Dom. Cien., ISSN: 2477-8818
Vol. 7, núm. 4. Diciembre Especial 2021, pp. 363-376

DOI: http://dx.doi.org/10.23857/dc.v7i4.2425
Ciencias Técnicas y Aplicadas
Artículo de Investigación

Análisis y evaluación de riesgos: aplicado a EMAPAL-EP, basado en la metodología de MAGERIT versión 3.0

Risks analysis and evaluation: applied to EMAPAL-EP, based on the MAGERIT version 3.0 methodology

Análise e avaliação de risco: aplicada ao EMAPAL-EP, com base na metodologia MAGERIT versão 3.0

Remigio Alfredo Avila-Torres [I]
jimmyaat@gmail.com
https://orcid.org/0000-0002-3090-2991

Juan Pablo Cuenca-Tapia [II]
jcuenca@ucacue.edu.ec
https://orcid.org/0000-0001-5982-634X

Correspondencia: jimmyaat@gmail.com

*__Recibido:__ 30 de octubre de 2021 *__Aceptado:__ 20 de noviembre de 2021 __* Publicado: 0__7 de diciembre de 2021

I. Ingeniero de Sistemas, Técnico de Sistemas. EMAPAL-EP, estudiante de la Maestría en Ciberseguridad. Unidad Académica de Posgrado, Universidad Católica de Cuenca, Cuenca, Ecuador.

II. Ingeniero de Sistemas, docente de la Maestría en Ciberseguridad, Unidad Académica de Posgrado, Universidad Católica de Cuenca, Cuenca, Ecuador.

Resumen

La EMAPAL-EP, en los últimos años ha apostado a las nuevas vanguardias tecnológicas, lo que ha significado grandes avances en sus diversos procesos, pero deberá tener en cuenta que, si no se toman las medidas de seguridad respectivas y se tratan estos riesgos de infraestructura tecnológica y los diversos procesos que llevan, estarán vulnerables a gran cantidad de amenazas, es por eso que, el propósito de este trabajo es obtener una valoración cuantitativa de la gestión de análisis y riesgos en la empresa. La metodología aplicada será magerit, la cual consta de cinco fases, empezando por la identificación de los activos relevantes, determinación de las amenazas a los que están expuestos, determinación de las medidas preventivas, medición del impacto residual y finalmente estimar el riesgo residual. Con el resultado del estudio, se presentará un plan para el tratamiento de los riesgos identificados y analizados, para dejarlos en un estado aceptable o mitigado.

Palabras clave: Vulnerabilidades; amenazas; riesgo; magerit; vanguardias tecnológicas.

Abstract

EMAPAL-EP, in recent years has bet on the new technological vanguards, which has meant great advances in its various processes, but it must take into account that, if the respective security measures are not taken and these risks of technological infrastructure and the various processes they carry will be vulnerable to a large number of threats, that is why the purpose of this work is to obtain a quantitative assessment of the analysis and risk management in the company. The applied methodology will be magerit, which consists of five phases, starting with the identification of the relevant assets, determining the threats to which they are exposed, determining the preventive measures, measuring the residual impact and finally estimating the residual risk. With the result of the study, a plan will be presented for the treatment of the identified and analyzed risks, to leave them in an acceptable or mitigated state.

Keywords: Vulnerabilities, threats, risk, magerit, technological vanguards.

Resumo

A EMAPAL-EP, nos últimos anos tem apostado nas novas vanguardas tecnológicas, o que tem significado grandes avanços nos seus diversos processos, mas deve ter-se em consideração que, caso não sejam tomadas as respectivas medidas de segurança e estes riscos de Infra-estrutura Tecnológica

e as diversas os processos que carregam estarão vulneráveis a um grande número de ameaças, por isso o objetivo deste trabalho é obter uma avaliação quantitativa da análise e gestão de riscos na empresa. A metodologia aplicada será magerit, que consiste em cinco fases, começando pela identificação dos ativos relevantes, determinando as ameaças a que estão expostos, determinando as medidas preventivas, medindo o impacto residual e finalmente estimando o risco residual. Com o resultado do estudo, será apresentado um plano de tratamento dos riscos identificados e analisados, de forma a deixá-los em estado aceitável ou mitigado.

Palavras-chave: Vulnerabilidades; ameaças; risco; magerit; vanguardas tecnológicas.

Introducción

La tecnología en todo el mundo pasó de ser lujos a herramientas necesarias, debido a que se ha convertido en un elemento muy importante para el actuar diario de las personas y empresas.

En la era actual, las empresas deben mejorar sus recursos tecnológicos para mantenerse en la competencia contra las demás, para ello deberán mejorar su productividad, competitividad y sus servicios, es así que, las nuevas tecnologías han llegado para resolver estos inconvenientes y ayudarles a mejorar a través de sistemas innovadores, equipos modernos, aplicativos, entre otros, los cuales de adaptan a las necesidades de cada una de ellas. Es decir, lo que antes tomaba varios días en hacer, ahora con la nueva tecnología se lo podrá hacer en horas, sin mayor complicación, ahorrando esfuerzos de personal y reduciendo sus costos.

Una de las partes más importantes dentro de las empresas es la gran cantidad de información que maneja como datos de clientes, proveedores, manejos contables, información confidencial, entre otras, lo que es muy valiosa para la compañía. Para ello el implementar un sistema de gestión de datos o herramientas para el manejo de datos, facilita su intercambio, un control correcto y un adecuado almacenaje de la información, lo que ayuda a la compañía a ser más competitiva. Un ejemplo de esto, en una empresa de ventas en línea que guarda en una base de datos, las preferencias de compras, para mandar promociones a sus cuentas. Gracias a estas tecnologías como el Big Data, las empresas pueden mejorar sus servicios al manejar la información de sus clientes.

Entre las grandes preocupaciones de las empresas esta la seguridad de la información, debido a que con el pasar del tiempo los delitos de robos, alteraciones, encriptación de información han aumentado considerablemente, lo que representa una pérdida económica, de prestigio y confianza de la entidad.

Se debe considerar que, para acceder a la información, no es necesario estar presente o conectado dentro de la empresa, la mayoría de los ciberdelitos se han realizado desde la red externa de la empresa, debido a fallas bien conocidas en los equipos implementados, mala configuración de sus servicios, entre otros.

Muchas de las empresas piensan que están protegidos con los equipos, aplicaciones y políticas de seguridad con las que cuentan, pero la verdad es otra puesto que la mayoría de técnicos de Tics, no son expertos en el manejo de seguridad, para ello las empresas deben pensar en contratar un estudio de profesionales en la materia de ciberseguridad, los cuales con sus conocimientos podrán detectar las amenazas y vulnerabilidades con las que cuentan la empresa, ya sea por usuarios internos y/o externos, sea de manera intencional o no, entre otros factores.

Algunos ataques de ciberseguridad muy conocidos en el medio tenemos el del Banco de Pichincha "El pasado 9 de febrero de 2021, las redes sociales hicieron eco de una supuesta filtración de información relacionada con el Banco Pichincha, Visa Titanium, Diners Club y Discover, tal como te explicamos aquí, la cual fue desmentida por la entidad bancaria, pero que aún deja muchas dudas"(Gilson Pilargote (Diario Expreso), 2021), en tal ataque se argumenta que 80 GB de información fueron sustraídos y publicados en empresas como GitHub y Mega File Share utilizando la cuenta de Threat Actor. Este acto ayudo a que el banco perdiera credibilidad ante sus clientes.

Otro de los casos muy conocidos en nuestro medio fue el de CNT, efectuado el 14 de julio de 2021, "CNT remplazó algunos equipos afectados por hackeo y otros se lograron reutilizar" (eluniversocom, 2021), la institución indica que el ataque fue causado por un virus ransomware, los cuales afectaron a los centros de servicios. La entidad compenso a sus clientes prepago dándoles un bono de 1 GB por siete días, 1 GB por un año a sus clientes pospago, entre otros beneficios.

Con los antecedentes mencionados se pretende contribuir de manera práctica, porque se va a construir una matriz de riesgos, alineando la plataforma tecnológica del negocio, dándole valor agregado dentro de la organización, con la optimización de recursos, control eficiente de riesgos y amenazas. De esta manera, las partes interesadas de la compañía, obtendrán herramientas que los direccionen a tomar mejores decisiones para tener los riesgos mitigados o en nivel aceptable.

Las secciones con las que cuenta el documento serán:

- Sección 1, se expone una breve introducción.
- Sección 2, se presenta el planteamiento del problema y sus objetivos.
- Sección 3, se explica el método y los materiales utilizados.

- Sección 4, se detalla los resultados del análisis de riesgos de la EMAPAL-EP.
- Sección 5, se realiza una discusión sobre los resultados de la investigación.
- Sección 6, se determina las conclusiones de la investigación.

Planteamiento del problema y objetivos

Problema

¿Cuáles son los riesgos de seguridad que están presentes en la Empresa Pública Municipal de Agua Potable, Alcantarillado y Saneamiento Ambiental del Cantón Azogues?

Objetivos

General

Analizar los riesgos de la información del área de TI en la empresa EMAPAL-EP, basado en la metodología de magerit versión 3, para determinar los riesgos presentes; y, elaborar un plan de tratamiento que permita mantenerlos en un nivel aceptable.

Materiales y Metodología

Los resultados se obtuvieron a través de la aplicación de la metodología de Magerit Versión 3, utilizando un método inductivo-deductivo para la obtención de los activos y amenazas presentes en la empresa, con un enfoque cuantitativo del tipo descriptiva, con la finalidad de cumplir con el objetivo general de esta investigación.

Desarrollo

Para comenzar con el desarrollo del proyecto es necesario determinar los pasos a seguir para obtener los resultados deseados.

Revisión del estado del arte. El cual cuenta con un análisis documental en el que nos muestra los avances obtenidos sobre un determinado tema de investigación. Esto nos ayudara para determinar las mejores opciones utilizadas para llegar a cumplir nuestras metas. Pueden utilizar herramientas de búsqueda como motores de búsqueda https://sholar.google.com, https://www.kkhson.in/library/oajse/, entre otras de acuerdo al tema de investigación.

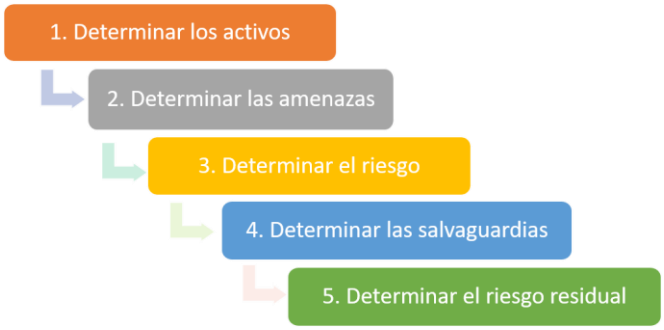
Diagnostico situacional. Se procede a determinar la situación actual de la empresa, mediante la aplicación de metodologías como el Magerit, octave, entre otros, apoyándose en los tipos de investigación que más se adapten a nuestras necesidades como inductivos, deductivos, científicos,

mixtos, etc.; y, de acuerdo al enfoque que deseamos darle como descriptivas, explicativas, etc., los cuales nos ayudaran a obtener y analizar los datos existentes.

Metodología. Se determina la metodología a ser implementada para la obtención de los resultados, en nuestro caso nos ayudaremos de magerit en su versión 3, que es una metodología de análisis y riesgos elaborada por la comisión de estrategias TIC, la cual es implementada para minimizar los riesgos al momento de implementación y uso de tecnologías de información. Su uso principal esta direccionado a la administración pública.

Fases de Magerit. La metodología de Magerit, se la puede dividir en cinco pasos principales como se muestra en la siguiente ilustración.

Ilustración 1 - Pasos metodología Magerit



Fuente: 1 (MAGERIT 3.0: MÉTODO DE ANÁLISIS DE RIESGOS – Interpolados, 2020)
Elaboración: El autor

Determinación de los activos. Un activo es un recurso que tiene un valor para la institución, la cual genera un beneficio a futuro sea económico o no, por lo que se debe proteger de manipulaciones o daños. Para determinar los activos fue necesario realizar una visita técnica a la empresa, para determinar con que insumos contaban, luego se realizó una entrevista con el personal de Tics y administrativo, para determinar su importancia dentro de la institución, de acuerdo a sus dimensiones de integridad, confidencialidad, disponibilidad, trazabilidad y autenticidad. Según lo estipula el libro 2 de Magerit del 2012.

Determinación de las amenazas. Se realizó el estudio de las amenazas y vulnerabilidades con los que cuenta los diferentes activos, pudiendo ser estos de desastres naturales, de origen, errores y fallos,

ataques intencionados, correlación de errores y taques, nuevas amenazas, nivel de la amenaza. Según lo estipula el libro 2 de Magerit del 2012.

Determinación del riesgo. Se realizó el proceso de análisis y evaluación de riesgos de acuerdo al estándar Magerit que permite valorar los riesgos en cada uno de los criterios de información evaluados, identificando las posibles causas que los originan de acuerdo al impacto ponderado con la tasa de ocurrencia. Según lo estipula el libro 1 y 3 de Magerit del 2012.

Determinación de salvaguardas. Se realizó el proceso de análisis de las salvaguardias existentes en la empresa, las cuales permiten la reducción del riesgo inherente, mediante procedimientos, medidas o mecanismos tecnológicos. Según lo estipula el libro 2 de Magerit del 2012.

Determinación de riesgo residual. Se realiza el proceso de análisis y evaluación de riesgos inherentes, después de implementar las salvaguardias existentes en la empresa, para así determinar el riesgo residual de los activos.

Desarrollo de contramedidas. Una vez identificado los riesgos residuales de la institución se procedió a determinar las posibles soluciones para mitigar estos riesgos, para lo cual nos basamos en la Norma ISO-IEC 27001, en su anexo A (Objetivos de control y Controles de Referencia).

Resultados y discusión

Aplicando la metodología Magerit V3, el inventario de activos de la empresa EMAPAL-EP, consta de 46 ítems agrupados en 9 tipos de activos y con una codificación diferente que nos ayuda a reconocerlos, los cuales se muestra en la tabla 1.

Tabla 1 - Inventario de Activos

[S] Servicios		**[SW] Aplicaciones (Software)**	
[S] [DIR]	Servicio de directorio	[SW] [SUB]	Desarrollo a medida
[S][IDM]	Gestión de identidad	[SW] [EMAIL_CLIENTE]	Cliente correo electrónico
[S][IPM]	Gestión de privilegios	[SW] [DBMS]	Sistema de gestión de BDD
[S][WWW]	World Wide Web	[SW] [OFFICE]	Ofimática
[S][EMAIL]	Servicio de correo Corporativo	[SW] [AV]	Anti virus
[HW] Equipos Informáticos		[SW] [OS]	Sistema operativo

[HW] [HOST]	Grandes Equipos
[HW] [MID]	Equipos medios
[HW] [MOBILE]	Informática móvil
[HW] [VHOST]	Equipo virtual
[HW] [PRINT]	Medios de impresión
[HW] [SCAN]	Escáneres
[HW] [SWITCH]	Conmutadores
[HW] [ROUTER]	Encaminadores
[HW] [FIREWALL]	Cortafuegos
[HW] [WAP]	Punto de acceso inalámbrico
[HW] [PABX]	Central telefónica
[HW] [IPPHONE]	Teléfono IP
[COM] Redes	
[COM] [PSTN]	Red telefónica
[COM] [WIFI]	Red inalámbrica
[COM] [LAN]	Red local
[COM][INTERNET]	Internet
[L] Instalaciones	
[L] [BUILDING]	Edificio Matriz
[L] [LOCAL]	Cuarto de Servidores
[SW] [HIPERVISOR]	Gestor de máquina virtual
[SW] [BACKUP]	Sistema de backup
[P] Personal	
[P] [ADM]	Administradores de sistemas
[P] [UI]	Usuarios internos
[P] [UE]	Usuarios externos
[P] [PROV]	Proveedores
[D] Datos / Información	
[D] [BACKUPS]	Copias de respaldo
[D] [SOURSE]	Código fuente
[D][TEST]	Datos de pruebas
[AUX] Equipamiento Auxiliar	
[AUX] [POWER]	Fuentes de alimentación
[AUX] [UPS]	Sistema de alimentación interrumpida
[AUX] [WIRE]	Cable eléctrico
[AUX] [FURNITURE]	Armarios
[MEDIA] Soporte de Información	
[MEDIA] [DISK]	Discos
[MEDIA] [VDISK]	Discos Virtuales
[MEDIA] [PRINTED]	Material impreso
[MEDIA] [USB]	Memorias usb

Fuente: (2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8)
Elaboración: Autor

Luego de levantado los activos, se procedió a obtener su valoración, seguido verificamos el análisis de amenazas y vulnerabilidades, para con todos los datos antes mencionados encontrar el riesgo potencial al que están sujetos.

Acabado el examen se determinó que existen 43 riesgos en nivel alto, 269 riesgos en nivel medio y 88 riesgos en nivel bajo, de los cuales se presenta un muestreo en la tabla 2.

Tabla 2 – Muestreo de los riesgos actuales contra los activos de seguridad

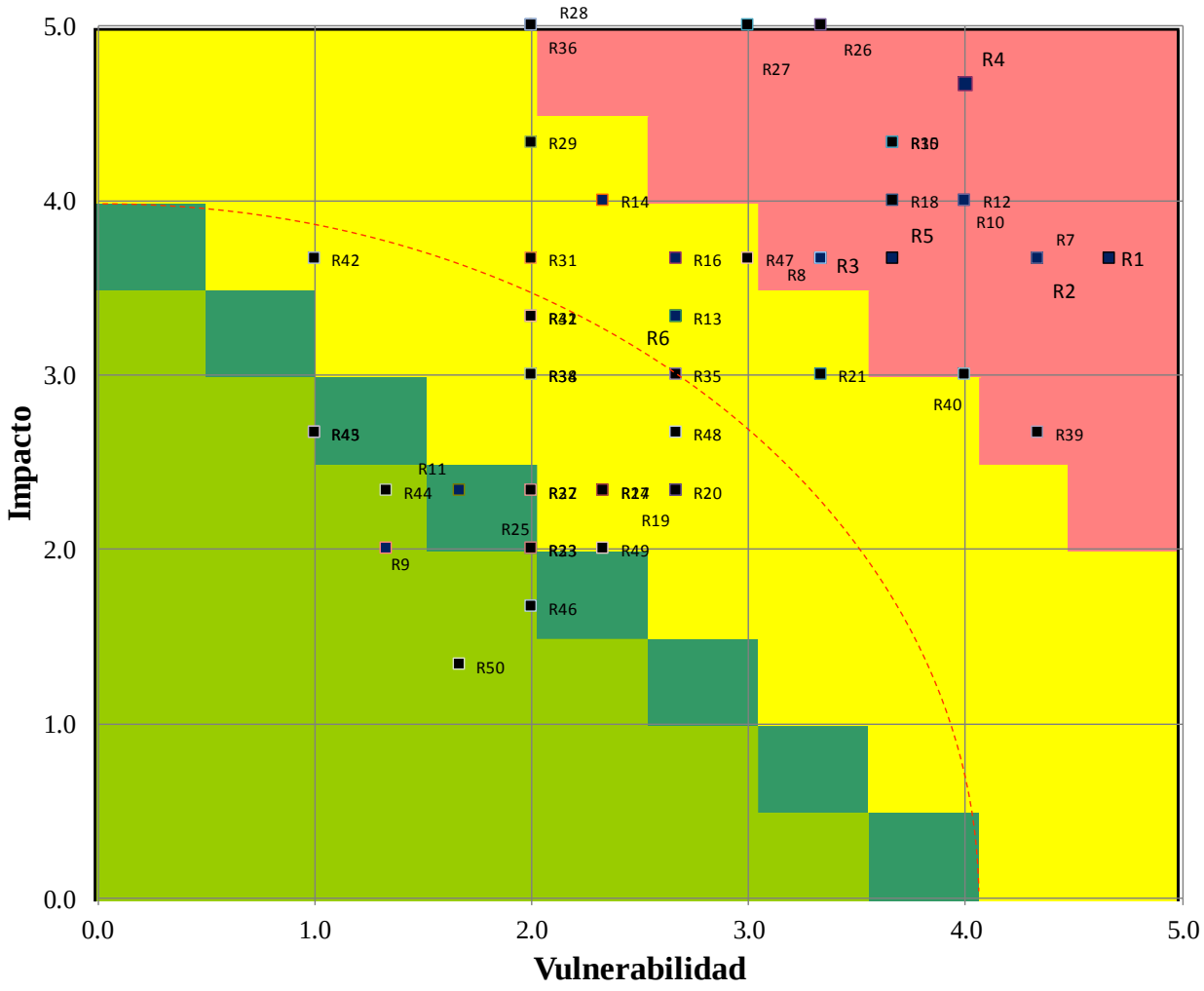
	Proceso	Tipificación riesgo	Riesgo evaluado	Observación	Criticidad	P	I	Voto	Calificación (Gerente)	Calificación (Tic)	Calificación (Usuario)
R1	[D] [BACKUPS]	R1	Errores de monitorización	Ausencia de control de cambios eficaz	Alto	4.7	3.7	VOTO IMPACTO	4.0	3.0	4.0
								VOTO PROBABILIDAD	5.0	5.0	4.0
R2	[D] [BACKUPS]	R2	Alteración accidental de la información	Falta de conocimientos de los usuarios para realizar tareas especificas	Alto	4.3	3.7	VOTO IMPACTO	4.0	4.0	3.0
								VOTO PROBABILIDAD	5.0	4.0	4.0
R3	[D] [BACKUPS]	R3	Destrucción de información	Procedimientos inadecuados para destrucción de medios	Medio	3.3	3.7	VOTO IMPACTO	4.0	4.0	3.0
								VOTO PROBABILIDAD	3.0	4.0	3.0
R4	[D] [BACKUPS]	R4	Fugas de información	Revelación por indiscreción	Alto	4.0	4.7	VOTO IMPACTO	5.0	5.0	4.0
								VOTO PROBABILIDAD	4.0	4.0	4.0
R5	[D] [BACKUPS]	R5	Repudio	Negación a posterior de actuaciones o compromisos adquiridos en el pasado	Medio	3.7	3.7	VOTO IMPACTO	3.0	4.0	4.0
								VOTO PROBABILIDAD	3.0	5.0	3.0
R6	[D] [BACKUPS]	R6	Modificación deliberada de la información	Alteración intencional de la información	Medio	2.7	3.3	VOTO IMPACTO	3.0	4.0	3.0
								VOTO PROBABILIDAD	2.0	3.0	3.0
R7	[D] [BACKUPS]	R7	Divulgación de información	Revelación de información	Alto	4.3	3.7	VOTO IMPACTO	4.0	3.0	4.0
								VOTO PROBABILIDAD	4.0	5.0	4.0
R8	[D] [SOURSE]	R8	Errores de los usuarios	Uso incorrecto de software y/o hardware	Medio	3.3	3.7	VOTO IMPACTO	4.0	4.0	3.0

								VOTO PROBABILIDAD	3.0	4.0	3.0
R9	[D] [SOURSE]	R9	Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	Bajo	1.3	2.0	VOTO IMPACTO	1.0	3.0	2.0
								VOTO PROBABILIDAD	1.0	2.0	1.0
R10	[D] [SOURSE]	R10	Errores de monitorización	Ausencia de control de cambios eficaz	Alto	4.0	4.0	VOTO IMPACTO	4.0	5.0	3.0
								VOTO PROBABILIDAD	4.0	4.0	4.0
R11	[D] [SOURSE]	R11	Errores de configuración	Introducción de datos de configuración erróneos	Bajo	1.7	2.3	VOTO IMPACTO	2.0	3.0	2.0
								VOTO PROBABILIDAD	1.0	2.0	2.0
R12	[D] [SOURSE]	R12	Alteración accidental de la información	Falta de conocimientos de los usuarios para realizar tareas especificas	Alto	4.0	4.0	VOTO IMPACTO	3.0	5.0	4.0
								VOTO PROBABILIDAD	4.0	4.0	4.0
R13	[D] [SOURSE]	R13	Abuso de privilegios de acceso	Falta de control de cierre de sesiones	Medio	2.7	3.3	VOTO IMPACTO	2.0	5.0	3.0
								VOTO PROBABILIDAD	2.0	3.0	3.0
R14	[D] [SOURSE]	R14	Acceso no autorizado	Desbordamiento de bufer o exploits	Medio	2.3	4.0	VOTO IMPACTO	3.0	5.0	4.0
								VOTO PROBABILIDAD	2.0	3.0	2.0
15	[D] [SOURSE]	R15	Repudio	Negación a posterior de actuaciones o compromisos adquiridos en el pasado	Alto	3.7	4.3	VOTO IMPACTO	4.0	5.0	4.0
								VOTO PROBABILIDAD	3.0	4.0	4.0
16	[D] [SOURSE]	R16	Modificación deliberada de la información	Alteración intencional de la información	Medio	2.7	3.7	VOTO IMPACTO	3.0	5.0	3.0
								VOTO PROBABILIDAD	2.0	3.0	3.0

Fuente: (2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8)
Elaboración: Autor

En la Ilustración 2, presenta el mapa de riesgos de los primeros 50 activos analizados en la sección anterior. De los cuales 10 están en la zona de riesgo alto (Zona Rosa), 30 en la zona de riesgo media (Zona Amarilla) y 10 están en la zona de riesgo baja (Zona Verde)

Ilustración 2 - Muestreo de mapa de riesgos



Elaboración: Autor

En la tabla 3, se presenta un muestreo de algunas de las salvaguardias para los riesgos encontrados de la tabla 2, basados en estándares de norma ISO-IEC 27001 de 2013.

Tabla 3 - Muestreo de salvaguardias

Tipificación Riesgo	Controles Sugeridos
R1	A.12.4.1 - Registro de eventos
R2	12.1.1 - Procedimientos documentados de operación
R3	11.2.7 - Seguridad en la reutilización o eliminación de los equipos
R4	A.13.2.4 - Acuerdos de confidencialidad o no divulgación A.7.2.3 - Procesos disciplinarios
R5	A.12.4.1 - Registro de eventos A.7.2.3 - Procesos disciplinarios
R6	A.12.4.1 - Registro de eventos A.7.2.3 - Proceso disciplinario
R7	A.13.2.4 - Acuerdos de confidencialidad o no divulgación A.7.2.3 - Procesos disciplinarios
R8	A.12.5.1 - Instalación de software en los sistemas operativos A.12.6.2 - Restricciones a la instalación de software
R9	A.12.4.3 - Registros del administrador y del operador
R10	A.12.4.1 - Registro de eventos
R11	A.12.4.1 - Registros de eventos
R12	12.1.1 - Procedimientos documentados de operación
R13	A.9.4.2 - Procedimientos seguros de inicio de sesión (log on)
R14	A.12.6.1 - Gestión de vulnerabilidades técnicas
R15	A.12.4.1 - Registro de eventos A.7.2.3 - Procesos disciplinarios
R16	A.12.4.1 - Registro de eventos A.7.2.3 - Proceso disciplinario

Fuente: (2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8)
Elaboración: Autor

Discusión

"Metodologías para el análisis de riesgos como: OCTAVE, MEHARI, MAGERIT, CRAMM, EBIOS y NIST SP 800-30, llegan a un mismo objetivo, con características propias y diferentes para las empresas en cada sector, contribuyendo una vez realizado un análisis de riesgos generar planes de contingencia y continuidad del negocio" (Tejena-Macías, 2018). Luego de revisado varios artículos similares se determinó que Magerit, es perfecta para nuestro estudio, debido a que se acopla con las necesidades de la EMAPAL-EP, permitiéndonos paso a paso identificar y realizar las tareas del análisis de riesgos, basados en los tres principios de seguridad de la CIA.

Conjuntamente con el análisis de riesgos, se puede utilizar estándares internacionales como el Cobit 5 o las familias de ISO - IEC 27000 y 31000, los cuales proporcionan lineamientos con buenas prácticas para dar soluciones a la protección de la seguridad de la información, en los cuales se puede basar la institución para tomar las mejoras decisiones para garantizar niveles aceptables de seguridad además de la documentación para los controles y posibles nuevos riesgos de la organización.

Conclusiones

Gracias a la revisión del protocolo y el entendimiento del estado del arte, nos ayudó a determinar la importancia de la ciberseguridad dentro de las organizaciones que manejan tecnologías informáticas para automatizar sus procesos.

Los resultados de la investigación ayudaron a reconocer los riesgos potenciales de la Empresa Pública Municipal de Agua Potable, Alcantarillado y Saneamiento ambiental del Cantón Azogues "EMAPAL-EP", con la aplicación de la metodología Magerit, la cual esta enfocada a instituciones gubernamentales.

Las amenazas encontradas con más peligro de sufrir ciberataques son: la información, servicios y los equipos de la empresa ya que no cuentan con la seguridad suficiente como salvaguardas o controles de seguridad, sin embargo, para el autor el activo más importante siempre será el ser humano, es decir los empleados que son los encargados de la administración y manejo de la información dentro de la empresa.

Se deberá realizar capacitaciones al personal de la empresa y en especial al área de Tics, acerca de temas de ciberseguridad, los cuales pueden ocasionar serios problemas de riesgos a la empresa.

Se deberá generar un departamento de ciberseguridad dentro de la institución.

Se deberá considerar contratar a personal para dedicarse exclusivamente para el trato de seguridad de la información, dentro de la institución, ya que a corto plazo será un problema muy serio, debido al aumento de los ciber atacantes cuyo tesoro más apreciado es la información.

Se deberá realizar un seguimiento al análisis de riesgos y vulnerabilidades, debido a que las vulnerabilidades cambian constantemente. Páginas como https://www.cvedetails.com/, nos ayudaran con esta tarea.

Es necesario realizar un estudio de costo beneficio para la adquisición de equipos o software que ayuden a mitigar los riesgos a los que está sometida la empresa.

Se deberá realizar auditorías para revisar el progreso del estudio.

"El Modelo de Auditoría de Ciberseguridad (CSAM), en un estudio de casos múltiples en una universidad canadiense. Se propone que el modelo se utilice para adelantar auditorías de ciberseguridad en cualquier organización o nación, y así evaluar la seguridad, su madurez y la preparación frente a la seguridad cibernética". (Sabillón & M., 2019)

El número de especialistas de ciberseguridad abastece la demanda del mismo. Según el estudio de Elías Carabaguíaz González "explica el proceso de investigación sobre las bases de aprendizaje

actuales respecto del tema de la seguridad informática, en comparación con la demanda actual de profesionales".(González, 2017)

Referencias

1. eluniversocom. (2021). CNT remplazó algunos equipos afectados por hackeo y otros se lograron reutilizar | Economía | Noticias | El Universo. https://www.eluniverso.com/noticias/economia/cnt-remplazo-algunos-equipos-afectados-por-hackeo-y-otros-se-lograron-reutilizar-nota/
2. Gilson Pilargote (Diario Expreso). (2021). Seguridad informática: teorías sobre la supuesta filtración de datos de usuarios del Banco Pichincha. 13/02/2021. https://www.expreso.ec/ciencia-y-tecnologia/banco-pichincha-hackeo-supuesto-hackers-seguridad-informatica-98823.html
3. González, E. C. (2017). Importancia del Aprendizaje de Ciberseguridad ante los Riesgos de las Tecnologías de Información. Tecnología Vital, 1(1). https://revistas.ulatina.ac.cr/index.php/tecnologiavital/article/view/56/57
4. MAGERIT 3.0: MÉTODO DE ANÁLISIS DE RIESGOS – Interpolados. (2020). https://interpolados.wordpress.com/2020/10/07/magerit-3-0-metodo-de-analisis-de-riesgos/
5. Sabillón, R., & M., J. J. C. (2019). Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, 32, 33–48. https://doi.org/10.17013/risti.32.33-48
6. Tejena-Macías, M. A. (2018). Análisis de riesgos en seguridad de la información. Polo Del Conocimiento, 3(4), 230. https://doi.org/10.23857/pc.v3i4.809