1= Nunca, 2= Casi nunca, 3= A veces, 4= Casi siempre y 5= Siempre en donde el resultado se basó en un rango del 1 al 5 el cuál se determina de la siguiente manera: 0 al 1= Muy Bajo, 1.1 al 2= Bajo, 2.1 al 3= Regular, 3.1 al 4= Alto y 4.1 al 5= Muy alto, dándonos como resultado que en Eficiencia Atogapan está en un nivel regular con un 2.7 y HCM Comunicaciones de igual forma con un 2.0, como lo evidencia la Figura N°1:

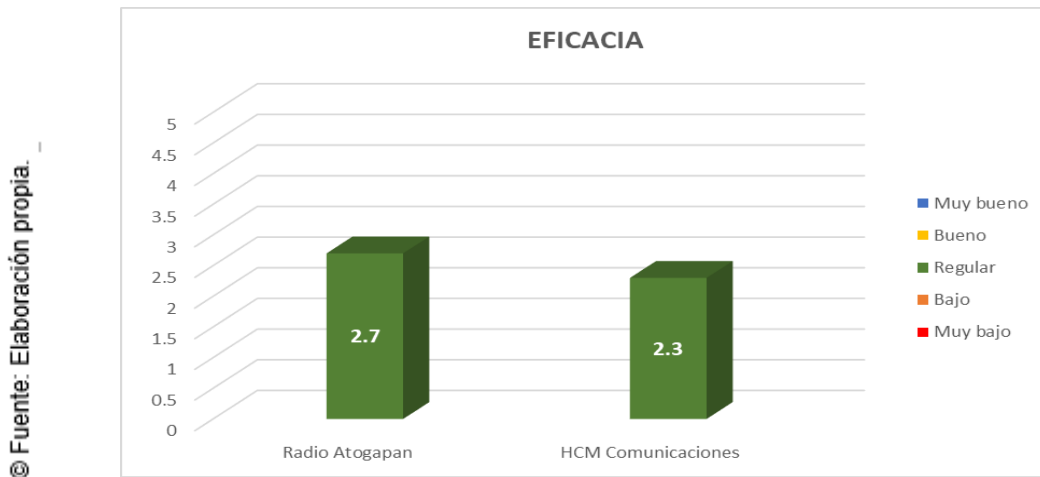
Figura 1.



El segundo fue para determinar la eficacia, el cuestionario contó con 7 preguntas, aplicándose 5 opciones de respuesta en dónde el equivalente es: 1= Nunca, 2= Casi nunca, 3= A veces, 4= Casi siempre y 5= Siempre en donde el resultado se basó en un rango del 1 al 5 el cuál se determina de la siguiente manera: 0 al 1= Muy Bajo, 1.1 al 2= Bajo, 2.1 al 3= Regular, 3.1 al 4= Bueno y 4.1 al 5= Muy bueno, dándonos como resultado que en Eficacia Atogapan está en un nivel regular con un 2.7 y HCM Comunicaciones de igual forma con un 2.3, como lo evidencia la Figura N°2:



Figura 2.

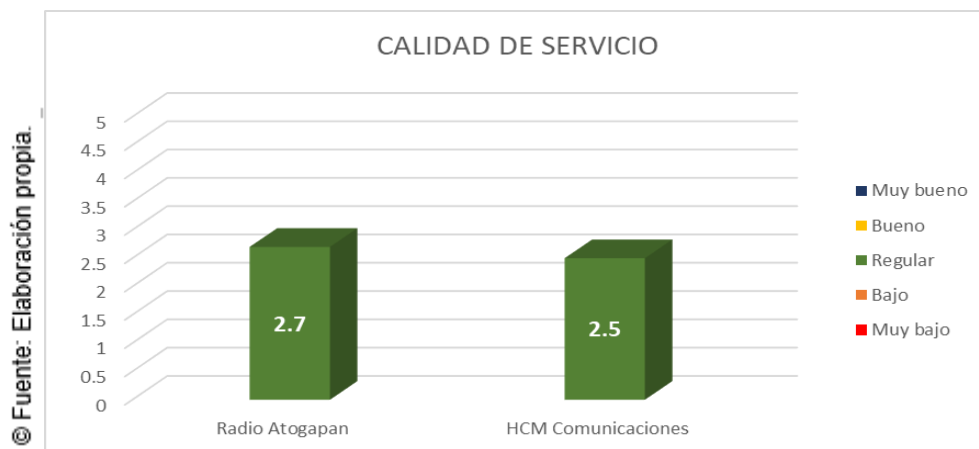


Nivel de eficacia

El tercero fue para determinar la calidad de servicio, el cuestionario contó con 6 preguntas, aplicándose 5 opciones de respuesta en dónde el equivalente es:

1= Nunca, 2= Casi nunca, 3= A veces, 4= Casi siempre y 5= Siempre en donde el resultado se basó en un rango del 1 al 5 el cuál se determina de la siguiente manera: 0 al 1= Muy Bajo, 1.1 al 2= Bajo, 2.1 al 3= Regular, 3.1 al 4= Alto y 4.1 al 5= Muy alto, dándonos como resultado que en Calidad de servicio Atogapan está en un nivel regular con un 2.7 y HCM Comunicaciones de igual forma con un 2.5, como lo evidencia la Figura N°3:

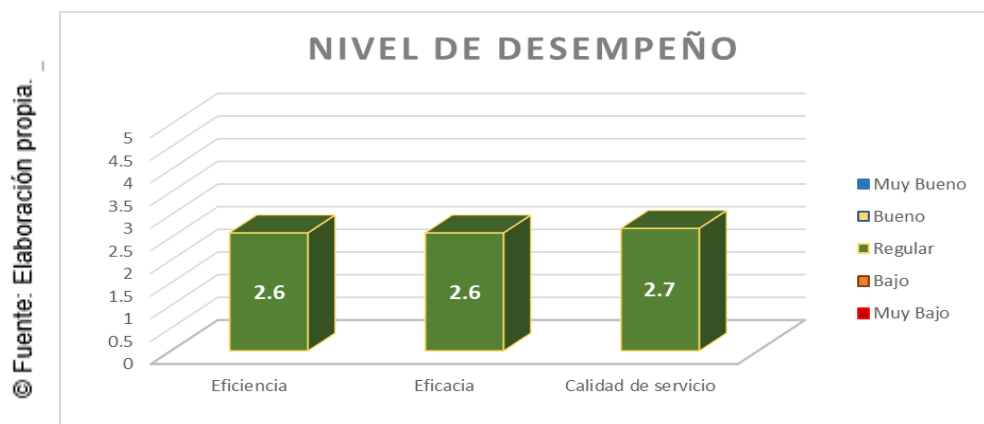
Figura 3.



Nivel de calidad de servicio

Finalmente, se determinó que según el puntaje total obtenido por las respuestas estas tendrían un equivalente, el cual está determinado de la siguiente manera: 0 al 1= Muy Bajo, 1.1 al 2= Bajo, 2.1 al 3= Regular, 3.1 al 4= Alto y 4.1 al 5= Muy alto, finalmente se determinó que en cuanto a eficiencia se obtuvo un puntaje de 2.27, en eficacia 2.45, y calidad de servicio 2.38, dándonos como resultado en los 3 casos, un nivel regular en cuanto a desempeño.

Figura 4.



Nivel de las dimensiones del desempeño

Otro punto muy importante que se genera debido al bajo desempeño del webcast, es el de pérdidas económicas, ya que la empresa Atogapan S.A cuenta con 20 patrocinadores los cuales auspician a los diferentes epicentros tal y como se muestra en la siguiente figura N°5:

Figura 5.



N° de auspiciadores por epicentro

Como se pudo apreciar en la figura N° 5, los 20 patrocinadores con los que actualmente cuenta Atogapan S.A, auspician los diferentes epicentros, cada uno cuenta con 2 a 4 auspiciadores respectivamente.

En la siguiente tabla N°1 se puede apreciar como en el mes de abril hubo muchos programas que no salieron al aire.

Tabla N° 1: Programas emitidos

RADIO ATOGAPAN - ABRIL 2018					
CIUDAD	FECHA DE TRANSMISIÓN				
	2	9	16	23	30
NUEVO LEÓN	X	✓	✓	X	✓
	2	9	16	23	30
EDOMEX	X	X	X	✓	✓
	3	10	17	24	
SONORA	✓	✓	✓	X	
	4	11	18	25	
CDMX	✓	✓	✓	✓	
	4	11	18	25	
COLOMBIA	✓	✓	X	X	
	5	12	19	26	
Q.ROO	✓	✓	✓	✓	
	6	13	20	27	
VERACRUZ	X	✓	X	X	
	7	14	21	28	
PUEBLA	X	X	✓	✓	

© Fuente: Elaboración propia.

Tal y como se aprecia en la tabla N°1, de los 34 programas que debieron emitirse en el mes de abril, sólo transmitieron 21, lo cual determina una pérdida económica significativa, ya que cada patrocinador representa la suma de S/.100 soles por programa emitido.

En la siguiente tabla N° 2 podremos apreciar la perdida económica que significó que 13 programas durante el mes de abril no salieran al aire.

Tabla N° 2: Análisis pérdidas y fallas.

EPICENTRO	N° DE AUSPICIADORES	N° PROGRAMAS NO EMITIDOS	MONTO UNITARIO	MONTO PERDIDO POR AUSPICIADOR	MONTO TOTAL
NUEVO LEÓN	4	2	S/ 100.00	S/ 200.00	S/ 800.00
EDOMEX	2	3	S/ 100.00	S/ 300.00	S/ 600.00
SONORA	2	1	S/ 100.00	S/ 100.00	S/ 200.00
CDMX	4	0	S/ 100.00	S/ -	S/ -
COLOMBIA	2	2	S/ 100.00	S/ 200.00	S/ 400.00
QROO	3	0	S/ 100.00	S/ -	S/ -
VERACRUZ	2	3	S/ 100.00	S/ 300.00	S/ 600.00
PUEBLA	3	2	S/ 100.00	S/ 200.00	S/ 600.00
<b>TOTALS/.</b>				S/	3,200.00

© Fuente: Elaboración propia.

El resultado obtenido de pérdidas económicas durante el mes de abril, asciende a la suma de S/. 3200.00 soles, lo cual determina que el desempeño ineficiente en el desempeño del webcast trae consecuencias económicas significativas, ya que, si el problema persiste, y las fallas se presentan dando como consecuencia la no transmisión de programas, se estima que esto acarrearía una pérdida monetaria de S/. 38400.00 soles al año aproximadamente.

Por ello, surge la siguiente pregunta: ¿Qué sucederá si se siguen teniendo los mismos problemas con el desempeño del webcast en la empresa Atogapan S.A y el Grupo HCM Comunicaciones SAC?, en respuesta a ello, se seguirán presentando deficiencias en su desempeño, llegando sólo a un nivel medio con predicciones de incluso llegar hasta un nivel bajo dada las incidencias constantes presentadas y la falta de control de los factores de riesgo en tecnologías de información, lo cual seguirá produciendo pérdida de audiencia, y de patrocinadores ocasionando una gran pérdida económica.

## 1.2 Trabajos previos

Díaz y Pertuz (2015), la investigación presenta como objetivo principal, el implementar una infraestructura de red que soporte servicios webcast para apoyo docente que optimice la forma de aprender de los alumnos de la carrera de Ingeniería de Sistemas a distancia de la Universidad de Cartagena, debido a que La Universidad de Cartagena, carece de una infraestructura en la cual se puedan manejar procesos críticos como la transmisión de video y webcast. Así mismo, el problema se desarrolla alrededor de los docentes quienes no cuentan con herramientas innovadoras como plataformas de apoyo. El tipo de metodología utilizado es mixta, debido a que inicialmente se llevó a cabo un estudio teórico detallado de la tecnología de streaming en cuanto a su infraestructura y la calidad de servicio. Además, se realizó una investigación de campo en diferentes escenarios de prueba que permitieron recolectar y analizar los datos y parámetros que conforman la infraestructura de un servicio de streaming con diseño de experimental debido a que, al identificarse las variables estudiadas, anteriormente mencionadas, se realizó uso y control de estas para llevar a cabo la realización de los escenarios de infraestructura de red. Fue mediante la encuesta que se recolectaron los datos. La investigación va dedicada a una pequeña población de la universidad de Cartagena, utilizando como muestra a la población estudiantil del Programa de Ingeniería de Sistemas a Distancia evalué la calidad del servicio. Los resultados obtenidos fueron modelo de referencia para futuras investigaciones que tengan por objeto la identificación de sistemas que busquen mejorar la comunicación entre docentes y estudiantes a través de una infraestructura de red sólida que soporte transmisiones críticas (voz y video), esta investigación concluye que los procedimientos enmarcados en esta metodología garantizan la implementación de un servicio de streaming con calidad para la población estudiantil seleccionada que pretende brindar beneficios al proceso de aprendizaje y comunicación entre docentes y estudiantes.

Este antecedente no sirvió para tener en cuenta el tipo de infraestructura necesaria para poder realizar el proceso de webcast de manera óptima, evitando riesgos probables que afecten en su desempeño.

Ponce Palacios (2014), Se planea modernizar las clases impartidas a los estudiantes, realizando las clases a través del uso de streaming, dictando también cursos mediante esta vía, para ello se desea implementar una red híbrida para varias universidades del Perú; debido a que hace falta la optimización en el uso del Ancho de Banda mientras se realizan las transmisiones de video en los lugares alejados del país. Para ello lo que se requiere es unir el poder que tienen las redes CDN y las P2P, y así poder obtener dicho beneficio a un bajo costo. Así mismo, el problema se desarrolla en que al poseer grandes datacenters estas permiten que todas se localicen en un solo punto, lo cual hace que no se realice de forma eficiente, originando el desperdicio de ancho de banda, no superando las expectativas del usuario. La metodología usada es de campo con diseño de proyecto factible para solucionar una problemática. Se utilizó la técnica de la aplicación de encuestas para la obtención de datos. Estas fueron aplicadas a estudiantes universitarios. La población fueron 326283 estudiantes universitarios de Lima y Callao y se utilizó una muestra de 127899 estudiantes. Los resultados obtenidos fueron: conocer el ancho de banda que se utiliza, la cantidad de usuarios que utilizan el servicio, haciendo un cálculo del ancho de banda generado por audio, ya que este es mucho menor al consumido por el video. En esta investigación se concluye que con los resultados obtenidos que mediante el desarrollo de esta tecnología se lograr tener recursos para las transmisiones académicas y podrán tener acceso todos los usuarios desde cualquier lugar y/o dispositivo asegurándose una buena calidad de servicio. Se estima alcanzar inicialmente a un público inicial de 127899 alumnos de las diferentes universidades del Perú.

Este antecedente nos sirvió para tener en cuenta cómo se puede aprovechar el ancho de banda para la realización de webcast, teniendo en cuenta que este es un activo importante dentro del proceso de webcast, obteniendo así transmisiones de alta calidad, lo cual garantizará un desempeño óptimo.

Paula y Rosario (2016), la investigación tiene como objetivo analizar la gestión de la seguridad de las tecnologías de información en las PYME, debido a que esta permite asegurar la integridad, disponibilidad y la confidencialidad de la información, datos y servicios de TI. Así mismo, el problema se desarrolla en el campo de la seguridad de la información, ya que la gran mayoría no ejecutan los procedimientos adecuados. La metodología de investigación usada es descriptiva y analítica, ya que pretendes analizar la de gestión de seguridad de TI en las medianas y pequeñas empresas. Se utilizó la técnica de la entrevista para obtener los datos dela investigación. Estas fueron aplicadas a las pymes. La investigación fue con diseño descriptivo utilizando un enfoque cuantitativo. La población de este estudio fue de 700 empresas tipo PYMES registradas en San francisco de Macorís y se utilizó la muestra de 100 empresas. Los resultados obtenidos fueron: que sólo 20 empresas cumplían con los requisitos para realizarse el estudio, esta investigación concluye que las empresas si tienen la necesidad de protección de datos, ya que el 100 % considera que existe una vinculación entre los recursos tecnológicos y las operaciones de sus negocios.

Este antecedente servirá para tener en cuenta los factores de riesgo a tomar en cuenta en cuanto a tecnologías de información refiere para poder así cuidar de la seguridad, así como el desarrollo óptimo dentro de las organizaciones.

Venegas Carazas (2015), La investigación tiene como objetivo obtener el nivel de madurez al aplicar RISK IT dentro del área de gestión de riesgos en la caja rural de ahorro y crédito Los Andes S.A. entre los meses de diciembre 2014 y diciembre 2015 en el departamento de Puno-Perú, dado que hoy en día la gran parte de las organizaciones realizan sus procesos operativos con TI, generándose una gran dependencia a las tecnologías de información, las organizaciones en general tienen una elevada inversión en tecnología, puesto que el no hacerlo ocasiona perder competitividad en el mercado, lo cual se traduce en pérdidas. Así mismo el problema se desarrolla dentro de los servicios micro financieros, la misma que gestiona sus riesgos de manera

integral, teniendo en el riesgo operacional uno de sus pilares fundamentales, dentro del cual se encuentra como un factor que forma parte de su composición el análisis de riesgos de tecnologías de información. La metodología utilizada es de investigación no experimental. La técnica utilizada fue el de la encuesta basándose en un modelo de madurez, el cual nos pudo dar a conocer el grado en el que se encontraba el nivel de madurez en la Gestión de Riesgos de Tecnologías de Información en los meses de diciembre 2014 y diciembre 2015. Estas se aplicaron partiendo desde la observación del investigador hasta la intervención de los trabajadores que laboran en esa área. Se aplicó un diseño descriptivo. El tipo de muestra utilizado fue no probabilístico según la experiencia del investigador.

Esta investigación concluye que el nivel de madurez al aplicar el RISK IT en un área de gestión de riesgos de las tecnologías de información entre los meses de diciembre 2014 se alcanzó un nivel 1 y en el mes diciembre 2015 se alcanzó un nivel 3.

Este antecedente servirá para tener en cuenta el riesgo operacional teniendo como uno de sus pilares fundamentales, el análisis de riesgos de tecnologías de información y las consecuencias que puede traer ello si no se toman en cuenta.

Dan Lonita. (2013), la investigación tiene como objetivo obtener una mejor comprensión de las principales diferencias y similitudes entre varias metodologías y herramientas de evaluación de riesgos de información de última generación, debido a que existe desconocimiento sobre que metodología es adecuada para cada proceso o empresa. Se utilizó la metodología descriptiva, porque permite describir las diferentes metodologías para los factores de riesgo. Se utilizó la técnica de entrevista, realizando encuestas con el propósito de registrar para analizar cada metodología aplicada. La población fueron 17 socios de la industria los cuales estaban interesados en la evaluación de cada metodología para los riesgos. Los resultados obtenidos fueron: que a mayoría de las metodologías simplemente



no están diseñados para implementarse en tan poco tiempo debido a complejidades intrínsecas. El único método que está diseñado para ser implementado en tan poco tiempo, es aquella que provee guías establecidas con ejemplos para su implementación.

Este antecedente servirá para medir el nivel de complejidad de la metodología que se desea implementar, facilitando así, la decisión de la metodología a usarse optando por el más adecuado para el presente proyecto de investigación.

Motake Katerina (2016), la investigación tiene como objetivo determinar el carácter particular y los propósitos establecidos para la metodología de evaluación de riesgos, debido a que los sistemas de suministro de agua y entornos peligrosos proporcionan una efectiva administración del sistema y precisión mejorada. Sin embargo, heredan ambas vulnerabilidades de IP tecnología y sistemas físicos lo cual lo caracterizan por presentar un mayor riesgo debido a su complejidad, naturaleza e importancia crítica. La metodología de investigación usada es descriptiva y explicativa, utilizó los métodos deductivos, analíticos, analógicos y principalmente de observación. Se utilizó la técnica de encuestas. La población fueron individuos dentro de una población amenazada y pueden ser agrupados por comunidades de amenazas dentro del ámbito general de TI. Los resultados que se obtuvieron fueron: Luego de la evaluación realizada, la metodología de Magerit es más adecuada para Infraestructuras críticas. Más específicamente, esta metodología es más amigable para el usuario que otras como lo es CRAMM. Además, esta metodología viene acompañada de una herramienta de software automatizada para el análisis y la gestión de riesgos en infraestructuras críticas que admite todas las etapas de la aplicación y selecciona contramedidas y cubre todo aspectos de seguridad, incluido el factor técnico, los procesos y las cuestiones de personal.

Este antecedente servirá para tener en cuenta los beneficios de Magerit y la herramienta de software de ayuda para el control de riesgos en una organización.

Cahuana Quispe (2016), la investigación tiene como objetivo hacer el análisis del nivel de eficacia del programa de las tecnologías de información, dirigido a alumnos que toman el curso de prótesis del VII semestre, a quienes se les dio clases usando las nuevas tecnologías, debido a que no se cuenta con infraestructura TI adecuada para mejorar la calidad de la enseñanza. Asimismo, el problema se desarrolla alrededor de estudiantes que no mejoran su rendimiento académico, por ello se les quiere brindar un mejor aprendizaje mediante el uso de las TICs. La metodología de investigación usada es de campo, siendo experimental, transversal y comparativo, trabajando con dos grupos, uno observacional y otro llamado control. Se aplicó la técnica de la encuesta con la herramienta del cuestionario para la recolección de datos. Estas fueron aplicadas a estudiantes matriculados en el curso de prótesis del VIII semestre. La investigación fue con diseño cuasi experimental. La población fueron los alumnos de VIII semestre y se utilizó la muestra de 40 alumnos divididos en dos grupos. Los resultados obtenidos fueron: que existe una diferencia estadísticamente significativa aplicada al rendimiento académico del grupo experimental y el grupo control, según la prueba inferencial aplicada del Chi cuadrado; obteniendo una significancia del 0.05, esta investigación concluye que existe una diferencia estadísticamente significativa en el rendimiento entre el grupo control y el experimental, según la prueba inferencial del chi cuadrado; por lo que se infiere que el programa Tics ha sido eficaz para el rendimiento académico, mejorando su nivel de eficacia de un nivel bajo a uno regular aumentando en un 18%.

Este antecedente nos servirá para evaluar la eficacia obtenida haciendo uso de las tecnologías de información.

Alva Arce (2014), la investigación tiene como objetivo demostrar en qué forma las tecnologías de información logran influir como instrumentos eficaces en el

proceso de capacitación del personal en la Oficina Nacional de Proceso Electorales (ONPE), debido a que no existen programas informáticos para dicho proceso. Asimismo, el problema se desarrolla en la ONPE donde no tienen programas de capacitación basados en las tecnologías de información que faciliten la capacitación a distancia y se convierta en una herramienta de consulta directa. La metodología de investigación es básica, basada en la búsqueda de conocimientos sobre las TIC y en la capacitación de los trabajadores. Se utilizó la técnica de la encuesta con la herramienta del cuestionario que se realizó al personal de trabajo. La investigación fue con diseño no experimental debido a que no se realiza la manipulación del factor causal para la determinar sus efectos. La población fue de 46 trabajadores y la muestra de 30 empleados que realizaron la encuesta de manera aleatoria. Los resultados obtenidos fueron que las tecnologías de información influyen de manera eficaz en la capacitación del personal. La influencia se determinó con el método estadístico de regresión y correlación, lo cual da lugar al hallazgo de la correlación conjunta óptima, que alcanzó 0.708, esta investigación concluye que las tecnologías de información y comunicación influyen como instrumentos eficaces con un alto nivel de influencia.

Este antecedente nos servirá para analizar la eficacia que tienen al ser aplicados los requerimientos necesarios en infraestructura Ti para el óptimo desempeño de los procesos.

Arias, Díaz y Vargas (2014), la presente investigación tiene como objetivo implementar una guía de gestión de riesgos basándose en la norma NTC-ISO 31000, para la gestión de incidentes y de peticiones de servicio en el área de help desk, en las empresas de servicios en Colombia. Debido a que, no existe prevención para lo que son los riesgos de TI. Asimismo, el problema se desarrolla en el área de help desk de las organizaciones que brindan servicios de TI en Colombia afectando así la calidad de servicio al usuario, esta como todas las áreas siempre presentar riesgos que no son correctamente controlados a tiempo y desencadenan daños que originan muchas pérdidas, ya sea de información, monetaria, credibilidad entre otras. La metodología de investigación utilizada es descriptiva, y está aplicado a la evaluación directa

de los procesos que se encuentran en el área de mesa de ayuda. Se utilizó la técnica de la encuesta con la herramienta del cuestionario para obtener información y hacer un análisis de la gestión de riesgos de TI en la organización. Como población fueron consideradas las organizaciones que brindan soporte en Colombia, y se trabajó con una empresa real y se utilizó la entrevista para la obtención de información para verificar el manejo de sus procesos, subprocesos y de las actividades que en esta área se realizan. Los resultados obtenidos son que realmente la prevención y utilización de una guía para los riesgos de TI representan un gran porcentaje de pérdidas anuales, esta investigación se concluye que luego de implementar la gestión de riesgos con guías puntuales que permitan hacer el seguimiento correcto es necesario, ya que les ayudara a dar continuidad al negocio, para así poder lograr una correcta gestión de riesgos y lograr mitigar estos , obteniendo como resultado el logro de los objetivos del área, en este caso fue para medir la calidad del servicio, incrementando un 25% luego de la implementación de la norma NTC-ISO 31000..

Este antecedente nos servirá para tomar en cuenta la elección correcta de metodología que será aplicada para el análisis de los factores de riesgo de TI y lo que representa en cuanto al crecimiento en la calidad de servicio.

Vargas García (2015), la investigación tiene como objetivo analizar la influencia causada tras la implementación de la metodología COBIT 5 para mejorar los procesos tecnológicos en el ámbito de gobierno y gestión, debido a que no se utiliza ningún manual ni guía para el control de riesgos. Asimismo, el problema se desarrolla dentro de EIS en donde pocas veces existe una comunicación efectiva, no se realiza el mantenimiento de los equipos, y no se sigue ningún tipo de normas internacionales. La metodología de investigación usada es el método científico para determinar si se ha implementado o no la metodología COBIT 5 correctamente en la gestión de riesgos de TI. Se utilizó la técnica de la encuesta con herramientas de cuestionario, además de la observación. Estas fueron aplicadas al director y al técnico de la escuela de Ingeniería de sistemas. La investigación fue con

diseño descriptivo. La población fue de dos personas, el técnico y el director de la facultad de Ingeniería de sistemas, en donde se obtuvo una muestra de dos personas, debido a que la población es muy pequeña. Los resultados obtenidos determinaron que un 13,99 % va orientada a un “pocas veces” y “nunca”, muchas veces no se utilizan los estándares que Cobit recomienda, manifestó el director de EIS, por ellos se concluye que al ser aplicados correctamente nos permite identificar problemas y vulnerabilidades que se presentan dentro de todas las administraciones de la EIS, mejorando su nivel de eficiencia en un 26%.

Este antecedente nos servirá para poder identificar y analizar la metodología correcta que será aplicada para el desarrollo de la presente investigación, orientada al nivel de eficiencia.

### 1.3 Teorías relacionadas al tema

Para entender con mayor claridad, a continuación, se fundamenta mejor el estudio, mediante teorías que sustentan la presente tesis.

#### **Desempeño:**

Según Elizondo y Sarabia (2015) definen que:” El desempeño es un resultado que denota la manera como se logra un resultado efectivo” (p.13)

Se puede entender por desempeño como el logro óptimo obtenido luego de ejecutado algún proceso o actividad.

Según Ariel Fox (2014) define que:” El desempeño es ser capaz de apreciar su propio papel en los resultados que está obteniendo” (p.43)

Se entiende por desempeño el poder identificar el cómo se está llevando a cabo el proceso o actividad realizada mediante los resultados reflejados.

Según Timothy Galpin (2013) define que:” Para medir el desempeño durante un proceso de cambio. Primero, es necesario ser capaz de determinar cuándo se ha alcanzado los objetivos.” (p.103)

Para lograr observar los cambios en el desempeño es importante identificar si los objetivos han sido cumplidos.

**Webcast:**

Según Chunga Chingel (2015) define que:” La Webcast es el proceso enviar tanto audio como video, juntos o separados (muy similar a lo que es una transmisión de televisión o radio) por la Internet. La definición de Webcast tiene raíz en las palabras World, Wide y Web, así como broadcast que es difusión y transmisión de información desde un emisor a diferentes receptores al mismo tiempo).” (p.25)

Podemos entender por webcast al audio y video que podemos compartir a través de internet diferentes usuarios al mismo tiempo.

Según Vasconcelos Santillán (2015) define que:” El webcast es equivalente de una videoconferencia, y el evento se transmite (en vivo o bajo demanda) desde el servidor web hacia la computadora del usuario. En general no se produce un archivo que el usuario pueda descargar.” (p.153)

El webcast es como realizar una videoconferencia, la cual es recibida por la computadora o dispositivo del usuario conectado a internet, en casi todos los casos no es posible acceder al archivo luego de terminada la transmisión, a menos de que sean publicados para su descarga.

Según Solís Sánchez (2015) define que:” Hay que destacar el webcasting como la herramienta web que permite una transmisión en tiempo real de lo que podamos estar diciendo, por lo regular quien hace webcast lo graba y luego lo pone como podcast en sitios diferidos para hacer difusión de los mensajes emitidos.” (p.113)

Podemos tomar al webcasting como una forma de transmitir en vivo de manera sencilla, para luego poder compartir dichos archivos como podcasts en alguna página de internet.

## **Dimensiones del desempeño del Webcast**

### **Eficiencia**

Según Guzmán Marcela (2014) define las dimensiones del desempeño como: “Eficiencia: hace referencia a la relación que existe entre un producto y la producción del o la de un servicio, y el de los insumos o los recursos involucrados para llegar a que se realice la producción. Lo cual nos quiere decir que se busca la realización de actividades con los mínimos recursos posibles” (p.12)

La eficiencia toma en cuenta dos puntos importantes como lo son la producción física de un bien o servicio y los recursos utilizados.

### **Eficacia**

Según Guzmán Marcela (2014) define las dimensiones del desempeño como: “Eficacia: Este refiere al nivel de grado del cumplimiento de los objetivos que se han establecido las empresas, es decir, en qué magnitud se están alcanzando los objetivos, sin considerarse necesariamente los recursos que se han asignado para ello. La eficacia esta conformada también por la sustentabilidad de estos resultados a través del tiempo, según corresponda a la naturaleza del bien o servicio entregado.” (p.11)

La eficacia es aquella que refleja los objetivos planteados realizados, en donde los resultados obtenidos demostraran el cumplimiento de ella.

para alcanzar ese nivel óptimo sin la necesidad de usar recursos extras.

### **Calidad de servicio**

Según Guzmán Marcela (2014) define las dimensiones del desempeño como: “La calidad del servicio: puede incluirse como una dimensión específica del derivado del concepto de lo que es la eficacia o tomarla como una dimensión adicional. En este documento se le toma como una dimensión adicional y no como parte de la eficacia y hace referencia al grado de cumplimiento de los atributos de los productos (bienes o servicios) entregados, tales como: accesibilidad, oportunidad, precisión y continuidad en lo que a entrega del servicio refiere, comodidad del usuario y atención, etc.” (p.11)

La calidad de servicio parte de la eficacia que pueda estar presente en un proceso, dando esto como resultado, además del cumplimiento óptimo de los productos y servicios entregados.

## **Factores de riesgo**

Según Salvador Molina (2015) definen al riesgo como: “La combinación de la probabilidad de ocurrencia de un evento y sus consecuencias” (p.11)

Podemos entender como riesgo la posibilidad de que ocurra un evento y esto traiga consigo un efecto que dañe o perjudique el desempeño de las tecnologías de información.

Según Estupiñán y Nievel (2015) definen al riesgo como: “La posibilidad de que un evento ocurra y que este genere un impacto en el alcance de los objetivos. El riesgo es medido en términos de probabilidad e impacto” (p.28)

El riesgo implica que pudiese ocurrir una situación que afecte los objetivos planteados.

Según Seth Godin (2015) definen al riesgo como: “EL riesgo implica ganar o perder. Si ponemos algo en juego, puede que obtengamos buenos resultados o puede que no” (p.4)

El riesgo puede tomar dos caminos, para lograr algo que tenga una consecuencia positiva o negativa.

## **Tecnologías de información:**

Según Gonzáles, Leyva y Gutiérrez (2013) lo definen como: “una palabra que encierra todo aquello que se relacione a las formas de crear, intercambiar y almacenar información a través de las tecnologías de información, dando como resultado imágenes, videos, datos, chats, y toda aquella multimedia posible. El objetivo principal es mejorar sus procesos, para así lograr que sus negocios eleven su grado de competitividad y puedan hacer frente al mercado, así como la productividad dentro de las empresas en la forma y manejo de la información.” (p.5)

Las tecnologías de información engloban todo aquello que engloba el crear, almacenar, y procesar datos en sus diferentes formas, siendo su objetivo la optimización de los procesos en las organizaciones.



Según Vasconcelos Santillán (2015) define las Tecnologías de información como: “Nos referimos al conjunto de dispositivos, servicios y actividades apoyadas por equipos de cómputo, y que se basan en la transformación de información numérica, también llamada digital” (p.2)

El autor define las tecnologías de información como un conjunto de equipos de cómputo que ayudan al procesamiento de información de manera digital.

Según Díaz Dumont (2015) cita a Ballón y Joo (2009) en donde definen que las Tecnologías de información: “son herramientas que debe aplicarse en la enseñanza y su uso debe ser considerado en los diferentes niveles educativos tanto primarios como secundarios, pues la humanidad de hoy, aprende, se comunica, se socializa, se informa y se expresa a través de la red” (p.6)

Las tecnologías de información apoyan mucho a la optimización de procesos, y el ámbito de la educación no es ajeno a ello, haciendo uso de ellas para la difusión del mismo.

### **Factores de riesgo de las tecnologías de información**

Según Baca, Solares y Acosta (2014) lo definen como: “un concepto conocido como sistema de medición de valor agregado de la productividad, como una propuesta e intento para identificar y evaluar el impacto de la TI sobre el desempeño de las unidades de negocio que están siendo influidas por la tecnología de la información.” (p.168)

Es imprescindible identificar el impacto que generan las TI y el riesgo que estas puedan ocasionar en el desempeño del negocio, mediante estándares o guías para la prevención de riesgos.

Según Cierco Jiménez de Parga (2011) lo definen como: “La ausencia de estándares se convierte en un claro factor de riesgo que puede comprometer sus inversiones. Además, estas capacidades asociadas a la disponibilidad de estándares que potenciarán a la competencia entre los proveedores, y por consiguiente, la capacidad de elección proveniente de los usuarios y el traslado a los mismos de los beneficios de la tecnología.” (p.27)

Estar preparados ante posibles riesgos en tecnologías de información, evitara que la organización sufra pérdidas importantes, por ello es que actualmente existen muchas guías y estándares que nos ayudaran a lograrlo.

Según ITIL (2009) lo definen como: “La complejidad de los servicios a lo largo de la cadena de suministro está aumentando, lo que genera desafíos para cualquier proveedor de servicio que implemente nuevos servicios o cambios en los servicios existentes de TI.” (p.219)

Dentro de una organización siempre se presentarán nuevos desafíos, sobre todo si se implementa un nuevo servicio o se realizan cambios en los servicios de TI, por ello es de vital importancia contar con un plan de riesgos y sobretodo tener en cuenta aquellos factores que puedan presentarse que lo ocasionen.

## **METODOLOGÍAS PARA EVALUAR LOS FACTORES DE RIESGO EN TECNOLOGÍAS DE INFORMACIÓN**

### **COBIT 5**

Según Fonseca Luna (2011) nos dice que: “Cobit es un marco de referencia que nos muestra las mejores prácticas que deben usar las empresas para controlar la información a través de las tecnologías de información (TI) y los riesgos que estos ocasionan. El cobit fue divulgado por *Information Systems and Control Foundation* (ISACA), en 1996”. (p.217)

Cobit permite describir las buenas practicas, las cuales pueden ser usadas por las empresas para gestionar los riesgos en tecnologías de información.

### **Dimensiones para la evaluación del riesgo según Cobit:**

Según Fonseca Luna (2011) nos dice que: “Según cobit, la medición del desempeño es esencial para el gobierno de TI, debido a que brinda soporte e incluye el monitoreo de objetivos que puede evaluar los resultados obtenidos en los procesos de TI y en su desempeño. Esto se logra mediante directrices generales que ofrecen herramientas para asignar responsabilidades a las partes involucradas en el desarrollo de TI en la compañía, y la medición a través de: Metas, matrices RACI, y métricas. En este contexto, las directrices

generales del cobit establecen un conjunto de actividades que se denominan entradas que representan los recursos que requiere el sistema para mantener sus operaciones en cada proceso, de cuya transformación exportan mediante salidas los recursos para continuar el ciclo. Tal como se evidencia en la figura N° 6 las entradas y salidas del proceso plan estratégico.

Figura 6.

© Fuente: Sistemas de control interno para organizaciones

Desde	Entradas	Salidas	Hacia					
PO5	Reportes de costo/beneficio	Plan estratégico de TI	PO2	PO6	PO8	PO9	A11	DS1
PO9	Evaluación del riesgo	Plan táctico de TI	PO2	PO6	PO9	A11	DS1	
PO10	Portafolio de proyectos actualizado	Portafolios de proyectos de TI	PO5	PO6	PO10	A16		
DS1	Requerimientos servicio nuevos/ actualizados: portafolio de servicios	Portafolio de servicios de TI	PO5	PO6	PO9	DS1		
*	Estrategia y prioridades del negocio	Estrategia de contratación externa de TI	DS2					
*	Portafolio de programas	Estrategia de adquisición de TI	A15					
ME1	Entradas a desempeño de planeación de TI							
ME4	Reporte estado de gobierno de TI; dirección estratégica de la empresa de TI.							

Entradas y salidas (Directrices generales)

Cobit proporciona un juego de materiales que requieren de su apropiado estudio para comprender todo lo que abarca este marco de referencia, sobre todo, en la versión 4.1, que incorpora determinados contenidos para ayudar al usuario a desarrollar y evaluar los controles internos en TI y los riesgos relacionados.

Cualquier dimensión de cobit puede ser usada para comprender el ambiente de control y los cuatro dominios antes mencionados, siendo el primero. Planificación y organización. Por ejemplo, cada proceso TI debe ser evaluado a través de los siguientes pasos, los que se inician con el dominio PO, Planeamiento y organización, y el objetivo de control PO1 es definir el plan estratégico TI. Este reconoce que la planeación estratégica es necesaria, para así poder manejar sus procesos y hacer uso de los activos de TI de manera

óptima, y que estos vayan acordes a lo que la organización o el negocio requiere". (p.233)

### **Estándar ISO 31000:2009**

Según Chicano Tejada (2015) nos dice que: "En cuanto a gestión, análisis y tratamiento de riesgos existe un estándar ISO (ISO 31000:2009) que incluye una serie de recomendaciones y actividades para que las organizaciones gestión en sus riesgos de un modo más adecuado y eficaz. No obstante, aunque sea un estándar, no ofrece certificación, por lo que solo debe ser tomada como una guía en la que encontrar los principios, el marco y el proceso para lograr una gestión de riesgos transparente, sistemática y creíble. A raíz de la ISO31000:2009, las organizaciones deben ser capaces de desarrollar sus propias estrategias de gestión de riesgos. (p.131)

### **Dimensiones para la evaluación del riesgo según la ISO 31000:2009:**

Según Oviedo B. (2015) nos dice que: "Para una mayor eficacia, la Gestión del Riesgo en una organización debe tener en cuenta los siguientes principios:

1. Crea valor. Contribuye a la consecución de objetivos, así como la mejora de aspectos tales como la seguridad y salud laboral, cumplimiento legal y normativo, protección ambiental, etc.
2. Está integrada en los procesos de una organización. No debe ser entendida como una actividad aislada sino como parte de las actividades y procesos principales de una organización.
3. Forma parte de la toma de decisiones. La Gestión del Riesgo ayuda a la toma de decisiones evaluando la información sobre las distintas alternativas.
4. Trata explícitamente la incertidumbre. La Gestión del Riesgo trata aquellos aspectos de la toma de decisiones que son inciertos, la naturaleza de esa incertidumbre y como puede tratarse.
5. Es sistemática, estructurada y adecuada. Contribuye a la eficiencia y, consecuentemente, a la obtención de resultados fiables.
6. Está basada en la mejor información disponible. Las entradas del proceso de Gestión del Riesgo están basadas en fuentes de información como la experiencia, la observación, las previsiones y la opinión de expertos.

7. Está hecha a medida. La Gestión del Riesgo está alineada con el contexto externo e interno de la organización y con su perfil de riesgo.
8. Tiene en cuenta factores humanos y culturales. Reconoce la capacidad, percepción e intenciones de la gente, tanto externa como interna, que puede facilitar o dificultar la consecución de los objetivos de la organización.
9. Es transparente e inclusiva. La apropiada y oportuna participación de los grupos de interés (Stakeholders) y, en particular, de los responsables a todos los niveles, asegura que la Gestión del Riesgo permanece relevante y actualizada.
10. Es dinámica, iterativa y sensible al cambio. La organización debe velar por que la gestión del riesgo detecte y responda a los cambios de la empresa.
11. Facilita la mejora continua de la organización. Las organizaciones deberían desarrollar e implementar estrategias para mejorar continuamente, tanto en la gestión del riesgo como en cualquier otro aspecto de la organización” (p.19)

## **MAGERIT**

Según Giménez Albacete (2015) nos dice que: “La inversión de esfuerzo en seguridad de la información debe realizarse según un método de análisis y gestión de riesgos. Magerit es una norma española, que cumple perfectamente este cometido, y cuyo análisis consta de 5 pasos: evaluación de activos, evaluación de amenazas en términos de la degradación que permita calcular el impacto, y de la frecuencia que determine el riesgo. Magerit aporta una clasificación de los activos, y una metodología para ordenar sus dependencias jerárquicas. También aporta un catálogo de amenazas, incluida la naturaleza del activo afectado, y la prioridad de la dimensión de seguridad afectada. De acuerdo con la terminología de la norma ISO 31000, MAGERIT es denominado un proceso para el área de gestión de riesgos, es decir, MAGERIT hace posible que dentro del proceso de la gestión de riesgos se pueda implementar un marco de trabajo y así ayudar al los miembros de gobierno y gerencia tomar decisiones acorde a los riesgos que las tecnologías de información generan.

MAGERIT estudia los riesgos generados por los sistemas de información y el entorno asociado a ellos, asumiendo por riesgo la posibilidad de que se produzca un daño o perjuicio. Recomienda las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados. Para MAGERIT, las tareas de análisis y tratamiento de los riesgos no son un fin en sí mismas, sino que se encajan en la actividad continua de gestión de la seguridad.” (p.3)

### **Dimensiones para la evaluación del riesgo según Magerit:**

Según Correa Visbal (2014) manifiesta que: “Las dimensiones para la evaluación de Magerit son:

#### **a) Toma de datos y procesos de información:**

En esta etapa se determina el alcance establecido para el SGSI, tomando en cuenta todos aquellos procesos involucrados dentro de la empresa, así como el análisis de los riesgos que produzcan los riesgos críticos. Aquí también se determina el nivel alcanzado de criticidad en las incidencias presentadas.

#### **b) Establecimiento de parámetros:**

En esta etapa es importante determinar que parámetros se utilizaran en el proceso de análisis de riesgos, empezando por:

1. Valor de los activos: se determina el valor económico de cada activo de la organización. Estos valores deben estar determinados por el valor independiente de reposición, configuración, uso, pérdida de oportunidad. Para ello se debe asignar una escala que permitirá determinar su nivel, tal como: muy alta, alta, media, baja, muy baja; luego de ellos a cada nivel se le asigna un valor económico.

2. Vulnerabilidad: aquí se evalúa las veces en las que una organización sufre amenazas concretas. Aquí también es recomendable asignarle una valoración a cada amenaza, como por ejemplo extrema frecuencia que quiere decir que sucede una vez al día o más, alta que quiere decir que es una vez cada dos semanas, media que ocurre una vez cada dos meses y baja que ocurre solo una vez al año, acorde a estas valoraciones se puede estimar las veces que ocurren por año.

3. Impacto: es el grado o porcentaje que el activo sufre al ocurrir un incidente, a estos parámetros también se les asignan una calificación o valoración como por ejemplo: muy alto (100%), alto (75%), medio (50%), bajo (20%) y muy bajo (5%)”.

4. Efectividad del control de seguridad: Mide del impacto que tendrá las medidas asignadas para proteger los riesgos detectados, determinando cuanto reducen dichas medidas implementadas para su prevención, utilizando una calificación como: muy alto (95%), alto (75%), medio (50%), bajo (30%), muy bajo (10%). Se debe tener en cuenta que estos han de ser utilizados siempre, durante todo el proceso o de lo contrario no se darán los resultados esperados.

a) **Análisis de activos:** identificar todos los activos con los que cuenta la empresa y que requiere para la realización de sus actividades; estando acorde a sus alcances predefinidos. Los activos se pueden clasificar en: físicos, lógicos, de personal, de entorno e infraestructura, intangibles. Se asignará una valoración de acuerdo a los parámetros descritos anteriormente”.

b) **Análisis de amenazas:** son todas aquellos incidentes ocurridos en la organización, los cuales producen que las empresas presenten deficiencias. Se clasifican en:

1. Accidentes: situaciones que no se dan voluntariamente y que en su mayoría no pueden ser evitadas. Pueden ser de los siguientes tipos: accidente físico, avería, interrupción de servicios esenciales, accidentes mecánicos o electromagnéticos”.

2. Errores: acciones realizadas de forma involuntaria, por el desarrollo de las actividades propias de la empresa, ya sea por desconocimiento o descuido del personal o terceros. Dentro de estos se pueden encontrar: errores en la utilización de los sistemas, en el desarrollo de aplicaciones, de actualización en los sistemas o aplicaciones, en la monitorización, de compatibilidad entre aplicaciones, inesperados (virus, troyanos, etc.)”.

3. “Amenazas intencionales presenciales: son provocadas por los trabajadores de la empresa de manera intencional, sabiendo aun el daño que ocasionan ciertas acciones ya sea físico o lógico. Se pueden encontrar las

siguientes: acceso físico no autorizado, acceso lógico no autorizado, indisponibilidad de recursos, filtración de datos a terceros”.

4. Amenazas intencionales remotas: son aquellas realizadas por personas que no son de la empresa, y aun así logran dañar la empresa. Se pueden encontrar, entre otras, las siguientes: acceso lógico no autorizado, suplantación del origen en una comunicación, gusanos, denegación de servicio”.

c) **Establecimiento de vulnerabilidades:** son aquellos puntos sueltos no identificados que tienen las empresas, y que dan cabida al ingreso de amenazas, dando como consecuencia el daño de los activos. Se debe tener claro que, sin vulnerabilidad, la amenaza no puede dañar un activo y que las vulnerabilidades por sí mismas no provocan daños, sino que estos son siempre provocados por las amenazas”.

d) **Establecimiento de impactos:** son aquellos que ocurren en la empresa como consecuencia de las amenazas presentadas, aprovechando una vulnerabilidad, afecte un activo. Al analizar los impactos, se deben tener en cuenta los siguientes aspectos: el resultado de la agresión de una amenaza sobre un activo, el efecto sobre cada activo, el valor económico de las pérdidas producidas en cada activo, las pérdidas cuantitativas o cualitativas”.

e) **Análisis de riesgo intrínseco:** el riesgo intrínseco en la metodología utilizada se toma como el riesgo en la situación actual de la empresa que se analiza. De acuerdo a esto, con los valores analizados en los puntos descritos anteriormente, sólo es necesario multiplicar los valores así:  $\text{Riesgo} = \text{Valor del activo} \times \text{Vulnerabilidad} \times \text{Impacto}$ ”.

f) **Influencia de salvaguardas:** las salvaguardas son los que controlan la seguridad, para ello se clasifican en dos tipos: preventivas (reducen las vulnerabilidades) y correctivas (reducen el impacto de las amenazas). En esta fase se trata de encontrar las soluciones de seguridad que existan en el mercado de ambos tipos”.

g) **Análisis de riesgos efectivo:** se evalúa como reducir los riesgos acordes a las salvaguardas identificados para cada situación, es decir, se calcula el riesgo efectivo que tendría la empresa para cada una de las amenazas identificadas. Este cálculo se realiza de la siguiente manera:



Riesgo efectivo = Riesgo intrínseco × Porcentaje de disminución de vulnerabilidad × Porcentaje de disminución de impacto”.

h) **Evaluación de riesgos:** En esta etapa se toman las decisiones por parte de la organización, decidiendo que medidas de seguridad implementar, guiándose de la lista de salvaguardas que permitirán reducir los riesgos. Las empresas requieren reducir los riesgos que han detectado hasta situarlos por debajo del denominado "umbral de riesgos" y que represente un menor costo”.

**Comparación entre las metodologías MAGERIT, ISO 31000:2009 y COBIT**

Todas las metodologías mencionadas son utilizadas para la gestión de riesgos, sin embargo, algunas poseen ventajas que otras no, que puede ser de gran significancia a la hora de elegir cual es la adecuada para la implementación en las empresas. Por ello, en la siguiente tabla N°3 se muestra la comparativa entre dichas metodologías:

Tabla N°3. Cuadro comparativo de metodologías

CARACTERÍSTICAS	MAGERIT	ISO 31000:2009	COBIT
Autorización para la implementación	Es de uso público, no necesita autorización previa para el uso.	Para implementar esta metodología se necesita de una persona certificada	Para implementar esta metodología se necesita de una persona certificada
Enfoque	Esta enfocado al la gestión de riesgos.	Esta enfocado al la gestión de riesgos.	No existe un estándar que abarque todos los temas (gestión, seguridad, calidad, desarrollo, continuidad, etc.).
Estándares de tratamiento	Investiga los riesgos de TI y los mitiga	Para riesgos tecnológicos con modelamiento UML	Ayuda a los administradores a entender como los asuntos de seguridad y control benefician sus áreas de operación

© Fuente: Elaboración propia

**Selección de la metodología para la evaluación de los factores de riesgo de tecnologías de información:**

Se reunió a tres expertos quienes realizaron la evaluación de las metodologías ISO 31000, Cobit y Magerit, y para ello se les entregó el instrumento de validación de expertos como se evidencia en el anexo 6, así mismo los valores asignados a la evaluación se evidencian en la tabla N°4.

Tabla N° 4. Validación de la selección de la metodología por expertos.

EXPERTOS	GRADO ACADÉMICO	ISO 31000:2009	COBIT	MAGERIT
Ordoñez Pérez, Adilio Christian	Doctor/Magister en Ingeniería de sistemas	25	23	30
Guevara Jiménez, Jorge	Magíster en Administración estratégica para empresas	28	27	30
Gálvez Tapia, Orleans Moisés	Magíster en Ingeniería de sistemas	28	18	30
<b>TOTAL</b>		<b>81</b>	<b>68</b>	<b>90</b>

© Fuente: Elaboración propia

De acuerdo a la evaluación de los expertos, la metodología ISO 31000:2009 alcanzó 81 puntos, seguido de Cobit con 68 puntos, la mayor puntuación alcanzada con 90 puntos corresponde a la metodología Magerit, por lo tanto, se desarrollará la metodología Magerit.

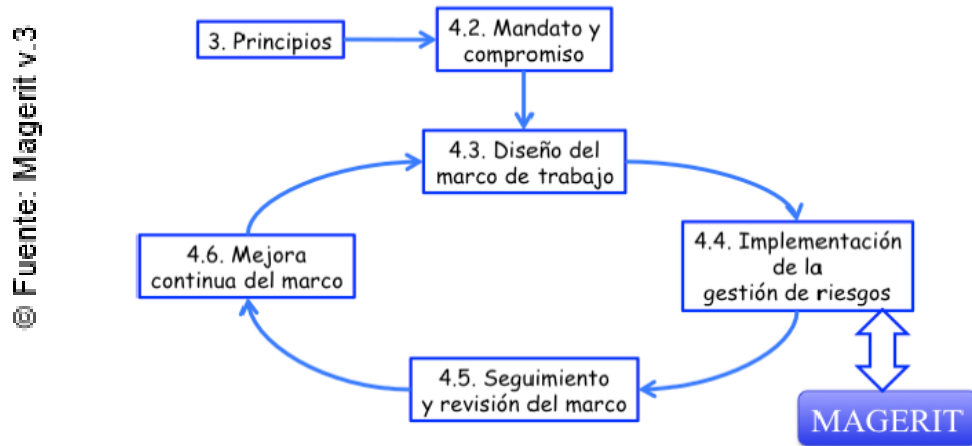
Si bien es cierto, tanto la ISO 31000: 2009 como Cobit pueden implementarse para la gestión de riesgos siendo estos los más conocidos, existen otras alternativas como lo es en este caso MAGERIT V.3 una metodología de análisis y gestión de riesgos elaborada por el *Consejo Superior de Administración Electrónica de España*, el cual a mi parecer ofrece un método sistemático para el análisis de riesgos derivado del uso de las tecnologías de información, el cual nos permite implementar medidas de control más adecuados que nos permitan tener los riesgos mitigados, además que posee una guía completa con el paso a paso de cómo realizar el análisis de los riesgos, el factor que hizo que optará por implementar esta metodología es que se ajusta a empresas pequeñas que recién se inician en la gestión de riesgos y la seguridad de sus activos, ya que no necesita que quién lo implemente sea un experto certificado, gracias a que como se mencionó posee una serie de libros, guías y una herramienta de software para ello.

### **Metodología seleccionada: MAGERIT**

De acuerdo con la normativa ISO 31000, nos dice que: “Magerit es conocido como el “Proceso de Gestión de los Riesgos”, tal y como lo menciona en su sección 4.4 (“Implementación de la Gestión de los Riesgos”) dentro del “Marco de Gestión de Riesgos”. MAGERIT permite la implementación de un Proceso de Gestión de Riesgos basándose en un marco de trabajo para que

las organizaciones tomen decisiones tomando en cuenta los riesgos que puede producir el uso de tecnologías de la información.”

Figura.7



Marco de trabajo de la gestión de riesgos.

Según Magerit 3.0 (2012) define que: “Existen varias formas de aproximación a lo que son los soportes para los sistemas TIC: guías informales, aproximaciones metódicas y herramientas de soporte. Lo que se busca es la objetividad para el análisis de riesgos, para así determinar cuan seguros son o inseguros y no vivir engañados. El gran reto es la aproximación a la complejidad de los problemas que se presentan, se considera complejo ya que hay muchos elementos que se deben considerar y que, si no se hace un control riguroso, las conclusiones obtenidas no será de confianza. Por ello Magerit realiza una aproximación metódica, evitando así la improvisación, sin depender de la arbitrariedad de los analistas.

Magerit establece los siguientes objetivos:

Directos:

1. Concientizar a los responsables de cada empresa de los riesgos que se presenten y la necesidad de gestionarlos.
2. Ofrecer un método que sea sistemático y así analizar los riesgos que se derivan del uso de las tecnologías de información y de las comunicaciones.
3. Ayudar a descubrir y a planificar los tratamientos a tiempo para mantener así los riesgos controlados.

4. Mantener a las organizaciones preparadas para los procesos de evaluación, las auditorías, certificaciones y/o acreditaciones con las que requieran contar. Se busca también la uniformidad de los informes que detallan los hallazgos y los resultados de las actividades de análisis y de la gestión de riesgos:

#### **Modelo de valor**

Es la caracterización del valor representativo que se le asigna a cada activo de la organización, así como la dependencia que existe entre ellas.

#### **Mapa de riesgos**

La relación entre las amenazas a las que están expuestos los activos.

#### **Declaración de aplicabilidad**

Este aplica a las salvaguardas en donde se determina si son de aplicación bajo estudio en el sistema de información o si por el contrario carece de sentido alguno.

#### **Evaluación de salvaguardas**

Realiza el análisis del nivel de la eficacia de las salvaguardas actuales, y su relación con el riesgo al que se enfrentan.

#### **Estado de riesgo**

Caracterización de cada uno de los activos acorde a su riesgo residual; es decir, a lo que se enfrenta tomando en cuenta las salvaguardas desplegadas.

#### **Informe de insuficiencias**

Ausencia o debilidad de las salvaguardas 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.” (p.8)

#### **Organización de las Guías**

La metodología consta de tres volúmenes:

Volumen 1: Método

Volumen 2: Catalogo de Elementos

Volumen 3: Guía de Técnicas

### **Volumen 1: Método**

Según Magerit 3.0 (2012) “Esta guía está estructurada de la siguiente manera:

El capítulo 1: Es una fase introductoria a esta metodología, pronunciando que organismos lo crearon.

El capítulo 2: presenta sus conceptos de manera informal. Se tomand las actividades de análisis y de tratamiento dentro de los procesos integrales de la gestión de riesgos.

El capítulo 3: Formaliza las tareas de análisis de los riesgos.

El capítulo 4: describe diversas opciones y criterios para el tratamiento de los riesgos y formaliza cada actividad de la gestión de riesgos.

El capítulo 5: se da prioridad a los proyectos de análisis de riesgos, en donde se realizan los primeros análisis de riesgos de un sistema y ocasionalmente cuando hay cambios dástricos y hay que volver a hacer el modelo.

El capítulo 6: Formalizar las actividades sobre planes de seguridad, también llamados planes directores o planes estratégicos.

El capítulo 7: da prioridad al desarrollo de sistemas de información y cómo el análisis de riesgos sirve para gestionar la seguridad del producto final desde su concepción inicial hasta su puesta en producción, así como a la protección del propio proceso de desarrollo.

El capítulo 8: Prevé problemas que aparecen con regularidad cuando se realizan análisis de riesgos.

Los apéndices recogen material de consulta:

1. Un glosario.
2. Referencias bibliográficas que sirven para el desarrollo de esta metodología.
3. Referencias al marco legal que encuadra las tareas de análisis y gestión en la Administración Pública Española.
4. El marco normativo de evaluación y certificación.

5. Las características que se requieren de las herramientas, presentes o futuras, para soportar el proceso de análisis y gestión de riesgos.
6. Una guía comparativa de cómo Magerit versión 1 ha evolucionado a la versión 2 y a esta versión 3.” (p.12)

### **Volumen II: Catalogo de Elementos**

Según Magerit 3.0 (2012) “El volumen II complementa al volumen I brindando ejemplos en el capítulo II que sirve para la aplicación de esta metodología.

- Tipos de activos
- Dimensiones y criterios de valoración
- Amenazas
- Salvaguardas

En este libro se determinan dos objetivos:

1. Facilitar la labor de los empleados que acometen el proyecto, en el sentido de ofrecerles elementos estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.
2. Homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan comparar e incluso integrar análisis realizados por diferentes equipos.” (p.1)

### **Volumen III: Guía de Técnicas**

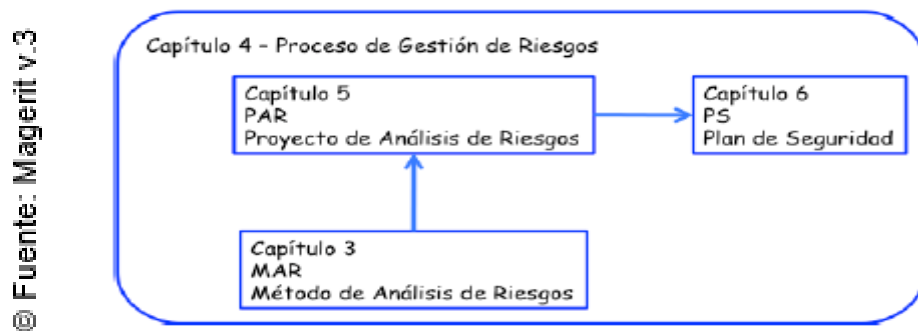
Según Magerit 3.0 (2012) “Aporta luz adicional y orientación sobre algunas técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos:

- Técnicas específicas para el análisis de riesgos
- Análisis mediante tablas
- Análisis algorítmico
- Árboles de ataque
- Técnicas generales
- Técnicas gráficas
- Sesiones de trabajo: entrevistas, reuniones y presentaciones

Valoración Delphi Se trata de una guía de consulta. Según el lector avance por las tareas del proyecto, se le recomendará el uso de ciertas técnicas específicas, de las que esta guía busca ser una introducción, así como proporcionar referencias para que el lector profundice en las técnicas presentadas”. (p.1)

## Proceso de Gestión de Riesgos

Figura.8



Actividades formalizadas

Según Magerit v.3 (2012) “El proceso de gestión de riesgos debe identificar y tratar urgentemente los riesgos críticos, pudiendo ir tratando progresivamente riesgos de menor criticidad”. (p.13)

Otra de las fases que aplica magerit es el método de análisis de riesgos el cual incluye está conformado de la siguiente manera:

### MÉTODO DE ANÁLISIS DE RIESGOS

Según Magerit v.3 (2012): “El análisis de riesgos se define como la aproximación metódica para analizar el riesgo siguiendo unos pasos pautados:

- Determinar los activos más importantes para la organización, su valor, de tal forma que no afecte el coste.
- Determinar a qué tipo de amenazas están expuestos dichos activos.
- Determinar qué salvaguardas están disponibles y que tan eficaces son frente al riesgo.

- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza”. (p.22)

## **PROYECTO DE ANÁLISIS DE RIESGOS**

Según Magerit v.3 (2012, p.62) “Cuando el análisis de los riesgos se realiza desde cero, se utilizan muchos recursos es mejor planificar todo eso dentro del proyecto, sea interno o se haga uso de una consultoría externa

En esta parte se debe tomar en cuenta lo necesario para que el proyecto se realice con éxito.

- PARTE 1 - Actividades preliminares
- PARTE 2 - Elaboración del análisis de riesgos
- PARTE 3 - Comunicación de resultados

### **Actividades preliminares**

En esta etapa se realizan las siguientes tareas que se deben tener en cuenta antes de hacer un análisis de riesgos.

#### **1.-Estudio de oportunidad**

En esta etapa del proyecto se realiza la factibilidad de lo que implica el tipo de proyecto dentro de cualquier organización.

#### **2.-Determinación del alcance del proyecto**

En esta etapa los objetivos deben ser planteado antes de que se finalice el proyecto logrando determinar y dominios que debe tener como alcance el proyecto. Para que el resultado de dicha actividad sea el perfil y el proyecto requiere en cuanto a el análisis y la gestión de riesgo.

#### **3.-Planificación del proyecto**

En esta etapa ya debe el análisis de riesgo ser ejecutados dentro del proyecto. Por lo tanto, se debe recabar toda la información a través de entrevistas y cuestionarios a todos aquellos involucrados que interactúan con los sistemas de información. Para ello es necesario elaborar un plan de trabajo para la ejecución del proyecto.



#### **4.-Lanzamiento del proyecto**

En esta etapa del proyecto es necesario elaborar las preguntas del cuestionario para la recopilación de información. Dicho resultado estará constituido por:

- El cuestionario para cada entrevista
- El Catálogo que contiene el tipo de activo
- La relación que existe entre cada dimensión de seguridad
- Los criterios de valoración.

En la siguiente etapa se realiza lo que es la elaboración de los análisis de riesgos. Según Magerit v.3 (2012, p.70) “Se desarrolla de la siguiente manera:

#### **5.-Elaboración del análisis de riesgos**

La mayoría de las actividades tienen que tener de dos a tres entrevistas con los empleados.

- La primera entrevista debe contener todas las necesidades que se requieren.
- En la segunda entrevista se debe validar que todos los datos se encuentran completos y hayan sido entendido a la perfección.
- Acorde a las circunstancias podrá ser necesario que se realice una entrevista extra.
- En todas aquellas tareas mencionadas debe cuidarte de manejar toda la documentación escrita mediante un proceso formal de gestión

#### **6.-Comunicación de resultados**

Para el informe que será presentado al final se debe mostrar gráficos de cada escenario en donde en el impacto ha sido mayor, así como aquellos que corrieron niveles de riesgos peligrosos en todos sus indicadores.

#### **7.-Documentación intermedia**

- Resultados de las entrevistas.
- Documentación auxiliar: planos, organigramas, requisitos, especificaciones, análisis funcionales, cuadernos de carga, manuales de usuario, manuales de explotación, diagramas de flujo de información y de procesos, modelos de datos, etc.
- Análisis de los resultados, con la detección de las áreas críticas claves.

- Información existente utilizable por el proyecto.

## **PLAN DE SEGURIDAD**

Según Magerit v.3 (2012, p.74) “En esta tapa que tiene que tomar en cuenta todos aquellos planes de seguridad establecidos, acorde a cada decisión tomada para el tratamiento de los riesgos. Se identifican las siguientes áreas:

- PS.1 Identificación de proyectos de seguridad
- PS.2 Plan de ejecución
- PS.3 Ejecución

### **Identificación de Proyectos de Seguridad**

Su principal objetivo es:

- Elaborar un grupo de programa sobre seguridad. Un programa que permita agrupar todas las actividades y tareas y aplicar la seguridad correspondiente.
- La agrupación debe realizarse según la conveniencia.
- Siempre debe mejorar cada implantación de una serie de salvaguardar los cuales llevarán el impacto y el riesgo obtenido a niveles residuales determinados.

### **Plan de Ejecución**

El principal objetivo es agrupar de forma ordenada temporalmente todos aquellos programas de seguridad.

La duración que debe tener cada proyecto de seguridad es muy importante, por ello es que se debe establecer los siguientes factores:

- La criticidad, gravedad o conveniencia de los impactos y riesgos que se afrontan, teniendo máxima prioridad los programas que afronten situación crítica.
- El costo de cada programa
- El personal debe tener la disponibilidad para hacerse cargo y responsabilizarse de la dirección.

Otros aquellos factores como lo son la elaboración del presupuesto de cada año de la empresa, relaciones con otras empresas u organizaciones, la evolución de su marco legal, reglamentario o contractual, etc.

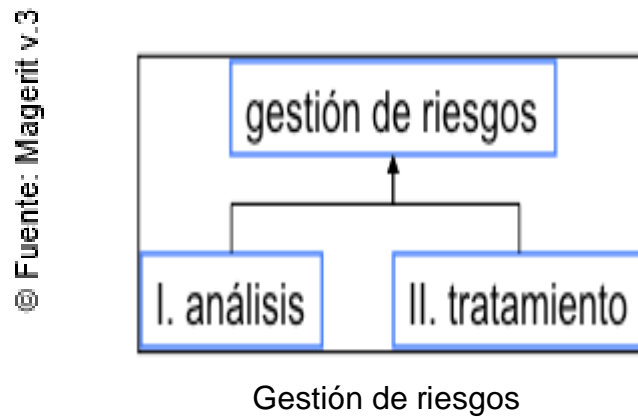
## Ejecución

Poder alcanzar todos los objetivos establecidos en el plan de seguridad para cada proyecto. Lo que se quiere alcanzar cuando se realiza cada tarea es:

- Implantar salvaguardas
- Modelo de valor actualizado
- Mapa de riesgo actualizado
- Estado de riesgo actualizado”.

## Proceso de gestión de riesgos

Figura.9



Según Magerit v.3 (2012, p.19) “Para realizar un correcto proceso de Gestión de Riesgos se deberá ejecutar dos grandes tareas:

### **Análisis de riesgos**

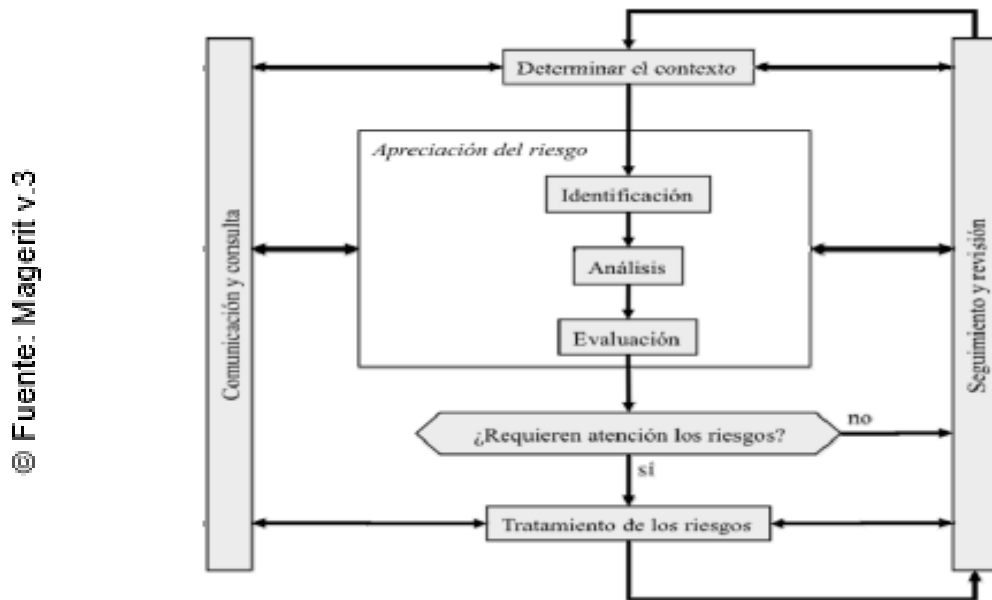
Que permite determinar qué tiene la organización y estimar lo que podría pasar.

### **Tratamiento de los riesgos**

Que permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la dirección asume.

Ambas actividades, análisis y tratamiento se combinan en el proceso denominado Gestión de Riesgos”.

Figura.10



Proceso de Gestión de riesgos

Según Magerit v.3 (2012, p.20) “Formalmente, la gestión de los riesgos está estructurada de forma metódica en las normas ISO como se ve en la figura anterior:

**La Determinación del contexto**

Lleva a una determinación de los parámetros y condicionantes externos e internos que permiten delimitar una política que se seguirá para gestionar los riesgos.

**La Identificación de los riesgos**

Busca una relación de los posibles puntos de peligro. Lo que se identifique será analizado en la siguiente etapa.

**El análisis de riesgos**

busca calificar los riesgos identificados, bien cuantificando sus consecuencias (análisis cuantitativo), bien ordenando su importancia relativa (análisis cualitativo). De una u otra forma, como resultado del análisis tendremos una visión estructurada que nos permita centrarnos en lo más importante.

## **La evaluación de los riesgos**

Aquí entran factores de percepción, de estrategia y de política permitiendo tomar decisiones respecto de qué riesgos se aceptan y cuáles no, así como de en qué circunstancias podemos aceptar un riesgo o trabajar en su tratamiento.

## **El tratamiento de los riesgos**

recopila las actividades encaminadas a modificar la situación de riesgo. Es una actividad que presenta numerosas opciones como veremos más adelante”.

## **HERRAMIENTA PILAR**

Según Magerit v.3 (2012, p.125) nos muestra una herramienta llamada PILAR, la cual: “es el acrónimo de “Procedimiento Informático-Lógico para el Análisis de Riesgos” es una herramienta desarrollada bajo especificación del Centro Nacional de Inteligencia para soportar el análisis de riesgos de sistemas de información siguiendo la metodología Magerit.

La herramienta soporta todas las fases del método Magerit:

- Determina los activos: identificación, clasificación, dependencias y valoración.
- Determina las amenazas.
- Evaluación de las salvaguardas.
- Estimación de los impactos

Los resultados se presentan en varios formatos: informes RTF, gráficas y tablas para incorporar a hojas de cálculo. De esta forma es posible elaborar diferentes tipos de informes y presentaciones de los resultados.”

## **1.4 Formulación del problema**

### **Problema General**

¿Qué relación existe entre los factores de riesgo en tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC?

## **Problemas Específicos**

¿Qué relación existe entre los factores de riesgo en tecnologías de información y el eficiente desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC?

¿Qué relación existe entre los factores de riesgo en tecnologías de información y el eficaz desempeño del webcast en las empresas Proyectos, Asesorías y Construcciones ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC?

¿Qué relación existe entre los factores de riesgo en tecnologías de información y la calidad de servicio en el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC?

### **1.5 Justificación del estudio**

#### **Justificación institucional**

Según ISOTools (2013), manifiesta que: “Todos los requisitos que demanda la norma ISO 31,000 se pueden aplicar a todo tipo de nivel, objetivo y áreas de la empresa. Así como al nivel estratégico como a cualquier otra actividad realizada. También ayuda a poder gestionar sus operaciones, proyectos, productos y servicios.” (p.1)

El presente proyecto de investigación contribuirá para que las organizaciones que deseen implementar webcast funcionen óptimamente, permitiendo así cumplir con sus objetivos, como lo es el caso de las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC cuya misión tiene como principio primordial brindarle un servicio de calidad al cliente.

#### **Justificación operativa**

Según IBNORCA (2018), manifiesta que: “A través de la implementación de los principios y la guía de la ISO 31,000 en la empresa, se podrá mejorar significativamente su eficacia operativa, la gobernanza y la confianza en todas las partes interesadas, así como minimizar cualquier pérdida. Esta norma

también permite fomentar el desempeño y mejora en la seguridad y la salud, estableciendo una base sólida para la ayuda en la toma de decisiones y así lograr una gestión proactiva en cada una de sus áreas.” (p.1)

El presente proyecto de investigación contribuirá para que los procesos de la organización funcionen de manera óptima, previniendo riesgos para su operatividad efectiva.

### **Justificación económica**

Según Dihane Lois (2013), manifiesta que: “El dinero utilizado en la compra de dispositivos que permitan prevenir los accidentes ya no es visto como un gasto sino como una inversión.” (p.1)

El presente proyecto de investigación contribuirá para que la pérdida económica generada por los programas no emitidos debido a la falta de control y evaluación de riesgos disminuya, siendo una suma considerable ya que por cada programa no emitido se puede llegar a perder al mes unos 3200 soles aproximadamente, ya que cada sponsor auspicia de 3 a cuatro programas, siendo al año 38400 soles, tomando en cuenta que cada día transmite un epicentro diferente y que no sólo existe un auspiciador por programa.

### **Justificación tecnológica**

Según Ciceri (2013), manifiesta que: “Todas las organizaciones se enfrentan de manera continua a la competencia del mercado global, existe un gran reconocimiento al papel central que juega la tecnología como determinante del éxito. Como prueba de ello, cada empresa ha optado por adoptar nuevas tecnologías, así como también introducir nuevos productos sofisticados de tecnología. Es por ello que es importante desarrollar estrategias tecnológicas tomando en cuenta que estas deben estar alineadas e integradas a las estrategias generales del negocio.” (p.1)

El presente proyecto de investigación contribuirá para que se tomen en cuenta los requerimientos mínimos necesarios en cuanto a tecnologías de información refiere para el desempeño óptimo del webcast.

## 1.6 Hipótesis

### Hipótesis General

**Ha:** Existe una relación positiva entre los factores de riesgo en tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

### Hipótesis Específicas

**H1:** Existe una relación positiva entre los factores de riesgo en tecnologías de información y el eficiente desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

**H2:** Existe una relación positiva entre los factores de riesgo en tecnologías de información y el eficaz desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

**H3:** Existe una relación positiva entre los factores de riesgo en tecnologías de información y la calidad de servicio en el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

## 1.7 Objetivos.

### Objetivo General

Determinar la relación entre los factores de riesgo en tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

### Objetivos Específicos

Determinar la relación entre los factores de riesgo en tecnologías de información y el eficaz desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.



Determinar la relación entre los factores de riesgo en tecnologías de información y el eficiente desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

Determinar la relación entre los factores de riesgo en tecnologías de información y la calidad de servicio en el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC

.

## **II. MÉTODO**

### **2.1 Diseño de investigación**

## **Método de investigación: Hipotético deductivo**

Cegarra Sánchez (2014) define que: “El método hipotético-deductivo se utiliza tanto en la vida ordinaria como en la investigación científica a través del camino lógico para encontrar la solución a los problemas que podemos plantearnos. Consiste en determinar alguna hipótesis acerca de las posibles soluciones al problema planteado y en comprobar con los datos disponibles si estos están disponibles si estos están de acuerdo con aquellas.” (p.82).

Por ello, es que se estableció este método para el desarrollo de la investigación, en donde a través de las hipótesis planteamos una solución al problema del proceso del cual es objeto nuestro estudio.

## **Tipo de investigación**

La presente investigación es explicativa-correlacional-básica porque se da a conocer una herramienta que ayudara a la solución de la problemática en el desempeño del webcast, el cual es el uso de la metodología Magerit para la prevención de riesgos.

Yáñez Deysi (2018) manifiesta que: “La investigación explicativa está orientada a determinar las causas que dan pie al origen de ciertos fenómenos. Consiste en un tipo de investigación cuantitativa la cual permite descubrir el por qué y el para qué de cada fenómeno.” (p.1).

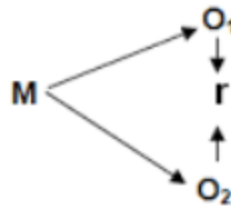
Mejía Jervis. (2018) manifiesta que: “La investigación correlacional tiene sus principios y bases en diversas pruebas estadísticas que muestran los coeficientes de correlación entre sus variables. Dichas coeficiente están representados numéricamente para así indicar la dirección y la fuerza de una relación.” (p.1).

Rodríguez Daniela. (2018) manifiesta que: “La investigación básica o fundamental busca que el conocimiento de los fenómenos y de la realidad puedan contribuir con la sociedad, ya que cada vez está más avanzado y así poder responder a cada reto que presente la humanidad. Este tipo de investigación no busca que sea aplicada prácticamente si

no que busca aumentar el conocimiento para hacer posible responder a preguntas o para que esos conocimientos puedan ser aplicados en otras investigaciones.” (p.1).

Cómo se muestra en la figura 6, el diseño correlacional está conformado por:

Figura 11.



Diseño correlacional

Donde:

**M=** Atogapan y el Grupo HCM Comunicaciones

**O1=** Variable 1: Factores de riesgo de tecnología de información.

**O2 =** Variable 2: Desempeño del webcast.

**r =** Correlación de los factores de riesgo de tecnología de información y el desempeño del webcast.

## 2.2 Variables, operacionalización

### Variables

#### Definición conceptual

**V1: Factores de riesgo de las tecnologías de información:** Según Baca, Solares y Acosta (2014) lo definen como: “un concepto conocido como sistema de medición de valor agregado de la productividad, como una propuesta e intento para identificar y evaluar el impacto de la TI sobre el desempeño de las unidades de negocio que están siendo influidas por la tecnología de la información.” (p.168)

**V2: Desempeño del webcast:** Según Gariboldi (2015) lo definen como: “Nuevas posibilidades surgen con la transmisión de programas televisivos o radiales efectuadas a través de Internet. Este modo de operar llamado webcast no alcanza niveles óptimos como para sustituir las transmisiones regulares. Se todas maneras a medida que superen sus limitaciones en la forma de transmitir, se espera lograr llegar a niveles superiores de imagen y calidad como la televisión actual”. (p.36)

### **Definición operacional**

**VI: Factores de riesgo de las tecnologías de información:** Son circunstancias o situaciones que aumentan las probabilidades de riesgo en tecnologías de información que pueden afectar el desempeño del webcast en la empresa Atogapan S.A, ya que actualmente no cuenta con medidas de prevención, control y evaluación ante posibles riesgos. Por ello, para evaluar y gestionar dichos factores de riesgo, se aplicará la metodología de Magerit en su V.3.

**VD: Desempeño del webcast:** Es un resultado que denota la manera en el que el desarrollo del webcast cumple los objetivos planteados, buscando que este se realice de manera óptima, teniendo en cuenta que este sea eficiente, eficaz y ofrezca calidad de servicio.

## Operacionalización de variables

Tabla 5: Operacionalización de las variables

TIPO	VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	ESCALA DE MEDICIÓN
Variable 1	FACTORES DE RIESGO DE LAS TECNOLOGÍAS DE INFORMACIÓN	ES un concepto conocido como sistema de medición de valor agregado de la productividad, como una propuesta e intento para identificar y evaluar el impacto de la TI sobre el desempeño de las unidades de negocio que están siendo influidas por la tecnología de la información	Son circunstancias o situaciones que aumentan las probabilidades de riesgo en tecnologías de información que pueden afectar el desempeño del webcast en la empresa Atogapan S.A, ya que actualmente no cuenta con medidas de prevención, control y evaluación ante posibles riesgos. Por ello, para evaluar y gestionar dichos factores de riesgo, se aplicará la metodología de Magerit en su V.3.	MÉTODO DE ANÁLISIS DE RIESGOS  PROYECTO DE ANÁLISIS DE RIESGO  PLAN DE SEGURIDAD	Ordinal  Ordinal  Ordinal
Variable 2	DESEMPEÑO DEL WEBCAST	Nuevas posibilidades surgen con la transmisión de programas televisivos o radiales efectuadas a través de Internet. Este modo de operar llamado webcast no alcanza niveles óptimos como para sustituir las transmisiones regulares. Se todas maneras a medida que superen sus limitaciones en la forma de transmitir, se espera lograr llegar a niveles superiores de imagen y calidad como la televisión actual	Es un resultado que denota la manera en el que el desarrollo del webcast cumple los objetivos planteados, buscando que este se realice de manera óptima, teniendo en cuenta que este sea eficiente, eficaz y ofrezca calidad de servicio.	EFICIENCIA  EFICACIA  CALIDAD DE SERVICIO	Ordinal  Ordinal  Ordinal

© Fuente: Elaboración propia

Tabla 6: Indicadores

VARIABLE	DIMENSIONES	ITEM	INDICADORES	VALORES	NÍVELES
DESEMPEÑO DEL WEBCAST	EFICIENCIA	1	Mantenimiento de equipos.	(1) Nunca	0 al 1 =Muy bajo
		2	Transmisiones realizadas.	(2) Casi nunca	1.1 al 2= Bajo
		3	Inversión en infraestructura TI.	(3) A veces	2.1 al 3= Regular
		4	Comunicación eficiente entre epicentros.	(4) Casi Siempre	3.1 al 4= Bueno
		5	Realización de procedimientos adicionales.	(5) Siempre	4.1 al 5= Muy bueno
		6	Uso de estándares o guías para el control de riesgos de TI.		
		7	Ancho de banda adecuado para transmisiones en vivo.		
	EFICACIA	8	Transmisiones óptimas.	(1) Nunca	0 al 1 =Muy bajo
		9	Incidencias resueltas eficaces.	(2) Casi nunca	1.1 al 2= Bajo
		10	Interrupciones durante la transmisión.	(3) A veces	2.1 al 3= Regular
		11	La plataforma funciona correctamente.	(4) Casi Siempre	3.1 al 4= Bueno
		12	Capacitación del personal.	(5) Siempre	4.1 al 5= Muy bueno
		13	Uso de guías para el correcto desempeño del webcast.		
		14	Logro de audiencia esperada.		
	CALIDAD DE SERVICIO	15	Uso de guías o manuales sobre calidad.	(1) Nunca	0 al 1 =Muy bajo
		16	Libre acceso a usuarios.	(2) Casi nunca	1.1 al 2= Bajo
		17	Programas emitidos a tiempo.	(3) A veces	2.1 al 3= Regular
		18	Acceso a archivos multimedia fuera de transmisión.	(4) Casi Siempre	3.1 al 4= Alto
		19	Interacción con los usuarios	(5) Siempre	4.1 al 5= Muy Alto
20		Calidad de imagen y audio óptima.			
MÉTODO DE ANÁLISIS DE RIESGOS	1	Determinar activos relevantes para la organización.	(1) Nunca	1 al 1 =Muy bajo	
	2	Determinar a qué amenazas están expuestos a aquellos activos.	(2) Casi nunca	1.1 al 2= Bajo	
	3	Control y mantenimiento de equipos.	(3) A veces	2.1 al 3= Regular	
	4	Estimar el impacto, definido como el daño sobre el activo.	(4) Casi Siempre	3.1 al 4= Alto	
	5	Estimar el riesgo por parte del personal.	(5) Siempre	4.1 al 5= Muy Alto	
	6	Frecuencia de fallas técnicas que representen riesgos.			
	7	Estudio de oportunidad.			
FACTORES DE RIESGO DE LAS TECNOLOGÍAS DE INFORMACIÓN	PROYECTO DE ANÁLISIS DE RIESGO	8	Asignación de responsabilidades.	(1) Nunca	0 al 1 =Muy bajo
		9	Servicios externos contratados adecuados.	(2) Casi nunca	1.1 al 2= Bajo
		10	Determinar estado del funcionamiento de procesos.	(3) A veces	2.1 al 3= Regular
		11	Existencia del personal suficiente para cada proceso.	(4) Casi Siempre	3.1 al 4= Alto
		12	Existencia de concientización e identificación de riesgos por parte del personal.	(5) Siempre	4.1 al 5= Muy alto
		13	Identificación de requerimientos mínimos para evitar los riesgos.		
		14	Capacitaciones para la gestión de riesgos.		
PLAN DE SEGURIDAD	PLAN DE SEGURIDAD	15	Identificación de riesgos con frecuencia.	(1) Nunca	1 al 1 =Muy bajo
		16	Documentación el estado de los procesos.	(2) Casi nunca	1.1 al 2= Bajo
		17	Aplicación de permisos y control de usuarios.	(3) A veces	2.1 al 3= Regular
		18	Licencias actualizadas de software.	(4) Casi Siempre	3.1 al 4= Alto
		19	Ambientes eléctricos estables.	(5) Siempre	4.1 al 5= Muy alto
		20	Realización de informes del estado del desempeño de los procesos.		

© Fuente: Elaboración propia

### 2.3 Población y muestra

#### Población

Según Álvarez Cáceres (2007) define la población como: “El conjunto de elementos, individuos o cosas que es objeto de interés y que se pueden estudiar la totalidad de sus elementos, y si esto no es posible, se pueden estudiar los elementos de una muestra.” (p.219)

Tabla N°7: Distribución de la población

N°	RADIO ATOGAPAN EPICENTROS	N° DE TRABAJADORES
1	Ciudad de México	4
2	Nuevo León	4
3	Estado de México	3
4	Sonora	4
5	Colombia	3
6	Quintana Roo	3
7	Veracruz	4
8	Puebla	3
9	HCM COMUNICACIONES	4
<b>TOTAL</b>		<b>32</b>

© Fuente: Elaboración propia.

La población objeto de estudio está constituida por 32 trabajadores pertenecientes a los epicentros de Radio Atogapan y HCM Comunicaciones.

#### Muestra

Según Álvarez Cáceres (2007) define la muestra como: “El subconjunto de la población seleccionada según un método determinado.” (p.222)

Para determinar el muestreo, aplicaremos la siguiente formula:

$$n = \frac{Z^2 \cdot p \cdot q \cdot N}{e^2 (N - 1) + Z^2 p \cdot q}$$



Dónde

$$\begin{aligned}
 Z^2 &= 1.96 \\
 Q &= 0.5 \\
 P &= 0.5 \\
 E &= 0.05 \text{ (5\% error muestral)} \\
 N &= 32
 \end{aligned}$$

$$n = \frac{Z^2 \cdot p \cdot q \cdot N}{e^2 (N-1) + Z^2 p \cdot q} = \frac{1.96 \times 0.5 \times 0.5 \times 32}{0.05 (32-1) + 1.96 \times (0.5 \times 0.5)} = 30$$

Resultado

$$n = 30$$

Luego de aplicada la fórmula para obtener el muestreo, ha dado como resultado que  $n = 30$ , lo cual quiere decir que los instrumentos de recolección de datos serán aplicados a aquella cantidad determinada de trabajadores para el posterior procesamiento de datos.

### Muestreo

Según Escudero Aragón (2014) define el muestreo como: “La técnica que permite determinar la población de estudio y la muestra representativa de los patrones globales de comportamiento del mercado.” (p.117)

### Muestreo probabilístico

Según Álvarez Cáceres (2007) define el muestreo probabilístico como: “Las técnicas de muestreo que utilizan el azar en la selección de los elementos de la muestra son las probabilísticas.” (p.227)

El muestreo probabilístico nos permite tomar elementos al azar, partiendo de nuestra población

## **Muestreo aleatorio simple**

Según Álvarez Cáceres (2007) define el muestreo aleatorio simple como: “La técnica de muestreo más utilizada, en ella están basados los estimadores y estadísticos de contraste utilizados en la mayoría de los estudios científicos.” (p.227)

Dentro del muestreo probabilístico tenemos el aleatorio simple, que nos permite tomar un grupo de sujetos (nuestra muestra) para el estudio posterior de un grupo más grande como lo es la población total.

## **2.4 Técnicas e instrumentos de recolección de datos, validez y confiabilidad**

### **Técnica**

Según Ibáñez Peinado (2015) define la técnica como: “El último nivel del método científico y reúne los procedimientos por medio de los cuales se observa, se analiza y se manipula la realidad.” (p.69)

La técnica es aquella herramienta que permitirá analizar y observar el objeto de estudio, y registrar así la obtención de información para el posterior uso de la investigación. En la presente investigación, siendo de tipo correlacional, es una pieza fundamental para la recolección de datos.

### **Técnica: Entrevista**

Según Lerma Gonzales (2009) define la entrevista como: “Interacción entre la persona que recolecta la investigación y el entrevistado, ya sea personal o por otro tipo de medio. Se utiliza formulario y se utiliza una guía de temas relevantes.” (p.35)

La entrevista es una técnica de recolección de datos mediante la interrogación, utilizando un instrumento de investigación con la cual se procede a hacer efectiva dicha entrevista.

## Instrumento de investigación: Cuestionario

Según Bernal Torres (2006) define el cuestionario como: “Son un conjunto de preguntas elaboradas para obtener los datos necesarios y así poder alcanzar los objetivos del proyecto de investigación. Siendo un plan formal para recoger información de la unidad de análisis que está siendo objeto de estudio y centro del problema de investigación.” (p.217)

El cuestionario es un instrumento de investigación al cual lo conforman un conjunto de preguntas formuladas acorde al tema de investigación, con el cual se recaba información para ser procesada y usada con el fin de cumplir los objetivos planteados.

## Validez

Según Anderson y Morgan (2001) definen que: “La validez es un constructo amplio que implica realizar interpretaciones y usos adecuados de los resultados o de la información obtenida de la prueba.” (p.21)

La validez reflejará el grado en el que el instrumento de investigación mide realmente las variables, en donde se atienden los criterios de validez de contenido, criterio y constructo, dando como resultado la validez total.

Tabla N°8: Validez por evaluación de expertos.

EXPERTOS	GRADO ACADÉMICO	EFICIENCIA	EFICACIA	CALIDAD DE SERVICIO	MÉTODO DE ANÁLISIS DE RIESGO	PROYECTO DE ANÁLISIS DE RIESGO	PLAN DE SEGURIDAD
Ordoñez Pérez, Adilio Christian	Doctor/Magister en Ingeniería de sistemas	95%	95%	95%	95%	95%	95%
Guevara Jiménez, Jorge	Magister en Administración estratégica para empresas	94%	96%	95%	95%	95%	95%
Gálvez Tapia, Orleans Moisés	Magister en Ingeniería de sistemas	80%	80%	80%	80%	80%	80%

© Fuente: Elaboración propia.

## Criterio

Según Luis Mora (2008) define que: “El criterio es el valor que nos ayuda a determinar cuándo los resultados han sido exitosos o no.” (p.155)

El criterio permite juzgar si algún dato o información es verdadero.

## Contenido

Según Oria y Romero (2015) definen que: “El contenido es un instrumento para el análisis del contexto, en el caso de la unidad, o para enfrentarse a la realización de un proyecto.” (p.25)

El contenido en cuanto información refiere es todo aquello que se encuentre dentro de algún producto.

## Constructo

Según León y Montero (2015) definen que constructo: “es una variable que no es directamente accesible a la observación. La inferimos por medio de indicadores a las que si tenemos acceso” (p.35).

## Confiabilidad

Según Guerrero y Ramos (2014) definen que: “La confiabilidad de un instrumento es considerada como el grado en el que, al aplicarse de manera repetitiva del mismo objeto de estudio, se producirán resultados iguales o similares” (p.230).

Para poder obtener la confiabilidad del instrumento se utilizó el estadístico Alfa de Cronbach, utilizando los datos recolectados a través de las encuestas realizadas tal y como se muestra en el anexo N° 3, aplicado a 30 trabajadores según se determinó la muestra, teniendo como niveles los que se muestran en la siguiente Tabla N°9:

Tabla N°9: Niveles de confiabilidad

Escala	Nivel
$0.00 < sig < 0.20$	Muy bajo
$0.20 \leq sig < 0.40$	Bajo
$0.40 \leq sig < 0.60$	Regular
$0.60 \leq sig < 0.80$	Aceptable
$0.80 \leq sig < 1.00$	Elevado

© Fuente: Cayetano, 2003

Para determinar el nivel de fiabilidad, se aplicó el estadístico de alfa de Cronbach para el indicador de eficiencia, eficacia y calidad de servicio perteneciente a los datos procesados del cuestionario de las dimensiones de la variable 2.

Figura 12.

©Fuente: IBM SPSS 21

**Resumen del procesamiento de los casos**

		N	%
Casos	Válidos	30	100,0
	Excluidos <sup>a</sup>	0	,0
	Total	30	100,0

a. Eliminación por lista basada en todas las variables del procedimiento.

**Estadísticos de fiabilidad**

Alfa de Cronbach	N de elementos
,948	7

**Resumen de procesamiento de la eficiencia**

Para el indicador de eficiencia se obtuvo un resultado de fiabilidad de 0,948 tal como se muestra en la figura N° 12, lo que demuestra que está en un nivel aceptable. Por lo tanto, el indicador es confiable.

Figura 13.

©Fuente: IBM SPSS 21

**Resumen del procesamiento de los casos**

		N	%
Casos	Válidos	30	100,0
	Excluidos <sup>a</sup>	0	,0
	Total	30	100,0

a. Eliminación por lista basada en todas las variables del procedimiento.

**Estadísticos de fiabilidad**

Alfa de Cronbach	N de elementos
,845	7

**Resumen de procesamiento de la eficacia**

Para el indicador de eficacia se obtuvo un resultado de fiabilidad de 0,845 tal como se muestra en la figura N° 13, lo que demuestra que está en un nivel aceptable. Por lo tanto, el indicador es confiable.

Figura 14.

Fuente: IBM SPSS 21

		N	%
Casos	Válidos	30	100,0
	Excluidos <sup>a</sup>	0	,0
	Total	30	100,0

a. Eliminación por lista basada en todas las variables del procedimiento.

**Estadísticos de fiabilidad**

Alfa de Cronbach	N de elementos
,838	6

Resumen de procesamiento de la calidad de servicio

Para el indicador de calidad de servicio se obtuvo un resultado de fiabilidad de 0,838 tal como se muestra en la figura N° 14, lo que demuestra que está en un nivel aceptable. Por lo tanto, el indicador es confiable.

En la siguiente figura N°15 podemos apreciar el nivel de confiabilidad general que abarca los 3 indicadores, el cual da dio un resultado de 0,839:

Figura 15.

Fuente: IBM SPSS 21

**Resumen del procesamiento de los casos**

		N	%
Casos	Válidos	30	100,0
	Excluidos <sup>a</sup>	0	,0
	Total	30	100,0

a. Eliminación por lista basada en todas las variables del procedimiento.

**Estadísticos de fiabilidad**

Alfa de Cronbach	N de elementos
,839	21

Resumen de procesamiento de datos general de la V2

Para determinar el nivel de fiabilidad, se aplicó el estadístico de alfa de Cronbach para el indicador de método de análisis de riesgo, proyecto de análisis de riesgo y plan de seguridad perteneciente a los datos procesados del cuestionario de las dimensiones de la variable 1.

Figura 16.

Fuente: IBM SPSS 21

		N	%
Casos	Válidos	30	100,0
	Excluidos <sup>a</sup>	0	,0
	Total	30	100,0

a. Eliminación por lista basada en todas las variables del procedimiento.

**Estadísticos de fiabilidad**

Alfa de Cronbach	N de elementos
,832	6

Resumen de procesamiento del método de análisis de riesgo

Para el indicador de método de análisis de riesgo se obtuvo un resultado de fiabilidad de 0,832 tal como se muestra en la figura N° 16, lo que demuestra que está en un nivel aceptable. Por lo tanto, el indicador es confiable.

Figura 17

Fuente: IBM SPSS 21

**Resumen del procesamiento de los casos**

		N	%
Casos	Válidos	30	100,0
	Excluidos <sup>a</sup>	0	,0
	Total	30	100,0

a. Eliminación por lista basada en todas las variables del procedimiento.

**Estadísticos de fiabilidad**

Alfa de Cronbach	N de elementos
,904	7

. Resumen de procesamiento de proyecto de análisis de riesgo

Para el indicador de proyecto de análisis de riesgo se obtuvo un resultado de fiabilidad de 0,904 tal como se muestra en la figura N° 17, lo que demuestra que está en un nivel aceptable. Por lo tanto, el indicador es confiable.

Figura 18

Fuente: IBM SPSS 21

**Resumen del procesamiento de los casos**

		N	%
Casos	Válidos	30	100,0
	Excluidos <sup>a</sup>	0	,0
	Total	30	100,0

a. Eliminación por lista basada en todas las variables del procedimiento.

**Estadísticos de fiabilidad**

Alfa de Cronbach	N de elementos
,831	7

. Resumen de procesamiento de plan de seguridad

Para el indicador de plan de seguridad se obtuvo un resultado de fiabilidad de 0,831 tal como se muestra en la figura N° 18, lo que demuestra que está en un nivel aceptable. Por lo tanto, el indicador es confiable.

En la siguiente figura N°19 podemos apreciar el nivel de confiabilidad general que abarca los 3 indicadores, el cual da dio un resultado de 0,942:

Figura 19.

Fuente: IBM SPSS 21

**Resumen del procesamiento de los casos**

		N	%
Casos	Válidos	30	100,0
	Excluidos <sup>a</sup>	0	,0
	Total	30	100,0

a. Eliminación por lista basada en todas las variables del procedimiento.

**Estadísticos de fiabilidad**

Alfa de Cronbach	N de elementos
,942	20

Resumen de procesamiento de datos general de la V.1



## 2.5 Métodos de análisis de datos

Para el análisis y procesamiento de datos, se utilizará cuadros y gráficos estadísticos haciendo uso del programa IBM SPSS versión 21, Los resultados obtenidos luego del procesamiento de datos, será resueltos bajo un enfoque descriptivo correlacional utilizando el coeficiente de correlación de Pearson aplicando la estadística descriptiva.

Según Velazquez Perea (2016) nos define que: “La estadística descriptiva se refiere a los métodos de recolección, descripción, visualización y resumen de los datos, que pueden ser presentados en forma numérica o grafica”. (p.9)

La estadística descriptiva es aplicada de forma que todos aquellos datos que han sido recolectados por el instrumento muestran sus resultados a través de gráficos estadísticos o de forma numérica.

### Hipótesis de investigación 1

#### a) Hipótesis Especifica (HE1)

Existe una relación positiva entre los factores de riesgo en tecnologías de información y el eficiente desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

#### b) Indicador 1: Eficiencia

**FRTIC: Eficiencia antes de utilizar la metodología Magerit.**

**EDW: Eficiencia después de utilizar la metodología Magerit.**

#### c) Hipótesis estadística1:

##### Hipótesis nula (H0):

No existe una relación positiva entre los factores de riesgo en tecnologías de información y el eficiente desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

**FRTIC, EDW = 0**

Se deduce que el indicador sin aplicar la metodología es mejor que cuando se pudiera aplicar.

### **Hipótesis alterna (HA):**

Existe una relación positiva entre los factores de riesgo en tecnologías de información y el eficiente desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

**FRTIC, EDW  $\neq$  0**

Se deduce que el indicador aplicando la metodología es mejor que si no se aplicara.

## **Hipótesis de investigación 2**

### **a) Hipótesis Especifica (HE2)**

Existe una relación positiva entre los factores de riesgo en tecnologías de información y el eficaz desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

### **b) Indicador 2: Eficacia**

**FRTIC: Eficacia antes de utilizar la metodología Magerit.**

**EDW: Eficacia después de utilizar la metodología Magerit.**

### **c) Hipótesis estadística1:**

**Hipótesis nula (H0):**

No existe una relación positiva entre los factores de riesgo en tecnologías de información y el eficaz desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

$$\text{FRTIC, EDW} = 0$$

Se deduce que el indicador sin aplicar la metodología es mejor que cuando se pudiera aplicar.

**Hipótesis alterna (HA):**

Existe una relación positiva entre los factores de riesgo en tecnologías de información y el eficaz desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

$$\text{FRTIC, EDW} \neq 0$$

Se deduce que el indicador aplicando la metodología es mejor que si no se aplicara.

**Hipótesis de investigación 3****a) Hipótesis Especifica (HE3)**

Existe una relación positiva entre los factores de riesgo en tecnologías de información y la calidad de servicio en el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

**b) Indicador 3: Calidad de servicio**

**FRTIC: Calidad de servicio antes de utilizar la metodología Magerit.**

**CDW: Calidad de servicio después de utilizar la metodología Magerit.**

**c) Hipótesis estadística1:**

**Hipótesis nula (H0):**

No existe una relación positiva entre los factores de riesgo en tecnologías de información y la calidad de servicio en el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

$$\text{FRTIC, EDW} = 0$$

Se deduce que el indicador sin aplicar la metodología es mejor que cuando se pudiera aplicar.

**Hipótesis alterna (HA):**

Existe una relación positiva entre los factores de riesgo en tecnologías de información y el eficaz desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

$$\text{FRTIC, EDW} \neq 0$$

Se deduce que el indicador aplicando la metodología es mejor que si no se aplicara.

**Nivel de Significancia**

El nivel de significancia que será utilizado en la presente investigación es  $\alpha = 5\%$  (error), equivalente a 0.05, esto permitirá realizar comparaciones y así determinar si se acepta o se rechaza la hipótesis.

Nivel de confiabilidad:  $(1-\alpha) = 0.95$

**2.6 Aspectos éticos**

Los datos presentados en esta investigación han sido obtenidos del grupo control cuasi experimental de la investigación y han sido procesados de forma adecuada sin adulterar ningún dato.

Se protegió la identidad de los trabajadores que fueron partícipes en la investigación y los resultados fueron obtenidos de manera confidencial.

Se siguió la investigación de acuerdo a los reglamentos y lineamientos estipulados en la Universidad César Vallejo.

Se respetó a los trabajadores, no se realizó ninguna discriminación, previamente para la realización del estudio se pidió la autorización previa de cada trabajador.

El trabajo que se realizó es original y no existe uno similar en la organización de estudio de la investigación.

Finalmente, los resultados de la investigación no han sido adulterados o plagiados de otras investigaciones y se hizo un buen uso de la investigación en beneficio de todos.

### **III. RESULTADOS**

### 3.1 RESULTADOS DESCRIPTIVOS

#### Dimensiones de los factores de riesgo de las tecnologías de información

#### Resultados de los datos por dimensiones de la variable 1:

#### EFICIENCIA

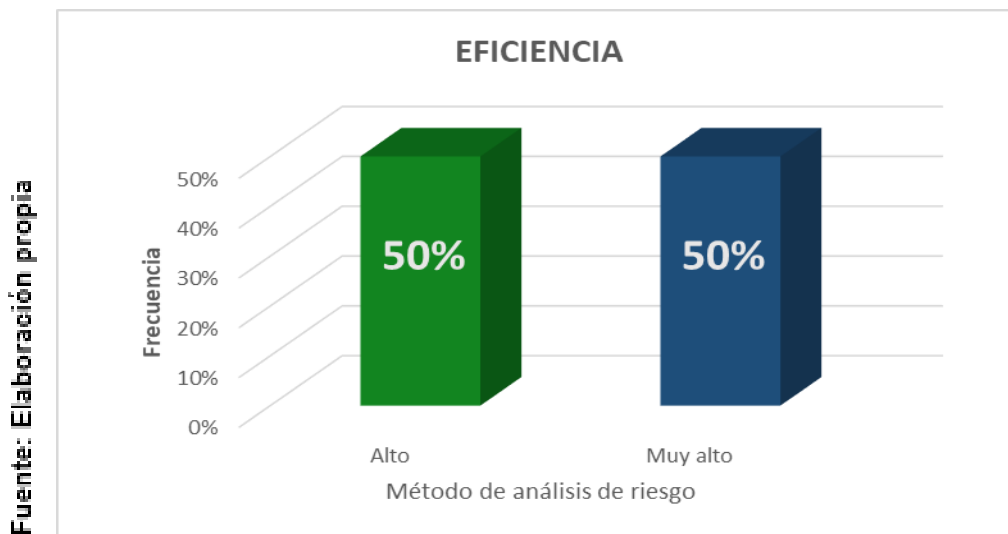
En la tabla N°16 y figura N°20, se presenta los niveles de eficiencia en el desempeño del webcast en la empresa Radio Atogapan S.A. y el grupo HCM Comunicaciones S.A.C Se observa que el 50% indica que los niveles de eficiencia se encuentran en un nivel “Alto”, y el otro 50% señala que se encuentra en un nivel “Muy alto”. Estos resultados muestran que tras la implementación de la metodología MAGERIT V.3 los niveles de eficiencia del desempeño del webcast tienden a ser alto o muy alto.

**Tabla N°16 frecuencia valores estadísticos de la dimensión de la Eficiencia**

Eficiencia				
Niveles	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos Alto	15	50,0	50,0	50,0
Muy alto	15	50,0	50,0	100,0
Total	30	100,0	100,0	

Fuente: SPSS 21

**Figura N°20**



**Gráfico de la frecuencia de los valores estadísticos de la dimensión de la Eficiencia**

## EFICACIA

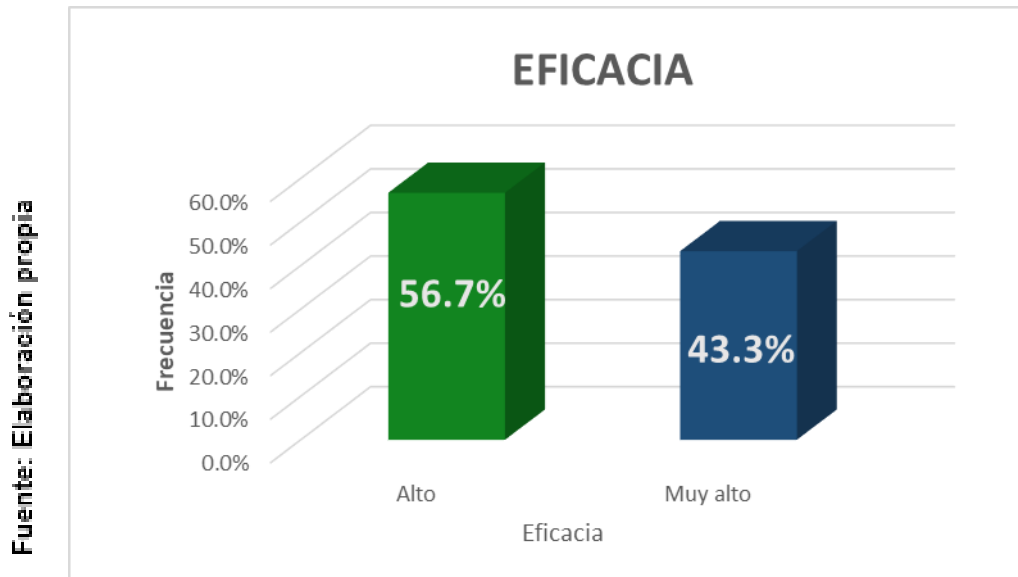
En la tabla N°17 y figura N°21, se presenta los niveles de eficiencia en el desempeño del webcast en la empresa Radio Atogapan S.A. y el grupo HCM Comunicaciones S.A.C Se observa que el 56,7% indica que los niveles de eficacia se encuentran en un nivel “Alto”, y el 43,3% señala que se encuentra en un nivel “Muy alto”. Estos resultados muestran que tras la implementación de la metodología MAGERIT V.3 los niveles de eficacia del desempeño del webcast tienden a ser alto o muy alto.

**Tabla N°17 frecuencia valores estadísticos de la dimensión de la Eficacia**

		Eficacia			
Niveles		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Alto	17	56,7	56,7	56,7
	Muy alto	13	43,3	43,3	100,0
	Total	30	100,0	100,0	

Fuente: SPSS 21

**Figura N°21**



**Gráfico de la frecuencia de los valores estadísticos de la dimensión de la Eficacia**



### CALIDAD DE SERVICIO

En la tabla N°18 y figura N°22, se presenta los niveles de la calidad de servicio en el desempeño del webcast en la empresa Radio Atogapan S.A. y el grupo HCM Comunicaciones S.A.C Se observa que el 6,7% indica que los niveles de la calidad de servicio se encuentran en un nivel “Alto”, y el 93,3% señala que se encuentra en un nivel “Muy alto”. Estos resultados muestran que tras la implementación de la metodología MAGERIT V.3 los niveles de la calidad de servicio del desempeño del webcast tienden a ser alto o muy alto.

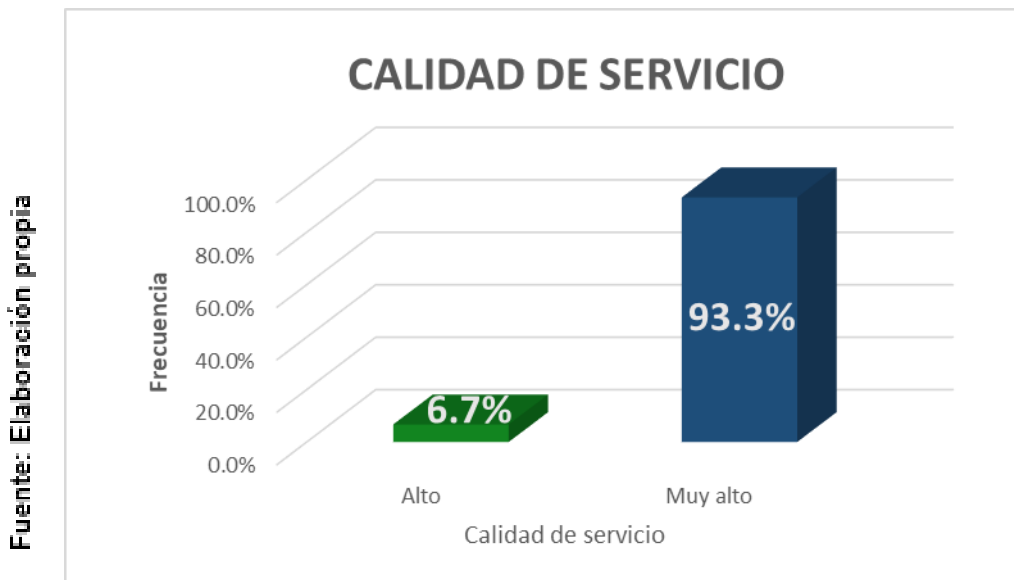
**Tabla N°18 Frecuencia valores estadísticos de la dimensión de la calidad de servicio**

**Calidad\_de\_servicio**

Niveles		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Alto	2	6,7	6,7	6,7
	Muy alto	28	93,3	93,3	100,0
	Total	30	100,0	100,0	

Fuente: SPSS 21

**Figura N°22**



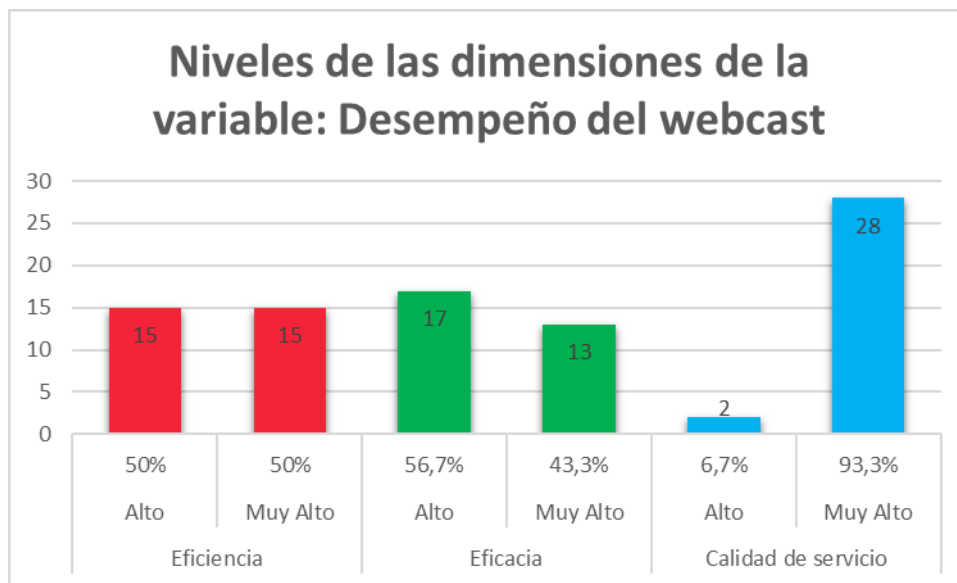
**Gráfico de la frecuencia de los valores estadísticos de la dimensión de la calidad de servicio**

**Tabla N°19 Resultados de los niveles de la variable: Desempeño del webcast**

Dimensión	Nivel	Frecuencia	Porcentaje
Eficiencia	Alto	15	50%
	Muy Alto	15	50%
Eficacia	Alto	17	56,7%
	Muy Alto	13	43,3%
Calidad de servicio	Alto	2	6,7%
	Muy Alto	28	93,3%

Fuente: Cuestionario dirigido a involucrados en el proceso

**Figura 23**



**Resultados de las dimensiones de la variable 2: Desempeño del webcast**

**Resultados de los datos por dimensiones de la variable 1:**

**MÉTODO DE ANÁLISIS DE RIESGO**

En la tabla N°19 y figura N°23, se presenta el nivel del método de análisis de riesgo de los factores de riesgo de las tecnologías de información en la empresa Radio Atogapan S.A. y el grupo HCM Comunicaciones S.A.C Se observa que el 66,7% indica que los niveles del método de análisis de riesgo se encuentran en un nivel “Alto”, y el otro 33,3% señala que se encuentra en un nivel “Muy alto”. Estos resultados muestran que tras la implementación de la metodología MAGERIT V.3 los niveles del método de análisis de riesgo de los factores de riesgo de las tecnologías de información tienden a ser alto o muy alto.

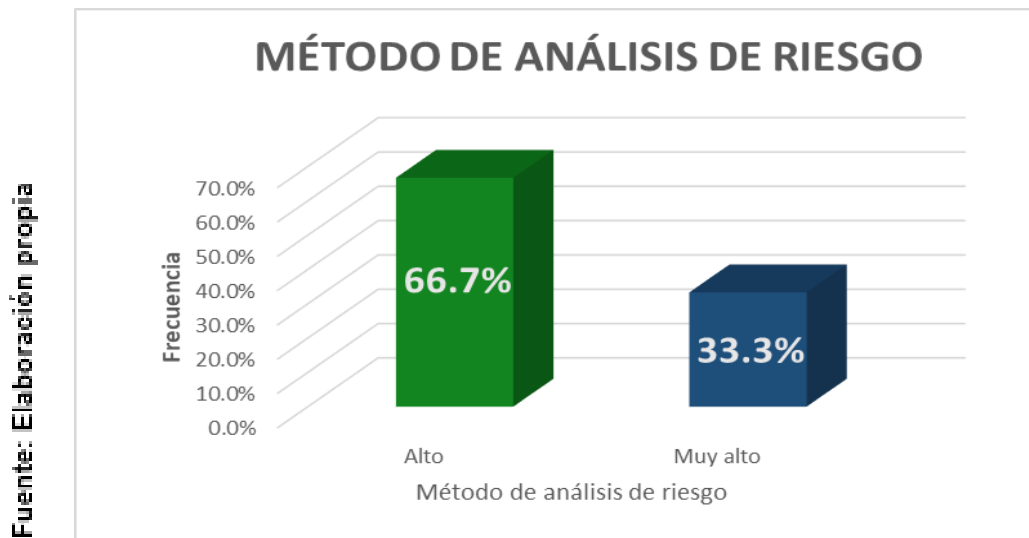
**Tabla N°20 frecuencia valores estadísticos de la dimensión del método de análisis de riesgo**

**Método\_de\_análisis\_de\_riesgo**

Niveles		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Alto	20	66,7	66,7	66,7
	Muy alto	10	33,3	33,3	100,0
Total		30	100,0	100,0	

Fuente: SPSS 21

**Figura N°24**



**Gráfico de la frecuencia de los valores estadísticos de la dimensión del método de análisis de riesgo**

### PROYECTO DE ANÁLISIS DE RIESGO

En la tabla N°20 y figura N°24, se presenta el nivel proyecto de análisis de riesgo de los factores de riesgo de las tecnologías de información en la empresa Radio Atogapan S.A. y el grupo HCM Comunicaciones S.A.C Se observa que el 10% indica que los niveles del plan de seguridad se encuentran en un nivel “Alto”, y el otro 90% señala que se encuentra en un nivel “Muy alto”. Estos resultados muestran que tras la implementación de la metodología MAGERIT V.3 los niveles del proyecto de análisis de riesgo de los factores de riesgo de las tecnologías de información tienden a ser alto o muy alto.

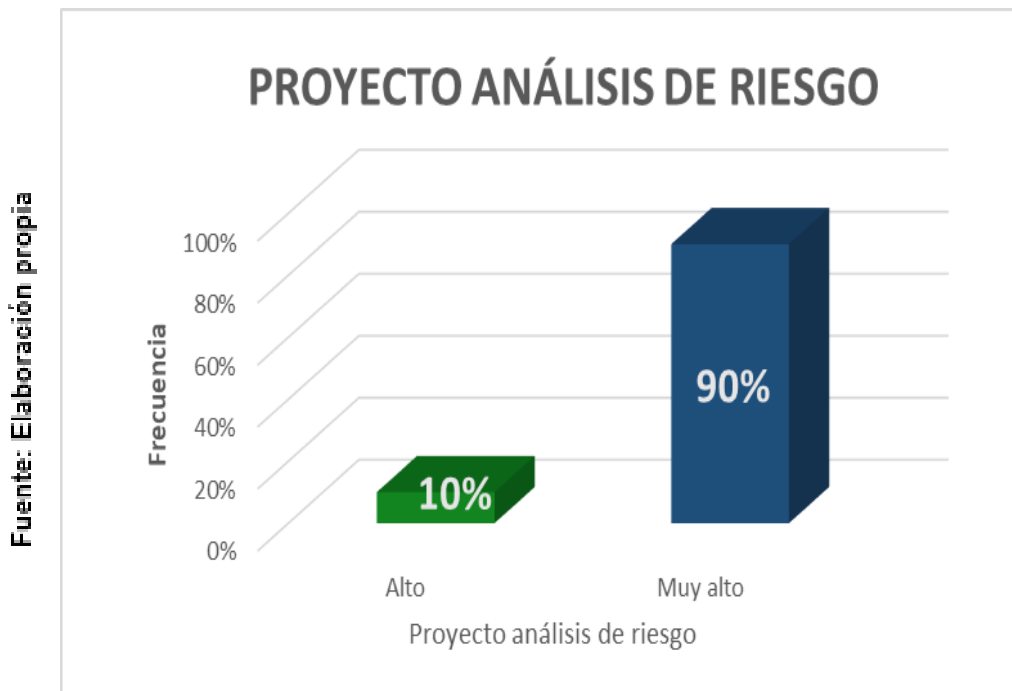
**Tabla N°21 frecuencia valores estadísticos de la dimensión proyecto de análisis de riesgo**

**Proyecto\_de\_análisis\_de\_riesgo**

Niveles		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Alto	3	10,0	10,0	10,0
	Muy alto	27	90,0	90,0	100,0
Total		30	100,0	100,0	

Fuente: SPSS 21

**Figura N°25**



**Gráfico de la frecuencia de los valores estadísticos de la dimensión de proyecto de análisis de riesgo**

**PLAN DE SEGURIDAD**

En la tabla N°21 y figura N°25, se presenta el nivel del plan de seguridad de los factores de riesgo de las tecnologías de información en la empresa Radio Atogapan S.A. y el grupo HCM Comunicaciones S.A.C Se observa que el 100% indica que los niveles del plan de seguridad se encuentran en un nivel “Muy alto”. Estos resultados muestran que tras la implementación de la metodología MAGERIT V.3 los niveles del plan de seguridad de los factores de riesgo de las tecnologías de información tienden a ser muy alto.

**Tabla N°22 Frecuencia valores estadísticos de la dimensión de plan de seguridad**

Niveles		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy alto	30	100,0	100,0	100,0

Fuente: SPSS 21

**Figura N°26**



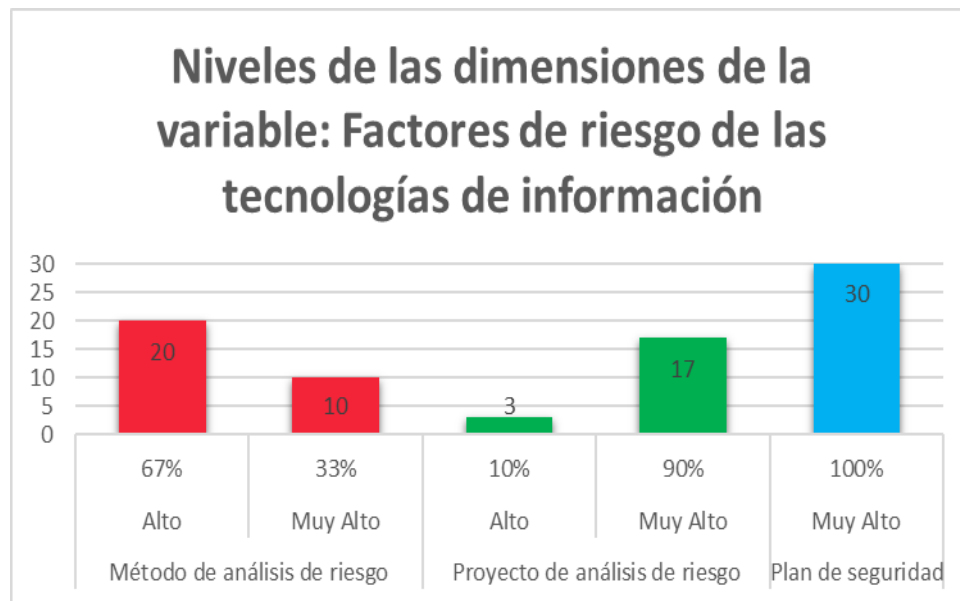
**Gráfico de la frecuencia de los valores estadísticos de la dimensión de plan de seguridad**

**Tabla N°23 Resultados de los niveles de la variable: Factores de riesgo de las tecnologías de información**

Dimensión	Nivel	Porcentaje	Frecuencia
Método de análisis de riesgo	Alto	67%	20
	Muy Alto	33%	10
Proyecto de análisis de riesgo	Alto	10%	17
	Muy Alto	90%	3
Plan de seguridad	Muy Alto	100%	30

Fuente: Cuestionario dirigido a involucrados en el proceso

Figura 27



**Resultados de las dimensiones de la variable 1:  
Factores de riesgo de las tecnologías de información**

### 3.2 RESULTADO INFERENCIAL

#### PRUEBA DE HIPOTESIS

Aquí veremos el estadístico a usar en la prueba de hipótesis, es decir, se analizó si el estadístico es paramétrico o no paramétrico.

**A.** Un Estadístico (Fórmula) paramétrico tiene las condiciones siguientes:

Características de las Pruebas Paramétricas:

- a. La Variable es cuantitativa
- b. Distribución Normal de la Muestra
- c. Varianzas Iguales

Para el presente desarrollo de tesis verificaremos si se cumplen estas características:

- a. La variable que se está usando es Cuantitativa, Ordinal.
- b. Verificaremos la normalidad de la muestra

**Prueba de Normalidad**

Ho= La Distribución de la muestra es normal

H1= La Distribución de la muestra no es normal

Nivel de Aceptación: 95%, Z=1,96

Nivel de Significancia: 5% = 0,05 (t)

**Regla de Decisión:**

Sig. < 0.05 entonces se rechaza Ho.

Sig. ≥ 0.05 entonces se acepta Ho.

**Tabla N°24. Prueba de Normalidad**

	Pruebas de normalidad		
	Shapiro-Wilk		
	Estadístico	gl	Sig.
Factores_de_riesgo_de_l as_TI	,926	30	,038
Desempeño_del_webca st	,921	30	,029

a. Corrección de la significación de Lilliefors

**Fuente: SPSS 21**

**Interpretación:** Tal como se muestra en la Tabla N°24, se aplicó la regla estadística de Shapiro-Wilk, siendo la muestra 30 personas, y dando como resultado el nivel de significancia menor a 0,05, por lo que se rechaza la hipótesis nula y se acepta la hipótesis alterna, entonces la distribución de la muestra no es normal y como la normalidad no se ha comprobado como verdadera, por lo tanto, el estadístico a usar en la prueba de hipótesis del trabajo de investigación será un estadístico no paramétrico. En la prueba de hipótesis de trabajo se usará el estadístico de Spearman por ser no paramétrico.

Tabla N°25 Coeficiente de Correlación Rho Spearman

Valor	Criterio
$R = 1,00$	Correlación grande, perfecta y positiva
$0,90 \leq r < 1,00$	Correlación muy alta
$0,70 \leq r < 0,90$	Correlación alta
$0,40 \leq r < 0,70$	Correlación moderada
$0,20 \leq r < 0,40$	Correlación muy baja
$r = 0,00$	Correlación nula
$r = -1,00$	Correlación grande, perfecta y negativa

Fuente: Hernández Sampieri, et al (2014, p.305)

### 3.3 PRUEBA DE HIPÓTESIS DE TRABAJO

#### A. Hipótesis General

Existe una relación positiva entre los factores de riesgo en tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

#### Hipótesis Nula (H0)

No existe una relación positiva entre los factores de riesgo en tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

#### Hipótesis de Investigación (H1)

Si existe una relación positiva entre los factores de riesgo en tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

- Nivel de Aceptación: 95%,  $Z=1.96$
- Nivel de Significancia: 5% = 0,05 (t)



**Regla de Decisión:**

Sig. < 0.05 entonces se rechaza Ho.

Sig. ≥ 0.05 entonces se acepta Ho.

**Tabla N°26 Correlación de Spearman entre los factores de riesgo de las tecnologías de información y el desempeño del webcast**

Correlaciones			Factores_de_riesgo_de_las_TI	Desempeño_del_webcast
Rho de Spearman	Factores_de_riesgo_de_las_TI	Coeficiente de correlación	1,000	,922**
		Sig. (bilateral)	.	,000
		N	30	30
	Desempeño_del_webcast	Coeficiente de correlación	,922**	1,000
		Sig. (bilateral)	,000	.
		N	30	30

\*\* La correlación es significativa al nivel 0,01 (bilateral).

**Fuente: SPSS 21**

**Interpretación:**

En los resultados que se muestran en la tabla N°26, se aprecia el grado de correlación entre las variables factores de riesgo de las tecnologías de información y el desempeño del webcast, determinado por el Rho de Spearman  $p = 0,922$ , lo que significa que existe una correlación muy alta, entre los factores de riesgo de las tecnologías de información y el desempeño del webcast, siendo el grado de significancia  $0,00 < a 0.05$ ; por ello existe evidencias estadísticas necesarias para aceptar la hipótesis alterna y rechazar la hipótesis nula con el 95% de nivel de confianza; Por lo tanto, existe una relación positiva entre los factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas Radio atogapan S.A y el grupo HCM Comunicaciones S.A.C.

**A. Hipótesis específicas**

**Hipótesis específica 1**

Existe una relación positiva entre los factores de riesgo en tecnologías de información y el eficiente desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

**Hipótesis Nula (H0)**

No existe una relación positiva entre los factores de riesgo en tecnologías de información y el eficiente desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

**Hipótesis de Investigación (H1)**

Si existe una relación positiva entre los factores de riesgo en tecnologías de información y el eficiente desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

- Nivel de Aceptación: 95%, Z=1.96
- Nivel de Significancia: 5% = 0,05 (t)

**Regla de Decisión:**

Sig. < 0.05 entonces se rechaza Ho.

Sig. ≥ 0.05 entonces se acepta Ho.

**Tabla N°27 Correlación de Spearman entre los factores de riesgo de las tecnologías de información y la eficiencia**

Correlaciones			Factores_de_riesgo_de_las_TI	Eficiencia
Rho de Spearman	Factores_de_riesgo_de_las_TI	Coefficiente de correlación	1,000	,906**
		Sig. (bilateral)	.	,000
		N	30	30
Eficiencia	Eficiencia	Coefficiente de correlación	,906**	1,000
		Sig. (bilateral)	,000	.
		N	30	30

\*\* . La correlación es significativa al nivel 0,01 (bilateral).

**Fuente: SPSS 21**

**Interpretación:**

En los resultados que se muestran en la tabla N°27, se aprecia el grado de correlación entre las variables factores de riesgo de las tecnologías de

información y la dimensión eficiencia del desempeño del webcast, determinado por el Rho de Spearman  $p= 0,906$ , lo que significa que existe una correlación muy alta, entre los factores de riesgo de las tecnologías de información y el desempeño del webcast, siendo el grado de significancia 0,00 símbolo menor a 0.05; por ello existe evidencias estadísticas necesarias para aceptar la hipótesis alterna y rechazar la hipótesis nula con el 95% de nivel de confianza; Por lo tanto, existe una relación positiva entre los factores de riesgo de las tecnologías de información y el eficiente desempeño del webcast en las empresas Radio atogapan S.A y el grupo HCM Comunicaciones S.A.C.

### **Hipótesis específica 2**

Existe una relación positiva entre los factores de riesgo en tecnologías de información y el eficaz desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

### **Hipótesis Nula (H0)**

No existe una relación positiva entre los factores de riesgo en tecnologías de información y el eficaz desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

### **Hipótesis de Investigación (H1)**

Si existe una relación positiva entre los factores de riesgo en tecnologías de información y el eficaz desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

- Nivel de Aceptación: 95%,  $Z=1.96$
- Nivel de Significancia: 5% = 0,05 (t)

### **Regla de Decisión:**

Sig. < 0.05 entonces se rechaza Ho.

Sig.  $\geq$  0.05 entonces se acepta Ho.

**Tabla N°28 Correlación de Spearman entre los factores de riesgo de las tecnologías de información y la eficacia**

**Correlaciones**

			Factores_de_riesgo_de_las_TI	Eficacia
Rho de Spearman	Factores_de_riesgo_de_las_TI	Coefficiente de correlación	1,000	,938**
		Sig. (bilateral)	.	,000
		N	30	30
	Eficacia	Coefficiente de correlación	,938**	1,000
		Sig. (bilateral)	,000	.
		N	30	30

\*\* . La correlación es significativa al nivel 0,01 (bilateral).

**Fuente: SPSS 21**

**Interpretación:**

En los resultados que se muestran en la tabla N°28, se aprecia el grado de correlación entre las variables factores de riesgo de las tecnologías de información y la dimensión eficacia del desempeño del webcast, determinado por el Rho de Spearman  $\rho = 0,938$ , lo que significa que existe una correlación muy alta, entre los factores de riesgo de las tecnologías de información y el desempeño del webcast, siendo el grado de significancia 0,000 símbolo menor a 0.05; por ello existe evidencias estadísticas necesarias para aceptar la hipótesis alterna y rechazar la hipótesis nula con el 95% de nivel de confianza; Por lo tanto, existe relación positiva entre los factores de riesgo de las tecnologías de información y el eficaz desempeño del webcast en las empresas Radio atogapan S.A y el grupo HCM Comunicaciones S.A.C.

**Hipótesis específica 3**

Existe una relación positiva entre los factores de riesgo en tecnologías de información y la calidad de servicio en el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

**Hipótesis Nula (H0)**

No existe una relación positiva entre los factores de riesgo en tecnologías de información y la calidad de servicio en el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

**Hipótesis de Investigación (H1)**

Si existe una relación positiva entre los factores de riesgo en tecnologías de información y la calidad de servicio en el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.

- Nivel de Aceptación: 95%, Z=1.96
- Nivel de Significancia: 5% = 0,05 (t)

**Regla de Decisión:**

Sig. < 0.05 entonces se rechaza Ho.

Sig. ≥ 0.05 entonces se acepta Ho.

**Tabla N°29 Correlación de Spearman entre los factores de riesgo de las tecnologías de información y la calidad de servicio**

Correlaciones			Factores_de_riesgo_de_las_TI	Calidad_de_servicio
Rho de Spearman	Factores_de_riesgo_de_las_TI	Coefficiente de correlación	1,000	,809**
		Sig. (bilateral)	.	,000
		N	30	30
	Calidad_de_servicio	Coefficiente de correlación	,809**	1,000
		Sig. (bilateral)	,000	.
		N	30	30

\*\* La correlación es significativa al nivel 0,01 (bilateral).

**Fuente: SPSS 21**

**Interpretación:**

En los resultados que se muestran en la tabla N°29, se aprecia el grado de correlación entre las variables factores de riesgo de las tecnologías de información y la dimensión eficacia del desempeño del webcast, determinado por el Rho de Spearman  $\rho = 0,809$ , lo que significa que existe una correlación muy alta, entre los factores de riesgo de las tecnologías de información y el desempeño del webcast, siendo el grado de significancia 0,00 símbolo menor a 0.05; por ello existe evidencias estadísticas necesarias para aceptar la hipótesis alterna y rechazar la hipótesis nula con el 95% de nivel de confianza; Por lo tanto, existe relación positiva entre los factores de riesgo de las tecnologías de información y la calidad de servicio en el desempeño del webcast en las empresas Atogapan S.A y el grupo HCM Comunicaciones S.A.C.

## **IV. DISCUSIÓN**

En el presente desarrollo de esta investigación, se obtuvo como resultado que con la implementación de la metodología MAGERIT V.3, se incrementó el nivel de las dimensiones del desempeño del webcast, tanto para la empresa Atogapan S.A y el grupo HCM Comunicaciones SAC, teniendo en cuenta que estas fueron evaluadas en una escala del 0 al 5, siendo 0 al 1= Muy Bajo, 1.1 al 2= Bajo, 2.1 al 3= Regular, 3.1 al 4= Alto y 4.1 al 5= Muy alto. En la dimensión de la eficiencia Atogapan S.A incrementó de un 2.7 a un 4.51 lo que equivale a un crecimiento promedio de 36.2%. De la misma manera el Grupo HCM Comunicaciones, incrementó de un 2 a un 4.18 lo que equivale a un crecimiento promedio de 43.6%. De la misma manera en su investigación Vargas García en “Propuesta tecnológica basada en Cobit 5 aplicada a la gestión de las TI en la EIS”, concluyó que al implementar COBIT 5 obtuvo un crecimiento del nivel de eficacia de un 26%.

También se obtuvo como resultado que con la implementación de la metodología MAGERIT V.3 se incrementó el nivel de eficacia de un 2.7 a un 4.45 para la empresa Atogapan S.A, representando un crecimiento del 40.8%, en el caso del grupo HCM Comunicaciones SAC, en la dimensión de la eficacia incrementó de un 2.3 a un 4.39 lo que equivale a un crecimiento promedio de un 41.8%. De la misma manera en su investigación Motake Katerina en “Risk Analysis and Risk Management in Critical Infrastructures”, concluyó que al implementar Risk Analysis obtuvo un crecimiento del nivel de eficacia de un 16%

En el nivel de la calidad del servicio, se obtuvo que tras la implementación de la metodología MAGERIT V.3 Atogapan S.A incrementó el nivel de la calidad de servicio de un 2.7 a un 4.51 lo que equivale a un crecimiento promedio de 36.2%. De la misma manera el Grupo HCM Comunicaciones, incrementó de un 2.5 a un 4.75 lo que equivale a un crecimiento promedio de 45%. De la misma manera en su investigación Arias, Díaz y Vargas en “Elaboración de una guía de gestión de riesgos basados en la norma NTC-ISO 31000 para el proceso de gestión de incidentes y peticiones de servicio del



área de mesa de ayuda de empresas de servicios de soporte de tecnología en Colombia”, concluyó que al implementar en la norma NTC-ISO 31000 obtuvo un crecimiento del nivel de la calidad de servicio de un 25%.

Los resultados obtenidos en la presente investigación comprueban que la utilización de una metodología orientada a los factores de riesgo de las tecnologías de información mejora el desempeño de los procesos como lo es en este caso el de webcast, confirmando así que los factores de riesgo de las tecnologías de información tienen una relación positiva con el desempeño del webcast, dado que posterior a la implementación de la metodología MAGERIT V.3, se incrementó el porcentaje de crecimiento de sus dimensiones.

## **V. CONCLUSIÓN**

Se concluye que los factores de riesgo de las tecnologías de información tienen una relación positiva con el desempeño del webcast, ya que permitió el incremento del porcentaje en sus niveles de eficiencia eficacia y calidad de servicio, logrando así alcanzar los objetivos de la presente investigación.

Se concluye que los factores de riesgo de las tecnologías de información tienen una relación positiva con el desempeño del webcast, ya que incrementó el porcentaje de crecimiento en el nivel de eficiencia en un 37.2%. Por lo tanto, se afirma que la metodología MAGERIT V.3 incrementa el porcentaje del nivel de eficiencia en el desempeño de webcast.

Se concluye que los factores de riesgo de las tecnologías de información tienen una relación positiva con el desempeño del webcast, ya que incrementó el porcentaje de crecimiento en el nivel de la calidad de servicio en un 36.8%. Por lo tanto, se afirma que la metodología MAGERIT V.3 incrementa el porcentaje del nivel de la calidad de servicio en el desempeño de webcast.

Se concluye que los factores de riesgo de las tecnologías de información tienen una relación positiva con el desempeño del webcast, ya que incrementó el porcentaje de crecimiento en el nivel de calidad de servicio en un 40.8%. Por lo tanto, se afirma que la metodología MAGERIT V.3 incrementa el porcentaje del nivel de calidad de servicio en el desempeño de webcast.

## **VI. RECOMENDACIONES**

## RECOMENDACIONES

Se sugiere plantear nuevas investigaciones o ampliar la existente, con el propósito de mejorar el desempeño del webcast y todos aquellos procesos que tienen relación con los factores de riesgo de las tecnologías de información, de esta manera las empresas Atogapan S.A y el grupo HCM Comunicaciones SAC podrán mantener en mejora continua el proceso del webcast y por consiguiente podrá generar valor para sí misma.

Para investigaciones similares se recomienda la implementación de la metodología MAGERIT en su V.3 o si hubiera una actualización posterior a ella, con el propósito de obtener mejoras en el desempeño, incrementando sus niveles de eficiencia, eficacia y calidad de servicio.

Otro punto muy importante, es optar por la herramienta PILAR en la versión más reciente, así como la de pago luego de comprobada la relación positiva que esta determina entre las variables.

Así mismo, para investigaciones similares se recomienda evaluar diferentes empresas en diferentes espacios con el fin de obtener el impacto generado en dichos casos, tomando como base el mismo proceso relacionado a los factores de riesgo de las tecnologías de información.

## VII. REFERENCIAS

## REFERENCIAS BIBLIOGRÁFICAS

15 Beneficios de Gestionar los Riesgos de acuerdo a ISO 31000 [Mensaje en un blog]. Santiago de Chile: ISOTools., (6 de abril del 2016). [Fecha de consulta: 27 de abril de 2018]. Recuperado de <https://www.isotools.cl/15-beneficios-de-gestionar-los-riesgos-de-acuerdo-a-iso-31000/>

ALVA, Rósel. Las tecnologías de información y comunicación como instrumentos eficaces en la capacitación del personal: El caso de la Oficina Nacional de Procesos Electorales (ONPE). Tesis (Magíster en Administración con mención en dirección de Recursos Humanos). Lima: Universidad Nacional Mayor de San Marcos, 2014. Disponible en [http://cybertesis.unmsm.edu.pe/bitstream/handle/cybertesis/3766/Alva\\_ar.pdf?sequence=1&isAllowed=y](http://cybertesis.unmsm.edu.pe/bitstream/handle/cybertesis/3766/Alva_ar.pdf?sequence=1&isAllowed=y)

ÁLVAREZ, Rafael. Estadística aplicada a las ciencias de la salud [en línea]. España, 2007 [fecha de consulta: 27 de mayo del 2018]. Disponible en: [https://books.google.com.pe/books?id=V2ZosgPYI0kC&source=gbs\\_navlinks\\_s](https://books.google.com.pe/books?id=V2ZosgPYI0kC&source=gbs_navlinks_s)

ARIAS, DÍAZ Y VARGAS. Elaboración de una guía de gestión de riesgos basados en la norma NTC-ISO 31000 para el proceso de gestión de incidentes y peticiones de servicio del área de mesa de ayuda de empresas de servicios de soporte de tecnología en Colombia. Tesis (Magíster en auditoría de sistemas). Bogotá: Universidad Católica de Colombia, 2014. Disponible en <http://metadirectorio.org/bitstream/10983/1758/1/Trabajo%20de%20Grado%20Especializacion%20Auditoria%20de%20Sistemas.pdf>

ARIEL, Erica. Más allá del sí: Un método para superar el autosabotaje y negociar con éxito [en línea]. España: Penguin Random House Grupo Editorial España, 2014 [fecha de consulta: 20 de abril del 2018]. Disponible en: [https://books.google.com.pe/books?id=gqDBAgAAQBAJ&source=gbs\\_navlinks\\_s](https://books.google.com.pe/books?id=gqDBAgAAQBAJ&source=gbs_navlinks_s)

BACA, ACOSTA Y SOLARES. Administración Informática I: Análisis y Evaluación de Tecnologías de Información [en línea]. México: Grupo Editorial Patria., 2014 [fecha de consulta: 23 de abril del 2018]. Disponible en: [https://books.google.com.pe/books?id=XhBAAQBAJ&source=gbs\\_navlinks\\_s](https://books.google.com.pe/books?id=XhBAAQBAJ&source=gbs_navlinks_s)  
ISBN: 978-607-438-862-6

BERNAL, César. Metodología de la investigación: para administración, economía, humanidades y ciencias sociales [en línea]. México, 2006 [fecha de consulta: 28 de mayo del 2018]. Disponible en: [https://books.google.com.pe/books?id=h4X\\_eFai59oC&source=gbs\\_navlinks\\_s](https://books.google.com.pe/books?id=h4X_eFai59oC&source=gbs_navlinks_s)

ISBN: 970-26-0645-4

CAHUANA, César. Eficacia de un programa de tecnologías de información y comunicación para mejorar el rendimiento académico en el curso de prótesis completa en estudiantes del VII semestre de la Universidad Alas Peruanas. Tesis (Magíster en educación superior). Arequipa: Universidad Católica de Santa María, 2016. Disponible en <https://tesis.ucsm.edu.pe/repositorio/bitstream/handle/UCSM/5244/B4.1295.MG.pdf?sequence=1&isAllowed=y>

CEGARRA, José. Los métodos de investigación [en línea]. España: Ediciones Díaz de Santos., 2012 [fecha de consulta: 28 de abril del 2018]. Disponible en: [https://books.google.com.pe/books?id=YROO\\_q6-wzgC&source=gbs\\_navlinks\\_s](https://books.google.com.pe/books?id=YROO_q6-wzgC&source=gbs_navlinks_s)

ISBN: 978-84-9969-027-8

CHICANO, Ester. Auditoría de seguridad informática. IFCT0109 [en línea]. España: IC Editorial., 2014 [fecha de consulta: 24 de abril del 2018]. Disponible en: [https://books.google.com.pe/books?id=8a3KCQAAQBAJ&source=gbs\\_navlink\\_s\\_s](https://books.google.com.pe/books?id=8a3KCQAAQBAJ&source=gbs_navlink_s_s)

ISBN: 978-84-16433-23-0



CHUNGA, Gerardo. Orientaciones para diseñar materiales didáctico multimedia [en línea]. Perú, 2015 [fecha de consulta: 21 de abril del 2018].

Disponible en:

[https://books.google.com.pe/books?id=OBbWDAAAQBAJ&source=gbs\\_navlinks\\_s](https://books.google.com.pe/books?id=OBbWDAAAQBAJ&source=gbs_navlinks_s)

CIERCO, David. Cloud computing: retos y oportunidades [en línea]. España: Fundación IDEAS., 2011 [fecha de consulta: 23 de abril del 2018]. Disponible en:

[https://books.google.com.pe/books?id=fTJXVjOD90C&source=gbs\\_navlinks\\_s](https://books.google.com.pe/books?id=fTJXVjOD90C&source=gbs_navlinks_s)

ISBN: 978-84-15018-65-0

DEL RÍO, Dionisio. Diccionario-Glosario De Metodología De La Investigación Social [en línea]. España: Publicaciones UNED., 2013 [fecha de consulta: 29 de abril del 2018]. Disponible en:

[https://books.google.com.pe/books?id=GK\\_KCQAAQBAJ&source=gbs\\_navlinks\\_s](https://books.google.com.pe/books?id=GK_KCQAAQBAJ&source=gbs_navlinks_s)

ISBN: 978-84-362-6803-4

DÍAZ Y PERTUZ. Metodología para implementar una infraestructura de red que soporte servicios webcast para apoyo docente en la Universidad de Cartagena. Tesis (Licenciado en Ingeniería de sistemas). Cartagena: Universidad de Cartagena, 2015. Disponible en

[http://190.242.62.234:8080/jspui/bitstream/11227/2933/1/Tesis\\_Diaz\\_Pertuz\\_15\\_Septiembre\\_2015.pdf](http://190.242.62.234:8080/jspui/bitstream/11227/2933/1/Tesis_Diaz_Pertuz_15_Septiembre_2015.pdf)

DÍAZ, Jorge. Learning Management System y su Influencia en el Rendimiento Académico de los Alumnos de Administración a Educación en distintas Universidades [en línea]. Perú: Green publishing, 2013 [fecha de consulta: 22 de abril del 2018]. Disponible en:

[https://books.google.com.pe/books?id=1j83CwAAQBAJ&source=gbs\\_navlinks\\_s](https://books.google.com.pe/books?id=1j83CwAAQBAJ&source=gbs_navlinks_s)

ISBN: 9783668051652

DIHANE, Lois. Seguridad laboral: es preferible prevenir que gastar [en línea]. elobservador.com.uy. 12 de noviembre del 2013. [Fecha de consulta: 28 de abril del 2018]. Disponible en: <https://www.elobservador.com.uy/seguridad-laboral-es-preferible-prevenir-que-gastar-n265007>

ELIZONDO, Rosa. Aplicación de las tecnologías de información [en línea]. México: Grupo Editorial Patria., 2015 [fecha de consulta: 20 de abril del 2018]. Disponible en: [https://books.google.com.pe/books?id=mjfABgAAQBAJ&source=gbs\\_navlinks\\_s](https://books.google.com.pe/books?id=mjfABgAAQBAJ&source=gbs_navlinks_s)

ISBN: 978-607-744-081-9

ESCUADERO, María. El proceso de investigación comercial (Marketing en la actividad comercial) [en línea]. España, 2014 [fecha de consulta: 27 de mayo del 2018]. Disponible en: [https://books.google.com.pe/books?id=q57KBAAAQBAJ&source=gbs\\_navlinks\\_s](https://books.google.com.pe/books?id=q57KBAAAQBAJ&source=gbs_navlinks_s)

ESTUPIÑÁN, Niebel. Administración de riesgos E.R.M. y la auditoría interna [en línea]. 2. a ed. Colombia: Imagen editorial., 2015 [fecha de consulta: 23 de abril del 2018]. Disponible en: [https://books.google.com.pe/books?id=psK4DQAAQBAJ&source=gbs\\_navlink\\_s\\_s](https://books.google.com.pe/books?id=psK4DQAAQBAJ&source=gbs_navlink_s_s)

ISBN: 978-958-771-092-2

EXPANSIÓN en alianza con CNN [en línea]. México: 2014 [fecha de consulta: 20 de abril de 2018]. Disponible en <https://expansion.mx/tecnologia/2014/05/05/guerra-de-precios-en-streaming>

FONSECA, Oswaldo. Sistemas de Control Interno Para Organizaciones [en línea]. Perú: Publicidad & Matiz., 2011 [fecha de consulta: 24 de abril del 2018]. Disponible en: [https://books.google.com.pe/books?id=plsiU8xoQ9EC&dq=cobit+es&source=gbs\\_navlinks\\_s](https://books.google.com.pe/books?id=plsiU8xoQ9EC&dq=cobit+es&source=gbs_navlinks_s)

ISBN: 978-9972-2948-3-9

GARIBOLDI, Gerardo. Comercio electrónico: conceptos y reflexiones básicas [en línea]. Argentina: BID INTAL., 2015 [fecha de consulta: 29 de abril del 2018]. Disponible en:

[https://books.google.com.pe/books?id=bdBuE46EmFMC&source=gbs\\_navlink\\_s\\_s](https://books.google.com.pe/books?id=bdBuE46EmFMC&source=gbs_navlink_s_s)

ISBN: 950-738-078-7

GIMÉNEZ, José. Seguridad en equipos informáticos. IFCT0510 [en línea]. España: IC Editorial., 2014 [fecha de consulta: 26 de abril del 2018].

Disponible en:

[https://books.google.com.pe/books?id=GK\\_KCQAAQBAJ&source=gbs\\_navlink\\_s\\_s](https://books.google.com.pe/books?id=GK_KCQAAQBAJ&source=gbs_navlink_s_s)

ISBN: 978-84-16433-27-8

GONZALES, LEYVA Y GUTIÉRREZ. Las fuerzas competitivas de mercado y su influencia en la incorporación de las TIC en las PyME. Un estudio exploratorio [en línea]. México: 2013 [fecha de consulta: 22 de abril del 2018].

Disponible en:

[https://books.google.com.pe/books?id=gjvNCQAAQBAJ&source=gbs\\_navlinks\\_s](https://books.google.com.pe/books?id=gjvNCQAAQBAJ&source=gbs_navlinks_s)

GUERRERO y RAMOS. Introducción al Turismo [en línea]. México, 2014 [fecha de consulta: 27 de mayo del 2018]. Disponible en:

[https://books.google.com.pe/books?id=5erhBAAAQBAJ&source=gbs\\_navlinks\\_s](https://books.google.com.pe/books?id=5erhBAAAQBAJ&source=gbs_navlinks_s)

ISBN: 978-607-438-875-6

GUZMÁN, Marcela. Evaluación de Programas: Notas Técnicas [en línea]. Chile: Naciones Unidas Cepal., 2014 [fecha de consulta: 22 de abril del 2018].

Disponible en:

[https://books.google.com.pe/books?id=QkV2FTeBJVAC&source=gbs\\_navlinks\\_s](https://books.google.com.pe/books?id=QkV2FTeBJVAC&source=gbs_navlinks_s)

ISBN: 978-92-1-323110-4

IBÁÑEZ, José. todos, técnicas e instrumentos de la investigación criminológica [en línea]. España, 2015 [fecha de consulta: 27 de mayo del 2018]. Disponible en:

[https://books.google.com.pe/books?id=ggTdBAAQBAJ&source=gbs\\_navlinks\\_s](https://books.google.com.pe/books?id=ggTdBAAQBAJ&source=gbs_navlinks_s)

ISBN: 978-84-9031-848-5

Implementación de nuevas tecnologías en la empresa [Mensaje en un blog]. Santa Fe: Ciceri, G., (13 de enero del 2013). [Fecha de consulta: 28 de abril de 2018]. Recuperado de <http://thinkconsulting.com.ar/blog/implementacion-de-nuevas-tecnologias-en-la-empresa/>

Investigación básica: características, definición, ejemplos [Mensaje en un blog]. Sevilla: Rodríguez, D. (2018). [Fecha de consulta: 28 de abril de 2018]. Recuperado de <https://www.lifeder.com/investigacion-basica/>

Investigación Correlacional: Definición, Tipos y Ejemplos [Mensaje en un blog]. Sevilla: Mejía, T. (2018). [Fecha de consulta: 28 de abril de 2018]. Recuperado de <https://www.lifeder.com/investigacion-correlacional/>

Investigación Explicativa: Características, Técnicas y Ejemplos [Mensaje en un blog]. Sevilla: Yanez, D. (2018). [Fecha de consulta: 28 de abril de 2018]. Recuperado de <https://www.lifeder.com/investigacion-explicativa/>

ISBN: 978-84-7978-823-0

La ISO actualiza su norma 31000 a su versión 2018 y brinda un instrumento actualizado que permite a las empresas mejorar su gestión del riesgo [Mensaje en un blog]. La Paz: IBNORCA., (22 de febrero del 2018). [Fecha de consulta: 27 de abril de 2018]. Recuperado de <http://www.ibnorca.org/index.php/news-and-events/458-la-iso-actualiza-su-norma-31000-a-su-version-2018-y-brinda-un-instrumento-actualizado-que-permite-a-las-empresas-mejorar-su-gestion-del-riesgo>

LEÓN Y MONTERO. Metodologías científicas en Psicología [en línea]. España, 2006 [fecha de consulta: 27 de mayo del 2018]. Disponible en:

[https://books.google.com.pe/books?id=Impu-qv4sUsC&source=gbs\\_navlinks\\_s](https://books.google.com.pe/books?id=Impu-qv4sUsC&source=gbs_navlinks_s) ISBN: 84-9788-316-0

LERMA, Héctor. Metodología de la investigación: Propuesta, anteproyecto y proyecto [en línea]. Colombia, 2016 [fecha de consulta: 28 de mayo del 2018].

Disponible en:

[https://books.google.com.pe/books?id=COzDDQAAQBAJ&source=gbs\\_navlink\\_s\\_s](https://books.google.com.pe/books?id=COzDDQAAQBAJ&source=gbs_navlink_s_s) ISBN: 978-958-771-347-3

LONITA, Dan. Current Established Risk Assessment Methodologies and Tools. Tesis (Maestría en ciencias computacionales). Países bajos: Universidad Twente, 2013. Disponible en [http://essay.utwente.nl/63830/1/MSc\\_D\\_Ionita.pdf](http://essay.utwente.nl/63830/1/MSc_D_Ionita.pdf)

LUIS, José. Bicentenario: el ayer y hoy de México [en línea]. México, 2008 [fecha de consulta: 27 de mayo del 2018]. Disponible en:

[https://books.google.com.pe/books?id=ITBOAQAAIAAJ&q=gbs\\_navlinks\\_s](https://books.google.com.pe/books?id=ITBOAQAAIAAJ&q=gbs_navlinks_s)

Metodología para la evaluación de riesgos MAGERIT [Mensaje en un blog].

Lima: Correa, L., (24 de marzo de 2014). [Fecha de consulta: 28 de mayo de 2018]. Recuperado de <http://metodologia-magerit.blogspot.com/>

MINISTERIO DE HACIENDAS Y ADMINISTRACIONES PÚBLICAS. Magerit- versión 3 .0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, [en línea]. España: 2012 [fecha de consulta: 26 de abril del 2018].

Disponible en:

[https://administracionelectronica.gob.es/pae\\_Home/pae\\_Documentacion/pae\\_Metodolog/pae\\_Magerit.html#.Wv0FPYjt7IU](https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Wv0FPYjt7IU)

MOLINA, Salvador. El ciclo del crédito [en línea]. España: Biblioteca Foro ECOFIN de LID Editorial Empresarial, S.L., 2015 [fecha de consulta: 23 de abril del 2018]. Disponible en:

[https://books.google.com.pe/books?id=CaR7CAAQBAJ&source=gbs\\_navlink\\_s\\_s](https://books.google.com.pe/books?id=CaR7CAAQBAJ&source=gbs_navlink_s_s)

ISBN: 9788483569986

MOTAQUI, Katerina. Risk Analysis and Risk Management in Critical Infrastructures. Tesis (Magíster en sistemas digitales). Grecia: Universidad Piraeus, 2016. Disponible en <http://www.uajms.edu.bo/revistas/wp-content/uploads/2017/10/id-art1.pdf>

Office of Government Commerce. ITIL Transición del servicio [en línea]. Reino Unido: TSO The stationery office., 2009 [fecha de consulta: 24 de abril del 2018]. Disponible en:

[https://books.google.com.pe/books?id=x4VTDs8RudAC&source=gbs\\_navlinks\\_s](https://books.google.com.pe/books?id=x4VTDs8RudAC&source=gbs_navlinks_s)

ISBN: 978-0-11-331227-6

ORIA Y ROMERO. Recetas para una Maestra Jardinera. Ingredientes para la Planificación Didáctica [en línea]. Argentina, 2015 [fecha de consulta: 27 de mayo del 2018]. Disponible en:

[https://books.google.com.pe/books?id=DQ6gBwAAQBAJ&source=gbs\\_navlink\\_s\\_s](https://books.google.com.pe/books?id=DQ6gBwAAQBAJ&source=gbs_navlink_s_s)

ISBN: 978-987-02-8140-5

OVIEDO, Antonio. Análisis para la Interpretación de la NOM 9001:2015: Sistema de Gestión de Calidad [en línea]. México: E-duca., 2018 [fecha de consulta: 24 de abril del 2018]. Disponible en:

[https://books.google.com.pe/books?id=ffdTDwAAQBAJ&source=gbs\\_navlinks\\_s](https://books.google.com.pe/books?id=ffdTDwAAQBAJ&source=gbs_navlinks_s)

PAULA Y ROSARIO. El Análisis de la Gestión de Seguridad de tecnologías de la información en las Pymes de San Francisco de Macorís. Tesis (Magíster en auditoría y seguridad informática). San Francisco de Macorís: Universidad Autónoma de Santo Domingo, 2014. Disponible en

<https://es.slideshare.net/ramonpaula08/tesis-sobre-el-analisis-de-la-gestion-de-seguridad-de-ti-en-las-pymes-de-la-ciudad-de-sfm-ao-2014>

PONCE, Gianpierre. Diseño de una red CDN/P2P orientada al streaming de materiales académicos en el Perú. Tesis (Licenciado en Ingeniería de las Telecomunicaciones). Lima: Universidad Católica del Perú, 2013. Disponible

en

[http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/5354/PONCE\\_GIANPIERRE\\_DISE%C3%91O\\_RED\\_CDN\\_P2P\\_STREAMING\\_MATERIAL\\_ES\\_ACADEMICOS\\_PERU.pdf?sequence=1&isAllowed=y](http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/5354/PONCE_GIANPIERRE_DISE%C3%91O_RED_CDN_P2P_STREAMING_MATERIAL_ES_ACADEMICOS_PERU.pdf?sequence=1&isAllowed=y)

PULIDO, BALLÉN Y ZÚÑIGA. Abordaje hermenéutico de la investigación cualitativa. Teorías, procesos, técnicas [en línea]. Colombia, 2015 [fecha de consulta: 27 de mayo del 2018]. Disponible en:

[https://books.google.com.pe/books?id=B2L6wakmplwC&source=gbs\\_navlinks\\_s](https://books.google.com.pe/books?id=B2L6wakmplwC&source=gbs_navlinks_s)

ISBN: 958-8325-24-8

SEMANAeconómica.com [en línea]. Perú: 2013 [fecha de consulta: 20 de abril de 2018]. Disponible en <http://semanaeconomica.com/article/sectores-y-empresas/tecnologia/128530-el-creciente-mercado-del-streaming-en-el-peru-y-sus-posibilidades/>

SETH, Godin. ¡Hazlo! [en línea]. España: Ediciones B, S.A., 2012 [fecha de consulta: 22 de abril del 2018]. Disponible en:

[https://books.google.com.pe/books?id=QZY4AwAAQBAJ&source=gbs\\_navlink\\_s\\_s](https://books.google.com.pe/books?id=QZY4AwAAQBAJ&source=gbs_navlink_s_s)

ISBN: 978-84-15389-58-3

SOLIS, David. Podcasting fácil para docentes y alumnos [en línea]. México: Grupo cultural ARGON., 2010 [fecha de consulta: 21 de abril del 2018].

Disponible en:

[https://books.google.com.pe/books?id=tQiNGcvbodAC&source=gbs\\_navlinks\\_s](https://books.google.com.pe/books?id=tQiNGcvbodAC&source=gbs_navlinks_s)

ISBN: 968-5599-13-0

TTIMOTHY, Galpin. Medir el desempeño: La cara humana del cambio [en línea]. España: Ediciones Díaz de Santos., 2013 [fecha de consulta: 21 de abril del 2018]. Disponible en:

[https://books.google.com.pe/books?id=cR8BAQAAQBAJ&source=gbs\\_navlinks\\_sl](https://books.google.com.pe/books?id=cR8BAQAAQBAJ&source=gbs_navlinks_sl)

SBN: 978-84-9969-629-4

VARGAS, Joffre. Propuesta tecnológica basada en Cobit 5 aplicada a la gestión de las TI en la EIS. Tesis (Licenciado en sistemas informáticos).

Riobamba: Escuela Superior Politécnica de Chimborazo, 2015. Disponible en

<http://dspace.espoch.edu.ec/bitstream/123456789/4397/1/18T00602.docx.pdf>

VASCONCELOS, Jorge. Tecnologías de la Información [en línea]. México:

Grupo Editorial Patria., 2015 [fecha de consulta: 21 de abril del 2018].

Disponible en:

[https://books.google.com.pe/books?id=6M1UCwAAQBAJ&source=gbs\\_navlinks\\_sl](https://books.google.com.pe/books?id=6M1UCwAAQBAJ&source=gbs_navlinks_sl)

[S](#)

ISBN: 978-607-744-246-2

VELAZQUEZ, Luis. Estadística Descriptiva y Probabilidad con Excel [en línea].

México, 2018 [fecha de consulta: 2 de junio del 2018]. Disponible en:

[https://books.google.com.pe/books?id=eJ8vDwAAQBAJ&source=gbs\\_navlinks\\_sl](https://books.google.com.pe/books?id=eJ8vDwAAQBAJ&source=gbs_navlinks_sl)

[S](#)

VENEGAS, Henry. Marco de trabajo RISK IT en la gestión de riesgos de

tecnología de la información en la Caja Rural de Ahorro y Crédito Los Andes

S.A. Tesis (Licenciado en Ingeniería de sistemas). Puno: Universidad Nacional del Altiplano, 2015. Disponible en

[http://repositorio.unap.edu.pe/bitstream/handle/UNAP/5561/Venegas\\_Carazas\\_Jhon\\_Yeffer.pdf?sequence=1&isAllowed=y](http://repositorio.unap.edu.pe/bitstream/handle/UNAP/5561/Venegas_Carazas_Jhon_Yeffer.pdf?sequence=1&isAllowed=y)

[Jhon\\_Yeffer.pdf?sequence=1&isAllowed=y](#)



## **ANEXOS**

### Anexo N° 1: Matriz de consistencia

Problemas	Objetivos	Hipótesis	Variables		Dimensiones	Items	Metodología
			General	1			
<b>General</b> ¿Qué relación existe entre los factores de riesgo en tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC?	<b>General</b> O <sub>0</sub> : Determinar la relación entre los factores de riesgo en tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.	<b>General</b> H <sub>0</sub> : Existe una relación positiva entre los factores de riesgo en tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.	1 Factores de riesgo de las tecnologías de información		Método de análisis de riesgo  Proyecto de análisis de riesgo	Determinar activos relevantes para la organización. Determinar a qué amenazas están expuestos a aquellos activos. Control y mantenimiento de equipos. Estimar el impacto, definido como el daño sobre el activo. Estimar el riesgo por parte del personal. Frecuencia de fallas técnicas que representen riesgos. Estudio de oportunidad. Asignación de responsabilidades. Servicios externos contratados adecuados. Determinar estado del funcionamiento de procesos. Existencia del personal suficiente para cada proceso. Existencia de concientización e identificación de riesgos por parte del personal. Identificación de requerimientos mínimos para evitar los riesgos. Capacitaciones para la gestión de riesgos. Identificación de riesgos con frecuencia. Documentación el estado de los procesos. Aplicación de permisos y control de usuarios. Licencias actualizadas de software. Ambientes eléctricos estables. Realización de informes del estado del desempeño de los procesos.	<b>Método de investigación:</b> Hipotético deductivo.  <b>Tipo de estudio:</b> Explicativo-correlacional-básica.  <b>Diseño de investigación:</b> Correlacional
<b>Específicos</b> P <sub>2</sub> : ¿Qué relación existe entre los factores de riesgo en tecnologías de información y el eficiente desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC?	<b>Específicos</b> H <sub>2</sub> : Existe una relación positiva entre los factores de riesgo en tecnologías de información y el eficiente desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.	Eficacia	Calidad de servicio	Transmisiones óptimas. Incidencias resueltas eficaces. Interrupciones durante la transmisión. La plataforma funciona correctamente. Capacitación del personal. Uso de guías para el correcto desempeño del webcast. Logro de audiencia esperada. Uso de guías o manuales sobre calidad. Libre acceso a usuarios. Programas emitidos a tiempo. Acceso a archivos multimedia fuera de transmisión. Interacción con los usuarios Calidad de imagen y audio óptima.	<b>Técnica e instrumento:</b> Entrevistas, Cuestionario		
<b>Específicos</b> P <sub>3</sub> : ¿Qué relación existe entre los factores de riesgo en tecnologías de información y la calidad de servicio en el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC?	<b>Específicos</b> H <sub>3</sub> : Existe una relación positiva entre los factores de riesgo en tecnologías de información y la calidad de servicio en el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.					Calidad de servicio	Calidad de servicio

## Anexo N° 2: Ficha técnica. Instrumento de recolección de datos

Autor	Romero Camones Jamie Evelyn	
Nombre de instrumento	Cuestionario	
Lugar	ATOGAPAN S.A. de C.V	
Fecha de aplicación	01 de abril del 2018	
Objetivo	Determinar la relación entre los factores de riesgo en tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.	
Tiempo de duración	28 días (Lunes a sábado)	
<b>Elección de técnica e instrumento</b>		
Variable	Técnica	Instrumento
Variable dependiente Desempeño del webcast	Entrevista	Cuestionario
Variable Independiente Factores de riesgo de las tecnologías de información	Entrevista	Cuestionario
Fuente: Elaboración propia		

Autor	Romero Camones Jamie Evelyn	
Nombre de instrumento	Cuestionario	
Lugar	Grupo HCM comunicaciones SAC	
Fecha de aplicación	01 de abril del 2018	
Objetivo	Determinar la relación entre los factores de riesgo en tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC.	
Tiempo de duración	28 días (Lunes a sábado)	
<b>Elección de técnica e instrumento</b>		
Variable	Técnica	Instrumento
Variable dependiente Desempeño del webcast	Entrevista	Cuestionario
Variable Independiente Factores de riesgo de las tecnologías de información	Entrevista	Cuestionario
Fuente: Elaboración propia		

### Anexo N° 3: Instrumento de investigación

#### CUESTIONARIO

Para medir los factores de riesgo asociados al desempeño del webcast dirigido al personal de los epicentros de Radio Atogapan.

Datos generales:

Epicentro: .....

Área y cargo: .....

Responda las preguntas en una escala del 1 al 5 colocando una X según consideres, en donde las opciones de respuesta tienen el equivalente a:

1= Nunca, 2= Casi nunca, 3= A veces, 4= Casi siempre y 5= Siempre.

	DIMENSIONES	ESCALA				
		1	2	3	4	5
<b>MÉTODO DE ANÁLISIS DE RIESGO</b>						
1	¿La empresa cuenta con infraestructura T.I adecuada para el correcto desempeño de las actividades?					
2	¿Cuentan con un método de identificación de amenazas para sus activos?					
3	¿Se realiza el control y mantenimiento de equipos con frecuencia?					
4	¿Se lleva el control de pérdidas causadas por la falta de transmisiones?					
5	¿La organización invierte en nuevas tecnologías de información?					
6	¿Son frecuentes las fallas presentadas por otras razones ajenas a la infraestructura TI?					
<b>PROYECTO DE ANÁLISIS DE RIESGO</b>						
7	¿Si se implementa un proyecto para la gestión de riesgo, cree que se le asignaría los recursos necesarios?					
8	¿Las computadoras están conectadas a una red de corriente estable?					
9	¿Cuentan con un servicio de internet adecuado para los procesos que realizan?					
10	¿La infraestructura TI con la que cuenta tiene un óptimo funcionamiento?					
11	¿Considera que se asigna el suficiente personal técnico y de apoyo al soporte de sistemas?					
12	¿El personal está concientizado sobre los riesgos a los que está expuesta la falta de transmisiones?					
13	¿Se definen las características mínimas de infraestructura TI para minimizar los riesgos?					
<b>PLAN DE SEGURIDAD</b>						
14	¿La empresa implementa planes de capacitación para la gestión de riesgos ?					
15	¿Se identifica con frecuencia los riesgos significativos?					
16	¿Se documenta el estado de cada transmisión ?					
17	¿Se tiene una cuenta establecida para cada usuario ?					
18	¿La empresa cuenta con las licencias de software actualizadas?					
19	¿Existe un responsable directo responsable de los cambios que se realizan en sus procesos?					
20	¿Se realizan informes oportunos que demuestren el eficiente desempeño del webcast?					

Fuente: MAGERIT

### CUESTIONARIO

Para medir las dimensiones del desempeño del webcast dirigido al personal de los epicentros de Radio Atogapan.

Datos generales:

Epicentro: .....

Área y cargo: .....

Responda las preguntas en una escala del 1 al 5 colocando una X según consideres, en donde las opciones de respuesta tienen el equivalente a:

1= Nunca, 2= Casi nunca, 3= A veces, 4= Casi siempre y 5= Siempre.

	DIMENSIONES	ESCALA				
		1	2	3	4	5
<b>EFICIENCIA</b>						
1	¿Se realiza supervisiones y mantenimiento de equipos antes de cada transmisión?					
2	¿La cantidad de transmisiones programadas es igual al de transmisiones realizadas?					
3	¿Se invierte en infraestructura TI para el mejor desempeño del webcast?					
4	¿La coordinación y comunicación entre el personal de trabajo es eficiente?					
5	¿Se realizan procedimientos para la evaluación de riesgos para cumplir con un eficiente desempeño?					
6	¿El ancho de banda con el que se cuenta es el adecuado para el eficiente desempeño durante la transmisión?					
7	¿Se ha pensado alguna vez en implementar un estandar o guía para el control de riesgos de TI?					
<b>EFICACIA</b>						
8	¿Las transmisiones programadas van acorde a las emitidas?					
9	¿La forma que manejan para resolver las incidencias presentadas funciona?					
10	¿ Los programas emitidos están libres de cortes durante las transmisiones?					
11	¿ La plataforma adoptada para la transmisión presenta fallos?					
12	¿ El personal encargado de la ejecución del webcast se capacita constantemente?					
13	¿Se ha pensado alguna vez en implementar una guía o estandar para realizar el webcast y que sea eficaz?					
14	¿Durante las transmisiones se logra alcanzar la audiencia esperada?					
<b>CALIDAD DE SERVICIO</b>						
15	¿Se ha pensado alguna vez en implementar una norma o guía estandarizada para garantizar la calidad de servicio?					
16	¿ Existe libre acceso a sus transmisiones?					
17	¿ Los programas son emitidos en las horas establecidas?					
18	¿Se puede acceder al contenido de la transmisión fuera de la programación en vivo?					
19	¿Existe interacción con los usuarios durante las transmisiones?					
20	¿La calidad de imagen y audio que se brinda durante las transmisiones es óptima?					

Fuente: MAGERIT

### CUESTIONARIO

Para medir los factores de riesgo asociados al desempeño del webcast dirigido al personal del Grupo HCM Comunicaciones SAC.

Datos generales:

Área y cargo: .....

Responda las preguntas en una escala del 1 al 5 colocando una X según consideres, en donde las opciones de respuesta tienen el equivalente a:

1= Nunca, 2= Casi nunca, 3= A veces, 4= Casi siempre y 5= Siempre.

	DIMENSIONES	ESCALA				
		1	2	3	4	5
<b>MÉTODO DE ANÁLISIS DE RIESGO</b>						
1	¿La empresa cuenta con infraestructura T.I adecuada para el correcto desempeño de las actividades?					
2	¿Cuentan con un método de identificación de amenazas para sus activos?					
3	¿Se realiza el control y mantenimiento de equipos con frecuencia?					
4	¿Se lleva el control de pérdidas causadas por la falta de transmisiones?					
5	¿La organización invierte en nuevas tecnologías de información?					
6	¿Son frecuentes las fallas presentadas por otras razones ajenas a la infraestructura TI?					
<b>PROYECTO DE ANÁLISIS DE RIESGO</b>						
7	¿Si se implementa un proyecto para la gestión de riesgo, cree que se le asignaría los recursos necesarios?					
8	¿Las computadoras están conectadas a una red de corriente estable?					
9	¿Cuentan con un servicio de internet adecuado para los procesos que realizan?					
10	¿La infraestructura TI con la que cuenta tiene un óptimo funcionamiento?					
11	¿Considera que se asigna el suficiente personal técnico y de apoyo al soporte de sistemas?					
12	¿El personal está concientizado sobre los riesgos a los que está expuesta la falta de transmisiones?					
13	¿Se definen las características mínimas de infraestructura Ti para minimizar los riesgos?					
<b>PLAN DE SEGURIDAD</b>						
14	¿La empresa implementa planes de capacitación para la gestión de riesgos ?					
15	¿Se identifica con frecuencia los riesgos significativos?					
16	¿Se documenta el estado de cada transmisión ?					
17	¿Se tiene una cuenta establecida para cada usuario ?					
18	¿La empresa cuenta con las licencias de software actualizadas?					
19	¿Existe un responsable directo responsable de los cambios que se realizan en sus procesos?					
20	¿ Se realizan informes oportunos que demuestren el eficiente desempeño del webcast?					

Fuente: MAGERIT

### CUESTIONARIO

Para medir las dimensiones del desempeño del webcast dirigido al personal del Grupo HCM Comunicaciones SAC.

Datos generales:

Área y cargo: .....

Responda las preguntas en una escala del 1 al 5 colocando una X según consideres, en donde las opciones de respuesta tienen el equivalente a:

1= Nunca, 2= Casi nunca, 3= A veces, 4= Casi siempre y 5= Siempre.

	DIMENSIONES	ESCALA				
		1	2	3	4	5
<b>EFICIENCIA</b>						
1	¿Se realiza supervisiones y mantenimiento de equipos antes de cada transmisión?					
2	¿La cantidad de transmisiones programadas es igual al de transmisiones realizadas?					
3	¿ Se invierte en infraestructura TI para el mejor desempeño del webcast?					
4	¿ La coordinación y comunicación entre el personal de trabajo es eficiente?					
5	¿Se realizan procedimientos para la evaluación de riesgos para cumplir con un eficiente desempeño?					
6	¿El ancho de banda con el que se cuenta es el adecuado para el eficiente desempeño durante la transmisión?					
7	¿Se ha pensado alguna vez en implementar un estandar o guía para el control de riesgos de TI?					
<b>EFICACIA</b>						
8	¿Las transmisiones programadas van acorde a las emitidas?					
9	¿ La forma que manejan para resolver las incidencias presentadas funciona?					
10	¿ Los programas emitidos están libres de cortes durante las transmisiones?					
11	¿ La plataforma adoptada para la transmisión presenta fallos?					
12	¿ El personal encargado de la ejecución del webcast se capacita constantemente?					
13	¿Se ha pensado alguna vez en implementar una guía o estandar para realizar el webcast y que sea eficaz?					
14	¿Durante las transmisiones se logra alcanzar la audiencia esperada?					
<b>CALIDAD DE SERVICIO</b>						
15	¿Se ha pensado alguna vez en implementar una norma o guía estandarizada para garantizar la calidad de servicio?					
16	¿ Existe libre acceso a sus transmisiones?					
17	¿ Los programas son emitidos en las horas establecidas?					
18	¿Se puede acceder al contenido de la transmisión fuera de la programación en vivo?					
19	¿Existe interacción con los usuarios durante las transmisiones?					
20	¿La calidad de imagen y audio que se brinda durante las transmisiones es óptima?					

Fuente: MAGERIT

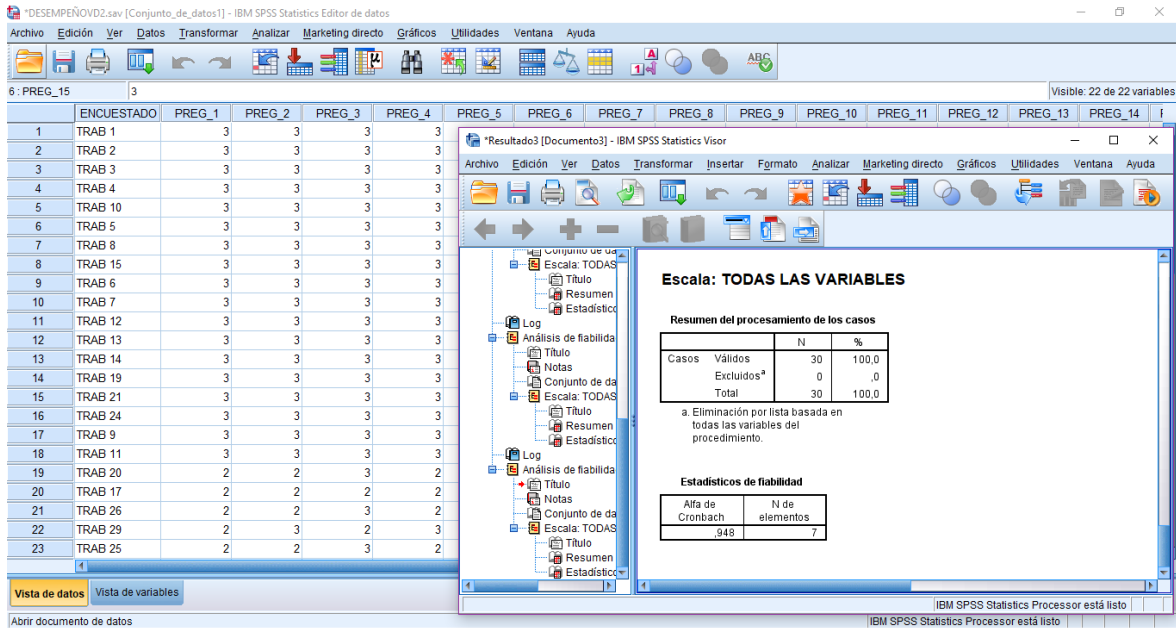




N° DE TRAB.	MÉTODO DE ANALISIS DE RIESGO						PROYECTO DE ANALISIS DE RIESGO						PLAN DE SEGURIDAD						T		
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18		19	20
1	4	5	5	5	4	4	4.5	5	4	4	5	5	5	4.71	5	5	5	5	5	5	5
2	4	5	5	5	4	4	4.5	5	4	4	5	5	5	4.71	5	5	5	5	5	5	5
3	4	5	5	5	4	4	4.5	5	4	4	5	5	5	4.71	5	5	5	5	5	5	5
4	4	5	4	5	4	4	4.3	4	4	4	4	5	5	4.43	5	4	5	5	5	5	5
5	4	5	4	5	4	4	4.3	4	4	4	4	5	5	4.57	5	4	5	5	5	5	5
6	4	5	4	5	4	4	4.3	4	4	4	4	5	5	4.43	5	4	5	5	5	5	5
7	4	5	4	5	3	3	4.0	4	4	4	4	5	5	4.43	5	4	5	5	5	5	5
8	4	5	4	5	4	4	4.3	5	4	4	5	5	5	4.71	5	4	5	5	5	5	5
9	3	5	5	5	4	4	4.3	5	4	5	5	5	5	5	5	5	5	5	5	5	5
10	3	5	5	5	4	4	4.3	5	4	5	5	5	5	5	5	5	5	5	5	5	5
11	3	5	5	5	3	3	4.0	4	4	5	5	5	5	4.71	5	5	5	5	5	5	5
12	4	5	5	5	5	5	4.8	4	4	5	4	5	5	4.57	5	5	5	5	5	5	5
13	4	5	5	5	4	4	4.5	4	4	5	4	5	5	4.57	5	5	5	5	5	5	5
14	4	5	5	5	4	4	4.5	4	4	5	4	5	5	4.57	5	5	5	5	5	5	5
15	4	5	5	5	4	4	4.5	4	4	5	4	5	5	4.57	5	5	5	5	5	5	5
16	4	5	4	4	4	4	4.2	5	4	5	4	5	5	4.57	5	4	4	5	5	5	4
17	4	5	4	4	4	4	4.2	5	4	5	4	5	5	4.57	5	4	4	5	5	5	4
18	4	5	4	4	4	4	4.2	5	4	5	4	5	5	4.57	5	4	4	5	5	5	4
19	4	5	5	5	5	5	4.8	4	4	5	4	5	5	4.71	5	5	5	5	5	5	5
20	4	5	5	5	4	4	4.5	4	4	5	4	5	5	4.71	5	5	5	5	5	5	5
21	4	5	5	5	4	4	4.5	4	4	5	4	5	5	4.71	5	5	5	5	5	5	5
22	4	5	4	5	4	4	4.3	5	4	5	4	5	4	4.57	5	5	5	5	5	5	4
23	4	5	4	5	3	3	4.0	5	4	5	4	5	4	4.57	5	5	5	5	5	5	4
24	3	5	5	4	3	3	3.8	5	4	5	4	5	5	4.71	5	4	4	5	4	5	5
25	3	5	5	4	4	4	4.2	4	4	5	4	5	5	4.57	5	4	4	5	4	5	5
26	3	5	5	4	4	4	4.2	4	4	5	4	5	5	4.57	5	4	4	5	4	5	5
27	4	5	4	5	4	4	4.3	5	4	5	4	5	4	4.71	5	4	5	5	5	5	5
28	4	5	4	5	4	4	4.3	5	4	5	4	5	4	4.71	5	4	5	5	5	5	5
29	4	5	4	5	4	4	4.3	5	4	5	4	5	4	4.71	5	4	5	5	5	5	5
30	4	5	4	5	4	4	4.3	5	4	5	4	5	4	4.86	5	4	5	5	5	5	5
							4.333							4.65							4.86

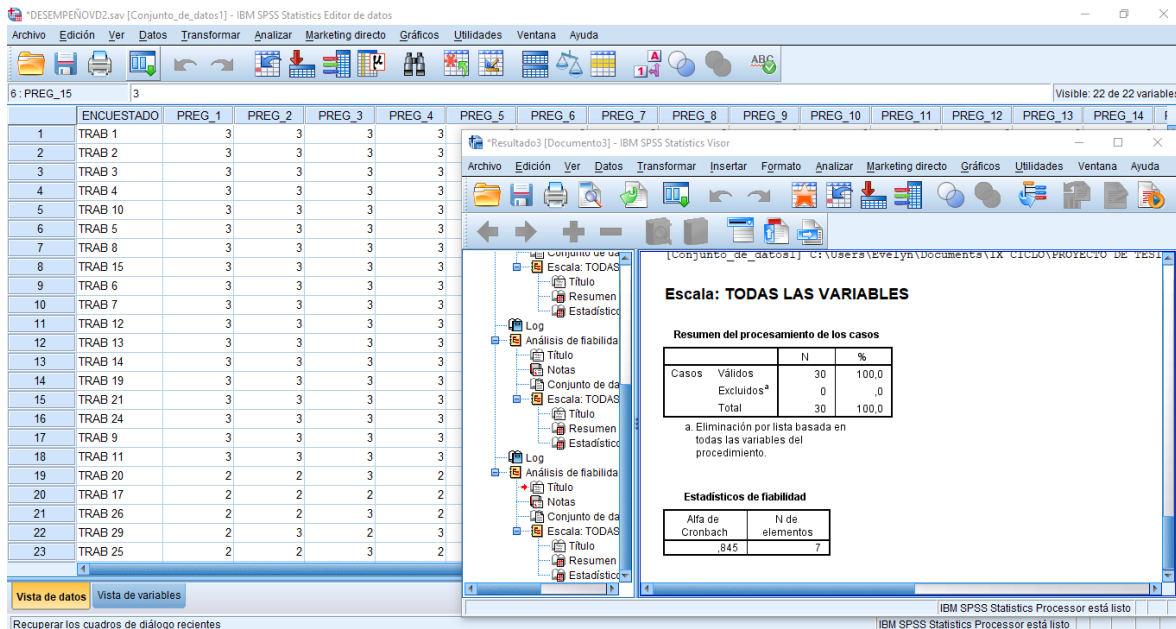
## Anexo N° 5: Resultados de la confiabilidad del instrumento

### Para el indicador de eficiencia



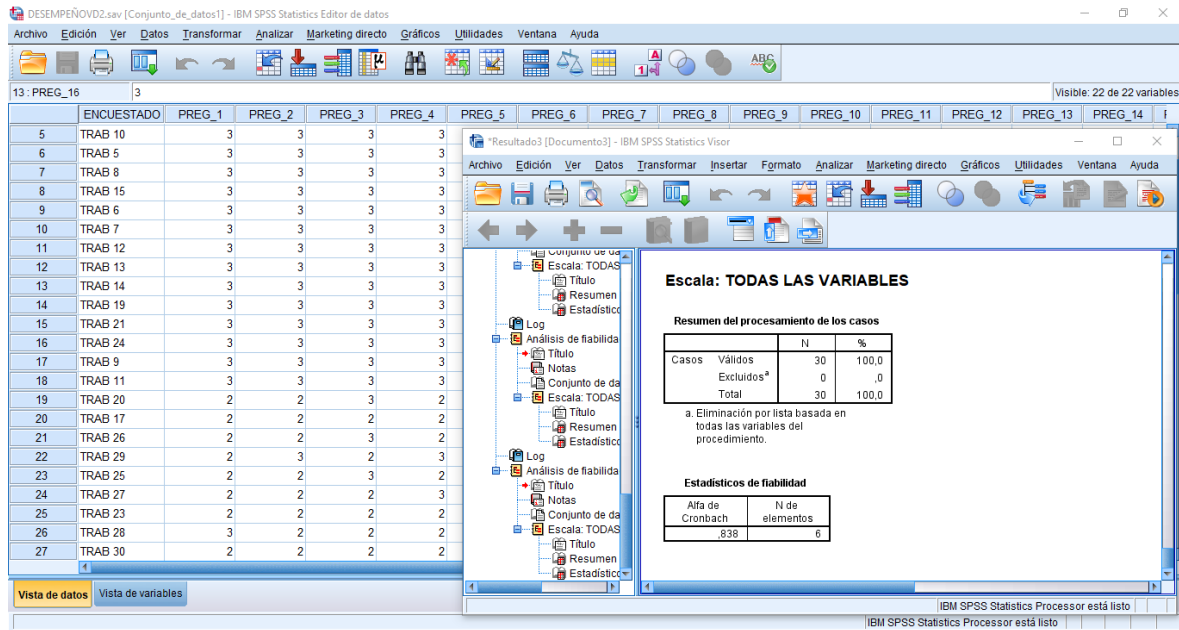
Como el resultado es 0,948 siendo mayor a 0,8. Por lo tanto, el instrumento es confiable para medir la eficiencia.

### Para el indicador de eficacia



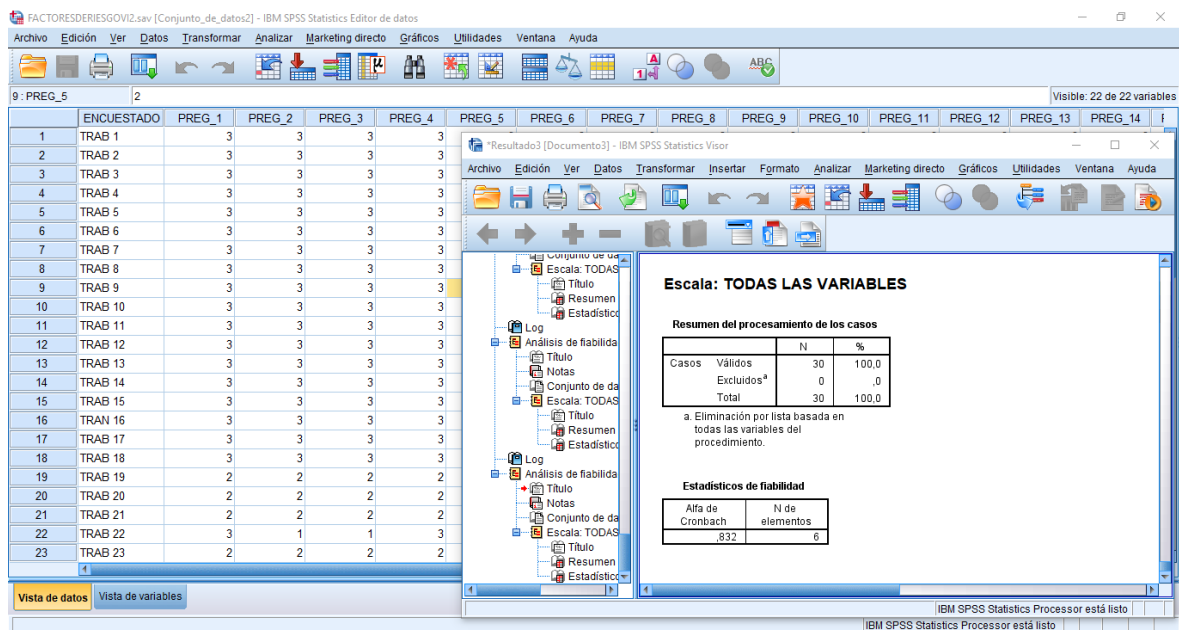
Como el resultado es 0,845 siendo mayor a 0,8 Por lo tanto, el instrumento es confiable para medir la eficacia.

### Para el indicador de calidad de servicio



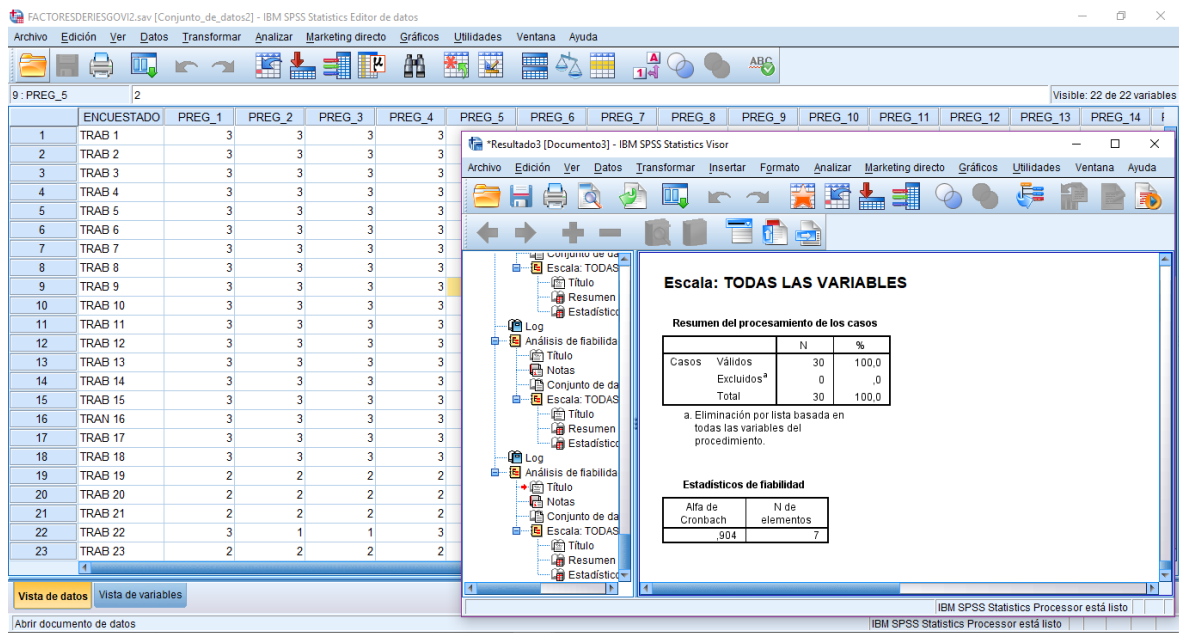
Como el resultado es 0,838 siendo mayor a 0,8. Por lo tanto, el instrumento es confiable para medir la calidad de servicio.

### Para el indicador de método de análisis de riesgo



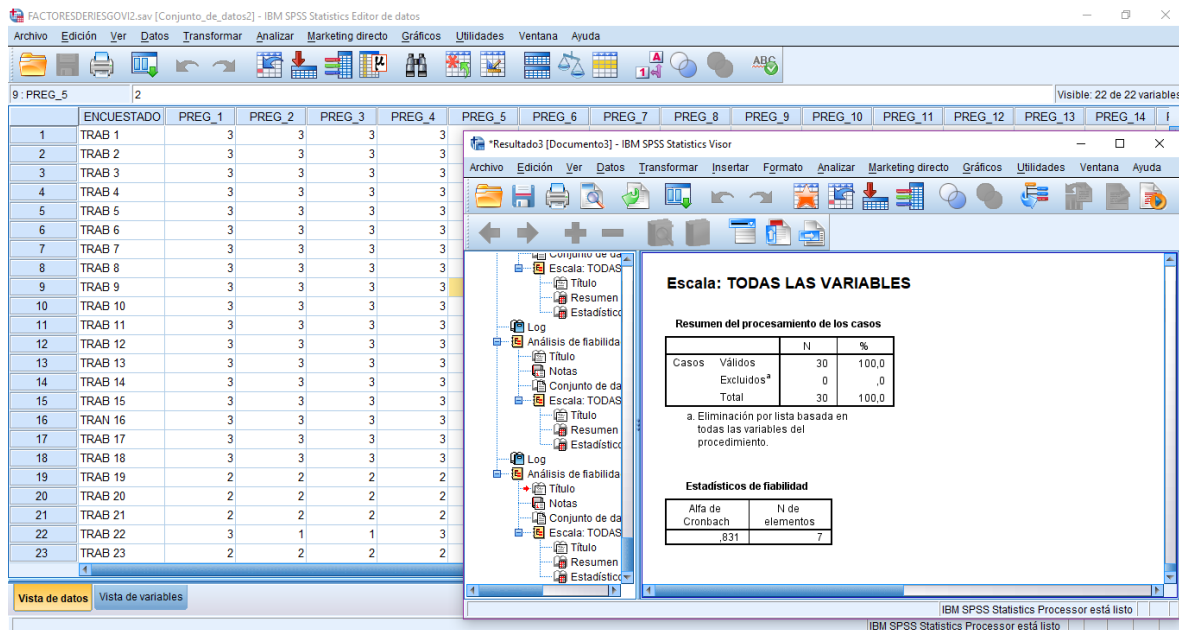
Como el resultado es 0,832 siendo mayor a 0,8. Por lo tanto, el instrumento es confiable para medir la método de análisis de riesgo.

## Para el indicador de proyecto de análisis de riesgo



Como el resultado es 0,904 siendo mayor a 0,8. Por lo tanto, el instrumento es confiable para medir la proyecto de análisis de riesgo.

## Para el indicador de plan de seguridad



Como el resultado es 0,831 siendo mayor a 0,8. Por lo tanto, el instrumento es confiable para medir la plan de seguridad.

### Anexo N° 6: Validación de la metodología

**Anexo 6: Validación del instrumento-Selección de la metodología**

**TABLA DE EVALUACIÓN DE EXPERTOS**

Apellidos y nombres del experto: ORDÓÑEZ BEREZ, ROSA CAROLINA

Título y/o grado: DOCTOR / MAGÍSTER EN INGENIERÍA DE SISTEMAS

Ph. D ( )	Doctor (X)	Magister ( )	Ingeniero ( )	Licenciado( )	Otro ( ) _____
-----------	------------	--------------	---------------	---------------	----------------

Universidad que labora: Universidad César Vallejo

Fecha: 09-05-2018

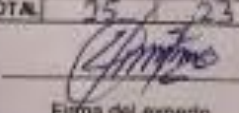
**TITULO DE PROYECTO**

**Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC**

**Evaluación de la metodología**

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar las metodologías involucradas, mediante una serie de preguntas en escala de 1 a 5, siendo 1 la menor calificación y 5 la mayor calificación.

	CRITERIOS	ISO 31000:2009	COBIT	MAGERIT	OBSERVACIONES
1	Buena concurrencia a los responsables de las organizaciones de la existencia de riesgos.	4	4	5	
2	Es una metodología que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones.	4	4	5	
3	Cuenta con todo un documento que reúne técnicas y ejemplos de cómo realizar el análisis de riesgos.	4	3	5	
4	Divide los roles de la organización en diferentes grupos, para identificar más riesgos y poder tomar decisiones para evitar cualquier riesgo.	4	4	5	
5	Los objetivos y resultados esperados en cada fase se distinguen fácilmente.	5	4	5	
6	Es libre y no requiere de autorización para su uso.	4	4	5	
<b>TOTAL</b>		<b>25</b>	<b>23</b>	<b>30</b>	

  
 Firma del experto

**Anexo 5: Validación del instrumento-Selección de la metodología**

**TABLA DE EVALUACIÓN DE EXPERTOS**

Apellidos y nombres del experto: Buenos Aires Jiménez Jorge A.

Título y/o grado: \_\_\_\_\_

Ph.D ( )	Doctor ( )	Magister (X)	Ingeniero ( )	Licenciado ( )	Otro ( ) _____
----------	------------	--------------	---------------	----------------	----------------

Universidad que labora: Universidad César Vallejo

Fecha: 14-05-18

**TITULO DE PROYECTO**

**Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC**

**Evaluación de la metodología**

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar las metodologías involucradas, mediante una serie de preguntas en escala de 1 a 5, siendo 1 la menor calificación y 5 la mayor calificación.

	CRITERIOS	ISO 31000:2009	COBIT	MAGERIT	OBSERVACIONES
1	Buena ocasión a los responsables de las organizaciones de la existencia de riesgos.	5	4	5	
2	Es una metodología que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones.	4	4	5	
3	Cuenta con todo un documento que reúne técnicas y ejemplos de cómo realizar el análisis de riesgos.	5	4	5	
4	Divide los activos de la organización en diferentes grupos, para identificar más riesgos y poder tomar contamedidas para evitar cualquier riesgo.	5	5	5	
5	Los objetivos y resultados esperados en cada fase se distinguen fácilmente.	5	5	5	
6	Es libre y no requiere de autorización para su uso.	4	5	5	
<b>TOTAL:</b>		<b>28</b>	<b>27</b>	<b>30</b>	

A. Buenos Aires Jiménez  
Firma del experto

**Anexo 6: Validación del instrumento-Selección de la metodología**

**TABLA DE EVALUACIÓN DE EXPERTOS**

Apellidos y nombres del experto: Gálvez Tapia O. Noris.

Título y/o grado: Magister en Ingeniería de Sistemas.

Ph. D ( )	Doctor ( )	Magister <input checked="" type="checkbox"/>	Ingeniero ( )	Licenciado ( )	Otro ( ) _____
-----------	------------	--	---------------	----------------	----------------

Universidad que labora: Universidad César Vallejo

Fecha: 14/05/2018

**TITULO DE PROYECTO**

**Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC**

**Evaluación de la metodología**

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar las metodologías involucradas, mediante una serie de preguntas en escala de 1 a 5, siendo 1 la menos calificación y 5 la mayor calificación.

	CRITERIOS	ISO 31000:2009	COBIT	MAGERIT	OBSERVACIONES
1	Busca concienciar a los responsables de las organizaciones de la existencia de riesgos.	4	3	5	
2	Es una metodología que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones.	4	3	5	
3	Cuenta con todo un documento que reúne técnicas y ejemplos de cómo realizar el análisis de riesgos.	5	3	5	
4	Divide los activos de la organización en diferentes grupos, para identificar más riesgos y poder tomar contramedidas para evitar cualquier riesgo.	5	3	5	
5	Los objetivos y resultados esperados en cada fase se distinguen fácilmente.	5	3	5	
6	Es libre y no requiere de autorización para su uso.	5	3	5	
<b>TOTAL</b>		<b>28</b>	<b>18</b>	<b>30</b>	

*Daisy*  
Firma del experto

## Validación del instrumento por los expertos.

### Evaluación del instrumento de investigación

#### TABLA DE EVALUACIÓN DE EXPERTOS

Apellidos y nombres del experto: Ordoñez Pérez, Adilio Christian

Título y/o grado: Doctor / Magister en Ingeniería de Sistemas

Ph. D ( )	Doctor (X)	Magister ( )	Ingeniero ( )	Licenciado( )	Otro ( ) _____
-----------	------------	--------------	---------------	---------------	----------------

Universidad que labora: Universidad César Vallejo

Fecha: \_\_\_\_\_

#### TITULO DE PROYECTO

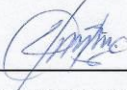
**Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC**

#### EFICIENCIA

#### Evaluación del instrumento

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar los indicadores, mediante una serie de preguntas con puntuaciones específicas los cuales validan los indicadores.

ITEMS	PREGUNTAS	VALORACIÓN				
		Deficiente 0-20%	Regular 21-50%	Bueno 51-70%	Muy bueno 71-80%	Excelente 81-100%
1	¿Tiene relación con el título de investigación?					95
2	¿Se mencionan las variables de investigación?					95
3	¿Facilitará el logro de los objetivos de investigación?					95
4	¿Guarda relación con las variables de investigación?					95
5	¿Permitirá el análisis y procesamiento de datos?					95
6	¿Las preguntas son sencillas de comprender y responder?					95
7	¿Será accesible a la población para la recolección de datos?					95
8	¿Las alternativas de respuesta permiten obtener la información de forma clara y precisa?					95

  
 \_\_\_\_\_  
 Firma del experto



**Evaluación del instrumento de investigación**

**TABLA DE EVALUACIÓN DE EXPERTOS**

Apellidos y nombres del experto: Ordoñez Pérez, Adilio Christian

Título y/o grado: Doctor / Magister en Ingeniería de Sistemas

Ph. D ( )	Doctor (X)	Magister ( )	Ingeniero ( )	Licenciado ( )	Otro ( ) _____
-----------	------------	--------------	---------------	----------------	----------------

Universidad que labora: Universidad César Vallejo

Fecha: \_\_\_\_\_

**TITULO DE PROYECTO**

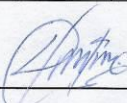
**Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC**

**EFICACIA**

**Evaluación del instrumento**

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar los indicadores, mediante una serie de preguntas con puntuaciones específicas los cuales validan los indicadores.

ITEMS	PREGUNTAS	VALORACIÓN				
		Deficiente	Regular	Bueno	Muy bueno	Excelente
		0-20%	21-50%	51-70%	71-80%	81-100%
1	¿Tiene relación con el título de investigación?					95
2	¿Se mencionan las variables de investigación?					95
3	¿Facilitará el logro de los objetivos de investigación?					95
4	¿Guarda relación con las variables de investigación?					95
5	¿Permitirá el análisis y procesamiento de datos?					95
6	¿Las preguntas son sencillas de comprender y responder?					95
7	¿será accesible a la población para la recolección de datos?					95
8	¿Las alternativas de respuesta permiten obtener la información de forma clara y precisa?					95

  
Firma del experto

**Evaluación del instrumento de investigación**

**TABLA DE EVALUACIÓN DE EXPERTOS**

Apellidos y nombres del experto: Ordoñez Pérez, Adilio Christian

Título y/o grado: Doctor / Magister en Ingeniería de Sistemas

Ph. D ( )	Doctor (x)	Magister ( )	Ingeniero ( )	Licenciado( )	Otro ( ) _____
-----------	------------	--------------	---------------	---------------	----------------

Universidad que labora: Universidad César Vallejo

Fecha: \_\_\_\_\_

**TITULO DE PROYECTO**

**Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC**

**CALIDAD DE SERVICIO**

**Evaluación del instrumento**

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar los indicadores, mediante una serie de preguntas con puntuaciones específicas los cuales validan los indicadores.

ITEMS	PREGUNTAS	VALORACIÓN				
		Deficiente	Regular	Bueno	Muy bueno	Excelente
		0-20%	21-50%	51-70%	71-80%	81-100%
1	¿Tiene relación con el título de investigación?					95
2	¿Se mencionan las variables de investigación?					85
3	¿Facilitará el logro de los objetivos de investigación?					95
4	¿Guarda relación con las variables de investigación?					95
5	¿Permitirá el análisis y procesamiento de datos?					95
6	¿Las preguntas son sencillas de comprender y responder?					95
7	¿Será accesible a la población para la recolección de datos?					95
8	¿Las alternativas de respuesta permiten obtener la información de forma clara y precisa?					95

  
\_\_\_\_\_  
Firma del experto

**Evaluación del instrumento de investigación**

**TABLA DE EVALUACIÓN DE EXPERTOS**

Apellidos y nombres del experto: Ordoñez Pérez, Adilio Christian

Título y/o grado: Doctor / Magister en Ingeniería de Sistemas

Ph. D ( )	Doctor (x)	Magister ( )	Ingeniero ( )	Licenciado( )	Otro ( ) _____
-----------	------------	--------------	---------------	---------------	----------------

Universidad que labora: Universidad César Vallejo

Fecha: \_\_\_\_\_

**TITULO DE PROYECTO**

**Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC**

**MÉTODO DE ANÁLISIS DE RIESGO**

**Evaluación del instrumento**

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar los indicadores, mediante una serie de preguntas con puntuaciones específicas los cuales validan los indicadores.

ITEMS	PREGUNTAS	VALORACIÓN				
		Deficiente	Regular	Bueno	Muy bueno	Excelente
		0-20%	21-50%	51-70%	71-80%	81-100%
1	¿Tiene relación con el título de investigación?					95
2	¿Se mencionan las variables de investigación?					95
3	¿Facilitará el logro de los objetivos de investigación?					95
4	¿Guarda relación con las variables de investigación?					95
5	¿Permitirá el análisis y procesamiento de datos?					95
6	¿Las preguntas son sencillas de comprender y responder?*					95
7	¿será accesible a la población para la recolección de datos?					95
8	¿Las alternativas de respuesta permiten obtener la información de forma clara y precisa?					95

  
Firma del experto

**Evaluación del instrumento de investigación**

**TABLA DE EVALUACIÓN DE EXPERTOS**

Apellidos y nombres del experto: Ordoñez Pérez, Adilio Christian

Título y/o grado: Doctor / Magister en Ingeniería de Sistemas

Ph. D ( )	Doctor (X)	Magister ( )	Ingeniero ( )	Licenciado ( )	Otro ( ) _____
-----------	------------	--------------	---------------	----------------	----------------

Universidad que labora: Universidad César Vallejo

Fecha: \_\_\_\_\_

**TITULO DE PROYECTO**

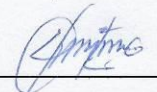
**Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC**

**PROYECTO DE ANÁLISIS DE RIESGO**

**Evaluación del instrumento**

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar los indicadores, mediante una serie de preguntas con puntuaciones específicas los cuales validan los indicadores.

ITEMS	PREGUNTAS	VALORACIÓN				
		Deficiente 0-20%	Regular 21-50%	Bueno 51-70%	Muy bueno 71-80%	Excelente 81-100%
1	¿Tiene relación con el título de investigación?					95
2	¿Se mencionan las variables de investigación?					95
3	¿Facilitará el logro de los objetivos de investigación?					95
4	¿Guarda relación con las variables de investigación?					95
5	¿Permitirá el análisis y procesamiento de datos?					95
6	¿Las preguntas son sencillas de comprender y responder?					95
7	¿Será accesible a la población para la recolección de datos?					95
8	¿Las alternativas de respuesta permiten obtener la información de forma clara y precisa?					95

  
Firma del experto

**Evaluación del instrumento de investigación**

**TABLA DE EVALUACIÓN DE EXPERTOS**

Apellidos y nombres del experto: Ordoñez Pérez, Adilio Christian

Título y/o grado: Doctor / Magister en Ingeniería de Sistemas

Ph. D ( )	Doctor (X)	Magister ( )	Ingeniero ( )	Licenciado( )	Otro ( ) _____
-----------	------------	--------------	---------------	---------------	----------------

Universidad que labora: Universidad César Vallejo

Fecha: \_\_\_\_\_

**TITULO DE PROYECTO**

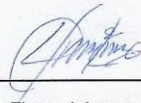
**Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC**

**PLAN DE SEGURIDAD**

**Evaluación del instrumento**

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar los indicadores, mediante una serie de preguntas con puntuaciones específicas los cuales validan los indicadores.

ITEMS	PREGUNTAS	VALORACIÓN				
		Deficiente 0-20%	Regular 21-50%	Bueno 51-70%	Muy bueno 71-80%	Excelente 81-100%
1	¿Tiene relación con el título de investigación?					95
2	¿Se mencionan las variables de investigación?					95
3	¿Facilitará el logro de los objetivos de investigación?					95
4	¿Guarda relación con las variables de investigación?					95
5	¿Permitirá el análisis y procesamiento de datos?					95
6	¿Las preguntas son sencillas de comprender y responder?					95
7	¿Será accesible a la población para la recolección de datos?					95
8	¿Las alternativas de respuesta permiten obtener la información de forma clara y precisa?					95



Firma del experto

**Evaluación del instrumento de investigación**

**TABLA DE EVALUACIÓN DE EXPERTOS**

Apellidos y nombres del experto: Guevara Jiménez Jorge A.

Título y/o grado: MAJISTER

Ph. D ( )	Doctor ( )	Magister <input checked="" type="checkbox"/>	Ingeniero ( )	Licenciado( )	Otro ( ) _____
-----------	------------	--	---------------	---------------	----------------

Universidad que labora: Universidad César Vallejo

Fecha: 06/06/18

**TITULO DE PROYECTO**

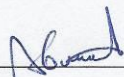
**Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC**

**EFICIENCIA**

**Evaluación del instrumento**

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar los indicadores, mediante una serie de preguntas con puntuaciones específicas los cuales validan los indicadores.

ITEMS	PREGUNTAS	VALORACIÓN				
		Deficiente 0-20%	Regular 21-50%	Bueno 51-70%	Muy bueno 71-80%	Excelente 81-100%
1	¿Tiene relación con el título de investigación?					90%
2	¿Se mencionan las variables de investigación?					90%
3	¿Facilitará el logro de los objetivos de investigación?					95%
4	¿Guarda relación con las variables de investigación?					95%
5	¿Permitirá el análisis y procesamiento de datos?					95%
6	¿Las preguntas son sencillas de comprender y responder?					98%
7	¿será accesible a la población para la recolección de datos?					95%
8	¿Las alternativas de respuesta permiten obtener la información de forma clara y precisa?					95%

  
Firma del experto

**Evaluación del instrumento de investigación**

**TABLA DE EVALUACIÓN DE EXPERTOS**

Apellidos y nombres del experto: Guvara Jimenez Jorge A.

Título y/o grado: Magister

Ph. D ( )	Doctor ( )	Magister <input checked="" type="checkbox"/>	Ingeniero ( )	Licenciado( )	Otro ( ) _____
-----------	------------	--	---------------	---------------	----------------

Universidad que labora: Universidad César Vallejo

Fecha: 06/06/18.

**TITULO DE PROYECTO**

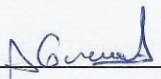
**Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC**

**EFICACIA**

**Evaluación del instrumento**

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar los indicadores, mediante una serie de preguntas con puntuaciones específicas los cuales validan los indicadores.

ITEMS	PREGUNTAS	VALORACIÓN				
		Deficiente 0-20%	Regular 21-50%	Bueno 51-70%	Muy bueno 71-80%	Excelente 81-100%
1	¿Tiene relación con el título de investigación?					95%
2	¿Se mencionan las variables de investigación?					95%
3	¿Facilitará el logro de los objetivos de investigación?					95%
4	¿Guarda relación con las variables de investigación?					95%
5	¿Permitirá el análisis y procesamiento de datos?					98%
6	¿Las preguntas son sencillas de comprender y responder?					98%
7	¿será accesible a la población para la recolección de datos?					95%
8	¿Las alternativas de respuesta permiten obtener la información de forma clara y precisa?					95%

  
Firma del experto

**Evaluación del instrumento de investigación**

**TABLA DE EVALUACIÓN DE EXPERTOS**

Apellidos y nombres del experto: Guevara Jimenez Jorge A.

Título y/o grado: MAGISTER

Ph. D ( )	Doctor ( )	Magister <input checked="" type="checkbox"/>	Ingeniero ( )	Licenciado( )	Otro ( ) _____
-----------	------------	--	---------------	---------------	----------------

Universidad que labora: Universidad César Vallejo

Fecha: 06/06/18

**TITULO DE PROYECTO**

**Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC**

**CALIDAD DE SERVICIO**

**Evaluación del instrumento**

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar los indicadores, mediante una serie de preguntas con puntuaciones específicas los cuales validan los indicadores.

ITEMS	PREGUNTAS	VALORACIÓN				
		Deficiente 0-20%	Regular 21-50%	Bueno 51-70%	Muy bueno 71-80%	Excelente 81-100%
1	¿Tiene relación con el título de investigación?					95%
2	¿Se mencionan las variables de investigación?					95%
3	¿Facilitará el logro de los objetivos de investigación?					95%
4	¿Guarda relación con las variables de investigación?					95%
5	¿Permitirá el análisis y procesamiento de datos?					95%
6	¿Las preguntas son sencillas de comprender y responder?					95%
7	¿será accesible a la población para la recolección de datos?					95%
8	¿Las alternativas de respuesta permiten obtener la información de forma clara y precisa?					95%

JG Camones  
Firma del experto



**Evaluación del instrumento de investigación**

**TABLA DE EVALUACIÓN DE EXPERTOS**

Apellidos y nombres del experto: Guevara Jiménez Jorge A.

Título y/o grado: MAGISTER

Ph. D ( )	Doctor ( )	Magister <input checked="" type="checkbox"/>	Ingeniero ( )	Licenciado( )	Otro ( ) _____
-----------	------------	--	---------------	---------------	----------------

Universidad que labora: Universidad César Vallejo

Fecha: 06/06/18.

**TITULO DE PROYECTO**

**Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC**

**MÉTODO DE ANÁLISIS DE RIESGO**

**Evaluación del instrumento**

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar los indicadores, mediante una serie de preguntas con puntuaciones específicas los cuales validan los indicadores.

ITEMS	PREGUNTAS	VALORACIÓN				
		Deficiente 0-20%	Regular 21-50%	Bueno 51-70%	Muy bueno 71-80%	Excelente 81-100%
1	¿Tiene relación con el título de investigación?					95%
2	¿Se mencionan las variables de investigación?					95%
3	¿Facilitará el logro de los objetivos de investigación?					95%
4	¿Guarda relación con las variables de investigación?					95%
5	¿Permitirá el análisis y procesamiento de datos?					95%
6	¿Las preguntas son sencillas de comprender y responder?					95%
7	¿será accesible a la población para la recolección de datos?					95%
8	¿Las alternativas de respuesta permiten obtener la información de forma clara y precisa?					95%

A. Guevara  
Firma del experto

**Evaluación del instrumento de investigación**

**TABLA DE EVALUACIÓN DE EXPERTOS**

Apellidos y nombres del experto: Guevara Jimenez Jorge A.

Título y/o grado: Magister

Ph. D ( )	Doctor ( )	Magister <input checked="" type="checkbox"/>	Ingeniero ( )	Licenciado( )	Otro ( ) _____
-----------	------------	--	---------------	---------------	----------------

Universidad que labora: Universidad César Vallejo

Fecha: 06/06/18

**TITULO DE PROYECTO**

**Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC**

**PROYECTO DE ANÁLISIS DE RIESGO**

**Evaluación del instrumento**

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar los indicadores, mediante una serie de preguntas con puntuaciones específicas los cuales validan los indicadores.

ITEMS	PREGUNTAS	VALORACIÓN				
		Deficiente 0-20%	Regular 21-50%	Bueno 51-70%	Muy bueno 71-80%	Excelente 81-100%
1	¿Tiene relación con el título de investigación?					95%
2	¿Se mencionan las variables de investigación?					95%
3	¿Facilitará el logro de los objetivos de investigación?					95%
4	¿Guarda relación con las variables de investigación?					95%
5	¿Permitirá el análisis y procesamiento de datos?					95%
6	¿Las preguntas son sencillas de comprender y responder?					98%
7	¿será accesible a la población para la recolección de datos?					95%
8	¿Las alternativas de respuesta permiten obtener la información de forma clara y precisa?					95%

Guevara  
Firma del experto

**Evaluación del instrumento de investigación**

**TABLA DE EVALUACIÓN DE EXPERTOS**

Apellidos y nombres del experto: Guevara Jimenez Jorge A

Título y/o grado: MAGISTER

Ph. D ( )	Doctor ( )	Magister <input checked="" type="checkbox"/>	Ingeniero ( )	Licenciado ( )	Otro ( ) _____
-----------	------------	--	---------------	----------------	----------------

Universidad que labora: Universidad César Vallejo

Fecha: 05/06/18

**TITULO DE PROYECTO**

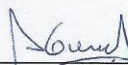
**Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC**

**PLAN DE SEGURIDAD**

**Evaluación del instrumento**

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar los indicadores, mediante una serie de preguntas con puntuaciones específicas los cuales validan los indicadores.

ITEMS	PREGUNTAS	VALORACIÓN				
		Deficiente 0-20%	Regular 21-50%	Bueno 51-70%	Muy bueno 71-80%	Excelente 81-100%
1	¿Tiene relación con el título de investigación?					95%
2	¿Se mencionan las variables de investigación?					100%
3	¿Facilitará el logro de los objetivos de investigación?					95%
4	¿Guarda relación con las variables de investigación?					95%
5	¿Permitirá el análisis y procesamiento de datos?					95%
6	¿Las preguntas son sencillas de comprender y responder?					95%
7	¿Será accesible a la población para la recolección de datos?					95%
8	¿Las alternativas de respuesta permiten obtener la información de forma clara y precisa?					95%

  
Firma del experto

**Evaluación del instrumento de investigación**

**TABLA DE EVALUACIÓN DE EXPERTOS**

Apellidos y nombres del experto: Galvez Tapia Orleaus

Título y/o grado: Ing. en Ingeniería de Sistemas

Ph. D ( )	Doctor ( )	Magister <input checked="" type="checkbox"/>	Ingeniero ( )	Licenciado ( )	Otro ( ) _____
-----------	------------	--	---------------	----------------	----------------

Universidad que labora: Universidad César Vallejo

Fecha: 06/06/2018

**TITULO DE PROYECTO**

**Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC**

**EFICIENCIA**

**Evaluación del instrumento**

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar los indicadores, mediante una serie de preguntas con puntuaciones específicas los cuales validan los indicadores.

ITEMS	PREGUNTAS	VALORACIÓN				
		Deficiente 0-20%	Regular 21-50%	Bueno 51-70%	Muy bueno 71-80%	Excelente 81-100%
1	¿Tiene relación con el título de investigación?				80	
2	¿Se mencionan las variables de investigación?				80	
3	¿Facilitará el logro de los objetivos de investigación?				80	
4	¿Guarda relación con las variables de investigación?				80	
5	¿Permitirá el análisis y procesamiento de datos?				80	
6	¿Las preguntas son sencillas de comprender y responder?				80	
7	¿Será accesible a la población para la recolección de datos?				80	
8	¿Las alternativas de respuesta permiten obtener la información de forma clara y precisa?				80	

Firma del experto

**Evaluación del instrumento de investigación**

**TABLA DE EVALUACIÓN DE EXPERTOS**

Apellidos y nombres del experto: Gálvez Tapia Orleaus

Título y/o grado: Mg. en Ingeniería de Sistema.

Ph. D ( )	Doctor ( )	Magister <input checked="" type="checkbox"/>	Ingeniero ( )	Licenciado ( )	Otro ( ) _____
-----------	------------	--	---------------	----------------	----------------

Universidad que labora: Universidad César Vallejo

Fecha: \_\_\_\_\_

**TITULO DE PROYECTO**

**Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC**

**EFICACIA**

**Evaluación del instrumento**

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar los indicadores, mediante una serie de preguntas con puntuaciones específicas los cuales validan los indicadores.

ITEMS	PREGUNTAS	VALORACIÓN				
		Deficiente 0-20%	Regular 21-50%	Bueno 51-70%	Muy bueno 71-80%	Excelente 81-100%
1	¿Tiene relación con el título de investigación?				80	
2	¿Se mencionan las variables de investigación?				80	
3	¿Facilitará el logro de los objetivos de investigación?				80	
4	¿Guarda relación con las variables de investigación?				80	
5	¿Permitirá el análisis y procesamiento de datos?				80	
6	¿Las preguntas son sencillas de comprender y responder?				80	
7	¿será accesible a la población para la recolección de datos?				80	
8	¿Las alternativas de respuesta permiten obtener la información de forma clara y precisa?				80	

Firma del experto

**Evaluación del instrumento de investigación**

**TABLA DE EVALUACIÓN DE EXPERTOS**

Apellidos y nombres del experto: Galvez Tapra Orteaus

Título y/o grado: Mg. en Ingeniería de Sistema.

Ph. D ( )	Doctor ( )	Magister <input checked="" type="checkbox"/>	Ingeniero ( )	Licenciado( )	Otro ( ) _____
-----------	------------	--	---------------	---------------	----------------

Universidad que labora: Universidad César Vallejo

Fecha: \_\_\_\_\_

**TITULO DE PROYECTO**

**Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC**

**CALIDAD DE SERVICIO**

**Evaluación del instrumento**

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar los indicadores, mediante una serie de preguntas con puntuaciones específicas los cuales validan los indicadores.

ITEMS	PREGUNTAS	VALORACIÓN				
		Deficiente 0-20%	Regular 21-50%	Bueno 51-70%	Muy bueno 71-80%	Excelente 81-100%
1	¿Tiene relación con el título de investigación?				80	
2	¿Se mencionan las variables de investigación?				80	
3	¿Facilitará el logro de los objetivos de investigación?				80	
4	¿Guarda relación con las variables de investigación?				80	
5	¿Permitirá el análisis y procesamiento de datos?				80	
6	¿Las preguntas son sencillas de comprender y responder?				80	
7	¿será accesible a la población para la recolección de datos?				80	
8	¿Las alternativas de respuesta permiten obtener la información de forma clara y precisa?				80	

Firma del experto

**Evaluación del instrumento de investigación**

**TABLA DE EVALUACIÓN DE EXPERTOS**

Apellidos y nombres del experto: Calvez Tapia Orleans

Título y/o grado: Mg. en Ing. de Sistemas

Ph. D ( )	Doctor ( )	Magister (X)	Ingeniero ( )	Licenciado ( )	Otro ( ) _____
-----------	------------	--------------	---------------	----------------	----------------

Universidad que labora: Universidad César Vallejo

Fecha: \_\_\_\_\_

**TITULO DE PROYECTO**

**Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC**

**MÉTODO DE ANÁLISIS DE RIESGO**

**Evaluación del instrumento**

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar los indicadores, mediante una serie de preguntas con puntuaciones específicas los cuales validan los indicadores.

ITEMS	PREGUNTAS	VALORACIÓN				
		Deficiente 0-20%	Regular 21-50%	Bueno 51-70%	Muy bueno 71-80%	Excelente 81-100%
1	¿Tiene relación con el título de investigación?				80	
2	¿Se mencionan las variables de investigación?				80	
3	¿Facilitará el logro de los objetivos de investigación?				80	
4	¿Guarda relación con las variables de investigación?				80	
5	¿Permitirá el análisis y procesamiento de datos?				80	
6	¿Las preguntas son sencillas de comprender y responder?				80	
7	¿Será accesible a la población para la recolección de datos?				80	
8	¿Las alternativas de respuesta permiten obtener la información de forma clara y precisa?				80	

Firma del experto

**Evaluación del instrumento de investigación**

**TABLA DE EVALUACIÓN DE EXPERTOS**

Apellidos y nombres del experto: Galvez Tapia Orleans  
 Título y/o grado: Mg. en Ingeniería de Sistemas.

Ph. D ( )	Doctor ( )	Magister <input checked="" type="checkbox"/>	Ingeniero ( )	Licenciado( )	Otro ( ) _____
-----------	------------	--	---------------	---------------	----------------

Universidad que labora: Universidad César Vallejo

Fecha: \_\_\_\_\_

**TITULO DE PROYECTO**

**Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC**

**PROYECTO DE ANÁLISIS DE RIESGO**

**Evaluación del instrumento**

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar los indicadores, mediante una serie de preguntas con puntuaciones específicas los cuales validan los indicadores.

ITEMS	PREGUNTAS	VALORACIÓN				
		Deficiente 0-20%	Regular 21-50%	Bueno 51-70%	Muy bueno 71-80%	Excelente 81-100%
1	¿Tiene relación con el título de investigación?				80	
2	¿Se mencionan las variables de investigación?				80	
3	¿Facilitará el logro de los objetivos de investigación?				80	
4	¿Guarda relación con las variables de investigación?				80	
5	¿Permitirá el análisis y procesamiento de datos?				80	
6	¿Las preguntas son sencillas de comprender y responder?				80	
7	¿Será accesible a la población para la recolección de datos?				80	
8	¿Las alternativas de respuesta permiten obtener la información de forma clara y precisa?				80	

Firma del experto



**Evaluación del instrumento de investigación**

**TABLA DE EVALUACIÓN DE EXPERTOS**

Apellidos y nombres del experto: Galvez Tapia Orleaux

Título y/o grado: Mg. en Ing. de Sistemas

Ph. D ( )	Doctor ( )	Magister <input checked="" type="checkbox"/>	Ingeniero ( )	Licenciado ( )	Otro ( ) _____
-----------	------------	--	---------------	----------------	----------------

Universidad que labora: Universidad César Vallejo

Fecha: \_\_\_\_\_

**TITULO DE PROYECTO**

**Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC**

**PLAN DE SEGURIDAD**

**Evaluación del instrumento**

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar los indicadores, mediante una serie de preguntas con puntuaciones específicas los cuales validan los indicadores.

ITEMS	PREGUNTAS	VALORACIÓN				
		Deficiente 0-20%	Regular 21-50%	Bueno 51-70%	Muy bueno 71-80%	Excelente 81-100%
1	¿Tiene relación con el título de investigación?				80	
2	¿Se mencionan las variables de investigación?				80	
3	¿Facilitará el logro de los objetivos de investigación?				80	
4	¿Guarda relación con las variables de investigación?				80	
5	¿Permitirá el análisis y procesamiento de datos?				80	
6	¿Las preguntas son sencillas de comprender y responder?				80	
7	¿Será accesible a la población para la recolección de datos?				80	
8	¿Las alternativas de respuesta permiten obtener la información de forma clara y precisa?				80	

  
Firma del experto

## Anexo N° 7: Entrevista para la realidad problemática



### Anexo 7: ENTREVISTA PARA DETERMINAR LA PROBLEMÁTICA EN LA EMPRESA PROYECTOS, ASESORÍAS Y CONSTRUCCIONES ATOGAPAN S.A. DE C.V

Nro. Entrevista	1
Nombre del entrevistado	Héctor Paz Díaz
Cargo	Director de Radio Atogapan
Fecha	27/04/2018

**1. ¿Cómo es que decidieron optar por realizar webcast para la emisión de sus programas?**

Estuvimos evaluando desde hace tiempo la emisión de programas en cuanto a protección civil refiere, y vimos que haciendo webcast de alguna forma algo accesible para todos los epicentros que están unidos en las transmisiones, así que decidimos optar por ello.

**2. ¿La empresa está cumpliendo con los objetivos planteados? ¿Por qué?**

No, aunque no podemos negar que la idea de realizar transmisiones en vivo ha tenido mucha acogida, no hemos logrado llegar a la cantidad de público que nos hablamos proyectado y eso más que nada se ha dado porque a veces dejamos de transmitir programa o se cancelan, lo cual hace que la gente deje de seguirnos.

**3. ¿El desempeño del webcast es eficaz?**

Lamentablemente debería decir que no, y precisamente es por ello que como le mencionaba, el público deja de seguir la programación, ha sucedido en varias oportunidades que se han presentado fallas técnicas en los epicentros y se ha dejado de transmitir.

**4. Actualmente, ¿Qué inconvenientes presentan a la hora de sus transmisiones?**

El más común es que la transmisión se detenga por falla de conexión, dificultades de audio, o como le mencionaba los problemas técnicos en el hardware que impiden que se emita algún programa.

**5. ¿Considera que una capacitación o difusión de información en cuanto a los factores de riesgo en tecnologías de información refiere antes de realizar webcast, serían de mucha ayuda?**

Definitivamente sí, justamente es ello lo que hace que tengamos deficiencia en este aspecto, si pudiéramos tener información en cuanto a los requerimientos mínimos para poder desempeñar un webcast óptimo, sería genial y así lo haríamos de conocimiento a los demás epicentros.

www.atogapan.mx  
Tels. 5595-8905  
5595-5271  
5035-9820  
5035-9819

Héctor Paz Díaz

Cerrada de Toluca No. 36  
Col. Olivar de los Padres  
Del. Álvaro Obregón  
Ciudad de México, CP. 01780

**Anexo 7: ENTREVISTA PARA DETERMINAR LA PROBLEMÁTICA EN LA EMPRESA GRUPO HCM COMUNICACIONES SAC**

Nro. Entrevista	1
Nombre del entrevistado	Hugo Ponciano Cayo Mamani
Cargo	Gerente General
Fecha	27/04/2016

**1. ¿Cómo es que decidieron optar por realizar webcast para la emisión de sus programas?**

La decisión se toma cuando empezó el boom de las transmisiones en vivo, en ese tiempo solo se emitía audio, y ante los altos costos de transmisión por señal abierta, se prueba ésta plataforma nueva y resulta ser novedoso para el público.

**2. ¿La empresa está cumpliendo con los objetivos planteados? ¿Por qué?**

Si, ya que en solo 2 años hemos captado a muchas personas que ven diariamente los programas que ofrece nuestra parrilla, además que ellos mismos recomiendan a sus allegados y eso hace que el número de seguidores aumente.

**3. ¿El desempeño del webcast es eficaz?**

Hay de todo, el desempeño sería medio, debido a que algunos programas pueden no tener la acogida deseada y para las personas es tan fácil como cerrar una ventana y dejar de ver el contenido

**4. Actualmente, ¿Qué inconvenientes presentan a la hora de sus transmisiones?**

El más común es que la transmisión se detenga por falla de conexión, dificultades de audio, o los problemas técnicos en el hardware que impiden que se emita algún programa.

**5. ¿Considera que una capacitación o difusión de información en cuanto a los factores de riesgo en tecnologías de información refiere antes de realizar webcast, serían de mucha ayuda?**

En definitiva, una buena información sobre los requerimientos mínimos a nivel software y hardware y capacitación constante, haría que las transmisiones tengan el nivel óptimo que se espera.



GRUPO HCM COMUNICACIONES S.A.C.  
R.U.C. 20601539935

HUGO P. CAYO MAMANI  
GERENTE GENERAL

## Anexo N° 8: Carta de aprobación de la empresa

Ciudad de México, 12 de mayo del 2018

### CARTA DE AUTORIZACIÓN

Por medio del presente el Director General de la empresa Radio Atogapan, autoriza a JAMIE EVELYN ROMERO CAMONES, identificada con DNI 43710298, estudiante de la Universidad César Vallejo en Lima, Perú, a realizar la aplicación de encuestas, entrevistas, cuestionarios y lo que considere necesario con el personal de la empresa, y a utilizar los datos del mismo con los fines que considere convenientes para ser usados exclusivamente en la elaboración de la tesis que viene realizando para obtener el título de Ingeniero de Sistemas.

Atentamente,



Héctor Paz Díaz  
Director General

Lima, 12 de mayo del 2018

**CARTA DE AUTORIZACIÓN**

Por medio del presente el Gerente General de la empresa Grupo HCM Comunicaciones SAC, autoriza a JAMIE EVELYN ROMERO CAMONES, identificada con DNI 43710298, estudiante de la Universidad César Vallejo en Lima, Perú, a realizar la aplicación de encuestas, entrevistas, cuestionarios y lo que considere necesario con el personal de la empresa, y a utilizar los datos del mismo con los fines que considere convenientes para ser usados exclusivamente en la elaboración de la tesis que viene realizando para obtener el título de Ingeniero de Sistemas.

Atentamente,

  
GRUPO HCM COMUNICACIONES S.A.C.  
R.U.C. 20561754935  
HUGO P. CAYO MAMANI  
GERENTE GENERAL

Hugo Ponciano Cayo Mamani  
Gerente General

## Anexo N° 9: Acta de implementación



Ciudad de México, 08 de agosto del 2018

### ACTA DE IMPLEMENTACIÓN

Por medio del presente el Director General de Radio Atogapan S.A de C.V, certifica que JAMIE EVELYN ROMERO CAMONES, identificada con DNI 43710298, estudiante de la Universidad César Vallejo en Lima, Perú, ha implementado la metodología MAGERIT V.3 en la empresa para la mejora del proceso del webcast, y así demostrar la relación que existe entre los factores de las tecnologías de información y el desempeño del webcast, brindando la capacitación correspondiente al personal involucrado para lograr la efectividad de la implementación de dicha metodología orientada a la gestión de riesgos de TI, la cual es parte de la elaboración de la tesis que viene realizando para obtener el título de Ingeniero de Sistemas.

Se expresa el agradecimiento por la implementación y el logro de las mejoras como consecuencia de la implementación, basado en las necesidades y procesos deficientes de la empresa. Se expide el presente documento a solicitud del interesado.

Atentamente,

  
Héctor Paz Díaz  
Director General

www.atogapan.mx  
Tel. 5095-8905  
5095-8271  
5035-9820  
5035-9819

Cerrada de Toluca No. 36  
Col. Olivar de los Padres  
Del. Álvaro Obregón  
Ciudad de México, CP. 01780

Lima, 01 de setiembre del 2018

### ACTA DE IMPLEMENTACIÓN

Por medio del presente el Gerente General de la empresa Grupo HCM Comunicaciones SAC, certifica que JAMIE EVELYN ROMERO CAMONES, identificada con DNI 43710298, estudiante de la Universidad César Vallejo en Lima, Perú, ha implementado la metodología MAGERIT V.3 en la empresa para la mejora del proceso del webcast, y así demostrar la relación que existe entre los factores de las tecnologías de información y el desempeño del webcast, brindando la capacitación correspondiente al personal involucrado para lograr la efectividad de la implementación de dicha metodología orientada a la gestión de riesgos de TI, la cual es parte de la elaboración de la tesis que viene realizando para obtener el título de Ingeniero de Sistemas.

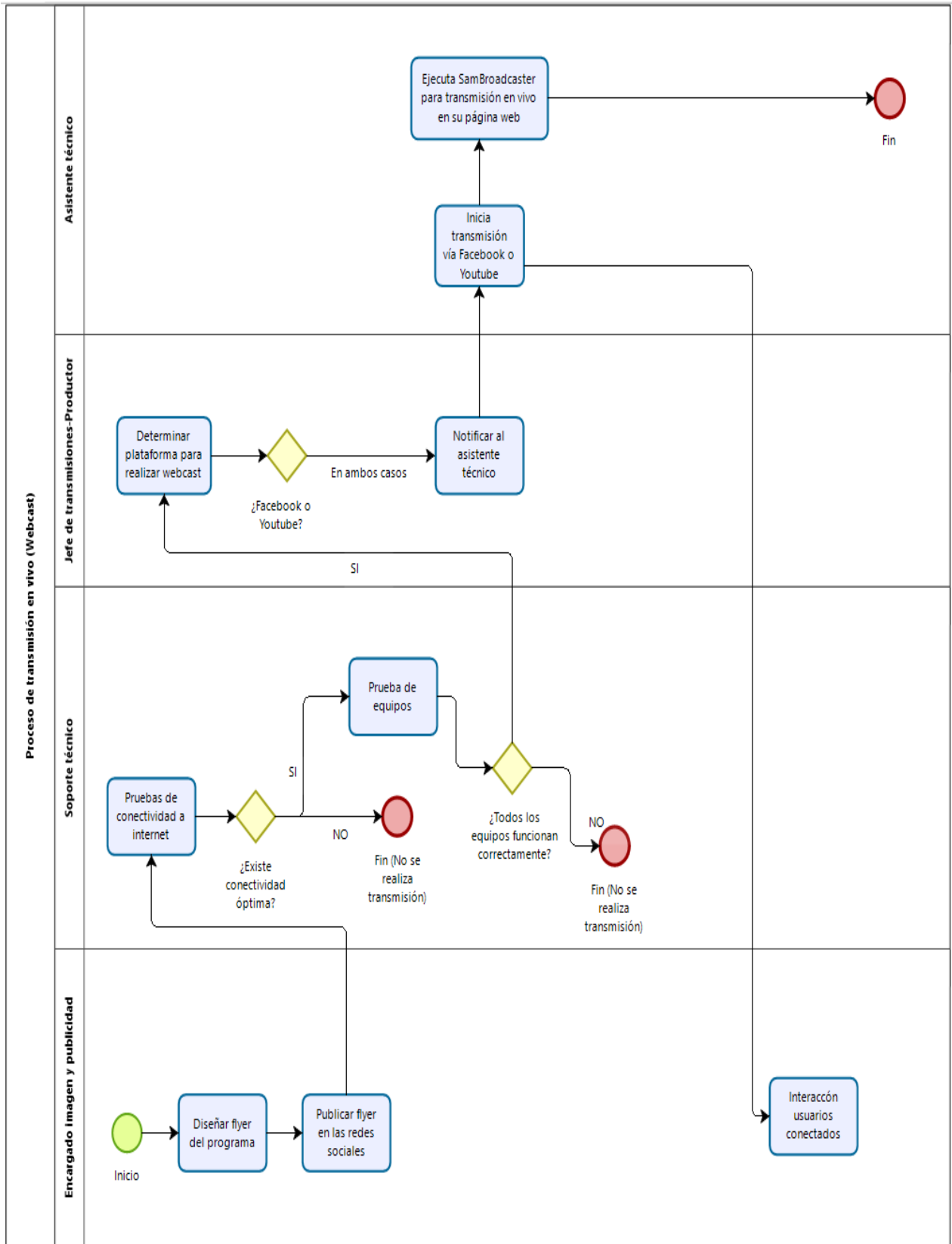
Se expresa el agradecimiento por la implementación y el logro de las mejoras como consecuencia de la implementación, basado en las necesidades y procesos deficientes de la empresa. Se expide el presente documento a solicitud del interesado.

Atentamente,

GRUPO HCM COMUNICACIONES S.A.S.  
R.U.C. 20601529113  
HUGO P. CAYO MAMANI  
GERENTE GENERAL

Hugo Ponciano Cayo Mamani  
Gerente General

### Anexo N° 10: Diagrama de procesos





**DESARROLLO DE LA METODOLOGÍA MAGERIT V.3 EN  
LA EMPRESA ATOGAPAN Y EL GRUPO HCM  
COMUNICACIONES**

Autor: Jamie Evelyn Romero Camones  
Consultor: Dr. Adilio Christian Ordoñez Pérez



**UNIVERSIDAD CÉSAR VALLEJO**

FACULTAD DE INGENIERIA

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

**Factores de riesgo de las tecnologías de información y el desempeño  
del webcast en las empresas ATOGAPAN S.A. y Grupo HCM  
Comunicaciones SAC**

**PROYECTO DE INVESTIGACIÓN**

AUTOR:

Romero Camones, Jamie Evelyn

ASESOR:

Dr. Adilio Christian Ordoñez Pérez

LÍNEA DE INVESTIGACIÓN:

Auditoría de sistemas y seguridad de la información

LIMA – PERÚ 2018

## Presentación

Señores miembros del Jurado:

Dando cumplimiento a las normas establecidas en el Reglamento de Grados y Títulos sección de Pregrado de la Universidad César Vallejo para la experiencia curricular de Metodología de la Investigación Científica, presento el plan de capacitación correspondiente al proyecto de investigación titulado: "Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC".

La investigación, tiene como propósito fundamental: Determinar la relación entre los factores de riesgo en tecnologías de información y el desempeño del webcast en las empresas ATOGAPAN S.A. y Grupo HCM Comunicaciones SAC, y como parte de ella se encuentra la capacitación realizada sobre la metodología MAGERIT V.3 y el uso de la herramienta PILAR 7.1 para poder ser implementada en la empresa.

Señores miembros del jurado espero que esta investigación sea evaluada y merezca su aprobación.

## Índice

	Página
Carátula .....	i
Presentación .....	ii
Índice .....	iii
Índice de tablas .....	iv
Índice de figuras .....	v
<b>1. ACTIVIDADES PRELIMINARES</b>	
1.1 Estudio de oportunidad .....	2
1.2 Determinación del alcance del proyecto .....	2
1.3 Planificación del proyecto .....	3
1.4 Lanzamiento del proyecto .....	5
<b>2. ANÁLISIS DE RIESGOS</b>	
2.1 Caracterización de activos .....	7
Identificación de activos .....	8
Servicios internos (IS) .....	8
Aplicaciones (SW) .....	8
Equipos (HW) .....	9
Comunicaciones (COM) .....	9
Soportes de información (MEDIA) .....	9
Equipamiento auxiliar (AUX) .....	10
Instalaciones (L) .....	10
Personal (P) .....	10
Valoración de los activos .....	12
2.2 Caracterización de las amenazas .....	15
Identificación de las amenazas .....	16
Valoración de las amenazas .....	19
2.3 Caracterización de las salvaguardas .....	22
Identificación de las salvaguardas .....	22
Valoración de las salvaguardas .....	26
2.4 Estimación del estado del riesgo .....	28
Estimación del impacto .....	28
Impacto potencial .....	29
Impacto residual acumulado .....	30
2.5 Estimación del riesgo .....	31
Riesgo potencial .....	31
Riesgo residual .....	33
Riesgo residual acumulado .....	33

2.6 Interpretación de los resultados	.....	35
<b>3. GESTIÓN DE RIESGOS</b>		
3.1 Toma de decisiones	.....	36
Identificación de riesgos críticos	.....	37
Calificación del riesgo	.....	38
3.2 Plan de seguridad	.....	43
Identificación de proyectos de seguridad	.....	43
Normativas de seguridad	.....	44
Eliminar fallos de seguridad evidentes	.....	46
Clasificación del inventarios	.....	46
3.3 Plan de ejecución	.....	47
3.4 Ejecución	.....	47
3.5 Factores de riesgo por dimensión	.....	48
3.6 Plan de contingencia	.....	49

## Índice de tablas

	Página
Tabla N°1: Personal de Radio Atogapan .....	1
Tabla N°2: Involucrados en el proyecto .....	3
Tabla N°3: Criterios de valoración .....	14
Tabla N°4: Valor propio de los activos .....	15
Tabla N°5: Identificación de amenazas a cada uno de los activos .....	16
Tabla N°6: Degradación de valor .....	20
Tabla N°7: Probabilidad de ocurrencia .....	20
Tabla N°8: Valoración de amenazas a cada uno de los activos .....	21
Tabla N°9: Valoración de salvaguardas .....	27
Tabla N°10: Impacto potencial sobre cada uno de los activos .....	28
Tabla N° 11 Colores valor del impacto .....	29
Tabla N°12: Riesgo potencial sobre cada uno de los activos .....	30
Tabla N°13: Colores del valor del riesgo .....	31
Tabla N°14: Identificación de riesgos críticos .....	35
Tabla N°15: Colores valoración de los riesgos .....	35
Tabla N°16: Resultados de riesgos residuales .....	43
Tabla N°17: Colores Valoración riesgos .....	44
Tabla N°18: Factores de riesgo en la dimensión de disponibilidad .....	53
Tabla N°19: Factores de riesgo en la dimensión de integridad .....	54
Tabla N°20: Factores de riesgo en la dimensión de confidencialidad .....	55
Tabla N°21: Factores de riesgo en la dimensión de Autenticidad .....	56
Tabla N°22 Cuadro de estrategias para prevenir fallas .....	57
Tabla N°23: Cuadro de Estrategias para la Recup. Inmediata .....	57
Tabla N°24 Cuadro de impacto de falla del servicio de internet .....	58
Tabla N°25 Cuadro de impacto de falla del func. del servidor .....	59
Tabla N°26 Cuadro de medidas para un error físico de disco .....	60
Tabla N°27 Cuadro de medidas para un error de memoria RAM .....	61
Tabla N°28 Cuadro de medidas para un error lógico de datos .....	62
Tabla N°29 Cuadro de impacto por fallas de disp. de a/v .....	63
Tabla N°30 Cuadro de Impacto de daños causadas por agua .....	64
Tabla N°31 Cuadro de Impacto de daños causadas por fuego .....	65
Tabla N°32 Cuadro de Impacto de daños de equipos en el edificio .....	66
Tabla N°33 Cuadro de alternativas de edificio y oficinas. .....	67
Tabla N°34 Cuadro de Impacto de interrupción de Fluido Eléctrico. ....	68
Tabla N°35 Cuadro de Impacto de ausencia de personal .....	69

	Página
Tabla N°1: Personal de Radio Atogapan .....	1
Tabla N°2: Involucrados en el proyecto .....	3
Tabla N°3: Criterios de valoración .....	14
Tabla N°4: Valor propio de los activos .....	15
Tabla N°5: Identificación de amenazas a cada uno de los activos .....	16
Tabla N°6: Degradación de valor .....	20
Tabla N°7: Probabilidad de ocurrencia .....	20
Tabla N°8: Valoración de amenazas a cada uno de los activos .....	21
Tabla N°9: Valoración de salvaguardas .....	27
Tabla N°10: Impacto potencial sobre cada uno de los activos .....	28
Tabla N° 11 Colores valor del impacto .....	29
Tabla N°12: Riesgo potencial sobre cada uno de los activos .....	30
Tabla N°13: Colores del valor del riesgo .....	31
Tabla N°14: Identificación de riesgos críticos .....	35
Tabla N°15: Colores valoración de los riesgos .....	35
Tabla N°16: Resultados de riesgos residuales .....	43
Tabla N°17: Colores Valoración riesgos .....	44
Tabla N°18: Factores de riesgo en la dimensión de disponibilidad .....	53
Tabla N°19: Factores de riesgo en la dimensión de integridad .....	54
Tabla N°20: Factores de riesgo en la dimensión de confidencialidad .....	55
Tabla N°21: Factores de riesgo en la dimensión de Autenticidad .....	56
Tabla N°22 Cuadro de estrategias para prevenir fallas .....	57
Tabla N°23:Cuadro de Estrategias para la Recup. Inmediata .....	57
Tabla N°24 Cuadro de impacto de falla del servicio de internet .....	58
Tabla N°25 Cuadro de impacto de falla del func. del servidor .....	59
Tabla N°26 Cuadro de medidas para un error físico de disco .....	60
Tabla N°27 Cuadro de medidas para un error de memoria RAM .....	61
Tabla N°28 Cuadro de medidas para un error lógico de datos .....	62
Tabla N°29 Cuadro de impacto por fallas de disp. de a/v .....	63
Tabla N°30 Cuadro de Impacto de daños causadas por agua .....	64
Tabla N°31 Cuadro de Impacto de daños causadas por fuego .....	65

### Índice de figuras

	Página
Figura N°1: Notificación para la realización de cuestionarios .....	4
Figura N°2: Comunicado lanzamiento del proyecto .....	6
Figura N°3: Acta de implementación del proyecto .....	7

Figura N°4: Identificación de las salvaguardas	.....	25
Figura N°5: Valoración de Salvaguardas	.....	30
Figura N°7: Impacto residual sobre cada uno de los activos	.....	33
Figura N°8: Riesgo residual sobre cada uno de los activos	.....	37
Figura N° 9: Interpretación de los resultados	.....	38



## 1. Actividades preliminares

El objetivo principal de esta fase es la de obtener una visión general de lo que incluye el proyecto, por ello es importante que antes de iniciar con el desarrollo de las etapas de Análisis y Gestión de riesgos de los sistemas de información de la empresa Atogapan SA se determinen las siguientes actividades que están dentro de esta fase, las cuales son:

- Estudio de oportunidad
- Determinación del alcance del proyecto
- Planificación del proyecto
- Lanzamiento del proyecto

El presente proyecto será desarrollado con la implementación de la metodología MAGERIT versión 3, utilizando el software de aplicación PILAR versión 7.1

Para la implementación de la metodología MAGERIT se contó con la ayuda y colaboración del personal de todos los epicentros de Atogapan SA involucrados en el proceso del webcast y del uso de los sistemas de información tal y como se muestra en la siguiente tabla N°1:

**TablaN°1: Personal de Radio Atogapan**

<b>N°</b>	<b>RADIO ATOGAPAN EPICENTROS</b>	<b>N° DE TRABAJADORES</b>
<b>1</b>	Ciudad de México	4
<b>2</b>	Nuevo León	4
<b>3</b>	Estado de México	3
<b>4</b>	Sonora	4
<b>5</b>	Colombia	3
<b>6</b>	Quintana Roo	3
<b>7</b>	Veracruz	4
<b>8</b>	Puebla	3
<b>9</b>	<b>HCM COMUNICACIONES</b>	4

**Fuente: Radio Atogapan y HCM Comunicaciones**

## **Estudio de oportunidad**

El objetivo de esta actividad es la de impulsar la implementación de la metodología MAGERIT V.3 en la empresa Atogapan SA.

En la empresa Atogapan SA se inició el uso de sistemas e infraestructura de TI dado el inicio del proyecto Radio Atogapan, pero no se tomaron en cuenta diversos aspectos como los requerimientos mínimos con los que deberían contar para un óptimo desempeño de sus transmisiones, así como de la seguridad de su información.

Mediante entrevistas y cuestionarios realizados a los trabajadores del área involucrada de transmisiones se percibió los incidentes significativos que existen, los cuales no permiten un desempeño correcto.

La falta de soporte y mantenimiento a los equipos es uno de los causales más importantes, por ello la falla de equipos y la vulnerabilidad de la información.

Los equipos con los que cuentan los epicentros que transmiten no son los adecuados para brindar una transmisión de calidad, además de ello se determinó que las contraseñas de los equipos no son confidenciales, lo cual puede provocar el robo de información.

Los antivirus con los que cuentan se encuentran desactualizados y no se realiza respaldos de la información con la que se cuenta.

## **Determinación del alcance del proyecto**

Luego de presentado los beneficios que presenta la implementación de la metodología MAGERIT, y aprobada la oportunidad de ejecutar el proyecto de análisis y gestión de riesgos, en esta actividad se determina los objetivos que debe cumplir dicha implementación y definir sus límites y dominio.

Los objetivos están determinados en tres ciclos:

- Definir los requerimientos mínimos con los que deben contar los epicentros para sus transmisiones.

- Analizar el estado actual en el que se encuentra la empresa y determinar las principales necesidades con las que cuenta, en cuanto a infraestructura y seguridad.
- Determinar mecanismos de salvaguarda.

El dominio del proyecto se centra en el área de transmisiones en donde el personal involucrados engloba los 8 epicentros, los cuales son:

**Tabla N° 2 Involucrados en el proyecto**

N°	RADIO ATOGAPAN EPICENTROS	N° DE TRABAJADORES	Representante	Cargo
1	Ciudad de México	4	Hector Paz	Presidente de epicentro
2	Nuevo León	4	Victor Estrada	Presidente de epicentro
3	Estado de México	3	Alejandro Romero	Presidente de epicentro
4	Sonora	4	Mariano Katase	Presidente de epicentro
5	Colombia	3	Henry Peralta	Presidente de epicentro
6	Quintana Roo	3	David Albores	Presidente de epicentro
7	Veracruz	4	Alberto Cerón	Presidente de epicentro
8	Puebla	3	Ulises Cruz	Presidente de epicentro
9	HCM Comunicaciones	4	Nick Becerra	Presidente de epicentro

**Fuente: Radio Atogapan y HCM Comunicaciones**

**Planificación del proyecto**

En la empresa Atogapan SA para la realización de las entrevistas y cuestionarios se notificará con antelación a los epicentros de cada estado, con un plazo mínimo de 10 días laborables. Tal como se evidencia en la figura N°1:

## Figura N°1



@Fuente: Elaboración propia

Lima, 30 de abril del 2018

### NOTIFICACIÓN PARA LA REALIZACIÓN DE CUESTIONARIOS

Sr. Hugo Ponciano Cayo Mamani  
Gerente general del Grupo HCM Comunicaciones SAC

Me dirijo a usted, para notificarle y a su vez pedirle la colaboración de los trabajadores de cada epicentro en la resolución de cuestionarios orientados al desempeño del webcast y a los factores de riesgo de las tecnologías de información que se toman en cuenta actualmente, el cual será instrumento para el procesamiento de datos que emitirá los resultados de la situación actual de la empresa en la presente elaboración del proyecto de tesis que vengo elaborando para obtener mi título de Ingeniero de Sistemas en la Universidad César Vallejo.

Sin más que decirle, adjunto los cuestionarios esperando su pronta respuesta.

Atentamente,

---

Jamie Evelyn Romero Camones  
Estudiante de Ingeniería de Sistemas  
Universidad César Vallejo

@Fuente: Elaboración propia

## **Notificación para la realización de cuestionarios**

Los cuestionarios servirán para determinar la situación actual de la empresa y la mejora obtenida dada la implementación de la metodología.

Las encuestas deberán arrojar porcentajes exactos del nivel en el que se encuentra cada dimensión establecida para determinar el desempeño del webcast.

El proyecto está constituido por los siguientes involucrados:

- Investigador: Jamie Evelyn Romero Camones estudiante de Ingeniería de Sistemas de la Universidad César Vallejo.
- Consultor: Dr. Adilio Cristhian Ordoñez Pérez.
- Grupo de usuarios: Está conformado por los que utilizan los sistemas de información: Presidente epicentro, jefe del departamento de logística, jefe de soporte técnico, mantenimiento de la base de datos, y auxiliar de webcasting.

### **Lanzamiento del proyecto**

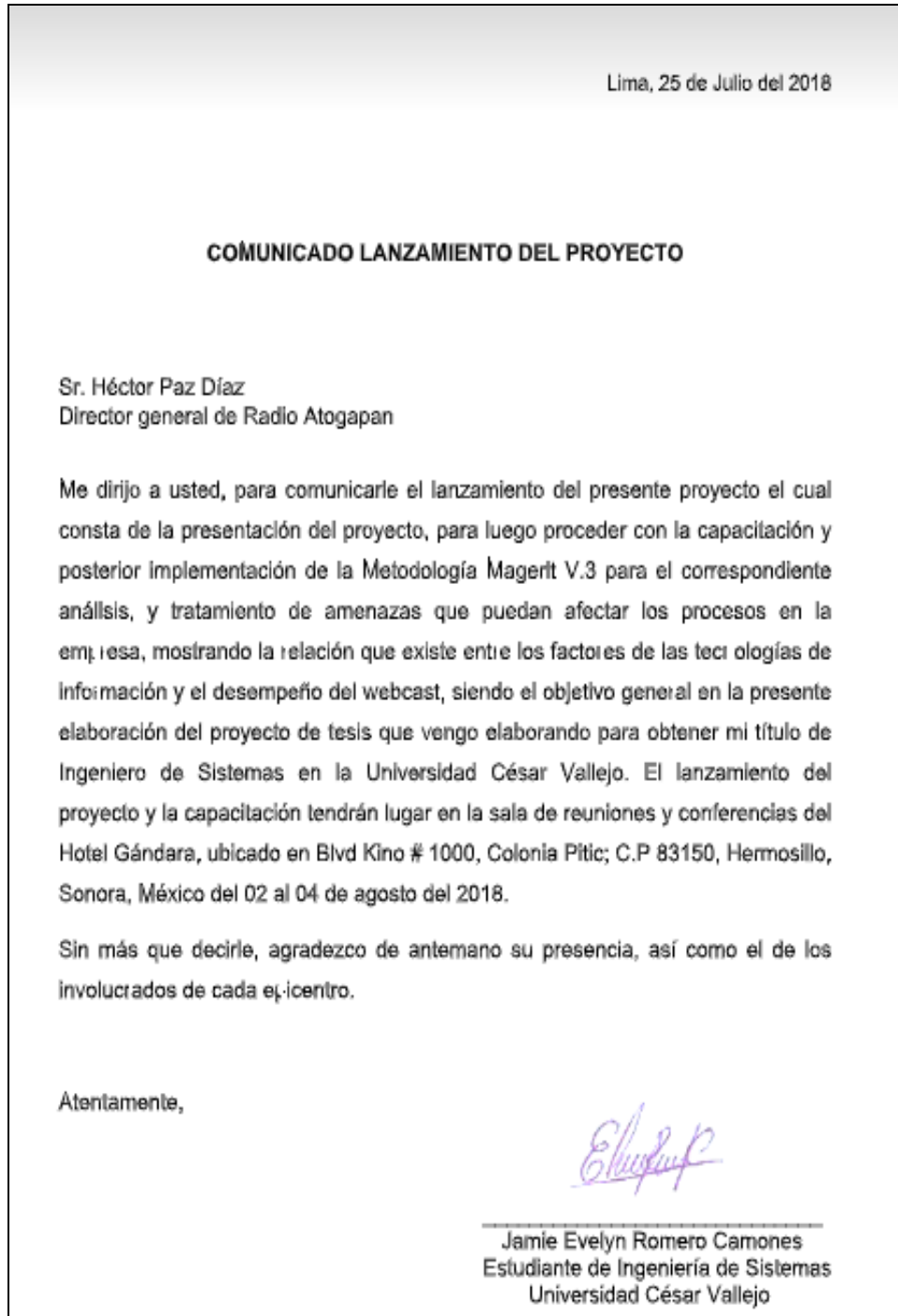
Para poder recolectar la información sobre los activos pertenecientes a la empresa, se ha escogido las fichas de captura de datos del apéndice 2 del libro de catálogo de elementos de MAGERIT V3, teniendo en cuenta los activos con los que cuentan y las dimensiones de seguridad para poder identificar las vulnerabilidades, impactos y salvaguardas efectivos. En cuanto a la seguridad de la información de Atogapan SA dependerá de la incorporación de las salvaguardas para prevenir y reducir riesgos.

El análisis de riesgos permitirá que pueda sistematizarse las medidas actuales a tomar en cuanto a la seguridad y mantener un nivel estable, así como la utilización correcta de equipos de información y la renovación de los mismos.

Lo primero que se hizo fue comunicar a los epicentros involucrados sobre el lanzamiento del proyecto, en donde en una reunión con los trabajadores del área correspondiente de cada epicentro implicado se presentó el proyecto, Así mismo

se realizó la capacitación debida para su correcta implementación y manejo de la herramienta PILAR 7.1. tal y como se muestra en la figura N°2:

### Figura N° 2 Comunicado lanzamiento del proyecto



@Fuente: Elaboración propia

Lima, 25 de Julio del 2018

### COMUNICADO LANZAMIENTO DEL PROYECTO

Sr. Hugo Fordiano Cayo Mamani  
Gerente general del Grupo HCM Comunicaciones SAC

Me dirijo a usted, para comunicarle el lanzamiento del presente proyecto el cual consta de la presentación del proyecto, para luego proceder con la capacitación y posterior implementación de la Metodología Magerit V.3 para el correspondiente análisis, y tratamiento de amenazas que puedan afectar los procesos en la empresa, mostrando la relación que existe entre los factores de las tecnologías de información y el desempeño del webcast, siendo el objetivo general en la presente elaboración del proyecto de tesis que vengo elaborando para obtener mi título de Ingeniero de Sistemas en la Universidad César Vallejo. El lanzamiento del proyecto y la capacitación tendrán lugar en Jr. Cornelio Borda Nro. 144 Lima-Perú del 13 al 15 de agosto del 2018.

Sin más que decirle, agradezco de antemano su presencia, así como el de los involucrados.

Atentamente,



Jamie|Evelyn Romero Camones  
Estudiante de Ingeniería de Sistemas  
Universidad César Vallejo

@Fuente: Elaboración propia



Además de ello se envió un oficio a la gerencia pidiendo la autorización para la implementación de la metodología, informándose que el proyecto quedó autorizado y listo para su ejecución, tal como se muestra en la figura N° 3:

### Figura N° 3

#### Acta de implementación del proyecto Atogapan y HCM Comunicaciones



The image shows a document titled "ACTA DE IMPLEMENTACIÓN" from Atogapan S.A. de C.V. The document is dated August 6, 2018, in Mexico City. It certifies that Jamie Evelyn Romero Camones, a student at Universidad César Vallejo, has implemented the MAGERIT V.3 methodology to improve the webcast process. The document is signed by Héctor Páez Díaz, Director General. Contact information for Atogapan is provided at the bottom left, and the company's address in Mexico City is at the bottom right.

**ATOGAPAN**  
ESPECIALISTAS EN PROTECCIÓN CIVIL

Ciudad de México, 06 de agosto del 2018

**ACTA DE IMPLEMENTACIÓN**

Por medio del presente el Director General de Radio Atogapan S.A de C.V, certifica que JAMIE EVELYN ROMERO CAMONES, identificada con DNI 43710298, estudiante de la Universidad César Vallejo en Lima, Perú, ha implementado la metodología MAGERIT V.3 en la empresa para la mejora del proceso del webcast, y así demostrar la relación que existe entre los factores de las tecnologías de información y el desempeño del webcast, brindando la capacitación correspondiente al personal involucrado para lograr la efectividad de la implementación de dicha metodología orientada a la gestión de riesgos de TI, la cual es parte de la elaboración de la tesis que viene realizando para obtener el título de Ingeniero de Sistemas.

Se expresa el agradecimiento por la implementación y el logro de las mejoras como consecuencia de la implementación, basado en las necesidades y procesos deficientes de la empresa. Se expide el presente documento a solicitud del interesado.

Atentamente,

  
Héctor Páez Díaz  
Diréctor General

www.atogapan.mx  
Tels. 5595-8905  
5595-5271  
5035-9820  
5035-9819

Cerrada de Toluca No. 36  
Col. Olivar de los Padres  
Del. Álvaro Obregón  
Ciudad de México, CP. 01780

@Fuente: Elaboración propia

Lima, 01 de setiembre del 2018

#### ACTA DE IMPLEMENTACIÓN

Por medio del presente el Gerente General de la empresa Grupo HCM Comunicaciones SAC, certifica que JAMIE EVELYN ROMERO CAMONES, identificada con DNI 43710298, estudiante de la Universidad César Vallejo en Lima, Perú, ha implementado la metodología MAGERIT V.3 en la empresa para la mejora del proceso del webcast, y así demostrar la relación que existe entre los factores de las tecnologías de información y el desempeño del webcast, brindando la capacitación correspondiente al personal involucrado para lograr la efectividad de la implementación de dicha metodología orientada a la gestión de riesgos de TI, la cual es parte de la elaboración de la tesis que viene realizando para obtener el título de Ingeniero de Sistemas.

Se expresa el agradecimiento por la implementación y el logro de las mejoras como consecuencia de la implementación, basado en las necesidades y procesos deficientes de la empresa. Se expide el presente documento a solicitud del interesado.

Atentamente,

GRUPO HCM COMUNICACIONES S.A.S.  
R.U.C. 20501530913  
  
HUGO P. CAYO MAMANI  
GERENTE GENERAL

Hugo Ponciano Cayo Mamani  
Gerente General

@Fuente: Elaboración propia

## 2. Análisis de riesgos

Toda organización se encuentra expuesta a riesgos, por ello es que se debe siempre estar alerta y prevenir dichos riesgos ante cualquier situación que pueda representar una amenaza y afecte negativamente a un activo, a un área o a toda la empresa.

El análisis de riesgos deberá alcanzar los siguientes objetivos:

- Determinar los activos significativos con los que cuenta la empresa.
- Determinar las amenazas a los que están expuestos los activos.
- Elegir las salvaguardas apropiados para los activos.
- Estimar el impacto que se generaría si se ve afectado por alguna amenaza.

Para el desarrollo de esta fase, se realizará encuestas a los usuarios involucrados con los sistemas de información de la empresa Atogapan SA.

EL análisis de riesgos nos permite saber cuánto vale y como están protegidos los activos y así poder evaluarlos. Esta fase es muy importante ya que podemos determinar dos cosas muy importantes: El equipo con el que cuenta la empresa el cual se obtiene por la confianza que pone la empresa en el proyecto.

### Caracterización de activos

Esta actividad cuenta con 3 sub-tareas:

- Identificación de los activos
- Dependencias entre los activos
- Valoración de los activos

### Identificación de los activos

Es muy importante que esta subtarea se realice una buena identificación ya que esto nos permitirá:

- Determinar las dependencias entre los activos
- Valorar los activos con precisión
- Identificar las amenazas y el alcance que pueden tener.

- Escoger el correcto salvaguardas para proteger el sistema.

### Servicios internos (IS)

Los servicios internos son aquellos que se brinda y son de uso de los empleados dentro de la organización.

ID_SW_PILAR	NOMBRE	DESCRIPCIÓN
[INTERNET_PIB]	INTERNET	Velocidad de 50MB- Proveedor TOTALPLAY

### Aplicaciones (SW)

Dentro de las aplicaciones y programas que se usan dentro de la empresa se encuentran:

ID_SW_PILAR	NOMBRE	DESCRIPCIÓN
[OBS_PIB]	OPEN BROADCASTER SOFTWARE	Software libre para la transmisión y grabación de programas de radio y tv por internet.
[OFF_PIB]	OFFICE	Microsoft Office 2016
[ANT_PIB]	ANTIVIRUS	Bit Defender Internet Security
[OS_PIB]	SISTEMA OPERATIVO	Windows 10 Enterprise
[OTR_PIB]	OTROS SOFTWARE	Adobe Photoshop, Illustrator

### Equipos (HW)

Los equipos informáticos con los que cuenta la empresa para el proceso de webcast y más:

ID_SW_PILAR	NOMBRE	DESCRIPCIÓN
[SERVBD_PIB]	SERVIDOR DE BASE DE DATOS	Donde se aloja de data de la empresa.
[PRINT_PIB]	IMPRESORAS	HP Officejet Pro 8615-14 PPM color/ 19 PPM en b/n
[PC_PIB]	COMPUTADORAS DE ESCRITORIO Y LAPTOPS	Hp Procesador Intel i5 Memoria Ram 6 gb

		Disco duros 1 tb
[ROUTER_PIB]	ROUTER	Netgear AR6300
[CAM_PIB]	CÁMARAS	C525 Portable Hd Webcam
[MIC_PIB]	MICRÓFONOS	Audio Technica AT2020

### Comunicaciones (COM)

Estos son los medios de transporte de información con los que cuenta la empresa:

ID_SW_PILAR	NOMBRE	DESCRIPCIÓN
[WIFI_PIB]	RED WIFI	Velocidad de 50 MB Proveedor TOTALPLAY
[LAN_PIB]	RED LAN	
[IEX_PIB]	INTERNET	

### Soportes de información (MEDIA)

La empresa utiliza los siguientes soportes de información:

ID_SW_PILAR	NOMBRE	DESCRIPCIÓN
[USB_PIB]	MEMORIA USB	Memorias de 32 gb kingston

### Equipamiento auxiliar (AUX)

Los equipos auxiliares con los que cuenta la empresa son:

ID_SW_PILAR	NOMBRE	DESCRIPCIÓN
[CABLING_PIB]	CABLEADO	Cableado para las conexiones
[MOB_PIB]	MOBILIARIO	Escritorios, Sillas de oficina Archivadores, etc.
[SISVG_PIB]	SISTEMA DE VIGILANCIA	Kit Videovigilancia Internet Tvi Full Hd 1080p
[SAI_PIB]	SISTEMA DE ALIMENTACION ININTERRUMPIDA	Ups Smart Apc Surt48xlbp, 864va/h
[AUXOTR_PIB]	OTROS EQUIPOS AUXILIARES	Fotocopiadora Brother Mfc- I2740dw Extensiones, cables etc.

## Instalaciones (L)

Los sistemas de información se localizan en la siguiente infraestructura, ubicado en Calle Toluca N°36 Col. Olivar de los Padres Del. Álvaro Obregón, Ciudad de México

ID_SW_PILAR	NOMBRE	DESCRIPCIÓN
[BUILDING_PIB]	OFICINA SEDE EPICENTROS	Sede central ubicada en Calle Toluca N°36 Col. Olivar de los Padres Del. Álvaro Obregón, la Ciudad de México.

## Personal (P)

El personal que está involucrado en este proyecto son:

ID_SW_PILAR	NOMBRE	DESCRIPCIÓN
[PRE_PIB]	PRESIDENTE EPICENTRO	Responsable de epicentro, quién toma las decisiones.
[JLC_PIB]	JEFE DEL DEPARTAMENTO DE LOGISTICA	Planificar la estrategia para las actividades de suministro de la empresa (transporte, almacenaje, distribución)
[JST_PIB]	JEFE DE SOPORTE TÉCNICO	Dirigir las actividades del departamento de soporte técnico para resolver problemas de software y hardware.
[DBA_PIB]	MANTENIMIENTO DE BD	Administrar la base de datos, realizar respaldos y velar por la integridad de los datos y la confidencialidad.
[AWC_PIB]	AUXILIAR WEBCASTING	Encargado del manejo de equipos para las transmisiones en vivo.

Gracias a la identificación de activos se pudo realizar la categorización de los mismos. Como se observa en la figura y el sistema OBS (Open Broadcaster Software) es fundamental, ya que las transmisiones se realizan a través de la utilización de dicho software, por ello está ubicado en la parte superior, además de

programas como office ya que son usados para documentación e informes, en dicho nivel también está ubicado el sistema operativo y el antivirus.

El servidor con el que cuentan está en la parte superior del resto de equipos de escritorio, ya que este almacena la información, seguido de ello se encuentra el Internet, la red LAN y wifi ya que sin ello no sería posible la realización del webcast.

Cómo activos inferiores están los quipos auxiliares como el router, impresora, micrófonos y cámaras.

### Valoración de los activos

Para poder realizar la valoración de los activos necesitaremos considerar información como:

- Dimensiones en las cuales los activos son importantes.
- Estimación de la valoración de dichas dimensiones.

### Criterios de valoración

A continuación, en la tabla N° 3 se muestran los criterios de valoración:

**Tabla N°3: Criterios de valoración**

NIVEL	CRITERIO
10	Nivel 10
9	Nivel 9
8	Alto (+)
7	Alto
6	Alto (-)
5	Medio (+)
4	Medio
3	Medio (-)
2	Bajo (+)
1	Bajo
0	Depreciable

**Fuente: Pilar 7.1**

## Dimensiones

Son aquellas características que hacen valioso un activo, esta representa una faceta o aspecto de dicho activo, estas se utilizan para valorar las consecuencias de la materialización de una amenaza, es decir que la valoración que recibe cada activo es la medida de perjuicio para la empresa si el activo se ve dañado en esa dimensión

- **[D] Disponibilidad:** Propiedad de los activos consistente en que las entidades autorizadas tienen accesos a los mismos cuando lo requieren.
- **[I] Integridad de los datos:** Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- **[C] Confidencialidad de los datos:** Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- **[A] Autenticidad de los usuarios y de la información:** Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- **[T] Trazabilidad del servicio y de los datos:** Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

En la siguiente tabla N°4 se puede apreciar la valoración de los activos ya antes clasificados:



**Tabla N° 4: Valor propio de los activos**

Activos	Dimensiones				
	[D]	[I]	[C]	[A]	[T]
<b>Servicios internos</b>					
Internet	[9]			[7]	
<b>Aplicaciones</b>					
OBS		[9]	[9]	[9]	[9]
Office		[7]	[7]	[7]	[7]
Antivirus		[7]	[7]	[7]	[7]
Sistema Operativo		[7]	[7]	[7]	[7]
Otros software		[5]	[5]	[5]	[5]
<b>Equipos</b>					
Servidor de base de datos		[9]	[9]	[9]	[9]
Impresoras		[5]	[5]	[5]	[5]
Computadoras y laptops		[9]	[9]	[9]	[9]
Router		[9]	[9]	[9]	[9]
Cámaras		[9]	[9]	[9]	[9]
Micrófonos		[9]	[9]	[8]	[9]
<b>Comunicaciones</b>					
Red WIFI			[6]		
Red LAN			[6]		
Internet		[7]	[7]		
<b>Equipos auxiliares</b>					
Cableado	[5]				
Mobiliario	[7]				
Sistema de vigilancia	[7]				
Sistema de alimentación ininterrumpida	[7]				
Otros equipos auxiliares	[5]				
<b>Soportes de información</b>					
Memoria USB		[7]	[7]		
<b>Instalaciones</b>					
Oficinas sede epicentros	[9]				
<b>Personal</b>					
PRESIDENTE EPICENTRO			[9]		
JEFE DEL DEPARTAMENTO DE LOGISTICA			[8]		
JEFE DE SOPORTE TÉCNICO			[8]		
MANTENIMIENTO DE BD			[7]		
AUXILIAR WEBCASTING			[8]		

**Fuente: Pilar 7.1**

Esta actividad nos ha permitido obtener el modelo de valor en donde cada activo es detallado, y se le asigna un valor según la dimensión, para que luego ese valor pueda estimar el riesgo e impacto generado en dichos activos.

## 2.2 Caracterización de las amenazas

La herramienta PILAR la cual es estandarizada por MAGERIT V.3 clasifica a las amenazas en cuatro grupos:

- [N] Desastres naturales
- [I] De origen industrial
- [E] Errores y fallos no intencionados
- [A] Ataques intencionados

Esta clasificación nos permite conocer el entorno al que se enfrentan los activos, y a qué consecuencias están expuestos y a que se debería en el caso que sucediese.

En esta actividad se realizan dos sub-tareas:

- Identificación de las amenazas
- Valoración de amenazas

### Identificación de las amenazas

El objetivo de esta tarea es identificar las amenazas relevantes sobre cada activo, una vez hecho el análisis, se logró identificar dichas amenazas tal y como se muestra en la siguiente tabla N°5:

**Tabla N°5 Identificación de amenazas a cada uno de los activos**

Activos	Amenazas
<b>INTERNET</b>	[I.8] Fallo de servicios de comunicaciones
<b>OBS</b>	[E.8] Difusión de software dañino
	[E.20] Vulnerabilidades de los programas
	[E.21] Errores de mantenimiento o actualización de los programas
	[A.8] Difusión de software dañino
	[A.22] Manipulación de programas
<b>OFFICE</b>	[E.8] Difusión de software dañino
	[E.20] Vulnerabilidades de los programas
	[E.21] Errores de mantenimiento o actualización de los programas
	[A.8] Difusión de software dañino
	[A.22] Manipulación de programas
<b>ANTIVIRUS</b>	[E.8] Difusión de software dañino

	[E.20] Vulnerabilidades de los programas
	[E.21] Errores de mantenimiento o actualización de los programas
	[A.8] Difusión de software dañino
	[A.22] Manipulación de programas
<b>SISTEMA OPERATIVO</b>	[E.8] Difusión de software dañino
	[E.20] Vulnerabilidades de los programas
	[E.21] Errores de mantenimiento o actualización de los programas
	[A.8] Difusión de software dañino
<b>OTROS SOFTWARE</b>	[A.22] Manipulación de programas
	[E.8] Difusión de software dañino
	[E.20] Vulnerabilidades de los programas
	[E.21] Errores de mantenimiento o actualización de los programas
<b>SERVIDOR DE BASE DE DATOS</b>	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.3] Contaminación medioambiental
	[I.5] Avería de origen físico o lógico
	[E.2] Errores del administrador del sistema o de la seguridad
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[E.23] Errores de mantenimiento/actualización de equipos
[A.11] Acceso no autorizado	
<b>IMPRESORAS</b>	[E.25] Pérdida de equipos
	[A.11] Acceso no autorizado
	[A.23] Manipulación del hardware
	[A.25] Robo de equipos
<b>COMPUTADORAS Y LAPTOPS</b>	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.*] Desastres industriales
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[E.23] Errores de mantenimiento/actualización de equipos
	[E.23] Caída del sistema por agotamiento del sistema
	[A.11] Acceso no autorizado
[A.7] Uso no previsto	
<b>ROUTER</b>	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.3] Contaminación medioambiental
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[A.11] Acceso no autorizado

<b>CÁMARAS</b>	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.*] Desastres industriales
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[E.23] Errores de mantenimiento/actualización de equipos
<b>MICRÓFONOS</b>	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.*] Desastres industriales
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[E.23] Errores de mantenimiento/actualización de equipos
<b>RED WIFI</b>	[A.14] Interceptación de información
	[E.9] Errores de re-encaminamiento
<b>RED LAN</b>	[A.14] Interceptación de información
	[E.9] Errores de re-encaminamiento
	[E.2] Errores del administrador del sistema / de la seguridad
	[A.5] Suplantación de usuarios
	[A.9] Re-encaminamiento de mensajes
	[A.12] Análisis de tráfico
	[A.11] Acceso no autorizado
<b>INTERNET</b>	[A.14] Interceptación de información
	[E.15] Alteración de la información
<b>CABLEADO</b>	[I.3] Contaminación medioambiental
<b>MOBILIARIO</b>	[N.1] Fuego
	[I.3] Contaminación medioambiental
<b>SISTEMA DE VIGILANCIA</b>	[I.3] Contaminación medioambiental
	[E.23] Errores de mantenimiento/actualización de equipos
<b>SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA</b>	[A.25] Robo de equipos
<b>OTROS EQUIPOS AUXILIARES</b>	[I.3] Contaminación medioambiental
<b>USB</b>	[E.15] Alteración de la información
	[E.19] Fugas de información
	[A.7] Uso no previsto
	[A.15] Modificación de la información
<b>EDIFICIO</b>	[N.1] Fuego
	[N.2] Daños por agua
	[N.*.1] Tormentas
	[N.*.4] Terremotos
	[N.*.9] Tsunamis
	[N.*.11] Calor extremo

	[I.*] Desastres industriales
	[A.27] Ocupación enemiga
<b>PRESIDENTE EPICENTRO</b>	[A.19] Revelación de información
	[A.29] Extorsión
	[A.30] Ingeniería social
	[E.19] Fugas de información
<b>JEFE DE LOGÍSTICA</b>	[A.19] Revelación de información
	[A.29] Extorsión
	[A.30] Ingeniería social
<b>JEFE DE SOPORTE TÉCNICO</b>	[A.19] Revelación de información
<b>MANTENIMIENTO BD</b>	[E.19] Fugas de información
	[A.19] Revelación de información
<b>AUXILIAR WEBCASTING</b>	[A.19] Revelación de información
	[A.29] Extorsión
	[A.30] Ingeniería social

**Fuente: Pilar 7.1**

**Valoración de las amenazas**

Los objetivos de esta tarea son:

- Evaluar la probabilidad de que ocurra una amenaza que afecte a cada activo.
- Estimar el impacto y daño que causaría la amenaza a cada dimensión del activo si llega a materializarse.

Para poder valorar dichas amenazas se ha tomado en cuenta la degradación de valor y la probabilidad de ocurrencia según la herramienta PILAR, tal y como se muestra en las tablas N° 6 y 7:

**Tabla N°6. Degradación de valor**

T	MUY ALTA
A	ALTA
M	MEDIA
B	BAJA
MB	MUY BAJA
0	

**Fuente Pilar 7.1**

**Tabla N°7. Probabilidad de ocurrencia**

CS	CASI SEGURO
MA	MUY ALTO
P	POSIBLE
PP	POCO PROBABLE
MB	SIGLOS
MR	MUY RARA
0	

**Fuente Pilar 7.1**

En la siguiente tabla N° 8 podemos observar la valoración que se le dio a las amenazas que dejan en riesgo a los activos:

**Tabla N°8 Valoración de amenazas a cada uno de los activos**

Tipo	Activos	Amenazas	P	[D]	[I]	[C]	[A]	[T]
<b>SERVICIOS INTERNOS</b>	<b>INTERNET</b>	[I.8] Fallo de servicios de comunicaciones	P	M				
	<b>APLICACIONES</b>	<b>OBS</b>	[E.8] Difusión de software dañino	P		M	M	
[E.20] Vulnerabilidades de los programas			P		M	M		
[E.21] Errores de mantenimiento o actualización de los programas			MA		B			
[A.8] Difusión de software dañino			P		T	T		
[A.22] Manipulación de programas			P		T	T		
<b>OFFICE</b>		[E.8] Difusión de software dañino	P		M	M		
		[E.20] Vulnerabilidades de los programas	P		M	M		
		[E.21] Errores de mantenimiento o actualización de los programas	MA		B			
		[A.8] Difusión de software dañino	P		T	T		
		[A.22] Manipulación de programas	P		T	T		
<b>ANTIVIRUS</b>	[E.8] Difusión de software dañino	P		M	M			
	[E.20] Vulnerabilidades de los programas	P		M	M			
	[E.21] Errores de mantenimiento o actualización de los programas	MA		B				
	[A.8] Difusión de software dañino	P		T	T			
	[A.22] Manipulación de programas	P		T	T			
<b>SISTEMA OPERATIVO</b>	[E.8] Difusión de software dañino	P		M	M			
	[E.20] Vulnerabilidades de los programas	P		M	M			
	[E.21] Errores de mantenimiento o actualización de los programas	MA		B				
	[A.8] Difusión de software dañino	P		T	T			
	[A.22] Manipulación de programas	P		T	T			
<b>OTROS SOFTWARE</b>	[E.8] Difusión de software dañino	P		M	M			
	[E.20] Vulnerabilidades de los programas	P		M	M			
	[E.21] Errores de mantenimiento o actualización de los programas	MA		B				

<b>EQUIPOS</b>	<b>SERVIDOR DE BASE DE DATOS</b>	[N.1] Fuego	PP	T				
		[N.2] Daños por agua	PP	A				
		[N.*] Desastres naturales	PP	T				
		[I.3] Contaminación medioambiental	PP	A				
		[I.5] Avería de origen físico o lógico	P	A				
		[I.6] Corte del suministro eléctrico	P	T				
		[I.7] Condiciones inadecuadas de temperatura o humedad	P	T				
		[E.23] Errores de mantenimiento/actualización de equipos	P	M				
	<b>IMPRESORAS</b>	[A.11] Acceso no autorizado	P	M	T	T		
		[E.25] Pérdida de equipos	P			A		
		[A.11] Acceso no autorizado	P		M	A		
		[A.23] Manipulación del hardware	P			A		
	<b>COMPUTADORAS Y LAPTOPS</b>	[A.25] Robo de equipos	P			A		
		[N.2] Daños por agua	PP	A				
		[N.*] Desastres naturales	PP	T				
		[I.*] Desastres industriales	P	T				
		[I.5] Avería de origen físico o lógico	P	A				
		[I.7] Condiciones inadecuadas de temperatura o humedad	P	T				
		[E.23] Errores de mantenimiento/actualización de equipos	P	M				
		[E.23] Caída del sistema por agotamiento del sistema	MA	A				
	<b>ROUTER</b>	[A.11] Acceso no autorizado	P	M	M	A		
		[A.7] Uso no previsto	P	M	B	M		
		[N.1] Fuego	PP	T				
	<b>CÁMARAS</b>	[N.2] Daños por agua	PP	A				
		[N.*] Desastres naturales	PP	T				
		[I.*] Desastres industriales	P	T				
		[I.5] Avería de origen físico o lógico	P	A				
		[I.7] Condiciones inadecuadas de temperatura o humedad	P	T				
		[E.23] Errores de mantenimiento/actualización de equipos	P	M				
		[A.11] Acceso no autorizado	P	M	M	A		
<b>MICRÓFONOS</b>	[N.2] Daños por agua	PP	A					
	[N.*] Desastres naturales	PP	T					
	[I.*] Desastres industriales	P	T					
	[I.5] Avería de origen físico o lógico	P	A					
	[I.7] Condiciones inadecuadas de temperatura o humedad	P	T					
	[E.23] Errores de mantenimiento/actualización de equipos	P	M					



COMUNICACIONES	RED WIFI	[A.14] Interceptación de información	P			M		
		[E.9] Errores de re-encaminamiento	P			M		
	RED LAN	[A.14] Interceptación de información	P			B		
		[E.9] Errores de re-encaminamiento	P			M		
		[E.2] Errores del administrador del sistema / de la seguridad	P			M		
		[A.5] Suplantación de la identidad	P			A		
		[A.9] Re-encaminamiento de mensajes	P			M		
		[A.12] Análisis de tráfico	P			B		
		[A.11] Acceso no autorizado	P			A		
	INTERNET	[A.14] Interceptación de información	P				M	
[E.15] Alteración de la información		P			B			
EQUIPOS AUXILIARES	CABLEADO	[I.3] Contaminación medioambiental	PP	A				
	SISTEMA DE VIGILANCIA	[N.1] Fuego	PP	T				
		[I.3] Contaminación medioambiental	PP	A				
	MOBILIARIO	[N.1] Fuego	PP	T				
		[I.3] Contaminación medioambiental	PP	A				
	SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA	[A.25] Robo de equipos	P	B				
OTROS EQUIPOS AUXILIARES	[I.3] Contaminación medioambiental	PP	A					
SOPORTES DE INFORMACIÓN	USB	[E.15] Alteración de la información	P			B		
		[E.19] Fugas de información	P			M		
		[A.7] Uso no previsto	P			B		
		[A.15] Modificación de la información	MA			T		
INSTALACIONES	EDIFICIO	[N.1] Fuego	P	T				
		[N.2] Daños por agua	P	T				
		[N.*.1] Tormentas	P	T				
		[N.*.4] Terremotos	P	T				
		[N.*.9] Tsunamis	P	T				
		[N.*.11] Calor extremo	P	T				
		[I.*] Desastres industriales	P	T				
		[A.27] Ocupación enemiga	P	T				
PERSONAL	PRESIDENTE EPICENTRO	[A.19] Revelación de información	MA			M		
		[A.29] Extorsión	P			M		
		[A.30] Ingeniería social	P			M		
		[E.19] Fugas de información	P			M		
	JEFE DE LOGÍSTICA	[A.19] Revelación de información	MA			M		
		[A.29] Extorsión	P			M		
		[A.30] Ingeniería social	P			M		
	JEFE DE SOPORTE TÉCNICO	[A.19] Revelación de información	MA			A		
	MANTENIMIENTO BD	[E.19] Fugas de información	P			M		
		[A.19] Revelación de información	MA			A		
AUXILIAR WEBCASTING	[A.19] Revelación de información	P			A			
	[A.29] Extorsión	P			A			
	[A.30] Ingeniería social	P			A			

Fuente: Pilar 7.1

### 2.3 Caracterización de salvaguardas

En esta actividad se identifican las salvaguardas que necesita la empresa, junto con la eficacia que estas tienen para mitigar el riesgo. La metodología MAGERIT la divide en etapas de estudio que pueden abarcar lapsos de tiempo corto o largo, en este caso se tomará tres fases:

- Etapa 1: POTENCIAL (Potential)
- Etapa 2: SITUACIÓN ACTUAL (Current)
- Etapa3: OBJETIVO (Target)

Así mismo estas fases cuentan con dos sub-tareas:

- Identificación de las salvaguardas pertinentes
- Valoración de las salvaguardas

#### Identificación de las salvaguardas pertinentes

En esta parte se utilizará la herramienta Pilar 7.1. que nos ayudará a elegir las salvaguardas de cada activo para así poder contrarrestar las amenazas que se presenten tal y como se muestra en la figura N°4:

**Figura 4: Identificación de las salvaguardas**

as...	tdp	salvaguarda	du...	fue...	co...	rec...	on /...	apli...
		SALVAGUARDAS						
<input type="checkbox"/>	G	EL	3					
<input type="checkbox"/>	T	EL	3				7	
<input type="checkbox"/>	G	PR	3					
<input type="checkbox"/>	G	EL	3					
<input type="checkbox"/>	G	PR	4				5	
<input type="checkbox"/>	G	PR	2				7	
<input type="checkbox"/>	G	PR	2				7	
<input type="checkbox"/>	G	PR	2				8	
<input type="checkbox"/>	G	PR	2					
<input type="checkbox"/>	G	PR	2				7	
<input type="checkbox"/>	G	PR	2				6	
<input type="checkbox"/>	F	EL	1				6	
<input type="checkbox"/>	F	PR	2				7	
<input type="checkbox"/>	F	EL	2					
<input type="checkbox"/>	P	PR	2				6	
<input type="checkbox"/>	G	PR	1					
<input type="checkbox"/>	G	CR	1				6	
<input type="checkbox"/>	T	PR	2				8	
<input type="checkbox"/>	G	CR	1				6	
<input type="checkbox"/>	T	MN	2				5	
<input type="checkbox"/>	G	RC	2				5	
<input type="checkbox"/>	G	AD	1				4	
<input type="checkbox"/>	G	AD	1				5	
<input type="checkbox"/>	G	AD	10				4	

**Fuente: Pilar 7.1**

Se eligieron diferentes tipos de salvaguardas de acuerdo a cada activo, las cuales son:

### **Protecciones generales:**

Con autorización previa: Este se encuentra en el grupo con acceso restringido a la información, además pertenece al grupo de control de acceso lógico, se eligió estas salvaguardas ya que actualmente, no se toman medidas de protección, dado que cualquiera puede acceder a los activos, tanto a la información, como al software, hardware y equipo de redes de la empresa. Esta salvaguarda protege a las siguientes dimensiones: Integridad, confidencialidad y autenticidad y hace frente a amenazas como lo son:

- Errores por parte de los usuarios
- Errores de los administradores de los sistemas, de la seguridad
- Alteración de la información
- Pérdida de la información
- Vulnerabilidad de los programas
- Errores de actualización y mantenimiento de los programas
- Suplantación de usuarios
- Abuso de privilegios de acceso
- Accesos no autorizados
- Revelación de información
- Manipulación de hardware

❖ Herramienta contra el código dañino: La empresa cuenta con herramientas contra ello, pero no se encuentra actualizado o son software ya vencidos lo cual hace que estén expuestos a virus, troyanos, etc. Por ello, se determinó el uso de las siguientes salvaguardas:

El programa debe actualizarse con frecuencia.

La base de datos de virus debe actualizarse regularmente.

Se deben revisar los programas y servicios de arranque del sistema.

Estas salvaguardas solo pueden ser aplicado a las aplicaciones y permiten que se haga frente a las siguientes amenazas:

- Ataques frente a la denegación de servicio (DOS).
- Procedimientos operativos.
- Ataques ocasionados en las mismas instalaciones de la empresa.

Esta salvaguarda permitirá asegurar la dimensión de Disponibilidad y será aplicado en la capa de servicios internos.

❖ Protecciones de las aplicaciones informáticas (SW): Para su protección se eligió las siguientes salvaguardas, dado que la empresa no cuenta con ninguna protección:

- Disposición de normativas para el uso autorizado de las aplicaciones
- Disposición de normativa relativa al cumplimiento de los derechos
- Control de instalación de software autorizado y productos con licencia
- Disposición de la realización de copias de seguridad
- Aplicación de perfiles de seguridad a los accesos de los usuarios para hacer frente a las amenazas de: errores de usuarios, difusión de software dañino, vulnerabilidad de los programas, errores de actualización y mantenimiento y uso no previsto. Esto debe permitir que se cumpla con lo siguiente:
  - Seguridad de los ficheros de datos.
  - Protección de los ficheros de configuración.
  - Seguridad de los mecanismos de comunicación entre procesos.

❖ Protección de equipos informáticos (HW): Los salvaguardas adecuados para los equipos informáticos son:

- Una normativa para el uso correcto de los equipos.
- Procedimientos de uso del equipo.
- Aplicar perfiles de seguridad para lo que son de parte de errores del administrador del sistema y la seguridad, accesos no autorizados, asegurando las dimensiones de la integridad y la confidencialidad.

- Protección física de los equipos sobre todo en equipos usados para el webcasting y el servidor de datos, evitando los accesos innecesarios y/o no autorizados.

Luego de evaluar las salvaguardas mencionados se debe implementar las siguientes salvaguardas:

- Evaluar el impacto en la confidencialidad de los datos.
- Evaluar el impacto en la integridad de los datos.
- Evaluar el estado del equipo informático.

❖ Protección de las comunicaciones: Para minimizar sus riesgos se han escogió las siguientes salvaguardas:

- Se debe de aplicar perfiles de seguridad que puedan contrarrestar errores de secuencia, usos no previsto protegiendo las dimensiones de integridad, confidencialidad y autenticidad.
- Aplicar una normativa para los servicios de red.
- Control de filtrado ya que no posee.

Las salvaguardas mencionadas hacen frente al acceso no autorizado.

Para proteger las comunicaciones mientras se use el servicio de Internet es imprescindible que se empleen las siguientes salvaguardas:

- Controlar la configuración de los navegadores
- Registrar las descargas
- Instalar herramientas antispysware
- Deshabilitar las cookies en los navegadores
- Registrar la navegación web
- Una normativa sobre el uso de los servicios de Internet
- Herramienta para la monitorización del tráfico

❖ Protección de los soportes de información: para los soportes de información se han establecido las siguientes salvaguardas:

- Proteger en uso de contenedores cerrados

- Normativa para la protección criptográfica de los contenidos.
- ❖ Elementos auxiliares:
  - Seguir las recomendaciones de cuidado del fabricante o proveedor.
  - Continuidad de operaciones: asegura la disponibilidad de los equipos auxiliares para contrarrestar la amenaza de contaminación medioambiental.
  - Climatización: La adecuada climatización de los equipos, cuidando que se encuentren en adecuados lugares con la temperatura y humedad ideal.
- ❖ Protección de las instalaciones:
  - Normativa para la seguridad de las instalaciones.
  - Disponer áreas específicas para los equipos informáticos por protección.
  - Refuerzo de vigilancia para el cuidado de la infraestructura TI
  - Protección contra explosiones o explosivos
- Gestión del personal:
  - Normativa para la gestión de personal en materia de seguridad.
  - Procedimientos relacionados a la seguridad por parte del personal.
  - Creación de normas para el personal en general
  - Normas en los contratos del personal que estipulen garantizar la confidencialidad de los datos frente a ataques como extorsión y ataques en el interior.
  - Procedimientos para la seguridad ante emergencias e incidentes.

Después de la evaluación e identificación de la salvaguarda requeridos, se tendrá la declaratoria de aplicabilidad que es un documento formal donde constan las salvaguardas necesarias para proteger los activos.

### **Valoración de las salvaguardas**

La valoración de salvaguardas tiene como objetivo los siguiente:

- Determinar la eficacia de las salvaguardas pertinentes como se muestra en la siguiente tabla N° 9:

**Tabla N°9: Valoración de salvaguardas**

Eficacia	Nivel	Madurez	Estado
0%	L0	Inexistente	Inexistente
10%	L1	Inicial/ad hoc	Iniciado
50%	L2	Reproducibile, pero intuitivo	Parcialmente realizado
90%	L3	Proceso definido	En funcionamiento
95%	L4	Gestionable y medible	Monitorizado
100%	L5	Optimizado	Mejora continua

Fuente: Pilar 7.1

**Figura N°5: Valoración de Salvaguardas**

asp...	tdp	salvaguarda	dud...	fue...	co...	rec...	c...	PILAR
SALVAGUARDAS								
<input type="checkbox"/>	G	EL	[IA]	Identificación y autenticación				n.a.
<input type="checkbox"/>	T	EL	[AC]	Control de acceso lógico		7		L2-L4
<input type="checkbox"/>	G	PR	[D]	Protección de la Información				n.a.
<input type="checkbox"/>	G	EL	[K]	Protección de claves criptográficas				n.a.
<input type="checkbox"/>	G	PR	[S]	Protección de los Servicios		5		L2-L3
<input type="checkbox"/>	G	PR	[SW]	Protección de las Aplicaciones Informáticas (SW)		7		L2-L4
<input type="checkbox"/>	G	PR	[HW]	Protección de los Equipos Informáticos (HW)		7		L2-L4
<input type="checkbox"/>	G	PR	[COM]	Protección de las Comunicaciones		8		L2-L5
<input type="checkbox"/>	G	PR	[IP]	Sistema de protección de frontera lógica				n.a.
<input type="checkbox"/>	G	PR	[MP]	Protección de los Soportes de Información		7		L2-L4
<input type="checkbox"/>	G	PR	[AUX]	Elementos Auxiliares		6		L2-L4
<input type="checkbox"/>	F	EL	[HW_0049]	Protección física del equipamiento		6		L3-L4
<input type="checkbox"/>	F	PR	[L]	Protección de las Instalaciones		7		L2-L4
<input type="checkbox"/>	F	EL	[PPS]	Protección del perímetro físico				n.a.
<input type="checkbox"/>	P	PR	[PS]	Gestión del Personal		6		L2-L4
<input type="checkbox"/>	G	PR	[PDS]	Servicios potencialmente peligrosos				n.a.
<input type="checkbox"/>	G	CR	[IR]	Gestión de incidentes		6		L2-L4
<input type="checkbox"/>	T	PR	[tools]	Herramientas de seguridad		8		L2-L5
<input type="checkbox"/>	G	CR	[V]	Gestión de vulnerabilidades		6		L2-L4
<input type="checkbox"/>	T	MN	[A]	Registro y auditoría		5		L2-L3
<input type="checkbox"/>	G	RC	[BC]	Continuidad del negocio		5		L2-L3
<input type="checkbox"/>	G	AD	[G]	Organización		4		L2-L3
<input type="checkbox"/>	G	AD	[E]	Relaciones Externas		5		L2-L3
<input type="checkbox"/>	G	AD	[NEW]	Adquisición / desarrollo		4		L2-L3

Fuente: Pilar 7.1

## 2.4 Estimación del estado del riesgo

En esta actividad o tarea se procesan e interpretan los resultados obtenidos en las actividades anteriores y así poder elaborar un informe que nos muestre el estado de riesgo en el que se encuentra la empresa.

Esta actividad se divide en dos tareas:

- Estimación del impacto
- Estimación del riesgo

El objetivo de estas tareas son el de disponer de una estimación fundada de lo que pudiese suceder si ocurre un impacto y del riesgo al que está expuesto de ocurrir.

### Estimación del impacto

Los objetivos de esta tarea son:

- Establecer el impacto potencial al que están sometidos los activos
- Establecer el impacto residual al que están sometidos los activos

En esta tarea se estima a los que están expuestos los activos de la empresa:

- El impacto potencial que refiere a los que está expuesto el activo tomando en cuenta su valor y la valoración de las amenazas, pero no los salvaguardas establecidos.
- El impacto residual que refiere al valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas.

La fórmula emplea un sistema de salvaguardas, el cual es ineficaz ( $e_i=0$ ) y deja el impacto en donde se encuentra, mientras que un sistema de salvaguardas eficaz ( $e_i=1$ ) reduce el impacto residual a 0.

$$\text{Impacto residual} = \text{impacto potencial} (1 - e^i)$$



### Impacto potencial

El impacto potencial es la medida del daño que cae sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos en varias dimensiones y la degradación que causan las amenazas, tal y como se muestra en la tabla N°10.

**Tabla N°10: Impacto potencial sobre cada uno de los activos**

Activos	Dimensiones				
	[D]	[I]	[C]	[A]	[T]
<b>Servicios internos</b>					
Internet	[9]			[7]	
<b>Aplicaciones</b>					
OBS		[9]	[9]		
Office		[7]	[7]		
Antivirus		[7]	[7]		
Sistema Operativo		[7]	[7]		
Otros software		[5]	[5]		
<b>Equipos</b>					
Servidor de base de datos	[9]	[9]	[9]		
Impresoras		[2]	[4]		
Computadoras y laptops	[9]	[6]	[8]		
Router	[9]	[6]	[8]		
Cámaras	[9]	[6]	[8]		
Micrófonos	[9]	[6]	[8]		
<b>Comunicaciones</b>					
Red WIFI			[5]		
Red LAN			[5]		
Internet		[5]	[6]		
<b>Equipos auxiliares</b>					
Cableado	[5]				
Mobiliario	[7]				
Sistema de vigilancia	[7]				
Sistema de alimentación ininterrumpida	[1]				
Otros equipos auxiliares	[5]				
<b>Soportes de información</b>					
Memoria USB		[7]	[7]		
<b>Instalaciones</b>					
Oficinas sede epicentros	[9]				
<b>Personal</b>					
PRESIDENTE EPICENTRO			[7]		
JEFE DEL DEPARTAMENTO DE LOGISTICA			[6]		
JEFE DE SOPORTE TÉCNICO			[8]		
MANTENIMIENTO DE BD			[1]		
AUXILIAR WEBCASTING			[1]		

**Fuente: Pilar 7.1**

En la siguiente tabla N° 11 se muestra la escala de colores, según el valor del impacto.

**Tabla N° 11 C Colores valor del impacto**

[10]	Nivel 10
[9]	Nivel 9
[8]	Alto (+)
[7]	Alto
[6]	Alto (-)
[5]	Medio (+)
[4]	Medio
[3]	Medio (-)
[2]	Bajo (+)
[1]	Bajo
[0]	Despreciable

Fuente: Pilar 7.1

**Impacto residual**

El impacto residual acumulado se calcula con los datos del impacto acumulado sobre un activo y salvaguardas apropiadas para las amenazas de ese activo

**Figura N°7: Impacto residual sobre cada uno de los activos**

[0001] impacto y riesgo > impacto repercutido

Exportar

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	[9]	[9]	[9]	[7]	
[INTERNET_PIB] INTERNET	[9]			[7]	
[OBS_PIB] OPEN BROADCASTER SOFTWARE		[9]	[9]		
[OFF_PIB] OFFICE		[7]	[7]		
[ANT_PIB] ANTIVIRUS		[7]	[7]		
[OS_PIB] SISTEMA OPERATIVO		[7]	[7]		
[OTR_PIB] OTROS SOFTWARE		[6]	[5]		
[SERVBD_PIB] SERVIDOR DE BASE DE DATOS	[9]	[9]	[9]		
[PRINT_PIB] IMPRESORAS		[2]	[4]		
[PC_PIB] COMPUTADORAS Y LAPTOPS	[9]	[6]	[8]		
[ROUTER_PIB] ROUTER	[9]	[6]	[8]		
[CAM_PIB] CAMARAS	[9]	[6]	[8]		
[MIC_PIB] MICRÓFONOS	[9]	[6]	[8]		
[WIFI_PIB] RED WIFI			[5]		
[LAN_PIB] RED LAN			[5]		
[IEX_PIB] INTERNET		[6]	[6]		
[CABLING_PIB] CABLEADO	[5]				
[MOB_PIB] MOBILIARIO	[7]				
[SISVG_PIB] SISTEMA DE VIGILANCIA	[7]				
[SAI_PIB] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA	[1]				
[AUXOTR_PIB] OTROS EQUIPOS AUXILIARES	[5]				
[USB_PIB] MEMORIAS USB		[7]	[7]		
[BUILDING_PIB] OFICINA SEDE EPICENTRO	[9]				
[PRE_PIB] PRESIDENTE EPICENTRO			[7]		
[JLC_PIB] JEFE DEL DEPARTAMENTO DE LOGISTICA			[6]		
[JST_PIB] JEFE DE SOPORTE TÉCNICO			[8]		
[DBA_PIB] MANTENIMIENTO DE BD			[7]		
[AWC_PIB] AUXILIAR WEBCASTING			[7]		

Fuente: Pilar 7.1

## 2.5 Estimación del riesgo

Los objetivos de la estimación del riesgo son:

- Determinar el riesgo potencial al que están expuestos los activos.
- Determinar el riesgo residual al que están expuestos los activos.

En esta tarea se puede hacer la estimación del riesgo al que están expuestos los activos:

- El riesgo potencial al que están expuestos los activos, teniendo en cuenta su valor y la valoración de las amenazas, pero no las salvaguardas determinadas.
- El riesgo residual al que están expuestos los activos, teniendo en cuenta su valor y la valoración de las amenazas, así como la eficacia de las salvaguardas determinadas.

Se emplea la siguiente formula:

$$\text{Riesgo residual} = \text{Impacto residual} \times \text{frecuencia}$$

### Riesgo potencial

Se denomina riesgo al daño probable sobre un activo o sistema, ya conociendo el impacto que puede generar las amenazas sobre los activos, se deriva el riesgo sin más que tener la probabilidad de ocurrencia, tal y como se muestra en la tabla N° 12.

**Tabla N°12: Riesgo potencial sobre cada uno de los activos**

Activos	Dimensiones				
	[D]	[I]	[C]	[A]	[T]
Servicios internos					
Internet	{6,2}			{4,5}	
Aplicaciones					
OBS		{6,2}	{6,2}		
Office		{5,1}	{5,1}		
Antivirus		{5,1}	{5,1}		
Sistema Operativo		{5,1}	{5,1}		
Otros software		{3,9}	{3,9}		
Equipos					
Servidor de base de datos	{6,6}	{6,2}	{6,2}		
Impresoras		{2,1}	{3,4}		
Computadoras y laptops	{6,6}	{4,5}	{5,7}		
Router	{6,6}	{4,5}	{5,7}		
Cámaras	{6,6}	{4,5}	{5,7}		
Micrófonos	{6,6}	{4,5}	{5,7}		
Comunicaciones					
Red WIFI			{3,9}		
Red LAN			{3,9}		
Internet		{3,8}	{4,5}		
Equipos auxiliares					
Cableado	{3,9}				
Mobiliario	{4,8}				
Sistema de vigilancia	{4,8}				
Sistema de alimentación ininterrumpida	{1,5}				
Otros equipos auxiliares	{3,6}				
Soportes de información					
Memoria USB		{5,7}	{5,1}		
Instalaciones					
Oficinas sede epicentros	{6,2}				
Personal					
PRESIDENTE EPICENTRO			{5,9}		
JEFE DEL DEPARTAMENTO DE LOGISTICA			{5,3}		
JEFE DE SOPORTE TÉCNICO			{6,0}		
MANTENIMIENTO DE BD			{5,4}		
AUXILIAR WEBCASTING			{5,1}		

**Fuente: Pilar 7.1.2**

La siguiente tabla nos muestra la escala de colores los cuales representan el valor de los riesgos, tal y como se muestra en la tabla N°13:

**Tabla N°13: Colores del valor del riesgo**

{9}	Catástrofe
{8}	Desastre
{7}	Extremadamente crítico
{6}	Muy crítico
{5}	Crítico
{4}	Muy alto
{3}	Alto
{2}	Medio
{1}	Bajo
{0}	Despreciable

**Fuente: Pilar 7.1.**

## Riesgo Residual

### Riesgo residual acumulado

La estimación del riesgo residual acumulado nos muestra en qué medida las amenazas afectan a los activos de orden superior que dependen de dicho activo. En la siguiente tabla N° 15 se muestran los resultados mayores a 3, los cuales son riesgos altos.

**Figura N°8. Riesgo residual sobre cada uno de los activos**

[0001] impacto y riesgo > riesgo repercutido

Exportar

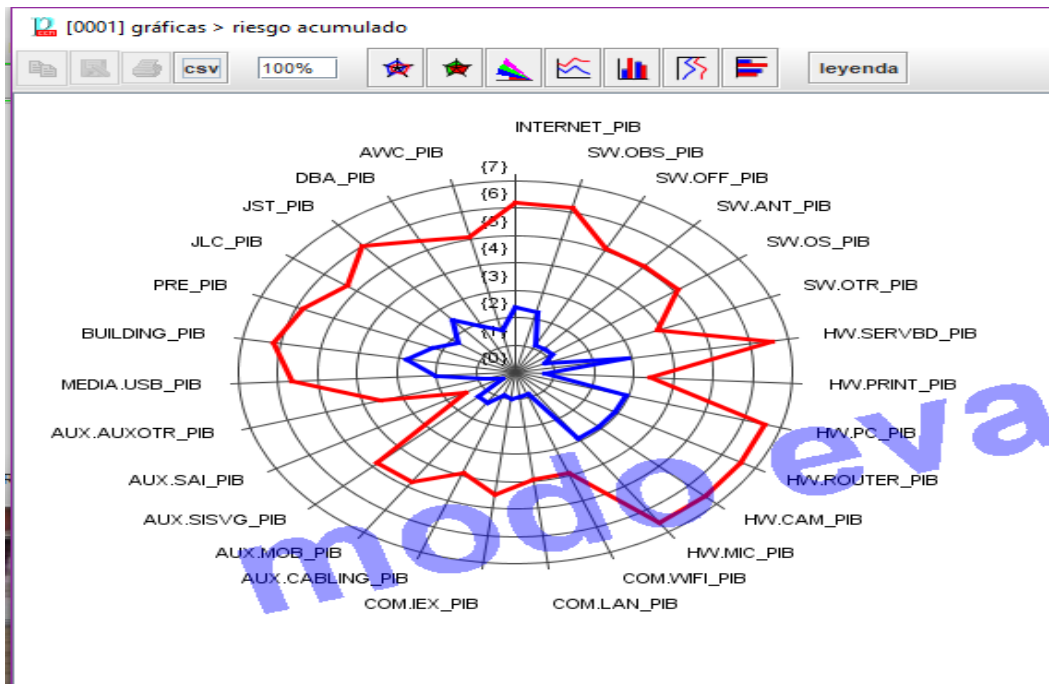
potencial current target PILAR

activo	[D]	[I]	[C]	[A]	[T]
[INTERNET_PIB] INTERNET	(6,2)	(6,2)	(6,2)	(4,5)	
[OBS_PIB] OPEN BROADCASTER SOFTWARE		(6,2)	(6,2)		
[OFF_PIB] OFFICE		(5,1)	(5,1)		
[ANT_PIB] ANTIVIRUS		(5,1)	(5,1)		
[OS_PIB] SISTEMA OPERATIVO		(5,1)	(5,1)		
[OTR_PIB] OTROS SOFTWARE		(3,9)	(3,9)		
[SERVBD_PIB] SERVIDOR DE BASE DE DATOS	(6,6)	(6,2)	(6,2)		
[PRINT_PIB] IMPRESORAS		(2,1)	(3,4)		
[PC_PIB] COMPUTADORAS Y LAPTOPS	(6,6)	(4,5)	(5,7)		
[ROUTER_PIB] ROUTER	(6,6)	(4,5)	(5,7)		
[CAM_PIB] CAMARAS	(6,6)	(4,5)	(5,7)		
[MIC_PIB] MICROFONOS	(6,6)	(4,5)	(5,7)		
[WIFI_PIB] RED WIFI			(3,9)		
[LAN_PIB] RED LAN			(3,9)		
[IEX_PIB] INTERNET		(3,8)	(4,5)		
[CABLING_PIB] CABLEADO	(3,9)				
[MOB_PIB] MOBILIARIO	(4,8)				
[SISVG_PIB] SISTEMA DE VIGILANCIA	(4,8)				
[SAI_PIB] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA	(1,5)				
[AUXOTR_PIB] OTROS EQUIPOS AUXILIARES	(3,6)				
[USB_PIB] MEMORIAS USB		(5,7)	(5,1)		
[BUILDING_PIB] OFICINA SEDE EPICENTRO	(6,2)				
[PRE_PIB] PRESIDENTE EPICENTRO			(5,9)		
[JLC_PIB] JEFE DEL DEPARTAMENTO DE LOGISTICA			(5,3)		
[JST_PIB] JEFE DE SOPORTE TÉCNICO			(6,0)		
[DBA_PIB] MANTENIMIENTO DE BD			(5,4)		
[AWC_PIB] AUXILIAR WEBCASTING			(5,1)		

Fuente: Pilar 7.1.

## 2.6 Interpretación de los resultados

**Figura N° 9: Interpretación de los resultados**



Fuente: Pilar 7.1.

### 3. Gestión de riesgos

Una vez realizado el análisis de riesgos, hemos determinado los impactos y los riesgos a los que se puede ver envuelto la empresa.

En dicho análisis pudo determinarse lo siguiente:

- Si aparece como crítico es que requiere atención urgente.
- Si aparece como grave requiere atención.
- Si aparece como apreciable, es que puede ser objeto de estudio para su tratamiento.
- Si aparece como asumible, es que no se tomaran decisiones para evitarlo.

#### 3.1 Toma de decisiones

##### Identificación de riesgos críticos

En toda empresa existen riesgos que dejan expuestos a los activos y afectan los procesos que se realizan dentro de ella, así como el desempeño de las mismas. Por ello, es que se identificó los activos que poseen un mayor nivel de riesgo con la finalidad de implementar salvaguardas para evitar que las amenazas se materialicen.

En la siguiente tabla N° 14 se muestran los activos con mayor riesgo:

**Tabla N°14 Identificación de riesgos críticos**

Activos	Dimensiones				
	[D]	[I]	[C]	[A]	[T]
<b>Servicios internos</b>					
Internet	{6,2}			{4,5}	
<b>Aplicaciones</b>					
OBS		{6,2}	{6,2}		
Office		{5,1}	{5,1}		
Antivirus		{5,1}	{5,1}		
Sistema Operativo		{5,1}	{5,1}		
<b>Equipos</b>					
Servidor de base de datos	{6,6}	{6,2}	{6,2}		
Computadoras y laptops	{6,6}	{4,5}	{5,7}		
Cámaras	{6,6}	{4,5}	{5,7}		
Micrófonos	{6,6}	{4,5}	{5,7}		
<b>Comunicaciones</b>					
Internet			{4,5}		
<b>Equipos auxiliares</b>					
Mobiliario	{4,8}				
Sistema de vigilancia	{4,8}				
<b>Soportes de información</b>					
Memorias usb		{5,7}	{5,1}		
<b>Instalaciones</b>					
Oficinas sede epicentros	{6,2}				

**Fuente: Realizado en Pilar 7.1**

Los riesgos están establecidos en una escala de colores según su valor, tal y como se muestra en la tabla N°15

**Tabla N°15: Colores valoración de los riesgos**

{9}	Nivel 9
{8}	Nivel 8
{7}	Extremadamente crítico
{6}	Muy crítico
{5}	Crítico
{4}	Muy alto
{3}	Alto
{2}	Medio
{1}	Bajo
{0}	Despreciable

**Fuente: Realizado en Pilar 7.1**

**Calificación del riesgo**

En esta etapa se gestionan los activos con riesgos críticos:

**Servicios internos**

En cuanto a la capa de servicios internos, tenemos el siguiente activo con más riesgo de amenazas:

**Internet:** Una vez realizado el análisis de amenazas de las cuales puede ser víctima y haber escogido las correctas salvaguardas, se pudo obtener como resultado que:

Teniendo las dimensiones establecidas, en cuanto a disponibilidad (6,2) y en cuanto a Autenticidad (4,5), lo cual significa que, si la amenaza se materializa, se vería afectada la transmisión de programas, ya que sin este servicio no puede realizarse el webcasting, además de que interrumpiría las actividades diarias como el envío de emails, mantenimiento y manejo de la página web entre otras actividades.



Por ello, las medidas establecidas para reducir esos riesgos son los siguientes:

El correcto mantenimiento de equipos como router, verificando el correcto funcionamiento y contar con un proveedor de servicio estable.

Restringir las paginas como redes sociales, la descarga de programas para que los trabajadores se concentren en sus actividades laborales, además de evitar descargas maliciosas que afecten los activos.

Además de ello para proteger la disponibilidad se deben adquirir equipos como cortafuegos para soportar cargas altas.

## Aplicaciones

**OBS (Open Broadcaster Software)** Una vez realizado el análisis de amenazas de las cuales puede ser víctima y haber escogido las correctas salvaguardas, se pudo obtener como resultado que:

La mayor amenaza que este software pueda tener es que el usuario que lo manipule sea ajeno, y que exista la suplantación de usuario sufriendo así amenazas a la integridad y confidencialidad (6,2), todo esto a que los usuarios no cuentan con claves de ingreso dejándolo vulnerable.

Si este tipo de amenaza se materializa podría sufrirse de difusión de información ajena a la que se trasmite, pudiendo ir en contra las normas de la empresa, perjudicando así a la empresa, al transmitir información errónea o alterando ella.

Las medidas tomadas para mitigar dichos riesgos son:

- Establecer contraseñas confidenciales para acceder al sistema.
- Mejorar la protección del software con privilegios de acceso.

**Antivirus** Pertenciente a la capa de aplicaciones, una vez realizado el análisis de amenazas de las cuales puede ser víctima y haber escogido las correctas salvaguardas, se pudo obtener como resultado que:

La amenaza a la que está expuesto este activo es a la propagación en el sistema de software dañino, perjudicando así en niveles altos a la integridad (5,1) y a la confidencialidad (5,1). Uno de los motivos por los cuales ha ocurrido este tipo de

problemas ha sido a través de la inserción de memorias USB sin un análisis respectivo de virus, propagando así Spyware, gusanos, troyanos, etc.

Las medidas establecidas para mitigar esos riesgos son:

- Adquisición de un antivirus óptimo para evitar la propagación de virus
- Actualizar el antivirus, mínimo 3 veces al mes.
- Evitar y restringir el ingreso de dispositivos ajenos a los equipos de la empresa.

**Sistema operativo** Pertenece a la capa de aplicaciones, una vez realizado el análisis de amenazas de las cuales puede ser víctima y haber escogido las correctas salvaguardas, se pudo obtener como resultado que:

Las amenazas que hacen que este activo se encuentre expuesto a altos riesgos son:

Errores de los usuarios y la descarga de software dañino, que dañan las dimensiones de integridad (5,1) y confidencialidad (5,1), este tipo de riesgos se corren debido al mal uso de los equipos, la desactualización del antivirus.

Las medidas para mitigar dichos riesgos son:

- Adquirir software con licencia
- Uso de claves de usuario al acceder al sistema.

**Servidor de base de datos** Pertenece a la capa de equipos, una vez realizado el análisis de amenazas de las cuales puede ser víctima y haber escogido las correctas salvaguardas, se pudo obtener como resultado que:

Este activo posee un nivel alto de riesgo, ya que la manipulación del hardware puede afectar la disponibilidad, integridad y confidencialidad (6,2), el problema con el servidor de la base de datos es que no se encuentra en un lugar adecuado, quedando vulnerable e inseguro. Si la amenaza llega a materializarse podría causar graves daños a la empresa, ya que esta almacena información muy importante como lo son los podcasts y videos de transmisión.

Las medidas para mitigar dichos riesgos son:

- Colocar el servidor en una habitación que cumpla con las medidas de seguridad necesarias para el control de acceso.
- Resguardar la seguridad física como prevención ante desastres naturales u otros.

**Computadoras y laptops** Perteneciente a la capa de equipos, una vez realizado el análisis de amenazas de las cuales puede ser víctima y haber escogido las correctas salvaguardas, se pudo obtener como resultado que:

Estos activos también presentan un alto nivel de riesgo, los cuales afectan principalmente las dimensiones de la disponibilidad (6,6), confiabilidad (4,5) y la integridad (5,7). Las amenazas más comunes en estos activos son aquellas que los propios usuarios puedan instalar, como juegos, programas personales o almacenamiento de información ajena a la empresa.

Las medidas para mitigar dichos riesgos son:

- Crear cuentas de usuario y administrador y restringir los accesos.
- Bloquear las descargas.

**Cámaras y micrófonos** Perteneciente a la capa de equipos, una vez realizado el análisis de amenazas de las cuales puede ser víctima y haber escogido las correctas salvaguardas, se pudo obtener como resultado que:

Estos activos también presentan un alto nivel de riesgo, los cuales afectan principalmente las dimensiones disponibilidad (6,6), confiabilidad (4,5) y la integridad (5,7). Las amenazas más comunes en estos activos son aquellas que los propios usuarios puedan generar, debido al mal uso de los activos.

Las medidas para mitigar dichos riesgos son:

- Exigir el uso de manual de equipos para su correcto uso.
- Nombrar un responsable de manejo de equipos capacitado.

**Internet** Perteneciente a la capa de comunicaciones, una vez realizado el análisis de amenazas de las cuales puede ser víctima y haber escogido las correctas salvaguardas, se pudo obtener como resultado que:

Estos activos también presentan un alto nivel de riesgo, los cuales afectan principalmente la confidencialidad (4,5) con errores de re encaminamiento de mensajes, por lo que si esas amenazas se materializan puede causar pérdida en la confidencialidad de la información, ya que, si se es víctima de un atacante, la información puede ser interceptada. Actualmente en la empresa existe un mal estado en la red donde están conectados los equipos, ya que no sigue un estándar que brinde seguridad y evite dichos ataques.

Las medidas para mitigar dichos riesgos son:

- Protección criptográfica para la confidencialidad de la información.
- Mantenimientos regulares del estado de la red LAN.

**Mobiliario** Pertenciente a la capa de equipos auxiliares, una vez realizado el análisis de amenazas de las cuales puede ser víctima y haber escogido las correctas salvaguardas, se pudo obtener como resultado que:

La amenaza que representa un alto riesgo es la de la contaminación ambiental, afectando la dimensión de la disponibilidad (4,8), esta amenaza es una de las que están más expuestas a materializarse, dado que el edificio es una construcción antigua.

Las medidas para mitigar dichos riesgos son:

- Reforzar la construcción.
- Cambio de locación.

**Sistema de vigilancia** Pertenciente a la capa de equipos auxiliares, una vez realizado el análisis de amenazas de las cuales puede ser víctima y haber escogido las correctas salvaguardas, se pudo obtener como resultado que:

La amenaza que representa un alto riesgo es la de la contaminación ambiental, afectando la dimensión de la disponibilidad (4,8), esta amenaza es una de las que están más expuestas a materializarse, dado que las cámaras están expuesta al polvo y el sistema de vigilancia está en una habitación que no reúne las condiciones óptimas.

Las medidas para mitigar dichos riesgos son:

- Mantenimiento continuo de equipos.
- Cambio de locación.

**Edificio** Perteneciente a la capa de instalaciones, una vez realizado el análisis de amenazas de las cuales puede ser víctima y haber escogido las correctas salvaguardas, se pudo obtener como resultado que:

Dentro de este activo se encuentran todos los demás activos, afectando la dimensión de la disponibilidad (6,2), ya que el edificio actual cuenta con sistema de seguridad, pero sólo de dos cámaras.

Las medidas para mitigar dichos riesgos son:

- Contratar una persona de seguridad que pueda controlar el ingreso autorizado al edificio.
- Colocar cámaras de seguridad en los interiores, ya que solo están en los exteriores y pasillos.

**Personal** Representa el personal involucrado que maneja y hace uso de los activos, y ese personal que se encuentra en la empresa son:

Presidente epicentro, jefe del departamento de logística, jefe de soporte técnico, mantenimiento de bd, y auxiliar de webcasting. Las principales amenazas de las que pudieran ser víctima el personal son: Ingeniería social, ya que todos usan los computadores de todos y no hay claves ni restricciones, lo que puede ocasionar pérdida y modificación de información; además de extorción por un atacante externo.

Las medidas para mitigar dichos riesgos son:

- Una normativa para que el personal cumpla con las políticas de seguridad.
- Prevención y reacción ante posibles extorsiones.

### 3.2 Plan de seguridad

Esta etapa del proyecto es sobre el plan de seguridad adoptados para materializar las decisiones adoptadas para el tratamiento de los riesgos. Esta etapa contiene tres tareas:

PS.1 Identificación de proyectos de seguridad

PS.2 Plan ejecución

PS.3 Ejecución

#### Identificación de proyectos de seguridad

El objetivo de esta tarea es elaborar un conjunto de programas de seguridad que contiene tres actividades:

Normativas de seguridad

Eliminar fallos de seguridad evidentes

Clasificación del inventario de: SW, HW, Soportes de información y elementos auxiliares.

**Normativas de seguridad:** Está basada en documentación que permitirá ejecutar el plan de seguridad.

1. Documentación del uso autorizado de las aplicaciones:

- Se aplicará sanciones a aquellos empleados que instalen aplicaciones con fines ajenos al trabajo.
- Los empleados están obligados a verificar que los dispositivos de almacenamiento o memorias USB que coloquen en los equipos no contenga virus.

2. Documentación del uso correcto de los equipos informáticos:

- Cada empleado tendrá una computadora o laptop asignada, haciendo responsable por ella.
- Los empleados no pueden cambiar la ubicación de los equipos, ni instalar programas previa autorización.

- No podrá ingerirse alimentos ni bebidas mientras se utilizan los equipos.
  - Mantener el área de los equipos limpios y sin humedad.
  - Sólo personal autorizado puede reparar o abrir los equipos.
3. Documentación del resguardo y protección de la información:
- El uso de memorias USB es exclusivamente para respaldo de información o usos de drivers de instalación por personal autorizado.
  - Los usuarios deberán hacer un respaldo de manera periódica de la información que manejen para evitar pérdidas.
4. Documentación para el uso del servicio de internet:
- El correo electrónico usado debe ser el corporativo y debe ser de uso únicamente laboral.
  - Los mensajes de correo, y los archivos adjuntos en ellos deben tratarse como propiedad de la empresa Radio Atogapan.
  - Queda prohibido usar el correo de otro compañero de labores.
  - El acceso a internet es exclusivamente para uso laboral.
5. Documentación para la protección de las instalaciones:
- Establecer reglas que permitan el cuidado de las instalaciones de la empresa por parte de los empleados.
6. Documentación en la gestión del personal:
- Establecer en los contratos de trabajo cláusulas que guarden la confidencialidad de la información de la empresa.
  - Establecer normas de conducta de trabajo para crear un buen ambiente laboral y de respeto entre los trabajadores de la empresa.

Con las salvaguardas establecidas en el nivel de riesgo actual orientado a las salvaguardas de nivel de riesgo objetivos, los riesgos disminuyen como se observa en la siguiente tabla N°16:

**Tabla N° 16: Resultados de riesgos residuales**

<b>Activos</b>	<b>[D]</b>	<b>[I]</b>	<b>[C]</b>	<b>[A]</b>	<b>[T]</b>
Servicios internos					
Internet	{2,4}			{0,91}	
Aplicaciones					
OBS		{2,2}	{2,3}		
Office		{1,0}	{1,1}		
Antivirus		{1,1}	{1,1}		
Sistema Operativo		{1,0}	{1,1}		
Equipos					
Servidor de base de datos	{2,9}	{2,6}	{2,6}		
Computadoras y laptops	{2,9}	{0,92}	{1,8}		
Cámaras	{2,9}	{0,92}	{2,0}		
Micrófonos	{2,9}	{0,92}	{2,0}		
Comunicaciones					
Internet		{0,82}	{0,99}		
Equipos auxiliares					
Mobiliario	{1,3}				
Sistema de vigilancia	{1,3}				
Soportes de información					
Memorias usb		{2,0}	{1,4}		
Instalaciones					
Oficinas sede epicentros	{2,8}				

**Fuente: Pilar 7.1**



Los riesgos están establecidos en una escala de colores según su valor, como se muestra en la siguiente tabla N°17:

**Tabla N° 17: Colores Valoración riesgos**

{9}	Nivel 9
{8}	Nivel 8
{7}	Extremadamente crítico
{6}	Muy crítico
{5}	Crítico
{4}	Muy alto
{3}	Alto
{2}	Medio
{1}	Bajo
{0}	Despreciable

**Fuente: Pilar 7.1**

### **Eliminar fallos de seguridad evidentes**

- Reubicación del servidor a una instalación segura, cumpliendo con las normas adecuadas para la protección del equipo.
- Establecer cuentas de usuarios con claves a cada empleado.
- Verificar que los antivirus sean actualizados, ya que existen muchos equipos que no cuentan con internet y por ello no se actualiza con la frecuencia debida.

### **Clasificación del inventario de: SW, HW, Soportes de información y elementos auxiliares.**

La empresa no contaba con una clasificación de activos, de manera detallada como la que se ha realizado de sus equipos en este proyecto, para hacer un análisis de sus riesgos y de las salvaguardas a utilizar para prevenirlos.

## Plan ejecución

El objetivo del plan de ejecución es ordenar los programas de seguridad.

Para ello se realizó un orden de ejecución que se determinó de la siguiente manera:

- Eliminar fallos evidentes de seguridad.
- Establecer equipos adecuados para el proceso de webcast.
- Clasificación de inventario.
- Normativas de seguridad.

## Ejecución

Esta es la puesta en marcha de la implementación de la metodología para el correcto análisis de los riesgos y como mitigarlos, logrando disminuir además el desempeño de los procesos involucrados, como lo es en ese caso el webcast.

## Factores de riesgo de las tecnologías de información por dimensiones

**Tabla N° 18: Factores de riesgo en la dimensión de disponibilidad**

DIMENSIÓN: DISPONIBILIDAD [D]
[I.8] Fallo de servicios de comunicaciones
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.3] Contaminación medioambiental
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[E.23] Errores de mantenimiento/actualización de equipos
[A.11] Acceso no autorizado
[I.*] Desastres industriales
[E.23] Caída del sistema por agotamiento del sistema
[A.7] Uso no previsto
[A.25] Robo de equipos
[N.*.1] Tormentas
[N.*.4] Terremotos
[N.*.9] Tsunamis
[N.*.11] Calor extremo
[A.27] Ocupación enemiga

**Fuente: Pilar 7.1**

**Tabla N° 19: Factores de riesgo en la dimensión de integridad**

<b>DIMENSIÓN: INTEGRIDAD DE LOS DATOS [I]</b>
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento o actualización de los programas
[A.8] Difusión de software dañino
[A.22] Manipulación de programas
[A.11] Acceso no autorizado
[E.23] Errores de mantenimiento/actualización de equipos
[A.7] Uso no previsto
[E.15] Alteración de la información
[A.15] Modificación de la información

**Fuente: Pilar 7.1**

**Tabla N° 20: Factores de riesgo en la dimensión de confidencialidad**

<b>DIMENSIÓN: CONFIDENCIALIDAD DE LOS DATOS [C]</b>
[E.8] Difusión de software dañino
[E.20] Vulnerabilidades de los programas
[A.22] Manipulación de programas
[A.11] Acceso no autorizado
[E.25] Pérdida de equipos
[A.23] Manipulación del hardware
[A.25] Robo de equipos
[E.23] Caída del sistema por agotamiento del sistema
[A.14] Interceptación de información
[E.2] Errores del administrador del sistema / de la seguridad
[A.5] Suplantación de la identidad
[A.9] Re-encaminamiento de mensajes
[A.7] Uso no previsto
[A.19] Revelación de información
[A.29] Extorsión
[A.30] Ingeniería social
[E.19] Fugas de información
[A.19] Revelación de información

**Fuente: Pilar 7.1**

**Tabla N° 21: Factores de riesgo en la dimensión de Autenticidad**

<b>DIMENSIÓN: AUTENTICIDAD DE LOS USUARIOS Y DE LA INFORMACIÓN [A]</b>
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento o actualización de los programas
[A.8] Difusión de software dañino
[A.22] Manipulación de programas
[A.11] Acceso no autorizado
[E.23] Errores de mantenimiento/actualización de equipos
[A.7] Uso no previsto
[E.15] Alteración de la información
[A.15] Modificación de la información

**Fuente: Pilar 7.1**

# **PLAN DE CONTINGENCIA**

## **2018**

Autor: Jamie Evelyn Romero Camones  
Consultor: Dr. Adilio Christian Ordoñez Pérez

**Lima, setiembre 2018**

## PLAN DE CONTINGENCIA

Para la empresa Atogapan S.A y el Grupo HCM Comunicaciones SAC es muy importante contar con las TICs como medio indispensable para la realización del proceso de webcast, tanto en el Grupo HCM Comunicaciones S.A.C en su sede Lima, así como Radio Atogapan S.A en sus diferentes sedes en los diferentes estados de México, por ello es de vital importancia cuidar de dichos activos para su correcto funcionamiento.

Es por ello que es importante resaltar que las mencionadas empresas tienen como misión brindar un servicio de calidad, por ello se necesita garantizar el menor tiempo de indisponibilidad de sus activos, tanto en lo que a recursos informáticos refiere como a los humanos.

Por todo aquello mencionado, el tener a los activos inoperativos por un lapso mayor al de 15 minutos puede representar grandes riesgos en el desempeño del proceso del webcast, además de pérdidas económicas y de audiencia.

Es necesario, prever como actuar al momento de que se presente alguna amenaza que ponga en riesgo los activos de la empresa, con el objeto de que el impacto generado en caso de materializarse la amenaza sea lo menor posible.

El plan de contingencia desarrollado para el área de las empresas involucrados en el proceso del webcast, así como de activos involucrados se tendrá en cuenta los activos más importantes como lo son: **Servicios Internos [IS], Equipamiento [E], Instalaciones [L] y la del Personal [P]**; debido a que es de vital importancia proteger estos activos que son la base fundamental para que el proceso de

webcast tenga un desempeño eficaz y eficiente, y que se brinde una buena calidad de servicio.

## DEFINICIONES

### PLAN DE CONTINGENCIA:

Según Aguilera López (2015) el plan de contingencia es: “un instrumento de gestión que contiene medidas (tecnológicas, humanas y de organización) que garanticen la continuidad del negocio protegiendo el sistema de información de los peligros que lo amenazan recuperándolo tras un impacto. El plan de contingencia consta de tres sub-planes independientes:

- **Plan de respaldo:** ante una amenaza se aplican medidas preventivas para evitar que se produzca un daño.
- **Plan de emergencias:** Contempla qué medidas tomar cuando se está materializando una amenaza o cuando acaba de producirse.
- **Plan de recuperación:** Indica las medidas que se aplicaran cuando se ha producido un desastre. El objetivo es evaluar el impacto y regresar lo antes posible a un estado normal del funcionamiento del sistema y de la organización.

### Diseño de estrategia de continuidad del proceso de webcast para las empresas Radio Atogapan S.A y el Grupo HCM Comunicaciones S.A.C

#### A. Estrategias para prevenir fallas.

**Tabla N°22 Cuadro de estrategias para prevenir fallas**

<b>ESTRATEGIA</b>	<b>CAPA A APLICAR</b>
Actualización continua del antivirus y frecuente escaneo de los archivos .	Equipamiento (Aplicaciones)
Activación del firewall y la revisión de los reportes de dicho firewall	Equipamiento (Aplicaciones)
Actualización constante del sw OBS para las transmisiones, así como las licencias del Sistema operativos y los programas a utilizar.	Equipamiento (Aplicaciones)
Mantenimiento constante al UPS y renovación oportuna para evitar daños a los equipos en caso de cortes eléctricos.	Equipamiento (Elementos auxiliares)
Implementar el cableado estructurado siguiendo un estándar.	Equipamiento (Elementos auxiliares)
Mantenimiento y cuidado de los dispositivos como el modem y router.	Equipamiento (Equipos) (Comunicación)
Impedir el acceso de los equipos a terceras personas.	Instalaciones
Adquisición de alarma contra incendios	Instalaciones

Fuente: Elaboración propia



B. Estrategias de recuperación inmediata

Tabla 23: Cuadro de Estrategias para la Recuperación Inmediata.

ESTRATEGIA	CAPA A APLICAR
Manual de restauración de los programas instalados y sus configuraciones	Equipamiento (Aplicaciones)
Manual de limpieza de virus	Equipamiento (Aplicaciones)
Contar con personal externo de confianza en caso de ocurrir alguna necesidad que antender que este fuera del alcance del personal interno.	Personal
Planificar la adquisición de un proveedor alterno de internet .	Servicios Internos
Manual de instalación de los equipos	Equipamiento (Equipos)
Manual del procedimiento de recuperación de información.	Servicios internos Equipamiento (Equipos)
Planificar la adquisición de un local mejor acondicionado.	Instalaciones

Fuente: Elaboración Propia.

## IMPACTO EN LOS ESCENARIOS POR CAPAS:

### 1.Servicios internos

#### Escenario I: Falla del servicio de internet

#### A. Impacto

Tabla N°24 Cuadro de impacto de falla del servicio de internet

IMPACTO	ÁREA AFECTADA
Interrupción del envío de información obtenida en las transmisiones realizadas.	Área de Sistemas

Fuente: Elaboración propia

#### B. Recursos de contingencia

- Servicio de internet alternativo

#### C. Procedimiento

##### C.1.Verificación.

- Verificación de la señal en el Router.
- Hacer pruebas de conexión del servidor al Router.
- Verificación de la configuración de la tarjeta de Red
- Hacer pruebas de descarte del funcionamiento de la tarjeta de red.
- Contactarse con el Proveedor de Internet para consultar la operatividad de su servicio.

**C.2 Corrección.**

- Corregir configuraciones de tarjeta de Red mediante Backup de configuraciones.
- Cambiar tarjeta de red con problema de funcionamiento.
- Reportar incidencia de falla al proveedor del servicio de internet.

Este procedimiento será realizado por el personal a cargo del área de soporte técnico.

**2. Equipamiento**

Equipos

Escenario II: Falla de funcionamiento del servidor

Tabla N°25 Cuadro de impacto de falla del funcionamiento del servidor

IMPACTO	ÁREA AFECTADA
Paralización de los programas o aplicaciones.	Todas las áreas
Pérdida de Hardware o software	Área de Sistemas
Falla en el proceso automático de backup	Área de Sistemas
Interrupción de las operaciones	Área de Sistemas

Fuente: Elaboración propia

**Posibles causas de fallo del servidor:**

**1. Error Físico de Disco de un Servidor.**

Si el disco presenta fallas que no puedan ser reparadas, se debe tomar las siguientes medidas:

Tabla N°26 Cuadro de medidas para un error físico de disco de un servidor.

TIPO DE FALLA	MEDIDAS
<b>Error Físico de Disco de un Servidor</b>	Ubicar el disco malogrado. Avisar a los interesados sobre la falla. Deshabilitar cualquier tipo de acceso lógico al área de informática. Retirar el disco malo y reponerlo con otro del mismo tipo, formatearlo y darle partición. Restaurar el último backup en el disco, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad. Habilitar el funcionamiento de los sistemas para el funcionamiento del negocio.

Fuente: Elaboración propia

## 2. Error de Memoria RAM

Tabla N°27 Cuadro de medidas para un error de memoria RAM

TIPO DE FALLA	MEDIDAS
<b>Error de Memoria RAM</b>	Avisar a los interesados sobre la falla. El servidor debe estar apagado, dando un correcto apagado del sistema. Ubicar las memorias malogradas. Retirar las memorias malogradas y reemplazarlas por otras iguales o similares. Retirar la conexión eléctrica del servidor, ésta se ubica detrás del servidor, ello evitará cualquier posible descarga eléctrica. Encender el Servidor y hacer pruebas de funcionamiento del equipo y de los sistemas.

Fuente: Elaboración propia

## 3. Error Lógico de Datos

La ocurrencia de errores en los sectores del disco duro del servidor puede deberse a una de las siguientes causas:

1. Caída del servidor de archivos por falla de software.
2. Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.

3. Apagar incorrectamente el servidor.
4. Fallas causadas usualmente por un error de chequeo de inconsistencia física.

Tabla N°28 Cuadro de medidas para un error lógico de datos

TIPO DE FALLA	MEDIDAS
<b>Error Lógico de Datos</b>	Verificar el suministro de energía eléctrica. En caso de estar conforme, proceder con el encendido del servidor de archivos, cargar el sistema operativo. Deshabilitar los servicios del servidor. Cargar un utilitario y los datos que nos permita verificar y corregir en forma global el contenido del disco duro del servidor. Al término de la operación de reparación se procederá a revisar que los funcionamientos de los sistemas estén correctos, para ello se debe empezar a correr los sistemas y así poder determinar si se puede hacer uso de ellos inmediatamente

Fuente: Elaboración propia

## B. Recursos de Contingencia

- Material de Reemplazo (Memoria, Disco Duro, etc.).
- Cargar el backup de respaldo tanto de la configuración como de la información del servidor.

## C. Procedimiento:

Este procedimiento será llevado a cabo por el personal a cargo del área de sistemas.

## Escenario III: Falla de los dispositivos de audio y video.

## A. Impacto

Tabla N°29 Cuadro de impacto por fallas de dispositivos de audio y video

IMPACTO	ÁREA AFECTADA
No se puede realizar las transmisiones, por fallas tanto de audio o video	Área de Sistemas

Fuente: Elaboración propia

## B. Recursos de Contingencia

- Cambiar los dispositivos averiados por unos nuevos que deberían tenerse de respaldo.

## C. Procedimiento:

### C.1. Verificación.

- Verificación el estado de los dispositivos.
- Hacer pruebas de descarte de funcionamiento de los dispositivos.
- Verificación de la configuración de los dispositivos.

### C.2. Corrección.

- Corregir configuraciones de tarjeta mediante Backup de configuración.
- Cambiar tarjeta con problema de funcionamiento.
- Reportar incidencia y cambio de tarjeta al interesado

Este procedimiento será ejecutado en su totalidad por el personal a cargo del área de sistemas.

### 3. Instalaciones

#### Edificio

#### Escenario IV: Indisponibilidad del edificio y sus oficinas por daños por agua

#### A. Impacto

Tabla N°30 Cuadro de Impacto de daños de equipos y estructura causadas por agua

IMPACTO	ÁREA AFECTADA
Indisponibilidad de realizar transmisiones	Área de Sistemas
Daño funcional de los equipos de grabación	
Probabilidad de corto circuito del servicio eléctrico	
Deterioro de la infraestructura del área	

Fuente: Elaboración propia

#### B. Recursos de Contingencia

- Habilitar el servicio de transmisiones interrumpidas.

#### C.Procedimiento:

##### C.1. Verificación.

- Verificación del estado de los equipos.
- Verificar y evaluar el posible daño en los equipos.
- En caso de tener equipos afectados hacer pruebas funcionales y descarte de fallas en los equipos.
- En caso de tener equipos afectados realizar el corte de energía alterna para prevenir corto circuito.

## C.2. Corrección.

- Cambiar equipo afectado por uno de respaldo.
- Habilitar funcionalidad del área y de los servicios.
- Reportar incidencia y cambio de equipo al interesado.

Este procedimiento será ejecutado en su totalidad por el personal a cargo del área de sistemas.

## Escenario V: Indisponibilidad del edificio y sus oficinas por daños por fuego

### A. Impacto

Tabla N°31 Cuadro de Impacto de daños de equipos y estructura causadas por fuego

IMPACTO	ÁREA AFECTADA
Indisponibilidad de realizar transmisiones	Área de Sistemas
Daño funcional de los equipos de grabación	
Daño en activos de la empresa	

Fuente: Elaboración propia

### B. Recursos de Contingencia

- Utilizar herramientas contra incendio como extintores.
- En caso de que el incendio no pueda ser controlado, llamar a la unidad de Bomberos en el menor tiempo posible.
- Habilitar la actividad interrumpida.

### C.Procedimiento:

#### C.1. Verificación.

- Verificación del estado de los equipos informáticos.



- Verificación y evaluación del posible daño.
- Evaluar el estado de los equipos e infraestructura para la continuidad de los servicios.

**C.2. Corrección.**

- Evaluar la adquisición de un local alternativo en caso de que la infraestructura presente daños irreparables.
- En caso de tener equipos reemplazar por equipos informáticos de respaldo.
- Evaluar la posible adquisición de nuevos equipos informáticos.
- Habilitar funcionalidad del área y de los servicios.
- Reportar incidencia y cambio de equipo al interesado.

Este procedimiento será ejecutado en su totalidad por el personal a cargo del área de sistemas.

**Escenario VI: Indisponibilidad del edificio y sus oficinas de transmisión**

**A. Impacto**

Tabla N°32 Cuadro de Impacto de daños de equipos y estructura en el edificio y sus oficinas de transmisión

IMPACTO	ÁREA AFECTADA
Caída de la red LAN: Servidores y equipos de comunicación	Todas las áreas
Interrupción de las comunicaciones internas y externas	Todas las áreas
Paralización de las operaciones informáticas	Todas las áreas
Pérdida de Hardware y software	Área de Sistemas

Fuente: Elaboración propia

**B. Recursos de Contingencia**

- Planificar la necesidad de un local alternativo mejor acondicionado.

**Alternativa de centro de operaciones (Edificio alternativo)**

Tabla N°33 Cuadro de alternativas de edificio y oficinas de transmisión

ALTERNATIVA	VENTAJAS	DESVENTAJAS
<b>A. Centro de operaciones (Edificio alternativo) propio</b>		
La empresa construirá su propio edificio y centro de operaciones	<ol style="list-style-type: none"> <li>1. Constituye activo fijo de la Empresa.</li> <li>2. Manejo de los procesos de transmisión y de sus podcasts solo por personal de la de la empresa.</li> </ol>	<ol style="list-style-type: none"> <li>1. Alta Inversión</li> <li>2. Tiempo en la construcción.</li> <li>3. Inversión adicional en seguridad.</li> <li>4. Recurso Humano adicional para el manejo de las operaciones.</li> </ol>
<b>B. Centro de operaciones (Edificio alternativo) outsourcing</b>		
La empresa construirá su propio centro de operaciones realizado por un especialista externo	<ol style="list-style-type: none"> <li>1. Menor inversión, ya que es compartido</li> <li>2. Tiempo de implementación menor</li> <li>3. La seguridad es parte del servicio</li> <li>4. No requiere RRHH adicional</li> </ol>	<ol style="list-style-type: none"> <li>1. Implementar procedimientos de seguridad interna extra por estar localizada en una entidad externa la BD.</li> </ol>

Fuente: Elaboración propia

**C.Procedimiento:**

- Restauración del edificio y el centro de operaciones

Este procedimiento será ejecutado en su totalidad por el personal a cargo del área de sistemas.

**Escenario VII: Interrupción de fluido eléctrico**

Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas Atogapan s.a. y Grupo HCM comunicaciones sac.

Romero Camones, Jamie Evelyn

Tabla N°34 Cuadro de Impacto de interrupción del Fluido Eléctrico.

IMPACTO	ÁREA AFECTADA
Pérdida total o parcial de la operatividad de los procesos de transmisión.	Área de Sistemas
Finalización incompleta de la creación de podcasts.	
Falla de los equipos	

Fuente: Elaboración propia

**B. Recursos de Contingencia**

Si se produjera en horas de la noche una interrupción del fluido eléctrico, se podrían paralizar los procesos de cierre y backup de los servidores. Por tal motivo es necesario revisar continuamente el estado de las baterías del UPS.

**C. Procedimiento:**

- Verificar el correcto mantenimiento del UPS y su estado.

Este procedimiento será ejecutado en su totalidad por el personal a cargo del área de sistemas.

**4. Personal**

**Edificio**

**Escenario VIII: Ausencia parcial o total del personal encargado de realizar el webcast**

**A. Impacto**

Tabla N°35 Cuadro de Impacto de ausencia de personal

IMPACTO	ÁREA AFECTADA
Interrupción de las funciones del personal que se ausenta	Todas las áreas
Posible interrupción de algunos de lo procesos .	

Fuente: Elaboración propia

## **B. Recursos de Contingencia**

Se presentan las funciones actuales que tienen a su cargo el personal del Área de sistemas y se asigna a otro personal capacitado para desarrollar dicha función.

## **C. Procedimiento:**

Este procedimiento será ejecutado en su totalidad por el personal a cargo del área de sistemas.

# **PLAN DE CAPACITACIÓN 2018 METODOLOGÍA MAGERIT V.3**

**Autor: Jamie Evelyn Romero Camones  
Consultor: Dr. Adilio Christian Ordoñez Pérez**

**Lima, agosto 2018**

## PRESENTACIÓN

Radio Atogapan promueve la capacitación de sus colaboradores en forma permanente, mediante la aplicación de un Plan de Capacitación anual, que se sustenta en 4 pilares básicos:

1. **Inducción:** Orientada a facilitar la integración del nuevo colaborador a la empresa RADIO ATOGAPAN Y HCM Comunicaciones.
2. **Capacitación preventiva:** Con la finalidad de mantener actualizado al colaborador.
3. **Capacitación correctiva:** Identificada en las evaluaciones de desempeño.
4. **Capacitación para el desarrollo:** Adquisición de nuevos conocimientos y habilidades. Esta capacitación está orientada a preparar al colaborador a ocupar puestos de mayor jerarquía en la organización.

En RADIO ATOGAPAN y el Grupo HCM Comunicaciones se entiende a la capacitación como la adquisición de conocimientos y desarrollo de habilidades/actitudes, con la finalidad de mejorar las competencias y lograr un mejor desempeño en los diversos niveles jerárquicos, adaptando al personal a las exigencias cambiantes del entorno y del momento.

La ejecución del Plan de Capacitación garantiza que los colaboradores adquirirán conocimientos y habilidades específicas relativas al trabajo que realizan, lo que permitirá modificar actitudes frente a diversos aspectos de la organización, el puesto de trabajo o el ambiente laboral. Uno de los objetivos de la capacitación es lograr que el perfil del colaborador se adecúe al perfil de conocimientos, habilidades y actitudes requerido para el puesto de trabajo.

## I. ACTIVIDAD DE LA EMPRESA

Radio Atogapan es una empresa dedicada al rubro de radio y transmisión en vivo de programas de radio orientados a la protección civil, siendo la primera radio dedicada a la difusión de programas de protección civil en México.

## II. MISIÓN Y VISIÓN

### MISIÓN

Promover y difundir la importancia de conocer la prevención de riesgos y la protección civil a los ciudadanos de México.

### VISIÓN

Ser reconocidos como la más importante radio difusora de protección civil a nivel no sólo nacional, sino internacional.

## II. JUSTIFICACIÓN

Lo más importante en la empresa RADIO ATOGAPAN y el Grupo HCM Comunicaciones es tener colaboradores que respondan a las exigencias de la función que realizan, por ello, propicia el crecimiento profesional de los mismos a fin de estimular la efectividad en el cargo que desempeñan. El mejor desempeño influirá directamente en los procesos que se realizan dentro de la empresa.

El Plan de Capacitación 2018 está estructurado de modo que, tomando como referencia las evaluaciones del desempeño del webcast realizadas, se identifiquen las necesidades de la implementación de una metodología que pueda hacer un análisis y tratamiento de las tecnologías de información; esto con la finalidad de mejorar el desempeño del proceso del webcast.

La capacitación está orientada a generar un cambio en cuantos a los niveles de eficacia, eficiencia y calidad de servicio siendo estas dimensiones del desempeño.

### **III. ALCANCE**

El presente plan de capacitación es de aplicación para el personal involucrado en el proceso de webcast.

### **IV. VIGENCIA**

El presente plan de capacitación entra en vigencia a partir de su aprobación. El plan no es limitativo y por ser una herramienta dinámica estará sujeta a variaciones de ser necesarias.

### **IV. FINES DEL PLAN DE CAPACITACIÓN**

Siendo su propósito general promover e instalar en el personal conocimientos que contribuyan a la mejora del desempeño del webcast y de gestión de riesgos de Ti, la capacitación se lleva a cabo para contribuir a:

1. Desarrollar los conocimientos, habilidades y destrezas de sus colaboradores para mejorar el desempeño del webcast.
2. Proyectar al colaborador a puestos de mayor nivel, complejidad y responsabilidad.
3. Brindar reconocimiento a los colaboradores identificados con los valores de la organización, competencias y con un alto rendimiento en sus labores.

### **V. OBJETIVOS DEL PLAN DE CAPACITACION**

#### **. Objetivos del Plan Estratégico**

1. Optimizar la aplicación de recursos y procesos.
2. Reforzar los valores, la comunicación y el desarrollo del personal.



## Objetivos Específicos

1. Prevención de la obsolescencia: Mejorar y atender los cambios tecnológicos y la adaptación de los empleados a estas nuevas oportunidades.
2. Mejorar la eficiencia, eficacia y calidad del servicio, en el proceso del webcast.
3. Desarrollo personal: Impartir a los participantes nuevos conocimientos y habilidades, desarrollo de competencias y destrezas personales y responsabilidad social que constituyen pilares de la empresa Atogapan.

## VI. METAS

1. Capacitar a todos los empleados de la empresa Radio Atogapan con especial preponderancia del personal operativo involucrado directamente en el proceso del webcast.
2. Obtener, en promedio, 36 horas de capacitación por colaborador.

## VII. ESTRATEGIA

La capacitación se abordará desde dos niveles:

- a. Para mejorar el desempeño actual del colaborador en su puesto, lo que implica un refuerzo y actualización de los conocimientos y desarrollo de competencias del colaborador con especial interés en las áreas operativas.
- b. Énfasis en la implementación de la metodología MAGERIT V.3, así como del uso de la herramienta PILAR 7.1.

## VIII. ACTIVIDADES DE CAPACITACIÓN A DESARROLLAR

En base a cuestionarios realizados por los trabajadores de la empresa Radio Atogapan, los cuales arrojaron cifras de nivel bajos en el desempeño del webcast, el Plan de Capacitación para el año 2018 considerará las siguientes actividades:

ACTIVIDAD	EXPOSITOR-CAPACITADOR
1. Capacitación del contenido de la metodología MAGERIT V.3	Las actividades de capacitación interna estarán a cargo de Jamie Evelyn Romero Camones.
2. Capacitación en seguridad	Ingeniero en computación Erick Álvarez Porcayo.
3. Capacitación del uso de la herramienta PILAR 7.1	Dirigida por Jamie Evelyn Romero Camones, encargada del área de desarrollo web en la empresa.

## IX. FINANCIAMIENTO

El monto de inversión del presente plan de capacitación e implementación de la metodología MAGERIT V.3, será financiada con los recursos propios de la empresa.

## X. PRESUPUESTO

El presupuesto considerado para el Plan de Capacitación e implementación asciende a S/ 14,914 o (\$ 74,570 pesos mexicanos).

**XII. LUGAR Y FECHA****ATOGAPAN S.A**

<b>LUGAR:</b>	Blvd Kino # 1000, Colonia Pitic; C.P 83150, Hermosillo, Sonora, México
<b>FECHA:</b>	Del 02 al 04 de Agosto del 2018
<b>N° DÍAS:</b>	3

**GRUPO HCM COMUNICACIONES SAC**

<b>LUGAR:</b>	Jr. Cornelio Borda Nro. 144 Lima-Perú
<b>FECHA:</b>	Del 13 al 15 de Agosto del 2018
<b>N° DÍAS:</b>	3

**XII. ANEXOS**

ANEXO N° 01: Plan de actividades y temas de capacitación.

**ANEXO Nº 01: Plan de actividades y temas de capacitación**

**PROGRAMA DE CAPACITACIÓN**  
Hermosillo, Sonora, México / 2018

# Radio Atogapan

con un enfoque en la Gestión Integral de Riesgos



## PROGRAMA

### JUEVES 02 DE AGOSTO:

<b>MAGERIT V.3</b>	
Qué es Magerit?	08:00-08:30
<b>ANÁLISIS DE RIESGOS</b>	
Identificación de activos	08:30-09:00
Dependencia entre los activos	09:00-09:30
Valoración de los activos	10:00-11:00
Identificación de las amenazas	11:00-11:30
Valoración de las amenazas	11:30-12:30
Identificación de las salvaguardas	12:30-13:00
<b>ALMUERZO</b>	
Valoración de las salvaguardas	14:00-15:00
Estimación del impacto	15:00-16:00
Impacto potencial	16:00-16:30
Impacto residual acumulado	16:30-17:00
Estimación del riesgo	17:00-18:00
<b>BREAK</b>	
Riesgo potencial	18:30-19:00
Riesgo residual	19:00-20:00
Riesgo residual acumulado	20:00-21:00

### VIERNES 03 DE AGOSTO:

<b>GESTIÓN DE RIESGOS</b>	
Identificación de riesgos críticos	08:00-11:30
Calificación del riesgo	11:30-13:00
<b>ALMUERZO</b>	
<b>PLAN DE SEGURIDAD</b>	
Identificación de proyectos de seguridad	14:00-16:00
Normativas de seguridad	16:00-18:00
<b>BREAK</b>	
Eliminar fallos de seguridad evidentes	19:00-20:30

### SÁBADO 04 DE AGOSTO:

<b>PILAR 7.1</b>	
Instalación del software	08:00-11:30
Componentes de PILAR 7.1	11:30-13:00
<b>ALMUERZO</b>	
<b>USO DE LA HERRAMIENTA PILAR 7.1</b>	
Identificación de componentes del software	14:00-16:00
Ingreso de datos	16:00-18:00
<b>BREAK</b>	
Manejo del software	19:00-20:30

**PROGRAMA DE CAPACITACIÓN**  
2018

**GRUPO HCM  
COMUNICACIONES**



**PROGRAMA**

**LUNES 13 DE AGOSTO:**

<b>MAGERIT V.3</b>	
Qué es Magerit?	08:00-08:30
<b>ANÁLISIS DE RIESGOS</b>	
Identificación de activos	08:30-09:00
Dependencia entre los activos	09:00-09:30
Valoración de los activos	10:00-11:00
Identificación de las amenazas	11:00-11:30
Valoración de las amenazas	11:30-12:30
Identificación de las salvaguardas	12:30-13:00
<b>ALMUERZO</b>	
Valoración de las salvaguardas	14:00-15:00
Estimación del impacto	15:00-16:00
Impacto potencial	16:00-16:30
Impacto residual acumulado	16:30-17:00
Estimación del riesgo	17:00-18:00
<b>BREAK</b>	
Riesgo potencial	18:30-19:00
Riesgo residual	19:00-20:00
Riesgo residual acumulado	20:00-21:00

**MARTES 14 DE AGOSTO:**

<b>GESTIÓN DE RIESGOS</b>	
Identificación de riesgos críticos	08:00-11:30
Calificación del riesgo	11:30-13:00
<b>ALMUERZO</b>	
<b>PLAN DE SEGURIDAD</b>	
Identificación de proyectos de seguridad	14:00-16:00
Normativas de seguridad	16:00-18:00
<b>BREAK</b>	
Eliminar fallos de seguridad evidentes	19:00-20:30

**MIÉRCOLES 15 DE AGOSTO:**

<b>PILAR 7.1</b>	
Instalación del software	08:00-11:30
Componentes de PILAR 7.1	11:30-13:00
<b>ALMUERZO</b>	
<b>USO DE LA HERRAMIENTA PILAR 7.1</b>	
Identificación de componentes del software	14:00-16:00
Ingreso de datos	16:00-18:00
<b>BREAK</b>	
Manejo del software	19:00-20:30

# **INFORME DEL PLAN DE CAPACITACIÓN 2018 METODOLOGÍA MAGERIT V.3**

Autor: Jamie Evelyn Romero Camones

Consultor: Dr. Adilio Christian Ordoñez Pérez

**Lima, agosto 2018**

## **i. INTRODUCCIÓN**

A continuación, se presenta el informe de la capacitación de MAGERIT .3 y el uso de la herramienta PILAR 7.1, perteneciente al desarrollo de tesis titulado “Factores de riesgo de las tecnologías de información y el desempeño del webcast en las empresas Radio Atogapan S.A y HCM Comunicaciones S.A.C. realizada por Jamie Evelyn Romero Camones bajo la asesoría y consultoría del Dr. Adilio Christian Ordoñez Pérez, realizado del 02 al 04 de agosto del 2018 en la empresa Atogapan y del 13 al 15 de Agosto en el Grupo HCM Comunicaciones.

La capacitación de la metodología Magerit V.3 y la herramienta pilar se enmarca en el análisis y gestión de riesgos de los activos de la empresa orientados a las tecnologías de información, el cual permitirá establecer la relación que existe entre ello y el desempeño de uno de sus procesos más importantes como lo es el webcast.

El presente informe, da en cuenta los objetivos de la capacitación, el programa de temas y horario de capacitación.

## **II. OBJETIVOS DE LA CAPACITACIÓN**

### **Objetivos del Plan Estratégico**

3. Optimizar la aplicación de recursos y procesos.
4. Reforzar los valores, la comunicación y el desarrollo del personal.

### **Objetivos Específicos**

4. Prevención de la obsolescencia: Mejorar y atender los cambios tecnológicos y la adaptación de los empleados a estas nuevas oportunidades.

5. Mejorar la eficiencia, eficacia y calidad del servicio, en el proceso del webcast.
6. Desarrollo personal: Impartir a los participantes nuevos conocimientos y habilidades, desarrollo de competencias y destrezas personales y responsabilidad social que constituyen pilares de la empresa Atogapan.

### **III. METODOLOGÍA DE TRABAJO**

La capacitación se desarrolló con énfasis en los requerimientos técnicos establecidos y el análisis de los activos con los que cuenta la empresa, haciendo una valoración de los mismos, así como de las amenazas, los riesgos y el impacto generado, para posteriormente establecer salvaguardas.

#### **A. PARTICIPANTES:**

El presente plan de capacitación es de aplicación para el personal involucrado en el proceso de webcast, estuvo dirigido a 28 trabajadores de los diferentes epicentros de la radio: Ciudad de México, Nuevo León, Estado de México, Sonora, Colombia, Quintana Roo, Veracruz y Puebla y del Grupo HCM Comunicaciones en Lima.

#### **B. FECHA Y LUGAR DE REALIZACIÓN DEL CURSO**

En Atogapan S.A la capacitación se llevó a cabo los días 02,03 y 04 de agosto del 2018. El horario del día jueves 02, fue desde las 08:00 a las 21:00hrs, el día viernes 03, de 08:00 a las 20:30hrs, y el día sábado 04, de 08:00 a las 20:00hrs.

En el Grupo HCM Comunicaciones la capacitación se llevó a cabo los días 13,14 y 15 de agosto del 2018. El horario del día lunes 13, fue desde las 08:00 a las 21:00hrs, el día martes 14, de 08:00 a las 20:30hrs, y el día miércoles 15, de 08:00 a las 20:00hrs.

#### **C. METODOLOGÍA TEÓRICO-PRÁCTICA:**

El curso tuvo una duración de 36 horas presenciales en donde se utilizó metodologías de trabajo participativas, expositivas, interactivas y dirigidas a la práctica. El Enfoque de la capacitación fue experiencial en donde se promovieron actividades lúdicas grupales e individuales.



## D. PROVISIÓN DE SUMINISTROS:

Para la capacitación, a cada participante se le entregó al inicio del curso el material de trabajo, el cual estaba compuesto de:

- ♣ Carpeta de la capacitación.
- ♣ Lápiz.
- ♣ Cuadernillo de apuntes.
- ♣ Memoria USB con el software PILAR 7.1 (Instalador)

## E. PROGRAMA Y CONTENIDO DEL CURSO DE CAPACITACIÓN

El desarrollo de los temas y el cronograma se estableció de la siguiente manera:

DÍA 1: 02 DE AGOSTO			
Item N°	Tema:	Expositor	Horario
	<b>MAGERIT V.3</b>		
1	Qué es Magerit?	Bach. Ing de sistemas Jamie Evelyn Romero Camones	08:00-08:30
	<b>ANÁLISIS DE RIESGOS</b>	Bach. Ing de sistemas Jamie Evelyn Romero Camones	
2	Identificación de activos	Bach. Ing de sistemas Jamie Evelyn Romero Camones	08:30-09:00
3	Dependencia entre los activos	Bach. Ing de sistemas Jamie Evelyn Romero Camones	09:00-09:30
4	Valoración de los activos	Bach. Ing de sistemas Jamie Evelyn Romero Camones	10:00-11:00
5	Identificación de las amenazas	Bach. Ing de sistemas Jamie Evelyn Romero Camones	11:00-11:30
6	Valoración de las amenazas	Bach. Ing de sistemas Jamie Evelyn Romero Camones	11:30-12:30
7	Identificación de las salvaguardas	Bach. Ing de sistemas Jamie Evelyn Romero Camones	12:30-13:00
	<b>ALMUERZO</b>		
8	Valoración de las salvaguardas	Bach. Ing de sistemas Jamie Evelyn Romero Camones	14:00-15:00
9	Estimación del impacto	Bach. Ing de sistemas Jamie Evelyn Romero Camones	15:00-16:00
10	Impacto potencial	Bach. Ing de sistemas Jamie Evelyn Romero Camones	16:00-16:30
11	Impacto residual acumulado	Bach. Ing de sistemas Jamie Evelyn Romero Camones	16:30-17:00
12	Estimación del riesgo	Bach. Ing de sistemas Jamie Evelyn Romero Camones	17:00-18:00
	<b>BREAK</b>		
13	Riesgo potencial	Bach. Ing de sistemas Jamie Evelyn Romero Camones	18:30-19:00
14	Riesgo residual	Bach. Ing de sistemas Jamie Evelyn Romero Camones	19:00-20:00
15	Riesgo residual acumulado	Bach. Ing de sistemas Jamie Evelyn Romero Camones	20:00-21:00

<b>DÍA 2: 03 DE AGOSTO</b>			
	<b>GESTIÓN DE RIESGOS</b>		
16	Identificación de riesgos críticos	Bach. Ing de sistemas Jamie Evelyn Romero Camones	08:00-11:30
17	Calificación del riesgo	Bach. Ing de sistemas Jamie Evelyn Romero Camones	11:30-13:00
	<b>ALMUERZO</b>		
	<b>PLAN DE SEGURIDAD</b>	Ing. en computación Erick Álvarez Porcayo	
18	Identificación de proyectos de seguridad	Ing. en computación Erick Álvarez Porcayo	14:00-16:00
19	Normativas de seguridad	Ing. en computación Erick Álvarez Porcayo	16:00-18:00
	<b>BREAK</b>		
20	Eliminar fallos de seguridad evidentes	Ing. en computación Erick Álvarez Porcayo	19:00-20:30
<b>DÍA 3: 04 DE AGOSTO</b>			
	<b>PILAR 7.1</b>		
21	Instalación del software	Bach. Ing de sistemas Jamie Evelyn Romero Camones	08:00-11:30
22	Componentes de PILAR 7.1	Bach. Ing de sistemas Jamie Evelyn Romero Camones	11:30-13:00
	<b>ALMUERZO</b>		
	<b>USO DE LA HERRAMIENTA PILAR 7.1</b>		
23	Identificación de componentes del software	Bach. Ing de sistemas Jamie Evelyn Romero Camones	14:00-16:00
24	Ingreso de datos	Bach. Ing de sistemas Jamie Evelyn Romero Camones	16:00-18:00
	<b>BREAK</b>		
25	Manejo del software	Bach. Ing de sistemas Jamie Evelyn Romero Camones	19:00-20:30

#### IV. ANEXOS

Anexo N°1 Fotos de la capacitación

Anexo N°2 Lista de participantes

### Anexo N°1 Fotos de la capacitación



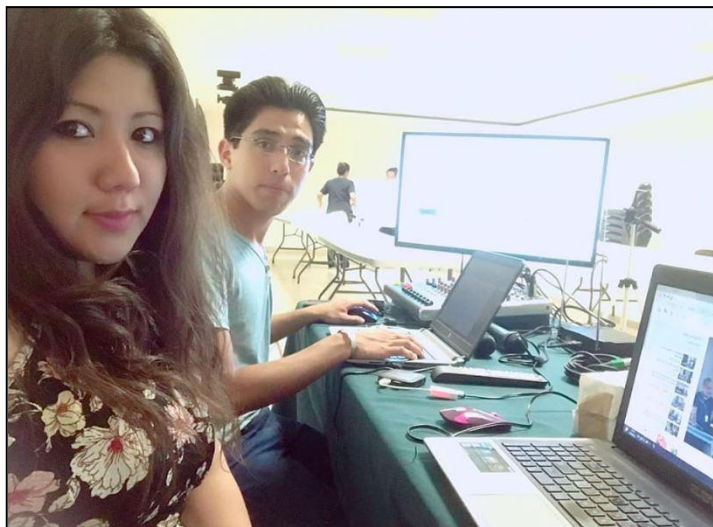
Material entregado en la capacitación a cada uno de los integrantes de los diferentes epicentros, el material constó de un folder con el programa de capacitación, unas hojas para anotaciones, un lápiz y una memoria USB con el software de instalación de la herramienta PILAR 7.1



Personal de epicentro en la capacitación brindada sobre MAGERIT V.3



El personal de Radio Atogapan reunido a punto de iniciarse la capacitación, el personal reunido fue de los diferentes estados de México en donde se encuentran los epicentros.



Expositores: Bach. Ing. de Sistemas Jamie Evelyn Romero Camones y el Ing. en Computación Erick Alvarez Porcayo probando equipos y preparando la capacitación a dictar sobre MAGERIT V.3.




Clausura de la capacitación: Foto de la expositora Bach. Ing. de Sistemas Jamie Evelyn Romero Camones y los presidentes de los diferentes epicentros de México y el Director General de Radio Atogapan Héctor Paz Díaz.



Representante de HCM Comunicaciones probando la herramienta PILAR 7.1

**Anexo N°2 Lista de participantes**

N°	Nombre	Cargo	Sede Epicentro
1	Victor Estrada	Presidente Epicentro	Nuevo León
2	Javier Rodriguez	Logista	Nuevo León
3	Gerardo Ávila	Soporte-Auxiliar webcast	Nuevo León
4	Alejandro Romero	Presidente Epicentro	Estado de México
5	Rodrigo Romero	Logista	Estado de México
6	Edgar Fett	Soporte-Auxiliar webcast	Estado de México
7	Mariano Katase	Presidente Epicentro	Sonora
8	Juan Serrano	Logista	Sonora
9	Ramses Contreras	Entrevistador	Sonora
10	Guillermo Moreno	Soporte-Auxiliar webcast	Sonora
11	Henry Peralta	Presidente Epicentro	Colombia
12	Diana Lave	Soporte-Auxiliar webcast	Colombia
13	David Albores	Presidente Epicentro	Quintana Roo
14	Julio Herrera	Logista	Quintana Roo
15	Gabriela Aguilar	Soporte-Auxiliar webcast	Quintana Roo
16	Alberto Cerón	Presidente Epicentro	Veracruz
17	Wendy Flandes	Soporte-Auxiliar webcast	Veracruz
18	Ulises Cruz	Presidente Epicentro	Puebla
19	Goretti Ixtlapale	Logista	Puebla
20	Ciro Fuentes	Soporte-Auxiliar webcast	Puebla
21	Hector Paz	Presidente Epicentro/Director general	Ciudad de México
22	Rafael Pérez	Entrevistador-Logista	Ciudad de México
23	Erick Alvarez	Soporte-Auxiliar webcast	Ciudad de México
24	Lucy Fuentes	Administradora	Ciudad de México
25	Nick becerra	Productor	Lima
26	Rául Zambrano	Controles	Lima
27	Carlos Sifuentes	Publicidad y diseño	Lima
28	Mario Rojas	Asistente de producción	Lima

 <b>UCV</b> UNIVERSIDAD CÉSAR VALLEJO	<b>ACTA DE APROBACIÓN DE ORIGINALIDAD DE TESIS</b>	Código : F06-PP-PR-02.02
		Versión : 09
		Fecha : 23-03-2018
		Página : 1 de 1

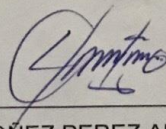
Yo, Dr. ORDOÑEZ PEREZ ADILIO CHRISTIAN, docente de la Facultad de Ingeniería y Escuela Profesional de Ingeniería de Sistemas de la Universidad César Vallejo Lima Norte, revisor de la tesis titulada:

**FACTORES DE RIESGO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y EL DESEMPEÑO DE WEBCAST EN LAS EMPRESAS ATOGAPAN S.A. Y GRUPO HCM COMUNICACIONES SAC**

del estudiante ROMERO CAMONES JAMIE EVELYN, constato que la investigación tiene un índice de similitud del <sup>26%</sup> 26% verificable en el reporte de originalidad del programa Turnitin.

El suscrito analizó dicho reporte y concluyó que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad Cesar Vallejo.

Los Olivos, 02 de diciembre del 2018.



Dr. ORDOÑEZ PEREZ ADILIO CHRISTIAN

Docente Asesor de Tesis

DNI: 20108357

The screenshot displays the Feedback Studio interface. The main document area shows the following text:

**UNIVERSIDAD CÉSAR VALLEJO**

FACULTAD DE INGENIERIA

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

FACTORES DE RIESGO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y EL DESEMPEÑO DE WEBCAST EN LAS EMPRESAS ATOGAPAN S.A. Y GRUPO HCM COMUNICACIONES SAC

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTOR:  
Romero Camones, Jamie Evelyn

ASESOR:  
Dr. Adilio Christian Ordoñez Pérez

The sidebar on the right contains a 'Resumen de coincidencias' (Summary of coincidences) panel with the following data:

- Resumen de coincidencias: 26 %
- Se están viendo fuentes estándar
- Ver fuentes en inglés (Beta)
- Coincidencias:
 

1	repositorio.ucv.edu.pe	7 %
2	Entregado a Universida...	4 %
3	dspace.ups.edu.ec	2 %
4	metodologia-magerit.bl...	2 %
5	www.seap.minhap.es	2 %
6	cybertesis.unmsm.edu...	1 %





**UNIVERSIDAD CÉSAR VALLEJO**

**Centro de Recursos para el Aprendizaje y la Investigación (CRAI)  
"César Acuña Peralta"**

**FORMULARIO DE AUTORIZACIÓN PARA LA  
PUBLICACIÓN ELECTRÓNICA DE LAS TESIS**

**1. DATOS PERSONALES**

Apellidos y Nombres: (solo los datos del que autoriza)

Romero Camones Jamie Evelyn

D.N.I. : 43710298

Domicilio : Cl. Los nogales M-15 Shangri-lá, Puente piedra

Teléfono : Fijo : 5511636 Móvil : 931693860

E-mail : jevromeroc@gmail.com

**2. IDENTIFICACIÓN DE LA TESIS**

Modalidad:

Tesis de Pregrado

Facultad : Ingeniería

Escuela : Ingeniería de Sistemas

Carrera : Ingeniería de Sistemas

Título : Ingeniero de Sistemas

Tesis de Post Grado

Maestría

Grado :

Mención :

Doctorado

**3. DATOS DE LA TESIS**

Autor (es) Apellidos y Nombres:

Romero Camones Jamie Evelyn

Título de la tesis:

Factores de riesgo de las tecnologías de información y el desempeño de webcast en las empresas Atogapan S.A. Y Grupo HCM Comunicaciones SAC.

Año de publicación : 2019

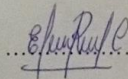
**4. AUTORIZACIÓN DE PUBLICACIÓN DE LA TESIS EN VERSIÓN ELECTRÓNICA:**

A través del presente documento,

Si autorizo a publicar en texto completo mi tesis.

No autorizo a publicar en texto completo mi tesis.



Firma :  .....

Fecha : 10/06/2019



# UNIVERSIDAD CÉSAR VALLEJO

## AUTORIZACIÓN DE LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN

CONSTE POR EL PRESENTE EL VISTO BUENO QUE OTORGA EL ENCARGADO DE INVESTIGACIÓN DE  
LA ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE  
SISTEMAS

A LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN QUE PRESENTA:

ROMERO CAMONES, JAMIE EVELYN

INFORME TITULADO:

FACTORES DE RIESGO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y EL  
DESEMPEÑO DE WEBCAST EN LAS EMPRESAS ATOGAPAN S.A. Y  
GRUPO HCM COMUNICACIONES SAC

PARA OBTENER EL TÍTULO O GRADO DE:

---

INGENIERO DE SISTEMAS

SUSTENTADO EN FECHA: 06/12/2018

NOTA O MENCIÓN: 15



FIRMA DEL ENCARGADO DE INVESTIGACIÓN