Revista Científica y Tecnológica UPSE

Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología Magerit

Contingency plan for the equipment and computer systems using the Magerit methodology

Enrique Ferruzola Gómez[1,*], Johanna Duchimaza S.[1], Johanna Ramos Holguín[1], María Fernanda Alejandro L.[2]

Universidad Agraria del Ecuador[1], Ecuador
Universidad Estatal Península de Santa Elena[2], Ecuador

Resumen

Las empresas necesitan un nivel alto de disponibilidad de la información, algunas requieren incluso un nivel incesante de la misma, sin esta disponibilidad resultaría difícil desempeñarse de manera eficaz. En caso de un desastre, la interrupción prolongada de los servicios de Tecnologías de Información puede llevar a pérdidas financieras significativas; perdiendo credibilidad y clientes, que repercuten en la mala imagen de la empresa. La investigación se desarrolla analizando la metodología Magerit, la cual permite el análisis y gestión de riesgos de los sistemas de información considerando su ubicación. Estos eventos, se manifiestan aún más en la vulnerabilidad física de las organizaciones situadas en zonas bajas, no solo ante inundaciones sino también ante sustracción de información o equipos como lo estarían las empresas situadas en zonas altas. Es habitual que las organizaciones tengan pérdidas debido a fallas o agresiones en sus sistemas de TI, los cuales afectan su nombradía. Este artículo expone mediante un análisis descriptivo, estándares y normas a considerar en la elaboración del plan de contingencia para equipos y sistemas informáticos, el análisis de gestión de riesgos, consecutivamente se expone cómo manejar la metodología Magerit y cómo utilizarla en el proceso de gobernabilidad de T.I.

Palabras clave:

Contingencia

Organizaciones

Magerit, desastres e información

Abstract

Companies need a high level of availability of information, some even require an unceasing level of information, without this availability it would be difficult to perform effectively. In the event of a disaster, the prolonged interruption of Information Technology services can lead to significant financial losses; losing credibility and customers, which result in the bad image of the company. The research is developed by analyzing the Magerit methodology, which allows the analysis and management of information systems risks considering their location. The above indicated; it is even more evident in the physical vulnerability of organizations located in low-lying areas, not only in the face of floods but also in the face of theft of information or equipment, as would companies located in high areas. It is common for organizations to have losses due to failures or aggressions in their IT systems, which affect their name. This article exposes, through a descriptive analysis, standards and norms to be considered in the elaboration of the contingency plan for computers and computer systems, the risk management analysis, consecutively is exposed how to handle the Magerit methodology and how to use it in the governance process of T.I.

Keywords:

Contingency

Organizations

Magerit, disasters and information

Recibido: *17 de diciembre de 2018* ***Aceptado:*** *12 de junio de 2019*

Forma de citar: Ferruzola, E., Duchimaza, J., Ramos, J., Alejandro, M. (2019). Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología Magerit. *Revista Científica y Tecnológica UPSE*, 6 (1), 34-41. DOI: 10.26423/rctu.v6i1.429

* *Autor para correspondencia.* *eferruzola@uagraria.edu.ec*

1. Introducción

Los procedimientos manuales de la mayoría de las organizaciones son prácticos por un corto período. En caso de existir interrupción prolongada de los servicios de Tecnologías de Información (TI) llevaría a pérdidas financieras significativas, incluyendo la pérdida de credibilidad de los clientes y del público en general, afectando la imagen corporativa de la empresa lo que llevaría a un fracaso total.

Cabe preguntarse ¿Por se necesita un plan de contingencia para desastres si existe una póliza de seguro para esta eventualidad?

La respuesta es que, si bien el seguro puede cubrir los costos materiales de los activos de las empresas en caso de un desastre, robo u otras amenazas, no servirá para recuperar la información almacenada perjudicando a la entidad.

El presente trabajo analiza la metodología Magerit, la cual permite el análisis y gestión de riesgos de los sistemas de información de las organizaciones o entidades públicas y privadas considerando la ubicación de la empresa. Existen organizaciones que están construidas en zonas bajas, cerca de ríos o mares lo que aumenta el riesgo para ellas por las frecuentes inundaciones que se están presentando ocasionadas por fuertes lluvias, desbordamiento de ríos, etc. haciendo vulnerable a las organizaciones situadas en esas zonas, además del riesgo de robo de información o de equipos a la que están expuestas la mayoría de las organizaciones.

Ante estos escenarios, sumados a los de desastres naturales mayores, existe la alta probabilidad de pérdidas potenciales o interrupciones no programadas de los recursos informáticos, por lo que es necesario que se desarrolle e implemente un Plan de Contingencia Informático que permita que las organizaciones cuenten con el acceso a sus sistemas informáticos de manera óptima y oportuna.

2. Materiales y Métodos

2.1. Metodología Magerit

Magerit es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión. La razón de ser de Magerit está directamente relacionada con la generalización del uso de las TI, que supone unos beneficios evidentes para los usuarios; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza. Interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, Magerit les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos (Abril, Jarol, & Bohada, 2013).

Magerit persigue los siguientes objetivos:

- Concientizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de gestionarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Preparar a la organización para procesos de evaluación, auditoria, certificación o acreditación, según corresponda en cada caso.

2.2. Ventajas de la metodología

- Las decisiones que deban tomarse y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente defendibles.
- Interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla.
- Permitirá saber cuánto valor tiene la información o los servicios que maneja la empresa y ayudará a protegerlos.
- Conocer el riesgo al que están sometidos los elementos de trabajo para poder gestionarlos.
- Tener una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

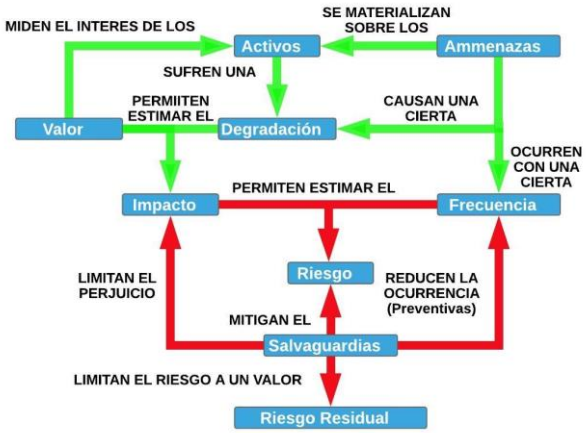

Figura 1. Proceso de la metodología Magerit

3. Análisis de Riesgos

En el análisis de riesgos se identifican y valoran los diversos elementos componentes del riesgo, obteniendo

una estimación de los umbrales de riesgo deseables (Chicano, 2014).

El análisis del riesgo contempla lo siguiente:

1. Identificación de activos de información.
2. Identificación de requerimientos legales y comerciales que son relevantes para los activos identificados.
3. Tasación de los activos identificados, considerando los requerimientos legales y comerciales, así como los impactos resultantes de una pérdida por confidencialidad, integridad y disponibilidad.
4. Identificación de amenazas y vulnerabilidades para cada activo previamente identificado.
5. Cálculo de la posibilidad de que las amenazas y vulnerabilidades ocurran.

Es sustancial deducir el requerimiento de la norma ISO 27001:2005 en relación con el riesgo. La exigencia es clara y no corresponde llevar a desaciertos. En primer lugar, se deben seguir los pasos para realizar el análisis del riesgo, y luego construir un nivel para determinar la evaluación del riesgo. Estos niveles son:

3.1. Inventario de activos

Un activo es algo que tiene valor o utilidad para la organización, sus operaciones comerciales y su continuidad, por esta razón; los activos necesitan tener protección para asegurar una correcta operación de la empresa y garantizar la prolongación en las operaciones.

Los activos de información son muy amplios y es importante estar conceptualmente claros en sus definiciones, para realizar un correcto análisis y una evaluación del riesgo. El proceso de identificación y tasación de activos debe realizarlo un grupo multidisciplinario compuesto por personas involucradas en los procesos y subprocesos que abarca el alcance del modelo. Es importante que los dueños de los activos principales conformen un grupo multidisciplinario. Como un dueño de activo se entiende aquella persona que tiene una responsabilidad por el control del mantenimiento, uso y seguridad de los activos, aprobada por la gerencia. Dentro del alcance del SGSI, los activos importantes deben identificarse con claridad, y posteriormente deben ser tasados para visualizar su impacto en la empresa por su deterioro o por fallas en: confidencialidad, integridad y disponibilidad (Fernández & Rivero, 2015).

3.2. Identificación de requerimientos legales y comerciales

Los requerimientos de seguridad en las organizaciones se derivan de tres fuentes:

1. La evaluación de los riesgos que afectan a las organizaciones. En esta fuente se determinan las amenazas de los activos, luego se ubican las vulnerabilidades, se evalúa su posibilidad de ocurrencia, y se estiman los potenciales impactos.
2. El aspecto legal, requerimientos contractuales que deben cumplirse.
3. El conjunto de principios, objetivos y requerimientos para procesar información, que la empresa ha desarrollado para apoyar sus operaciones. Al identificar los activos de información, se debe analizar si existen requerimientos legales y comerciales relacionados con estos activos identificados. De ser el caso, se debe revisar si dichos requerimientos involucran otros activos de información (Jáuregui, 2014).

3.3. Identificación de amenazas y vulnerabilidades

En las organizaciones, los activos de información están sujetos a distintas formas de amenazas. Una amenaza puede causar un incidente no deseado que genera daño a la organización y a sus activos.

Cuando la empresa inicia la identificación de amenazas que pudiesen afectar sus activos, conviene clasificarlas por su naturaleza, para así facilitar su ubicación. A continuación, mostramos seis tipos en los que se pueden clasificar las amenazas:

1. Amenazas naturales: inundaciones, tsunamis o maremotos, tornados, huracanes, sismos, tormentas, incendios forestales.
2. Amenazas a instalaciones: fuego, explosión, caída de energía, daño de agua, perdida de acceso, fallas mecánicas.
3. Amenazas humanas: huelgas, robos, epidemias, materiales peligrosos, problemas de transporte, pérdida de personal clave.
4. Amenazas tecnológicas: virus, hacking, pérdida de datos, fallas de hardware, fallas de software, fallas en la red, fallas en las líneas telefónicas.
5. Amenazas operacionales: crisis financieras, pérdida de proveedores, fallas en equipos, aspectos regulatorios, mala publicidad.
6. Amenazas sociales: motines, protestas, sabotaje, vandalismo, bombas, violencia laboral, terrorismo.

Las amenazas se pueden originar de fuentes o eventos accidentales. Para que una amenaza cause daño a algún activo de información tendría que explotar una o más vulnerabilidades del sistema, aplicaciones o servicios usados por la organización. Una vez identificadas las distintas amenazas que pueden afectar un activo, se debe evaluar su posibilidad de ocurrencia. Por cada amenaza, para medir su posibilidad de ocurrencia, se recomienda utilizar una escala de Likert, como la que se presenta a continuación en la ilustración (Navarro & González, 2015).

Tabla 1. Escala de Likert

1	2	3	4	5
Muy Bajo	Bajo	Medio	Alto	Muy alto

Las vulnerabilidades son debilidades de seguridad asociadas con los activos de información de una organización. Al tratar de definir las vulnerabilidades, la mejor manera es pensar en las debilidades del sistema de seguridad. Las vulnerabilidades no causan daño. Simplemente son condiciones que pueden hacer que una amenaza afecte un activo. Las vulnerabilidades pueden clasificarse como:

1. Seguridad de los recursos humanos: falta de entrenamiento en seguridad, carencia de toma de conciencia en seguridad, falta de mecanismos de monitoreo, falta de políticas para el uso correcto de las telecomunicaciones, no eliminar los accesos al término del contrato de trabajo, carencia de procedimiento que asegure la entrega de activos al término del contrato de trabajo, empleados desmotivados.
2. Control de acceso: segregación inapropiada de redes, falta de política sobre escritorio y pantalla limpia, falta de protección al equipo de comunicación móvil, política incorrecta para control de acceso, contraseñas sin modificarse.
3. Seguridad física y ambiental: Control de acceso físico inadecuado a oficinas, salones y edificios, ubicación en áreas sujeta a inundaciones, almacenes desprotegidos, carencia de programas para sustituir equipos, mal cuidado de equipos, susceptibilidad de equipos a variaciones de voltaje.
4. Gestión de operaciones y comunicación: Complicadas interfaces para usuarios, control de cambio inadecuado, gestión de red inadecuada, carencia de mecanismos que aseguren el envío y recepción de mensajes, carencia de tareas segregadas, carencia de control de copiado, falta de protección en redes públicas de conexión (Arjonilla & Medina, 2013).

4. Resultados

4.1. Actividades previas al desastre

Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de la información, las cuales nos asegurarán un proceso de recuperación para las organizaciones con el menor costo posible (Dettmer, 2006). A continuación, detallaremos las siguientes a realizar:

4.1.1. Establecimiento de plan de acción

En esta fase de planeamiento se establecen los procedimientos y normas a seguir relativos a:

a) Instalaciones físicas de la empresa

En caso de que se pueda suscitar un robo, sismo o incendio se deberían tomar las siguientes medidas preventivas:

Robos:

- Al entrar y salir de las instalaciones se deberá observar previamente que no exista ningún individuo sospechoso.
- Queda prohibido dar información personal de los empleados o información confidencial de la organización.
- Contar con personal para resguardo de las instalaciones de la empresa.
- Instalación de alarma.
- Contratar pólizas de seguros

Sismos:

- Ubicar y revisar periódicamente, que se encuentren en buen estado las instalaciones de agua, y sistema eléctrico.
- Fijar a la pared repisas, cuadros armarios, estantes, espejos y libreros. Evitar colocar objetos pesados en la parte superior de éstos, además asegurar al techo las lámparas.
- Debe de existir y ubicarse en un lugar de fácil acceso y visible los números telefónicos de emergencia y un botiquín, de ser posible un radio portátil y una linterna con pilas.
- Todo el personal debería portar siempre una identificación.
- Realizar simulacros de manera periódica.

Incendios:

- Estar siempre alerta. La mejor manera de evitar los incendios es la prevención.
- Procurar no almacenar productos inflamables.
- Cuidar que los cables de los aparatos eléctricos se encuentren en perfectas condiciones.
- No se deben realizar demasiadas conexiones en contactos múltiples, para evitar la sobre carga de los circuitos eléctricos.
- Por ningún motivo mojar las instalaciones eléctricas. Recuerde que el agua es un buen conductor de la electricidad.
- Todo contacto o interruptor debe tener siempre su tapa debidamente aislada.
- Antes de salir de la empresa la última persona en hacerlo, deberá revisar que los aparatos eléctricos estén apagados o perfectamente desconectados.
- Que esté prohibido fumar en las instalaciones de la empresa debido a que este hábito contaminante, no deja una buena impresión en los clientes y puede

causar desagrado ante los no fumadores o puede causar un incendio.

- Bajo ningún motivo se debe sustituir los fusibles por alambre o monedas, ni usar cordones eléctricos dañados o parchados.
- Contar con una alarma de incendios.
- Tener en un lugar visible y accesible un extintor contra incendios.
- Realizar simulacros de manera periódica.
- Debe de existir y ubicarse en un lugar de fácil acceso y visible los números telefónicos de emergencia y un botiquín.

b) Equipos de cómputo

Inventario actualizado de los equipos de manejo de información (computadoras, impresoras, etc.), especificando su contenido (software que usa) y su ubicación (Trujillo, 2011).

Las empresas podrían optar por la toma de una Póliza de Seguros Comerciales, como parte de la protección de los Activos Institucionales, pero haciendo la salvedad en el contrato, que, en caso de siniestros, la restitución del computador siniestrado se podrá hacer por otro de mayor potencia (por actualización tecnológica), siempre y cuando esté dentro de los montos asegurados (Vieites, 2014).

Se deberá realizar una señalización o etiquetado de los computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. Por ejemplo, etiquetar (colocar un sticker) de color rojo al Servidor, color amarillo a las computadoras con Información importante o estratégica y color verde a las computadoras de contenidos normales.

c) Obtención y almacenamiento de los respaldos de información (BACKUPS)

Se obtendrán copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los Sistemas o aplicativos de la Institución. Para lo cual se debe contar con:

- Backups del Sistema Operativo.
- Backups del Software Base - Paquetes y/o Lenguajes de Programación.
- Backups de Productos Desarrollados (Considerando tanto los programas fuentes, como los programas objetos correspondientes).
- Backups de los Datos (Bases de Datos, Índices, y todo archivo necesario para la correcta ejecución de los Productos Desarrollados).
- Backups del Hardware, mediante convenio con otra Institución que tenga equipos similares o mayores y que brinden la seguridad de poder continuar con las actividades para ser puestos a nuestra disposición, al ocurrir una contingencia y mientras se busca una solución definitiva al siniestro producido. Este tipo de convenios debe tener tanto las consideraciones de equipamiento como ambiente y facilidades de trabajo (Date, 2001).

4.2. Actividades durante el desastre

Una vez presentada la Contingencia o Siniestro, se deberán ejecutar las siguientes actividades, planificadas previamente:

4.2.1. Plan de emergencias

En este plan se establecen las acciones que se deben realizar cuando se presente un siniestro, así como la difusión de las mismas.

Es conveniente prever los posibles escenarios de ocurrencia del siniestro:

- Durante el día.
- Durante la noche o madrugada.
- Este plan deberá incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro, debiendo detallar:
- Vías de salida o escape.
- Plan de Evacuación del Personal. Plan de puesta a buen recaudo de los activos (incluyendo los activos de Información) de la Institución (si las circunstancias del siniestro lo posibilitan)
- Ubicación y señalización de los elementos contra el siniestro (extintores, etc.)
- Secuencia de llamadas en caso de siniestro, tener a la mano: elementos de iluminación (linternas), lista de teléfonos de Bomberos, Ambulancia, Jefatura de Seguridad y de su personal (equipos de seguridad) nombrados para estos casos.
- A continuación, detallamos ciertas normas sugeridas para el caso que se presente un siniestro, sea este robo, sismo o incendio que son los más comunes.

Robos:

Por ejemplo: El personal de Sudamericana de Software con el fin de resguardar su integridad, deberá tener en cuenta las siguientes recomendaciones:

- Mantener la calma: No resistirse, en especial si el criminal está armado o se nota que esté bajo el influjo de drogas.
- Inteligencia: Tratar de retener frases expresadas por el atacante y evitar mirarlo directo a los ojos para prevenir enfrentamientos.
- Memoria: Aprenderse el número de placas y características del automóvil en caso de que los agresores escapen en un vehículo.
- Sencillez: La gente debe evitar ser ostentosa y mantenerse atenta a lo que sucede a su alrededor.

Sismos:

Si el Sismo no es fuerte, tranquilícese, acabará pronto, si es fuerte, mantenga la calma, agudice la atención para evitar riesgos y recuerde las siguientes instrucciones:

- Si está dentro del edificio, quédese dentro, hasta poder salir calmadamente; si está fuera, permanezca fuera, buscando un área despejada.
- Dentro de un edificio busque estructuras fuertes: como por ejemplo una mesa, bajo el dintel de una puerta, junto a un pilar, pared maestra o en un rincón y proteja su cabeza.
- Apague todo fuego, con extintores. No utilice ningún tipo de llama (cerilla, encendedor, vela, etc.) durante o inmediatamente después del temblor.
- Fuera de un edificio, aléjese de cables eléctricos, cornisas, cristales, pretiles, etc.
- No se acerque ni penetre al edificio para evitar ser alcanzado por la caída de objetos peligrosos (cristales, cornisas, etc.) Vaya hacia lugares abiertos, no corra y cuidado con el tráfico.

Incendios:

- Conserve la calma: no grite, no corra, no empuje. Puede provocar un pánico generalizado. A veces este tipo de situaciones causan más muertes que el mismo incendio.
- Busque el extintor más cercano y trate de combatir el fuego. Si no sabe manejar el extintor, busque a alguien que pueda hacerlo por usted.
- Si el fuego es de origen eléctrico no intente apagarlo con agua.
- Cierre puertas y ventanas para evitar que el fuego se extienda, a menos que éstas sean sus únicas vías de escape.
- Al momento de abrir una puerta, verifique que la chapa no esté caliente antes de abrirla; sí lo está, lo más probable es que haya fuego al otro lado de ella, no la abra.
- En caso de que el fuego obstruya las salidas, no se desespere y colóquese en el sitio más seguro. Espere a ser rescatado.
- Si hay humo colóquese lo más cerca posible del piso y desplácese "a gatas". Tápese la nariz y la boca con un trapo, de ser posible húmedo.
- Si se incendia su ropa, no corra: tírese al piso y ruede lentamente. De ser posible cúbrase con una manta para apagar el fuego.

4.3. Actividades después del desastre

Después de ocurrido el siniestro o desastre es necesario realizar las actividades que se detallan en el Plan de contingencias establecido previo a su ejecución. Se deben tomar en cuenta los puntos que se detallan a continuación.

4.3.1. Evaluación de daños

Inmediatamente después que el siniestro ha concluido, se deberá evaluar la magnitud del daño que se ha producido, que sistemas se están afectando, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo (BID, 2010).

Para la evaluación de los daños se realizarán las preguntas o indagaciones necesarias por parte del equipo encargado de la vigilancia y/o supervisión del área en donde se produjo el siniestro.

El objetivo de establecer esta evaluación hace que los encargados de cada área puedan reconocer el tipo de desastre que se produjo sea este en el ámbito físico o lógico.

Cuando se obtengan los resultados de la evaluación realizada, el equipo encargado de la supervisión verificará en cuál de los puntos establecidos en el plan de contingencias encaja el siniestro.

Si se tratase de un desastre en el ámbito lógico se deben verificar los siguientes puntos:

- Para la información existente de la institución se debe verificar la calidad e integridad de la misma (hacer las pruebas sobre los programas que antes del desastre funcionaban correctamente)
- La calidad e integridad de la información de respaldo.
- En lo posible volver al estado original de la información antes del desastre (Jiménez, 2016).
- Si se tratase de un desastre en el ámbito físico se deben verificar los siguientes puntos:
- Por una Suspensión o caída del suministro eléctrico, el estado del hardware (Equipos de cómputo, Equipos de telecomunicaciones)
- Si se trata de un siniestro de fuerza mayor como son: incendios, inundaciones, maremotos, tornados, robo a la empresa; se deben seguir los lineamientos establecidos en el plan de contingencias para desastres de gran magnitud.

4.4. Priorización de actividades del plan de acción

Con la evaluación de daños reales y su comparación contra el Plan de acción, tendremos la lista de las actividades que debemos realizar, siempre priorizándola en vista a las actividades estratégicas y urgentes de la empresa.

Será muy importante el evaluar la dedicación del personal a las actividades que puedan no haberse afectado, para ver su asignación temporal a las actividades afectadas, en apoyo al personal de los sistemas afectados y soporte técnico.

4.5. Ejecución de actividades

Para la ejecución de actividades previamente planificadas en el Plan de acción se definen los siguientes equipos de trabajo:

Equipo de Salvaguarda de información

Equipo de Salvaguarda de hardware

Equipo de Salvaguarda de la empresa

Cada uno de estos equipos cuenta con un coordinador que deberá reportar diariamente el avance de los trabajos de recuperación y, en caso de producirse algún problema, reportarlo de inmediato a la jefatura a cargo del Plan de Contingencias.

Los trabajos de recuperación tendrán dos etapas, la primera la restauración del servicio usando los recursos de la Institución o local de respaldo, y la segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar el buen servicio de nuestro Sistema e imagen Institucional, como para no perjudicar la operatividad de la Institución o local de respaldo.

4.6. Evaluación de resultados

Una vez concluidas las labores de Recuperación del (los) sistema(s) que fueron afectados por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción y como se comportaron los equipos de trabajo.

De la evaluación de resultados y del siniestro en sí, darán como resultado dos tipos de recomendaciones, una la retroalimentación del plan de Contingencias y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionó el siniestro (Sosa & Hernández, 2007).

4.7. Retroalimentación del plan de acción

Con la evaluación de resultados, se debe optimizar el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente.

El otro elemento es evaluar cuál hubiera sido el costo de no haber tenido nuestra Institución el plan de contingencias llevado a cabo.

5. Discusión

Los resultados de esta investigación y la propuesta de la metodología Magerit para plan de contingencia de los equipos y sistemas informáticos para la gestión de seguridad de la información no pueden ser considerados como reglas generales o resultados definitivos que puedan ser replicados en cualquier empresa o proyecto debido a las metas estratégicas que plantean las diferentes empresas. Sin embargo, el principal aporte de esta investigación se ve reflejado en el uso de Magerit como un medio para potenciar un proyecto estratégico mediante el gobierno corporativo de TI, basado en el análisis de riesgo, la protección y uso adecuado de uno de los activos más importantes de una organización "La información". Esta característica difiere claramente de los enfoques de versiones anteriores de Magerit, en los cuales el principal punto de análisis se centraba en los procesos, dejando el análisis y gestión de riesgo para que sea tratado mediante otro marco de referencia con sus propios procesos.

El método de análisis presentado cuenta con una amplia aceptación en la industria de TI, debido a que están respaldados por varios estándares, y marcos de referencia; esta característica facilita que su utilización sea repetible en otros ambientes o empresas adaptándolos según sus propias necesidades.

6. Conclusiones

Mediante la elaboración de un plan de contingencia para los equipos tecnológicos dentro de un sistema informático, la utilización de la metodología MAGERIT es esencial para garantizar la seguridad de los datos o información. Esto es muy útil para las empresas que inician con la gestión de la seguridad de la información, ya que se basa en el análisis del impacto que puede tener ante alguna amenaza o catástrofe natural, logrando tener medidas preventivas y correctivas apropiadas para la seguridad de información.

Con la aplicación de la metodología Magerit a través del software se logra determinar cuáles son los procesos críticos que tengan las organizaciones y así determinar cuáles son las medidas que se deben tener en cuenta para mejorar y garantizar la seguridad, confidencialidad, integridad y disponibilidad de los procesos e información que se manejan en las organizaciones.

7. Bibliografía

1. Abril, A., Jarol, P., & Bohada, J. (2013). *Análisis de riesgos en seguridad de la información.* Tunjan, Colombia. Retrieved from http://www.revistasjdc.com/main/index.php/rciyt/article/view/292
2. Arjonilla, S., & Medina, J. (2013). *La gestión de los sistemas de información en la empresa: teoría y casos prácticos (3a. ed.).* Madrid: Difusora Larousse - Ediciones Pirámide.
3. BID. (2010). *Un tema del desarrollo: la reducción de la vulnerabilidad frente a lo desastres.* Madrid: BID.
4. Chicano, E. (2014). *Auditoría de seguridad informática (MF0487_3).* Antequera: IC Editorial.

5. Date, C. J. (2001). *Introducción a los sistemas de bases de datos.* México: Alhambra Mexicana.

6. Dettmer, J. (2006). *Educación y desastres: reflexiones sobre el caso de México.* México: Red Revista Latinoamericana de Estudios Educativos.

7. Fernández, L., & Rivero, P. (2015). *Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad.* Madrid: AENOR - Asociación Española de Normalización y Certificación.

8. Jáuregui, H. M. (2014). *Manual de aseguramiento de calidad ISO-9000.* Madrid: McGraw-Hill Interamericana.

9. Jiménez, J. A. (2016). *Evaluación: seguridad de un sistema de información.* Madrid: El Cid Editor | apuntes.

10. Navarro, E., & González, M. (2015). *La seguridad de los datos de carácter personal (2a. ed.).* Madrid: Ediciones Díaz de Santos.

11. Sosa, M., & Hernández, F. (2007). *Propuesta metodológica para la evaluación del riesgo en proyectos de inversión en tecnologías de información y comunicación.* Madrid: El Cid Editor.

12. Trujillo, M. (2011). *Planes de contingencias.* México: Ecoe Ediciones.

13. Vieites, Á. G. (2014). *Seguridad en equipos informáticos.* Madrid: RA-MA Editorial.