UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

AUDITORÍA DE LA SEGURIDAD INFORMÁTICA A LA EMPRESA MARKGLOB DE LA CIUDAD DE MACHALA.

CAMINOS CUENCA SANDRA YULIANA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

AUDITORÍA DE LA SEGURIDAD INFORMÁTICA A LA EMPRESA MARKGLOB DE LA CIUDAD DE MACHALA.

CAMINOS CUENCA SANDRA YULIANA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

AUDITORÍA DE LA SEGURIDAD INFORMÁTICA A LA EMPRESA MARKGLOB DE LA CIUDAD DE MACHALA.

CAMINOS CUENCA SANDRA YULIANA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

GONZALEZ SANCHEZ JORGE LUIS

MACHALA, 26 DE AGOSTO DE 2019

MACHALA
26 de agosto de 2019

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado AUDITORÍA DE LA SEGURIDAD INFORMÁTICA A LA EMPRESA MARKGLOB DE LA CIUDAD DE MACHALA., hacemos constar que luego de haber revisado el manuscrito del precitado trabajo, consideramos que reúne las condiciones académicas para continuar con la fase de evaluación correspondiente.

GONZALEZ SANCHEZ JORGE LUIS
0703333898
TUTOR - ESPECIALISTA 1

CHIMARRO CHIPANTIZA VICTOR LEWIS
0703703413
ESPECIALISTA 2

ILLESCAS ESPINOZA WILMER HENRY
0704128776
ESPECIALISTA 3

Fecha de impresión: lunes 26 de agosto de 2019 - 11:37

URKUND

Urkund Analysis Result

Analysed Document: SANDRACAMINOS CUENCA.docx (D54780511)
Submitted: 8/12/2019 7:41:00 AM
Submitted By: jgonzalez@utmachala.edu.ec
Significance: 0 %

Sources included in the report:

Instances where selected sources appear:

0

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

La que suscribe, CAMINOS CUENCA SANDRA YULIANA, en calidad de autora del siguiente trabajo escrito titulado AUDITORÍA DE LA SEGURIDAD INFORMÁTICA A LA EMPRESA MARKGLOB DE LA CIUDAD DE MACHALA., otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

La autora declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

La autora como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 26 de agosto de 2019

CAMINOS CUENCA SANDRA YULIANA
0705389518

RESUMEN

En la sociedad del conocimiento el manejo de la información y gestión de datos es vital en toda empresa o institución, con el objeto de automatizar procesos secuenciales, mejorar las prestaciones en sistemas e integrar herramientas de software en la ejecución de tareas, contribuyendo a lograr la competitividad en un mercado cada vez más exigente y volátil. La auditoría informática es una ciencia interdisciplinaria que conjuga a todos los departamentos involucrados en una organización, evaluando la seguridad, procesos computacionales y calidad de la información para garantizar un correcto desempeño minimizando los riesgos a un costo rentable. La empresa MarkGlob es una entidad dedicada a realizar estudios de mercado y estrategias publicitarias en la ciudad de Machala, emplea múltiples recursos digitales e información en sus labores; por ello en este estudio se pretende identificar las medidas/controles que realiza al mantener la seguridad en sus instalaciones, explicar la manera en que armoniza los riesgos/potencialidades informáticas.

Palabras Clave: Auditoria informática, seguridad, controles, empresa, publicidad.

ASTRACT

In the knowledge society the management of information and data management is vital in any company or institution, with the aim of automating sequential processes, improving the performance of systems and integrating software tools in the execution of tasks, contributing to achieve competitiveness in an increasingly demanding and volatile market. The computer audit is an interdisciplinary and intrinsic science that brings together all the departments and involved in an organization, evaluating security, computational processes and quality of information to guarantee a correct performance minimizing the risks at a profitable cost. The company MarkGlob is an entity dedicated to carrying out market studies and advertising strategies in the city of Machala, using multiple digital resources and information in its work; For this reason, the aim of this study is to identify the measures / controls carried out by maintaining the security of its facilities, to explain how it harmonizes risks / information potentialities.

Keywords: Computer audit, security, controls, company, advertising.

ÍNDICE DE CONTENIDOS

PORTADA....1
ÍNDICE DE CONTENIDOS....4
ÌNDICE DE ILUSTRACIONES....4
ÍNDICE DE CUADROS....5
INTRODUCCIÓN....6
1. FUNDAMENTACIÓN TEÓRICA....8
1.1 Auditoría Informática....8
1.2 MarkGlob....8
1.3 Riesgos y amenazas en sistemas computacionales....8
1.4 Métodos para auditoria de TIC`s....9
1.4.1 COBIT....9
1.4.2 CRAMM (CCTA Risk Analysis and Management Method)....10
1.4.3 MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)....10
1.4.4 OCTAVE (Operationally Critical Threats Assets and Vulnerability Evaluation)....10
1.5 Seguridad informática y de la información....10
2. METODOLOGÍA....11
2.1 Investigación Bibliográfica....11
2.2 Estudio de caso....11
2.3 Sistematización....11
3. DESARROLLO....12
4. CONCLUSIONES Y RECOMENDACIONES....15
5. REFERENCIAS BIBLIOGRÀFICAS....16

ÌNDICE DE ILUSTRACIONES

Ilustración 1. Comportamiento de seguridad en usencia de políticas de seguridad....6
Ilustración 2. Logotipo de empresa analizada....8
Ilustración 3. Principales amenazas en procesos empresariales....9
Ilustración 4. Metodología propia de control interno en MarkGlob....12

ÍNDICE DE CUADROS

Cuadro 1. Controles aplicados al sistema computacional de MarkGlob 13
Cuadro 2. Riesgos y vulnerabilidades detectadas en la empresa 13

INTRODUCCIÓN

La era digital caracterizada en la sociedad globalizada promueve el uso de las Tecnologías de la comunicación e información (TIC´s) como soporte en el desarrollo de los menos favorecidos, pero se da poca relevancia a sus riesgos y afectaciones a la vida cotidiana, convirtiendo la seguridad de datos personales e institucionales en un derecho más que una ventaja u obligación corporativa, debido a que trasforma todo proceso o actividades gestada en medios computacionales (CARVAJAL, 2018).

La auditoría informática es el eje del estudio pertinente, gracias a que faculta medir la capacidad para gestionar riesgos dentro de una empresa, evaluar su nivel de seguridad en torno a las fortalezas y debilidades de sus sistemas; por medio del análisis a los controles empleadas para maximizar su eficiencia en sintonía con las bondades digitales (Caycedo & Arcetales, 2017).

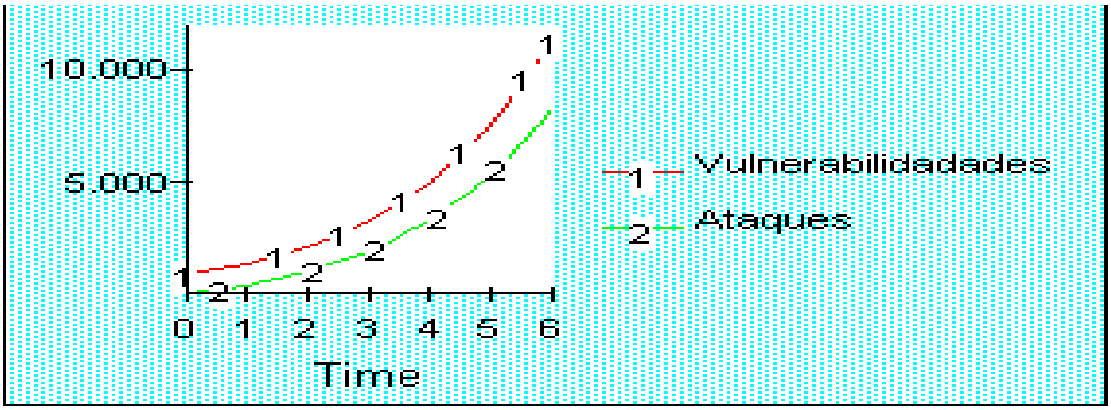

Ilustración 1. Comportamiento de seguridad en usencia de políticas de seguridad
Fuente: (Vera & Vera, 2017)

Los objetivos del control interno en una empresa, observado desde la perspectiva de las TIC´s para mantener seguridad y rentabilidad son:

- Impulsar la eficacia, eficiencia, efectividad y transparencia en las operaciones a un costo factible
- Preservar la confiabilidad, calidad, accesibilidad e integridad en los datos
- Satisfacer los requerimientos legales y consideraciones técnicas para brindar servicios de calidad
- Mantener en óptimas condiciones sus bienes, promover buen uso de recursos físicos, lógicos y económicos
- Proteger y preservar el patrimonio contra pérdida, uso inadecuado e irregularidades o actos ilícitos frente a cualquier amenaza (Cadenas & Garcia , 2016)

Es importante denotar que en cuestiones de seguridad y control interno es absoluto el empoderamiento humano, concientizar sobre la cultura en protección de datos, no como un activo corporativo sino como un recurso estratégico en el desarrollo organizacional e integrar los sistemas informáticos a la vida cotidiana adecuadamente sintonizando riesgos y cualidades heurísticamente (Ibarra, 2018).

La empresa MarkGlob es una de las más destacas a nivel local, debido a su participación en marketing e interacción en publicidad políticas y corporativa, siendo un aliado estratégico para los emprendedores o marcas en ascenso; por tal motivo se analiza como concatena la seguridad con el uso de las tecnologías utilizando las consideraciones competentes de la auditoria informática.

1. FUNDAMENTACIÓN TEÓRICA

Comprende la argumentación cognitiva del proyecto, sustentar en criterios de otros autores sobre estudios relacionados a la materia; se destaca los términos y propuestos teóricos necesarios en la delimitación del caso práctico.

1.1 Auditoría Informática

Es una filosofía de mejora continua instaurada en toda entidad pública o privada, consagra un conjunto de técnicas y procedimientos destinado a evaluar, medir e implementar controles orientados a conservar la seguridad de datos, optimizar tareas, conservar la integridad de los sistemas computacionales con una relación costo/beneficio rentable para la empresa (Espinoza, Abad, & Pinos, 2017).

1.2 MarkGlob

Es una empresa de asesores comerciales, localizada en Machala, fundada el 1 de febrero del 2013 por Severo García Cabrera con el objeto de atender las necesidades en estrategias comerciales, marketing y publicidad a las marcas locales o nacionales.

Ilustración 2. Logotipo de empresa analizada
Fuente: (Markglob, 2013)

1.3 Riesgos y amenazas en sistemas computacionales

Son los factores que posibilitan efectuar un ataque o daño a las instalaciones de datos e información, comprenden condicionantes externas, naturales e internas capaces de explotar una debilidad para viabilizar una situación que vulnere la seguridad del sistema.

Los principales riesgos en medios informáticos son:

- Uso de aplicaciones que expresen datos personales o ubicaciones en tiempo real
- Configuración incorrecta al gestionar acceso a la información
- Falencia de certificador o protocolos de telecomunicaciones e internet
- Phising, pharming, e interacciones mal intencionadas en redes sociales
- Intercepciones, corrupción, perdida o hurto de datos (Wlosinski, 2016)

Las amenazas latentes en sistemas computaciones son:

- Virus, ebot o código malicioso
- Fraudes electrónicos
- Ataques de fuerza bruta
- Inyección SQL
- Divulgación o mal uso de información corporativa
- Desastres naturales
- Acceso no autorizado a los medios digitales (Figueroa, Rodríguez, Bone, & Saltos, 2017)

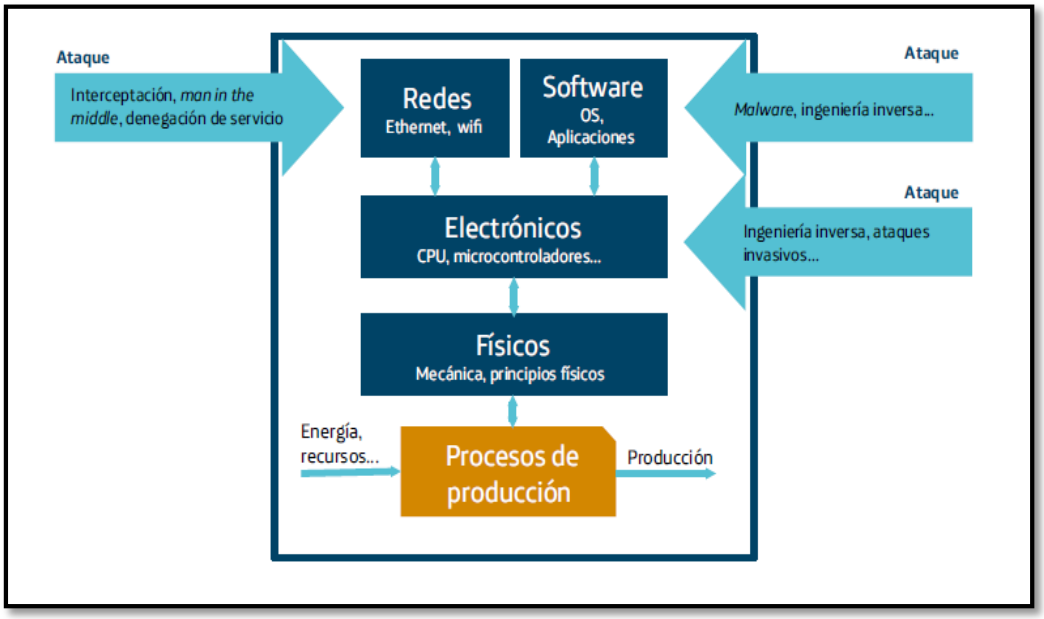

Ilustración 3. Principales amenazas en procesos empresariales
Fuente: (Ariel y Fundación Telefónica, 2016)

1.4 Métodos para auditoria de TIC`s

Los procedimientos más destacables dentro de la literatura revisada al examinar la seguridad de sistemas son:

1.4.1 COBIT

Sus iniciales significan Objetivos de Control para Información y Tecnologías Relacionadas comprende un conjunto de procesos para separar gobierno de gestión en TIC`s, evalúa y propone medidas planificadas en función de los objetivos estratégicos de la empresa en base a su valor monetario y nivel de prestaciones a la organización (Zambrano & Molina, 2017).

1.4.2 CRAMM (CCTA Risk Analysis and Management Method)

Esta metodología está pensada para empresas grandes, instaurado en sistemas británicos para analizar los riesgos latentes en forma cuantitativa y cualitativa; además se basa en una disciplina constante e integra con mejores continuas e investigaciones para reducir al mínimo los riesgos presentes en las organizaciones a través de medidas vanguardistas (Arévalo & Moscoso, 2017).

1.4.3 MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)

Es una técnica que primero identifica los activos de la información, diagnostica las amenazas del entorno, luego evalúa sus impactos e implementa nociones que salvaguarden los recursos más relevantes gestionando el riesgo residual (Crespo & Cordero, 2018).

1.4.4 OCTAVE (Operationally Critical Threats Assets and Vulnerability Evaluation)

Desarrollada por el Equipo de Respuesta ante Emergencias Informáticas, básicamente evaluar los posibles riesgos y propone controles que equilibren las vulnerabilidades con las facilidades digitales en los procesos empresariales (Tejena, 2018).

1.5 Seguridad informática y de la información

EL primer término compete a mantener al mínimo los riesgos a los activos informáticos, priorizando la confiabilidad en el uso adecuado e idóneo de los mismos; mientras que la seguridad de la información se limita a la calidad, disponibilidad, confiabilidad e integridad de los datos para ser empleados dinámicamente en cualquier actividad requerida por la institución en forma holística y ágil (Quiroz & Macías, 2017).

Las medidas más utilizadas en prevención y protección de activos computacionales son:

- Diseñar contraseñas fuertes con cifrado o estudios cuidadosos
- No conectarse a redes públicas WIFI
- Restringir uso de datos y privilegios de red a usuarios de confianza
- Utilizar antivirus y firewall actualizados
- Actualizar programas con frecuencia
- Realizar respaldos del contenido regularmente
- Implementar políticas de seguridad con sanciones y acciones preventivas
- Aplicar controles biométricos e incentivar cultura de protección de datos (Agrela, 2018).

2. METODOLOGÍA

Las técnicas empleadas en la recopilación, análisis e interpretación de conocimientos afines a la temática abordada son los siguientes:

2.1 Investigación Bibliográfica

Consiste en una indagación académica fomentada en unas revisiones exhaustivas del estado del arte en lo referente a seguridad informática, entorno a publicaciones con el rigor competente como artículos científicos, trabajos de grado, tesis, entre otros (MORGAN, 2017).

2.2 Estudio de caso

En un proceso enfocado a estudiar una realidad en particular, apreciar su contexto desde una perspectiva objetiva, construyendo las secuencias o inferencias que explican la relación entre sus partes a la vez que se fundamente epistemológicamente en las ciencias referentes al área del conocimiento analizada (Polo, 2015).

2.3 Sistematización

Es una técnica de amplio espectro de aplicación, principalmente en cuestiones de ordenamiento e interpretación de datos en forma holística, analizando el estudio simultáneamente desde múltiples puntos de vista para componer una secuencia lógica que solvente las necesidades propuestas, integrando las partes sintetizadas como relaciones coherentes en forma conjunta consolidándose como unidad (Rodríguez & Pérez, 2017).

3. DESARROLLO

Los resultados del análisis se expresan mediante matrices, cuadros o ilustraciones para sintetizar el contenido con la finalidad de facilitar su entendimiento, tales hallazgos se describen en este inciso.

El sistema de control en MarkGlob se esquematiza a través de la ilustración 4.

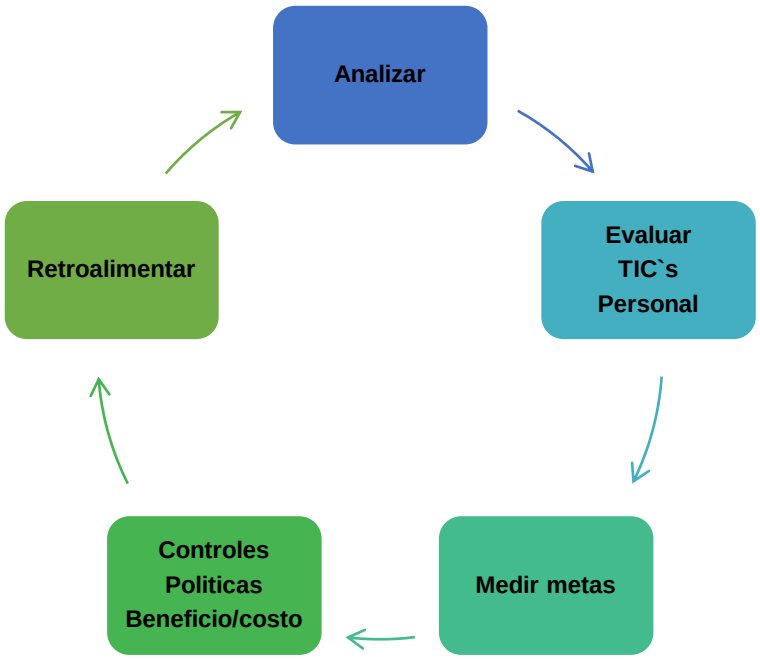

Ilustración 4. Metodología propia de control interno en MarkGlob
Fuente: Autora

Cabe destacar que la empresa, no aplica estándares internacionales, pero si se adapta en base a legislaciones, normativas o filosofías de control para gestar coherencia entre su seguridad y potencialidades en el medio laboral.

Los procedimientos implementados en cuestiones de auditoria computacional son:

- Realizar respaldos constantes en nube privada
- Diseñar contraseñas seguras y cambiarlas regularmente
- Evaluar los sistemas mediante informes y reportes
- Medir parámetros técnicos de calidad en redes e internet
- Monitorear posibles vulnerabilidades e implementar controles
- Diseñar plan de contingencia y mantener cohesión de equipo

Cuadro 1. Controles aplicados al sistema computacional de MarkGlob

Sistema Informático	Controles
Ordenadores y línea de equipos marca Apple	No hay virus ni malware para su sistema operativo, eficiencia, prestigio y licencia en toda su infraestructura digital
Red lan interna y privada	Velocidad alta y estable, mejores prestaciones que redes alquiladas, permite monitorear flujo de datos
Red wifi con nube personal física 2Teras	Respaldos dinámicos de información, evita robo o pérdida de datos
Pasa información por cableado interno en red entre computadoras sin net	Evitar transferir archivos por internet y solo se envía a externos por red privada que es segura
Data center con router, servidor propio	Permite regular y medir variables en tiempo real, asegura certificados web de protocolos seguros
Dominio privado, manejo de redes sociales y servicios de google	Interactuar con el mercado desde una infraestructura segura, pagando servicios tecnológicos afines
Redes eléctricas, de datos, dispositivos, equipos e instalaciones	Mantenimiento preventivo y predictivo para minimizar riesgos

Fuente: (Cabrera, 2019)

Cuadro 2. Riesgos y vulnerabilidades detectadas en la empresa

Sistema Informático	Riesgos y vulnerabilidades
Ordenadores	Virus y malware/daños o mal uso
Personal	Uso indebido de información o datos institucionales
Redes e internet	Infiltraciones, robo o pérdida de información
Equipos e instalaciones	Deterioro, falta de mantenimiento y recursos monetarios

Infraestructura física y tangible	Cámaras de seguridad, planes de contingencia, seguros y recursos financieros

Fuente: (Cabrera, 2019)

Se observa que MarkGlob opta por la eficiencia, prestigio e integridad; al gestar sus sistemas en equipos de uso exclusivo evita varios riesgos nominales, también tiene planes de mantenimiento y respaldo de datos desde un servidor virtual propio evitando así falencias en su información, presenta novedad al transferir archivos por una red privada sin internet e implementar servicios pagados de Google para realizar conexiones a terceros; pese a ello, su mayor activo son el recurso humano que está debidamente calificado para responder inmediatamente ante cualquier eventualidad.

El mercado de la era digital, es un medio complejo caracterizado por la Dinamicidad de su interacción cliente/empresa, facilidad de transacciones o pagos, posicionamiento en buscadores web, relaciones en redes sociales y publicidad electrónica que garantizan un alcance amplio; conjugado con herramientas informáticas de análisis para gestar en forma eficiente las decisiones en respuesta al comportamiento de su área de desempeño, por lo cual es imperioso tecnificarse e instaurar una marca corporativa sólida en las plataformas virtuales (Llanes, Sala, & Leiva, 2018).

Una de las mejores formas de garantizar el correcto control interno y aplicación adecuada de las políticas en seguridad informática es un manual de procedimientos; gracias a que expresa en forma clara como ejecutar las actividades, delinear sanciones, delegar responsabilidades, describir políticas, métodos para medir y monitorear el estado de la organización e incentivar el empoderamiento como clave en proteger eficazmente la empresa (Vergara, 2017).

4. CONCLUSIONES Y RECOMENDACIONES

- La mejor medida implementada en MarkGlob es la prevención y disciplina, emplean una cultura sistematizada al controlar los riesgos, utilizar adecuadamente los recursos digitales en forma consciente e intrínseca, siguiendo sus protocolos internos a la vez que maximizan las comodidades prestadas a los servicios o acciones en la ejecución de negocios.
- El activo más importante de la empresa son sus empleados; mantenerlos preparados, comprometidos con la marca y unidos como equipo, permite responder oportunamente frente a cualquier evento, evitar infiltraciones o mal uso de datos, además permite gobernar eficientemente las TIC`s al derogar al ser humano como principal ente de control, también tiene ventaja competitiva al comunicarse fluidamente internamente e interactuar en forma dinámica para proteger los recursos corporativos de MarkGlob conjuntamente desde todas las perspectivas posibles.

- El uso de tecnologías exclusivas permite mantenerse por encima del nivel promedio en seguridad, evita virus o infecciones nominales de las marcas tradicionales, pagar por servicios drive en Google da las ventajas de respaldar dinámicamente la información y acceder desde cualquier parte a ella; además el uso de redes privadas con dominio propio, cámaras de vigilancia e implementación de una cultura interna de seguridad basada en la responsabilidad y unidad corporativa garantizar integridad en sus sistemas informáticos.

5. REFERENCIAS BIBLIOGRÀFICAS

Agrela, J. M. (8 de Agosto de 2018). *Postedin SpA.* Obtenido de CIBERSEGURIDAD EN EL MARKETING DIGITAL: PROTEJE TU MARCA: https://www.postedin.com/blog/ciberseguridad-marketing-digital-proteje-marca/

Arévalo, F. M., & Moscoso, L. P. (2017). Metodología Ágil para la Gestión de Riesgos Informáticos. *Revista Killkana Técnica. Vol. 1, No. 2*, 32-42.

Ariel y Fundación Telefónica. (2016). *CIBERSEGURIDAD, LA PROTECCIÓN, DE LA INFORMACIÓN EN UN MUNDO DIGITAL.* Barcelona España: Editorial Ariel, S.A.

Cabrera, S. G. (22 de Junio de 2019). Ingeniero en Marketing/Gerente de MarkGlob. (S. C. Gonzàles, Entrevistador)

Cadenas Oleas, B. N., & Garcia Rondon , I. (2016). EL CONTROL INTERNO PARA LA GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN. *Caribeña de Ciencias Sociales*.

CARVAJAL, E. T. (2018). Tecnologías, seguridad informática y derechos humanos. *IUS ET SCIENTIA, Vol.4, nº 1*, 19-39.

Caycedo Casas, D., & Arcetales Fernandez , X. (2017). Auditoría informática: un enfoque efectivo. *Dominio de las Ciencias Vol. 3*, 157-173.

Crespo Martínez, E., & Cordero Torres, G. (2018). ESTUDIO COMPARATIVO ENTRE LAS METODOLOGÍAS CRAMM Y MAGERIT PARA LA GESTIÓN DE RIESGO DE TI EN PYMES. *UDA AKADEM, No 1*, 38-47.

Espinoza, J. J., Abad, C. R., & Luis Fernando Pinos Castillo, y. O. (2017). Sistema cobit en los procesos de auditor´ıas de los sistemas informàticos. *REVISTA CIENCIA E INVESTIGACIÒN, VOL. 2, NO. 8*, 65-68.

Figueroa-Suárez, J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C., & Saltos-Gómez, J. A. (2017). La seguridad informática y la seguridad de la información. *Polo del Conocimiento (Edición núm. 14) Vol. 2 No 12*, 145-155.

Ibarra, R. V. (2018). 2018. *Paakat: Revista de Tecnología y Sociedad, Año 8, Núm 14.*, 2-13.

Llanes, R. P., Sala, H. V., & Leiva, I. R. (2018). Estrategias de comercio electrónico y marketing digital para pequeñas y medianas empresas. *Revista Cubana de Ciencias Informáticas, Vol 12, No 3*, 192-208.

Markglob. (2013). *MarkGlob: Marketing + Planificaciòn*. Obtenido de Nosotros: http://www.markglob.com/nosotros.html

MORGAN, L. C. (2017). La investigación-acción: una propuesta para la formación y titulación en las carreras de Educación Inicial y Primaria de una institución de educación superior privada de Lima. *Educación Vol. XXVI, N° 51*, 137-157.

Polo, M. P. (2015). Ceremonial y protocolo: métodos y técnicas de investigación científica. *Opción, Año 31, No. Especial 1* , 1137-1156.

Quiroz-Zambrano, S. M., & Macías-Valencia, D. G. (2017). Seguridad en informática: consideraciones. *Dominio de las Ciencias Vol. 3, núm. 4*, 137-156.

Rodríguez Jiménez, A., & Pérez Jacinto, A. O. (2017). Métodos científicos de indagación y de construcción del conocimiento. *Revista Escuela de Administración de Negocios, núm. 82*, 1-26.

Tejena Macias , M. (2018). Análisis de riesgos en seguridad de la información. *Polo del Conocimiento, Vol 3, No 4*, 230-244.

Vera, V. D., & Vera, J. C. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. *Scientia et Technica Año XXII, Vol. 22, No. 2.*, 193-198.

Vergara, I. M. (2017). LOS MANUALES DE PROCEDIMIENTOS COMO HERRAMIENTAS DE CONTROL INTERNO DE UNA ORGANIZACIÓN. *Revista Científica de la Universidad de Cienfuegos, Vol 9, No 2*, 247-252.

Wlosinski, L. G. (2016). Amenazas Dispositivos de Computación Móviles, Vulnerabilidades y Factores de Riesgo son Ubicuas. *ISACA Journal Volume 4*.

Zambrano Vera , M. F., & Molina Sabando, L. (2017). Diagnóstico situacional del Gobierno de las Tecnologías de Información. Caso Universidad Laica Eloy Alfaro de Manabí. *Revista Ciencia UNEMI, Vol 10, No 19*, 111-122.