Dom. Cien., ISSN: 2477-8818
Vol. 5, núm. 3, julio 2019, pp. 317-342

DOI: 10.23857/dc.v5i3.937

Ciencias de la computación y telecomunicaciones

Artículo de investigación

Gestión de riesgos en la infraestructura de un centro de datos. Caso de estudio: Coordinación Zonal 6 Sur del Instituto Nacional de Estadística y Censos, Ecuador

Risk management in the infrastructure of a data center. Case study: Zonal 6 South Coordination of the National Institute of Statistic and Census, Ecuador

Gerenciamento de risco na infraestrutura de um data center. Estudo de caso: Zonal 6 Coordenação Sul do Instituto Nacional de Estatística e Censo, Equador

Elena del Rocío Vícuña-Altamirano [I]

edvicunaa@psg.ucacue.edu.ec

Martín Geovanny Zhindón-Mora [II]

mgzhindonm@ucacue.edu.ec

Recibido: 11 de abril de 2019 ***Aceptado:** 08 de junio de 2019 * **Publicado:** 05 de julio de 2019

[I] Ingeniera en Sistemas, Jefatura de Posgrados. Universidad Católica de Cuenca, Cuenca, Ecuador.

[II] Ingeniero en Sistemas, Jefe de Tecnologías de la Información, Jefatura de Posgrados, Universidad Católica de Cuenca, Cuenca, Ecuador.

Resumen

Las entidades gubernamentales deben cumplir con ciertas normativas, políticas, procesos, resoluciones, etc.; las cuales sirven para lograr objetivos institucionales. El realizar una gestión de riesgos sobre los activos que posee una organización, ayuda a alcanzar dichos objetivos y a la continuidad del negocio.

Las normas de la familia 31000 del Instituto Ecuatoriano de Normalización, están enfocadas a la gestión de riesgos, combinadas con una metodología apropiada, como MAGERIT, permitiendo a la Institución identificar sus activos principales, las amenazas y su evaluación, en base al impacto y probabilidad o frecuencia de ocurrencia para definir un nivel de riesgo, siendo los más altos, los prioritarios, ya que cumplen con ciertas condicionantes para realizar salvaguardas, las cuales posteriormente deben ser medidas, dándoles su respectivo seguimiento y monitoreo, para que sus resultados esperados sean comparados con los obtenidos.

Es necesario contar con una gestión de riesgos para la infraestructura del centro de datos de la Coordinación Zonal 6 Sur, para el alcance de sus objetivos institucionales y continuidad de negocio, motivo por el cual, en el presente artículo se desarrolla una metodología basada en las normas de gestión de riesgo INEN, en combinación con una de las metodologías más utilizadas por su nivel de madurez (MAGERIT), que permiten gestionar el riesgo en la infraestructura del centro de datos en cuanto a sus activos de forma asertiva por su rapidez y eficacia.

Palabras clave: centro de datos; gestión de riesgo; normas INEN; metodología MAGERIT; amenaza; vulnerabilidad; salvaguarda.

Abstract

Government entities must comply with certain regulations, policies, processes, resolutions, etc. .; which serve to achieve institutional objectives. Carrying out a risk management on the assets that an organization possesses, helps to achieve said objectives and the continuity of the business.

The standards of the 31000 family of the Ecuadorian Institute of Normalization, are focused on risk management, combined with an appropriate methodology, such as MAGERIT, allowing the Institution to identify its main assets, threats and their evaluation, based on the impact and probability or frequency of occurrence to define a level of risk, the highest being the priority ones, since they meet certain conditions to carry out safeguards, which subsequently must be measured, giving them their respective monitoring and monitoring, so that their expected results are compared with the obtained ones

It is necessary to have a risk management for the infrastructure of the data center of the Zonal Coordination 6 South, for the scope of its institutional objectives and business continuity, which is why, in this article, a methodology based on the risk management standards INEN, in combination with one of the most used methodologies for their level of maturity (MAGERIT), which allow managing the risk in the infrastructure of the data center in terms of its assets assertively for its speed and efficiency .

Keywords: data center; risk management; INEN standards; MAGERIT methodology; threat; vulnerability; Safeguard.

Resumo

As entidades governamentais devem cumprir certos regulamentos, políticas, processos, resoluções, etc. que servem para alcançar objetivos institucionais. Realizar uma gestão de risco sobre os ativos que uma organização possui, ajuda a atingir os objetivos e a continuidade do negócio.

Os padrões da família 31000 do Instituto Equatoriano de Normalização, estão focados na gestão de riscos, combinados com uma metodologia adequada, como a MAGERIT, permitindo que a Instituição identifique seus principais ativos, ameaças e sua avaliação, com base no impacto e na probabilidade ou frequência de ocorrência para definir um nível de risco, sendo os mais altos os prioritários, pois preenchem determinadas condições para a realização de salvaguardas, que posteriormente devem ser medidas, proporcionando-lhes o respectivo monitoramento e monitoramento, para que os resultados esperados sejam comparados com os obtidos

É necessário ter uma gestão de risco para a infraestrutura do data center da Coordenação Zonal 6 Sul, para o alcance de seus objetivos institucionais e continuidade de negócio, razão pela qual, neste artigo, uma metodologia baseada na as normas de gestão de risco INEN, em combinação com uma das metodologias mais utilizadas para seu nível de maturidade (MAGERIT), que permitem gerenciar o risco na infraestrutura do data center em termos de seus ativos assertivamente por sua velocidade e eficiência .**Palavras-chave:** centro de dados; gerenciamento de risco; Padrões INEN; Metodologia MAGERIT; ameaça vulnerabilidade; Salvaguardar.

Introducción

En el Ecuador se ha evidenciado una tendencia de crecimiento con respecto al acceso a Internet mediante la utilización de computadores y dispositivos móviles (INEC, 2016), debido al incremento de proveedores con costos accesibles para satisfacer las necesidades de comunicación, presencia, transacciones, conectividad, entre algunas de las principales razones de usuarios y empresas. Por lo que empresas de diferentes actividades comerciales, tamaños, públicas o privadas están proclives a riesgos internos y/o externos especialmente relacionados con el aspecto tecnológico. Los activos que poseen las empresas constituyen parte fundamental para alcanzar sus objetivos, además de agregar valor a la organización. Entre estos activos se encuentra la información que en la actualidad se ha convertido en un elemento fundamental (Galván., 2013), y exige una gobernanza corporativa lo que conlleva a que la información contenida en el centro de datos tenga una gobernanza de Tecnologías de la Información (TI),para la continuidad del negocio (Pérez, Puentes, & Yesica María, 2015).

Al igual que en otros países, en el Ecuador todas sus entidades gubernamentales debe aplicar las normas técnicas ecuatorianas vigentes proporcionadas por el Instituto Nacional Ecuatoriano de Normas (INEN), en cuanto a la seguridad de la información se cuenta en el sector público con la aplicación del Esquema Gubernamental de Seguridad de la Información (EGSI) el cual se basa en la normativa ISO 27000 y que establece un conjunto de directrices prioritarias para gestión de la seguridad de la información e inicia un proceso de mejora continua en las instituciones de administración pública mediante un proceso

sistemático, documentado y conocido por toda la organización para garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno, actores principales, actores secundarios y las tecnologías (Secretaria Nacional de Administración Pública, 2013).

El Instituto Nacional de Estadística y Censos (INEC), es el órgano rector de la estadística nacional y el encargado de generar las estadísticas oficiales del Ecuador para la toma de decisiones en la política pública. Está compuesto por Administración Central, Coordinación Zonal Centro 3, Coordinación Zonal Litoral 8 y la Coordinación Zonal 6 Sur. Las Coordinaciones Zonales tienen la misión de coordinar los procesos, actividades técnicas y administrativas que permitan el levantamiento, supervisión, control y funcionamiento óptimo de las operaciones estadísticas asignadas; posee una estructura organizacional diferente a la de Administración Central, posee unidades de gestión y son descentralizadas. La Coordinación Zonal 6 Sur del INEC, actualmente no cuenta con una gestión de riesgos enfocada a la infraestructura de sus centros de datos (INEC, 2015).

Y ésta, al formar parte de la institución gubernamental responsable de la estadística oficial del país, es imprescindible garantizar la continuidad y disponibilidad de servicios tecnológicos para el desarrollo normal de actividades y la seguridad de datos e infraestructura, a partir de una evaluación de la situación actual de la infraestructura de su centro de datos; identificando sus activos con sus respectivas vulnerabilidades y posibles amenazas, para realizar una valoración de riesgos existentes y sugerir las salvaguardas necesarias para el tratamiento de los mismos, además de aplicar cíclicamente una mejora continua de la gestión del riesgo, comunicación y seguimiento con sus respectivos informes para comparación y análisis, entorno (Vargas Borbúa, Reyes Chicango, & Recalde Herrera, 2017). Desarrollar la capacidad de seguridad frente a ataques y la mitigación de los riesgos, con el fin de garantizar protección y disponibilidad al consumidor virtual de la información a través de infraestructura

confiable en esta era digital (Ministerio de Telecomunicaciones y de la Sociedad de la Información - Secretaría de Educación Superior Ciencia Tecnología e Innovación, 2019).

El problema científico planteado se fundamentó en que, debido a que no se cuenta con una gestión de riesgos en la infraestructura de su centro de datos en la Coordinación Zonal 6 Sur del INEC, la unidad de Gestión de Tecnologías de la Información y Comunicación Zonal (GTICZ), y la alta gerencia, no poseen una guía que permita determinar la acción de gestión apropiada y las prioridades para manejar los riesgos e implementar controles seleccionados para protegerse contra ellos o mitigarlos.

El objetivo del presente artículo se basó en desarrollar una metodología para una gestión de riesgos de la infraestructura de su centro de datos de la Coordinación Zonal 6 Sur del INEC.

Es fundamental contar con una gestión de riesgos en la infraestructura del centro de datos de la Coordinación Zonal 6 Sur del INEC, para garantizar el cumplimiento del objetivo estratégico institucional mediante la continuidad del negocio que brinda su centro de datos (Galván., 2013).

Adicionalmente, es importante identificar y desarrollar una metodología como guía para una adecuada integración entre leyes, reglamentos, normativas, procedimientos y acciones para una gestión de riesgos en la infraestructura de un centro de datos en una entidad gubernamental, en este caso de estudio de la Coordinación Zonal 6 Sur del INEC.

Introducción

En el Ecuador se ha evidenciado una tendencia de crecimiento con respecto al acceso a Internet mediante la utilización de computadores y dispositivos móviles (INEC, 2016), debido al incremento de proveedores con costos accesibles para satisfacer las necesidades de comunicación, presencia, transacciones, conectividad, entre algunas de las principales razones de usuarios y empresas. Por lo que empresas de diferentes actividades comerciales, tamaños, públicas o privadas están proclives a riesgos internos y/o externos especialmente relacionados con el aspecto tecnológico. Los activos que poseen las

empresas constituyen parte fundamental para alcanzar sus objetivos, además de agregar valor a la organización. Entre estos activos se encuentra la información que en la actualidad se ha convertido en un elemento fundamental (Galván., 2013), y exige una gobernanza corporativa lo que conlleva a que la información contenida en el centro de datos tenga una gobernanza de Tecnologías de la Información (TI),para la continuidad del negocio (Pérez, Puentes, & Yesica María, 2015).

Al igual que en otros países, en el Ecuador todas sus entidades gubernamentales debe aplicar las normas técnicas ecuatorianas vigentes proporcionadas por el Instituto Nacional Ecuatoriano de Normas (INEN), en cuanto a la seguridad de la información se cuenta en el sector público con la aplicación del Esquema Gubernamental de Seguridad de la Información (EGSI) el cual se basa en la normativa ISO 27000 y que establece un conjunto de directrices prioritarias para gestión de la seguridad de la información e inicia un proceso de mejora continua en las instituciones de administración pública mediante un proceso sistemático, documentado y conocido por toda la organización para garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno, actores principales, actores secundarios y las tecnologías (Secretaria Nacional de Administración Pública, 2013).

El Instituto Nacional de Estadística y Censos (INEC), es el órgano rector de la estadística nacional y el encargado de generar las estadísticas oficiales del Ecuador para la toma de decisiones en la política pública. Está compuesto por Administración Central, Coordinación Zonal Centro 3, Coordinación Zonal Litoral 8 y la Coordinación Zonal 6 Sur. Las Coordinaciones Zonales tienen la misión de coordinar los procesos, actividades técnicas y administrativas que permitan el levantamiento, supervisión, control y funcionamiento óptimo de las operaciones estadísticas asignadas; posee una estructura organizacional diferente a la de Administración Central, posee unidades de gestión y son descentralizadas. La Coordinación Zonal 6 Sur del INEC, actualmente no cuenta con una gestión de riesgos enfocada a la infraestructura de sus centros de datos (INEC, 2015).

Y ésta, al formar parte de la institución gubernamental responsable de la estadística oficial del país, es imprescindible garantizar la continuidad y disponibilidad de servicios tecnológicos para el desarrollo normal de actividades y la seguridad de datos e infraestructura, a partir de una evaluación de la situación actual de la infraestructura de su centro de datos; identificando sus activos con sus respectivas vulnerabilidades y posibles amenazas, para realizar una valoración de riesgos existentes y sugerir las salvaguardas necesarias para el tratamiento de los mismos, además de aplicar cíclicamente una mejora continua de la gestión del riesgo, comunicación y seguimiento con sus respectivos informes para comparación y análisis, entorno (Vargas Borbúa, Reyes Chicango, & Recalde Herrera, 2017). Desarrollar la capacidad de seguridad frente a ataques y la mitigación de los riesgos, con el fin de garantizar protección y disponibilidad al consumidor virtual de la información a través de infraestructura confiable en esta era digital (Ministerio de Telecomunicaciones y de la Sociedad de la Información - Secretaría de Educación Superior Ciencia Tecnología e Innovación, 2019).

El problema científico planteado se fundamentó en que, debido a que no se cuenta con una gestión de riesgos en la infraestructura de su centro de datos en la Coordinación Zonal 6 Sur del INEC, la unidad de Gestión de Tecnologías de la Información y Comunicación Zonal (GTICZ), y la alta gerencia, no poseen una guía que permita determinar la acción de gestión apropiada y las prioridades para manejar los riesgos e implementar controles seleccionados para protegerse contra ellos o mitigarlos.

El objetivo del presente artículo se basó en desarrollar una metodología para una gestión de riesgos de la infraestructura de su centro de datos de la Coordinación Zonal 6 Sur del INEC.

Es fundamental contar con una gestión de riesgos en la infraestructura del centro de datos de la Coordinación Zonal 6 Sur del INEC, para garantizar el cumplimiento del objetivo estratégico institucional mediante la continuidad del negocio que brinda su centro de datos (Galván., 2013).

Adicionalmente, es importante identificar y desarrollar una metodología como guía para una adecuada integración entre leyes, reglamentos, normativas, procedimientos y acciones para una gestión de riesgos

en la infraestructura de un centro de datos en una entidad gubernamental, en este caso de estudio de la Coordinación Zonal 6 Sur del INEC.

Tabla 1 Matriz de diagnóstico de nivel de cumplimiento de normas y metodología de gestión de riesgos

Criterio de diagnóstico	**Variables**	**Nombre del Indicador**	**Técnicas**	**Fuentes de información**	**Tipo de valor**
			Numerador o dato	**Denominador**	**Cuantitativo**
Evaluar la cantidad de principios adoptados según norma ISO 31000:2018	Principios, marco de referencia en la CZ6S	Cumplimiento de Normas ISO 31000:2018	Número de principios y marco de referencia de la CZ6S acordes a los principios de la norma ISO 31000:2018	Total de principios y marco de referencia de la norma ISO 31000:2018	Porcentaje
			0	**8**	**0%**

La tabla 1 muestra el porcentaje de cumplimiento de normas 31000, de la metodología MAGERIT y el porcentaje total final.

Pasos en la CZ6S	Cumplimiento de MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información	Número de pasos de la CZ6S acordes a MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información	Total de pasos de MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información	Porcentaje
		1	**3**	**33%**
			Total porcentaje de cumplimiento de normas 31000 y MAGERIT v 3.0	**33%**

Metodología

El desarrollo del presente trabajo de investigación se lo realizará por fases, siendo como primera la recopilación de información para un diagnóstico superficial del tipo empírico de la gestión de riesgo en la infraestructura del centro de datos de la Coordinación Zonal 6 Sur del INEC.

Y la segunda fase el uso de una metodología cualitativa con un alcance descriptivo, la investigación de campo se realizó con fundamento en las normas técnicas orientadas para la gestión de riesgo del INEN

combinada con la metodología de análisis y gestión de riesgos MAGERIT, permitirán el establecer los principios básicos y el marco de gestión de riesgos, la identificación de activos, la definición y valoración de amenazas, una propuesta y evaluación de salvaguardas, cálculo del impacto residual y riesgo residual, el seguimiento y revisión, finalmente un registro e informe para las partes interesadas.

Resultados

Inicialmente, se debe incrementar un principio acorde a la información estadística que genera, este es: gestión del riesgo a nivel de toda la organización para asegurar los activos tecnológicos, además, garantizar y proteger uno de los activos más importantes para la Coordinación Zonal 6 Sur del INEC, sus datos estadísticos.

Identificación de activos

Para recaudar la información de los activos de la infraestructura del centro de datos de la Coordinación Zonal 6 Sur, se realizó un levantamiento de los mismos mediante observación, registrándolos en una matriz por tipo de activo y activo tecnológico, referidos a los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios (Consejo Superior de Administración Electrónica, 2012) cotejando con la información preliminar con la que cuenta la Coordinación Zonal 6 Sur del INEC.

Definición y valoración de amenazas

Una vez que se identificaron los activos que forman parte de la infraestructura del centro de datos, se determinaron las amenazas en cada activo, el impacto, la probabilidad para determinar el nivel de riesgo, de acuerdo a la tabla de escalas cualitativas, tabla 2, con análisis cualitativo, mediante el establecimiento de una escala de calificación de atributos para describir la magnitud de las consecuencias potenciales y la probabilidad de que se produzcan estas consecuencias.

Tabla 2. Escalas cualitativas de impacto, probabilidad o frecuencia y riesgo

Impacto	Probabilidad	Riesgo
MA: muy alto	MA: prácticamente seguro (1 vez a la semana)	MA: crítico
A: alto	A: probable (1 vez trimestral)	A: importante
M: medio	M: posible (al menos 1 vez al año)	M: apreciable
B: bajo	B: poco probable (1 vez cada tres años)	B: bajo
MB: muy bajo	MB: muy raro (1 vez cada cinco años)	MB: despreciable

La tabla 2 muestra las escalas cualitativas de impacto, probabilidad y riesgo.

El análisis cualitativo es recomendable realizarlo cuando recién se está implementando la gestión del riesgo, con una escala de calificación de atributos, para describir la magnitud de las consecuencias potenciales y la probabilidad de que se produzcan estas consecuencias, que en combinación determinan el riesgo, como se muestra en la tabla 3.

Tabla 3. Combinación del impacto y probabilidad para calcular el riesgo

		Probabilidad				
Riesgo		MB	B	M	A	MA
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

La tabla 3 muestra la combinación del impacto y frecuencia o probabilidad para calcular el riesgo en la matriz. (Consejo Superior de Administración Electrónica, 2012).

En cuanto a las amenazas se consideró que, si son de origen natural, acordes al entorno, como: contaminación, fallos eléctricos, etc., defectos de las aplicaciones originalmente en su diseño o en su implementación, vulnerabilidades técnicas o, simplemente, 'vulnerabilidades'. Otras amenazas causadas por las personas de forma accidental, típicamente por error o por omisión y de forma deliberada por cada activo con sus respectivas amenazas, determinando su impacto y probabilidad para obtener el nivel de riesgo del resultado de su combinación.

Otro punto importante se centró en identificar los activos más significativos y sujetos a mayor riesgo, su valor, las amenazas más relevantes y determinar sus tipos, para luego priorizarlos, por lo que deben ser ordenados por su nivel más alto, omitiendo las amenazas no relevantes.

Propuesta y evaluación de salvaguardas

Las salvaguardas planteadas han sido elegidas de acuerdo a la metodología de MAGERIT. Cada acción de protección tiene un costo, por lo que se debe analizar si el valor a emplear en la salvaguarda es justificable comparando el costo del activo, con el costo del impacto de la pérdida del activo. Además, es prudente establecer un principio de proporcionalidad salvaguardando lo más valioso y obviando lo irrelevante, tomando en cuenta que no todas las salvaguardas pueden ser aplicables y/o justificables, tomando en cuenta que el valor monetario no exceda el valor del activo, siendo mejor su reemplazo antes que su protección, dando como resultado la "declaración de aplicabilidad". Mediante la selección de la o las mejores opciones para el tratamiento del riesgo, en un balance entre costo-beneficio, esfuerzo y/o desventajas de implementación sean acordes a las obligaciones, compromisos y los puntos de vista de las partes interesadas, a los objetivos, los criterios del riesgo y los recursos disponibles de la organización, con la siguiente escala como muestra la tabla 4.

Tabla 4. Eficacia y madurez de salvaguardas

Factor	Nivel
0%	L0: inexistente
	L1: inicial
	L2: reproducible, pero intuitivo
	L3: proceso definido
	L4: gestionado y medible
100%	L5: optimizado

La tabla 4 muestra el nivel de eficacia y madurez de las salvaguardas. (Consejo Superior de Administración Electrónica & Amutio Gómez, 2012).

A través de análisis de las salvaguardas y su madurez se debe fijar el nivel de la salvaguarda actual con respecto al objetivo que se pretende lograr.

En el nivel L0 se consideran a los procedimientos inexistentes y que no han sido evaluados, tales como acciones inmediatas requeridas como adquisiciones de equipos tecnológicos, conexiones, colocaciones, además desarrollo de planes de control y de mantenimientos/limpiezas.

Los niveles L1 y L2 son procedimientos existentes, pero aún faltan mejorarse, tales como el aseguramiento de equipos, cambios de repuestos, configuraciones de respaldo, desarrollo de planes de aplicación de garantía para los equipos, planes de emergencia, planes de contingencia, pruebas de funcionamiento, simulacros, entre los principales.

Por otro lado, los niveles L3 y L4 son aquellos procedimientos que están siendo implementados de forma correcta y que podrían optimizarse, entre los cuales están los planes de mantenimiento/limpieza y mantenimientos preventivos de equipos tecnológicos. Por último, el nivel L5 son los procedimientos optimizados, probados y comparables, en este caso no hay ninguno, como muestra la tabla 5.

Tabla 5. Nivel de madurez de salvaguardas actuales por riesgos agrupados

	Nivel de salvaguardas actuales					
Riesgos agrupados	L0	L1	L2	L3	L4	Total de salvaguardas por riesgos
Agotamiento de baterías		2				2
Agotamiento de nitrógeno en climatizador	1		2			3
Agotamiento de químicos en extinguidores para equipo electrónico		1	2			3
Algún tipo de plaga (insectos, roedores, etc.)	14		1	3	2	20
Corto circuito			7			7
Defecto de fábrica	1	6	18			25
Desconexión física	7	9				16
Falla de biométrico	1		1			2
Falla de cableado de red				1		1
Falla de cableado eléctrico			1			1
Falla de equipo	2	1	9			12

Falla de extintor	1					1
Falla de luces de emergencia	1					1
Falla de rack			1			1
Falla de suministro de energía eléctrica	11	1				12
Incendio		14				14
Inundación		14				14
Robos		1				1
Terremoto		15				15
Total salvaguardas por nivel	39	64	42	4	2	151

preventivas que pueden impedir completamente que la amenaza se materialice, otras limitan la degradación, algunas detectan inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye, pero siempre existirá riesgo residual y un impacto residual que debe ser medido.

Impacto residual y riesgo residual

Según la metodología MAGERIT al modificar el impacto y el riesgo, van de un valor potencial a uno residual, donde se mantienen los activos, sus dependencias, la magnitud de degradación es la cambiante dependiendo de la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real, debe ser calculada nuevamente en el riesgo residual y se mantienen los activos, sus dependencias, la magnitud de degradación y la probabilidad de amenazas. Para el cálculo se utiliza el impacto residual y la probabilidad residual, todo esto por cada activo considerado en la infraestructura del centro de datos.

El impacto y riesgo residual pueden ser cualitativos, hasta que aparecen grandes inversiones y hay que determinar su justificación económica, por lo que se requiere pasar a cuantitativo, pudiendo emplear rangos por montos, en el presente caso de estudio se reserva el valor monetario de los activos por lo que se establecerá con escalas numéricas, de acuerdo a cada activo considerado en la infraestructura del centro de datos de la Coordinación Zonal 6 Sur del INEC, por cada salvaguarda a emplearse por el activo se debe evaluar la disminución en impacto o degradación, tomando como límite el impacto inicial evaluado dándole un peso a la efectividad de salvaguarda, tabla 6, para el cálculo del impacto residual.

Posteriormente, se debe dar un peso al riesgo calculado anteriormente (riesgo = impacto * probabilidad), de acuerdo a la tabla 7, se debe estimar la probabilidad o frecuencia de ocurrencia de la amenaza que se está tratando, para que corresponda a un peso la efectividad de acuerdo a la probabilidad, tabla 8, para el cálculo del riesgo residual.

Se puede determinar con los resultados obtenidos que, a mayor disminución del impacto, menor impacto residual en comparativa con el impacto inicial. En consecuencia, a menor probabilidad en la sucesión de una amenaza tomando en cuenta la efectividad de la salvaguarda, menor riesgo residual en comparación al riesgo inicial.

Tabla 6. Escala para determinación de la disminución del impacto

Descripción	Abreviatura	Valor
Muy alta disminución del impacto	MA	5
Alta disminución del impacto	A	4
Media disminución del impacto	M	3

Baja disminución del impacto	B	2
Muy baja disminución del impacto	MB	1

Tabla 7. Escala para la determinación del riesgo previamente calculado en la definición y valoración de las amenazas por activo

Descripción	Abreviatura	Valor
Crítico el riesgo	MA	5
Importante el riesgo	A	4
Apreciable el riesgo	M	3
Bajo el riesgo	B	2
Despreciable o insignificante el riesgo	MB	1

Tabla 8. Escala para la determinación de la probabilidad de amenaza en base a aplicación de salvaguarda(s) y el riesgo previamente calculado.

Descripción	Abreviatura	Valor
prácticamente seguro (1 vez a la semana)	MA	5
probable (1 vez trimestral)	A	4
posible (al menos 1 vez al año)	M	3
poco probable (1 vez cada tres años)	B	2
muy raro (1 vez cada cinco años)	MB	1

Seguimiento y revisión

Es necesario asegurar y mejorar la calidad y la eficacia del diseño, la implementación y los resultados en todas etapas del proceso para la gestión del riesgo del centro de datos, incluyendo planificar, recopilar y analizar información, registrar resultados y proporcionar retroalimentación, sus resultados deben incorporarse a todas las actividades de la gestión del desempeño, de medición y de informe de la organización.

Los resultados obtenidos en el cálculo del impacto residual y del riesgo residual por cada activo considerado en la infraestructura del centro de datos de acuerdo a las salvaguardas, contiene un análisis completo de los riesgos por cada activo considerado en la Coordinación Zonal 6 Sur del INEC, permite decidir realizar o no las salvaguardas, y hasta qué punto disminuirían, atenuarían o eliminarían los riesgos, en caso de aplicarlas que efectos se tendrían para la toma de decisiones, entrando en un proceso cíclico para una gestión de riesgos.

Es recomendable realizar una auditoría mediante un proceso de revisión sistemática, basada en evidencia frente a criterios predeterminados. Si bien toda auditoría es una revisión, no toda revisión es una auditoría. Asegura que se gestione el riesgo para lo que debe contarse con un programa integral para monitorear y registrar los indicadores de desempeño del riesgo, que se alinean con los indicadores de desempeño de la organización, con advertencias de forma temprana, los indicadores de impacto y riesgo deben estar bajo continuo monitoreo por la realidad cambiante.

Registro e informe

Por último, siempre es importante realizar un registro e informe, cuyo propósito es el documentar e informar a través de los mecanismos apropiados a las partes involucradas pertinentes. Su creación, conservación y tratamiento de la información documentada es una parte integral de la gobernanza de la organización y debería mejorar la calidad del diálogo con las partes interesadas, apoyar a la alta dirección y a los órganos de supervisión a cumplir sus responsabilidades, además sirve para dar seguimiento y como fuente de verificación.

Este debe ser de utilidad y concreto para la alta dirección y partes interesadas, mostrando la situación actual, su análisis, comparativos, correcciones y recomendaciones para el monitoreo y mejora continua, siendo mucho mejor utilizar plantillas para ser mejoradas, manteniendo homogeneidad, y, conteniendo tanto una parte técnica como una gerencial, para facilitar la toma de decisiones con fundamentos que las justifiquen.

Conclusiones

La aplicación de una metodología de análisis de riesgos como MAGERIT garantiza una adecuada gestión de riesgos de la infraestructura del centro de datos de la Coordinación Zonal 6 Sur del INEC.

A futuro se puede escalar la gestión de riesgos a la infraestructura del centro de datos de la Coordinación Zonal 6 Sur del INEC en las otras coordinaciones zonales del INEC y en entidades gubernamentales por cumplir con la normativa vigente.

Los beneficios de una adecuada gestión de riesgos en la infraestructura del centro de datos de la Coordinación Zonal 6 Sur del INEC, reditúa en menores costos de administración, mantenimiento y adquisición de equipos, pérdida de recursos, entre otras razones; además permite realizar actividades estratégicas, de pronóstico, monitoreo, un mejor control operativo, lo cual genera por ende mayor confianza y permite establecer niveles de disponibilidad y calidad de procesos, actividades, servicios, etc.

El aplicar la metodología probada como MAGERIT permite a las organizaciones a establecer su estrategia, lograr sus objetivos y tomar decisiones matemáticamente lógicas a partir de información precisa, oportuna y actualizada. En combinación con las normas INEC de la familia 31000 para una gestión de riesgos adecuada al tipo de entidad.

Referencias Bibliográficas

Agencia de Regulación y Control de Electricidad. (2015). Plan Integral de Respuesta a Emergencias (p. 86). p. 86. Retrieved from https://www.regulacionelectrica.gob.ec/wp-content/uploads/downloads/2015/12/Plan-Integral-de-Respuesta-a-Emergencias-PIRE.pdf

Arteaga-Martínez, M. M. (2017). Gestión de riesgos de TI. Documentos de Docencia, 3(0). https://doi.org/https://doi.org/10.16925/greylit.2073

Consejo Superior de Administración Electrónica. (2012a). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. 75. Retrieved from administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8/2012_Magerit_v3_libro2_catalogo de elementos_es_NIPO_630-12-171-8.pdf%0Ahttp:/

Consejo Superior de Administración Electrónica. (2012b). MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas. Retrieved from http://administracionelectronica.gob.es/ctt/resources/Soluciones/184/Area descargas/Libro-III-Guia-de-Tecnicas.pdf?idIniciativa=184&idElemento=87&idioma=en

Contraloría General del Estado Ecuatoriano. (2018). Reglamento Administración Y Control De Bienes Del Sector Público (pp. 1–39). pp. 1–39. Retrieved from www.lexis.com.ec

Contraloría General del Estado Ecuatoriano. (2019). Normas De Control Interno Para El Sector Público De La República Del Ecuador (pp. 1–101). pp. 1–101. Retrieved from http://www.contraloria.gob.ec/documentos/normatividad/NTCI-DOCUMENTO.pdf

Fang, C., Marle, F., & Xie, M. (2016). Applying importance measures to risk analysis in engineering project using a risk network model. IEEE Systems Journal, 11(3), 1–9. https://doi.org/10.1109/JSYST.2016.2536701

Galván., V. G. (2013). DATACENTER Una mirada por dentro (Primera Ed). https://doi.org/10.13140/RG.2.1.3434.8401

Guerrero Julio, M. L., & Gómez Flórez, L. C. (2012). Gestión de riesgos y controles en sistemas de información: del aprendizaje a la transformación organizacional. Estudios Gerenciales, 28(125), 87–95. https://doi.org/10.1016/S0123-5923(12)70011-6

INEC. (2015). Estatuto orgánico de gestión organizacional por procesos (p. 50). p. 50. Retrieved from http://www.ecuadorencifras.gob.ec/LOTAIP/2018/DATH/enero/Estatuto_organico_inec.pdf

INEC. (2016). Tecnologías de la Información y Comunicaciones (TIC´S) 2016. Retrieved from http://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2016/170125.Presentacion_Tics_2016.pdf

Instituto Nacional de Estadística e Informática de Perú. (2007). Manual de procedimientos administrativos de la Oficina Técnica de Informática del Instituto Nacional de Estadística e Informática del Perú (p. 30). p. 30. Retrieved from https://www.inei.gob.pe/media/pte/MAPRO/ManualProcedimientoOTIN_2007.pdf

Instituto Nacional de Estadisticas y Censos. (2019). Código de buenas prácticas estadísticas del Ecuador (p. 24). p. 24. Retrieved from http://www.ecuadorencifras.gob.ec/documentos/web-inec/Bibliotecas/Catalogo_y_Codigo_INEC/Codico_de_buenas_practics_estadisticas_del_Ecuador.pdf

Ministerio de Economía Fomento y Turismo Instituto Nacional de Estadísticas. (2017). Balance de Gestión Integral Ministerio de Economía, Fomento y Turismo Instituto Nacional de Estadística de Chile (p. 98). p. 98. Retrieved from https://www.ine.cl/institucional/balance-gestión

Ministerio de Telecomunicaciones y de la Sociedad de la Información - Secretaría de Educación Superior Ciencia Tecnología e Innovación. (2019). Libro Blanco Desarrollo e Innovación y Transferencia del Conocimiento en TIC 2019. Retrieved from https://www.telecomunicaciones.gob.ec/wp-content/uploads/2019/01/libro-blanco-lineas-de-investigacion.pdf

Ministerio del Interior. (2019). Gestión de Riesgos se fortalece en las provincias – Ministerio del Interior. Retrieved May 5, 2019, from https://www.ministeriointerior.gob.ec/gestion-de-riesgos-se-fortalece-en-las-provincias/

Molina-Miranda, M. F. (2017). Análisis de riesgos de centro de datos basado en la herramienta pilar de Magerit. Espirales Revista Multidisciplinaria de Investigación, 1(11). https://doi.org/10.31876/re.v1i11.125

Norma 410. (2009). Normas De Control Interno De La Contraloria General Del Estado. Ultima.

Orduña, Hernán; Sánchez, Elkin y Hernández, A. (2018). Adecuación del centro de cómputo de la British Petroleum (Data center de la BP) (Universidad Santo Tomás). Retrieved from http://e-journal.uajy.ac.id/14649/1/JURNAL.pdf

Pérez, T., Puentes, A. M., & Yesica María, P. (2015). Un enfoque de buenas prácticas de gobierno corporativo de TI. Tecnura, 159–169. https://doi.org/http://dx.doi.org/10.14483/udistrital.jour.tecnura.2015.SE1.a14

Secretaría Central de ISO. (2018). GESTIÓN DEL RIESGO — DIRECTRICES (ISO 31000:2018, IDT). Ecuador.

Secretaria Nacional de Administración Pública. Acuerdo Ministerial 166 - Esquema gubernamental de seguridad de la información EGSI. , Registro Oficial Nro. 88 § (2013).

Simbaña, M. K. (2018). PLAN INFORMÁTICO 2018-2022 BASADO EN LA NORMA ISO/IEC 27001:2013 PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN, INFRAESTRUCTURA Y RECURSOS TECNOLÓGICOS EN LA UNIDAD EDUCATIVA FISCAL “KASAMA” DE SANTO DOMINGO (UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES). Retrieved from http://e-journal.uajy.ac.id/14649/1/JURNAL.pdf

Soler González, R., Varela-Lorenzo, P., Oñate-Andino, A., Naranjo-Silva, E., & Naranjo-Silva, E. (2018). La gestión de riesgo: el ausente recurrente de la administración de empresas // Risk management: the recurrent absence of business administration. Ciencia Unemi, 11(26), 51. https://doi.org/10.29076/issn.2528-7737vol11iss26.2018pp51-62p

Suárez Grajales, S., & Ambiental, A. (2015). Mapas de crisis basados en las TIC como herramientas para dar respuesta oportuna en caso de ocurrencia de un evento de carácter desastroso. Retrieved from http://repositorio.utp.edu.co/dspace/handle/11059/6095

Tejena-mac, M. A., & Alfaro, E. (2018). Análisis de riesgos en seguridad de la información Risk analysis in information security Análise de risco em segurança da informação. 3(4), 230–244. https://doi.org/10.23857/casedelpo.2018.3.4.abril.230-244

Vanegas, D., & Pardo, C. (2014). Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT. Sistema y Telemática, 12(30), 33–46. Retrieved from http://repository.icesi.edu.co/biblioteca_digital/handle/10906/77514

Vargas Borbúa, R., Reyes Chicango, R. P., & Recalde Herrera, L. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa/ Cyber-defense and cybersecurity, beyond the virtual world: Ecuadorian model of cyber-defense governance. URVIO - Revista Latinoamericana de Estudios de Seguridad, 20(20), 31–45. https://doi.org/10.17141/urvio.20.2017.2571

Velasco, J. (2013). Servidores históricos y los primeros centros de datos. Retrieved June 11, 2018, from Blogthinkbig website: https://blogthinkbig.com/servidores-historicos-primeros-centros-de-datos