PLAN DE CONTINGENCIA INFORMÁTICO PARA EL GAD MUNICIPAL DEL CANTÓN BOLÍVAR

Autor: Ing. Varela Muñoz Ramón Agustín; Ing. Molina Aquino Bethsy Alexandra; Ing. Lectong Anchundia Miriam Lizeth; Ing. Pinargote Cusme Mariana Karolina.

Correo: agucho_0@hotmail.com; mirylectong18@gmail.com; mkpinargote@hotmail.com; alitaquinex1202@hotmail.com

RESUMEN:

El objetivo de esta investigación fue elaborar un Plan de Contingencia para mejorar los procesos administrativos en el GAD Municipal del cantón Bolívar. Para la ejecución de este trabajo fue necesario realizar el análisis, detección, evaluación y priorización de amenazas potenciales de las que puede ser víctima la institución. Se utilizó la metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, cumpliendo con los procesos de cada una de sus fases a fin de establecer los activos más importantes de la organización y las amenazas a las que están expuestos, determinar qué protecciones hay dispuestas y su eficacia frente al riesgo y el impacto del daño sobre el activo. Con estos resultados se obtuvo información relevante para el desarrollo del Plan, con el que se contribuyó a que la institución conociera sus vulnerabilidades y, de esta manera, se ayudó a precautelar la integridad de la información y componentes físicos y lógicos con los que cuenta, obteniendo así la seguridad requerida en los datos que se generan y procesan en la institución.

Palabras Clave: Plan de contingencia, seguridad informática, equipos informáticos, municipio.

INTRODUCCIÓN

En la actualidad las empresas públicas y privadas han experimentado transformaciones en el ámbito de la seguridad; la situación actual nos da a conocer que los sistemas informáticos son el activo más valioso y al mismo tiempo el más vulnerable. La seguridad informática ha adquirido gran relevancia, dada las cambiantes condiciones y nuevas plataformas de computación disponibles, situación que converge en la aparición de nuevas amenazas para los sistemas informáticos. Generalmente, no se invierte ni el capital humano ni económico necesario para prevenir el daño y/o pérdida de la información confidencial en las empresas; a raíz de ello, han surgido muchos problemas relacionados con el uso de computadoras, amenazas que afectan negativamente tanto a individuos como a empresas.

Según Gallardo - Jácome (2011), dentro del ámbito de la gestión de riesgos en el Ecuador, el sector educativo tiene especial relevancia, dado que las instituciones escolares constituyen la instancia ideal en la que se pueden construir los fundamentos de una cultura de gestión de riesgos; a diferencia de los Gobiernos Autónomos Descentralizados Municipales del Ecuador que no cuentan con un plan de contingencia informático, debido a la falta de conocimientos técnicos y de la normativa vigente de control interno de la Contraloría General del Estado por parte de los profesionales que trabajan en esta área tan importante de la institución, además los administradores de las instituciones públicas generalmente presentan cierta resistencia al momento de realizar una inversión en este tipo de planes por razones económicas, puesto a que los presupuestos son reducidos, sin muchas veces conocer los beneficios que conlleva tener un plan de contingencia informático en casos de desastres naturales de gran magnitud tales como terremotos, tormentas, inundaciones entre otros, de origen humano (retaliaciones, celos profesionales, competencia, huelga, problemas laborales…), y de origen técnico (fallas del hardware, del software, con el suministro de energía, entre otros). La ISO 27001:2007 recomienda, para llevar a cabo una gestión de riesgo, que se defina primero el alcance del estándar en la institución y, en base a ello, identificar todos los activos de información (Velasco, 2008).

El Gobierno Autónomo Descentralizado del cantón Bolívar es una entidad pública que brinda servicios a la sociedad, por lo cual es indispensable recurrir a los recursos informáticos como un medio de proveer información fiable y oportuna a todos los niveles de la misma, por lo que es de vital importancia que dicha información sea lo más exacta posible. Por tal razón, se desarrolló un Plan de Contingencia de los sistemas y equipos informáticos con el objetivo de salvaguardar los datos que se generan en los diversos procesos administrativos que se realizan en la institución y, de esta manera, garantizar una comunicación segura y eficaz.

DESARROLLO

Para el desarrollo del Plan de Contingencia del GAD Municipal del cantón Bolívar, se aplicó la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT), misma que consta de cinco fases y a través de las cuales se recopiló la información necesaria.

FASE 1: ESTABLECER LOS ACTIVOS MÁS IMPORTANTES DE LA ORGANIZACIÓN, SU INTERRELACIÓN Y SU VALOR, EN EL SENTIDO DE QUÉ PERJUICIO (COSTE) SUPONDRÍA SU DEGRADACIÓN. Se determinaron los activos más importantes de la organización y el análisis FODA para la institución, los resultados se obtuvieron realizando un censo de ámbito informático, incluyendo en este: hardware, software, talento humano y los servicios utilizados. Para el levantamiento de la información fue necesaria la utilización de matrices, mismas que fueron llenadas en una hoja de cálculo como se muestran en los cuadros 1 – 3.

Cuadro 1. Matriz utilizada para determinar el hardware (ordenadores, impresoras, UPS, ordenadores tipo servidores y equipos de red).

NOMBRE DEL ACTIVO											
ITEM	DETALLE	Cantidad	Precio_ Unitario	Precio_ Total	Año de Compra	Meses de Uso	Depreciación Anual	Depreciación Mensual	Depreciación Actual	Valor actual del bien	Valor Unitario del Bien
									TOTAL		

Cuadro 2. Matriz utilizada para determinar el software

SOFTWARE				
ITEM	DETALLE	CANTIDAD	LICENCIA	PRECIO ANUAL
			TOTAL	

Cuadro 3. Matriz utilizada para determinar el Talento Humano Institucional

TALENTO HUMANO - ÁREA ADMINISTRATIVA		
ITEM	DEPENDENCIA MUNICIPAL	NUMERO DE EMPLEADOS
	TOTAL	

FASE 2: ESTABLECER A QUÉ AMENAZAS ESTÁN EXPUESTOS ESTOS ACTIVOS: Se considera como amenazas a las “cosas que ocurren” y a todo lo que puede ocurrir, interesa lo que puede pasarle a los activos y causar un daño. Se tomó en cuenta cuatro clasificaciones principales que puedan haber, tales como:

- Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta (desastres naturales).

- Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada (desastres de origen industriales).
- Fallos no intencionales causados por las personas (Errores y fallos no intencionados).
- Fallos deliberados causados por las personas (Ataques intencionados).

FASE 3: DETERMINAR QUÉ PROTECCIONES HAY DISPUESTAS Y QUÉ EFICACES SON FRENTE AL RIESGO: Esta fase fue omitida en la investigación ya que la misma metodología la define o permite aplicarla si las estimaciones de impacto y riesgo son “potenciales” y no existiera salvaguarda alguna desplegada en la matriz para la valoración de impactos y frecuencia de la fase cuatro.

FASE 4: DETERMINAR EL IMPACTO DEL DAÑO SOBRE EL ACTIVO: Se procedió a estimar el impacto, donde se utilizó un catálogo de posibles amenazas sobre los activos de un sistema de información. Para cada amenaza se recurre a una matriz, tal como se ilustra en el cuadro 4, donde se detalla a precisión el tipo, la descripción de la amenaza, la estimación del impacto sobre el activo y la estimación del riesgo.

Cuadro 4. Matriz para la valoración de impactos y frecuencia

<table>
<tr><td colspan="11">[CÓDIGO] Descripción sucinta de lo que puede pasar</td></tr>
<tr><td colspan="5">TIPOS DE ACTIVOS:
• Que se puede ver afectado por este tipo de amenazas.</td><td colspan="6">DIMENSIONES:
1. De seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante.</td></tr>
<tr><td colspan="11">DESCRIPCIÓN:
Complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas.</td></tr>
<tr><td colspan="5">ESTIMACIÓN DEL IMPACTO</td><td colspan="6">ESTIMACIÓN DEL FRECUENCIA</td></tr>
<tr><td colspan="2" rowspan="2">IMPACTO</td><td colspan="3">DEGRADACION</td><td rowspan="7"></td><td colspan="2" rowspan="2">RIESGO</td><td colspan="4">FRECUENCIA</td></tr>
<tr><td>1 %</td><td>10 %</td><td>100%</td><td>PF</td><td>FN</td><td>F</td><td>MF</td></tr>
<tr><td rowspan="5">VALOR</td><td>MA</td><td>M</td><td>A</td><td>MA</td><td rowspan="5">IMPACTO</td><td>MA</td><td>A</td><td>MA</td><td>MA</td><td>MA</td></tr>
<tr><td>A</td><td>B</td><td>M</td><td>A</td><td>A</td><td>M</td><td>A</td><td>MB</td><td>MA</td></tr>
<tr><td>M</td><td>MB</td><td>B</td><td>M</td><td>M</td><td>B</td><td>M</td><td>A</td><td>MA</td></tr>
<tr><td>B</td><td>MB</td><td>MB</td><td>B</td><td>B</td><td>MB</td><td>B</td><td>M</td><td>A</td></tr>
<tr><td>MB</td><td>MB</td><td>MB</td><td>MB</td><td>MB</td><td>MB</td><td>MB</td><td>B</td><td>M</td></tr>
<tr><td colspan="11">MOTIVO:
Razón detallada por la cual se considera el impacto y el riesgo de la amenaza en el gobierno autónomo descentralizado municipal del cantón Bolívar.</td></tr>
</table>

MA= muy alto, A= alto, M= medio, B= bajo, MB= muy bajo.
PF= poco frecuente, FN= frecuencia normal, F= frecuente, MF= muy frecuente.

FASE 5: ESTIMAR EL RIESGO, DEFINIDO COMO EL IMPACTO PONDERADO CON LA TASA DE OCURRENCIA (O EXPECTATIVA DE MATERIALIZACIÓN) DE LA AMENAZA: Después de realizar la estimación del impacto, se procede con la estimación del riesgo, utilizando para este la matriz que se muestra en el cuadro 5, logrando de esta manera determinar las prioridades en cuanto a activos se refiere y así poder combatir las potenciales amenazas y establecer qué activos necesitan intervención inmediata.

Cuadro 5. Estimación de Riesgo

Estimar el riesgo							
Código	**Amenaza**	**Vulnerabilidad**		**Impacto**		**Valor de activo**	**Riesgo intrínseco**
		Siglas	**VAL**	**Siglas**	**VAL**		

Las salvaguardas a establecer han sido seleccionadas teniendo en cuenta los atributos del bien y la información a proteger (confidencialidad, integridad y disponibilidad). En la selección de las salvaguardas se consideró las características de la amenaza, la vulnerabilidad o probabilidad de materialización y el impacto o daño producido por una potencial amenaza. Se elaboró un listado de amenazas para los equipos y sistemas de información valorando el riesgo para cada una de ellas, según el impacto y la frecuencia de estas; además, se establecieron salvaguardas para cada una de estas amenazas según la magnitud de riesgo dentro de la institución.

RESULTADOS

Luego de realizar el proceso que implicó la aplicación del MAGERIT se consiguió desarrollar un Plan de contingencia informático para el GAD Municipal del cantón Bolívar, mismo que permitió brindar seguridad a los datos institucionales, mejorando así los procesos administrativos, servicios de comunicación, control de acceso y operaciones en la administración de los recursos informáticos.

CONCLUSIONES

Mientras el valor de los equipos informáticos se deprecia cada vez más en su valor monetario, el valor de la información incrementa de una manera considerable para la institución.

Con la ponderación del riesgo se puede establecer qué activos dentro de la institución están propensos a múltiples amenazas de diversa índole, que podrían materializarse en cualquier momento.

Con la utilización de actividades destinadas a la protección de los equipos y sistemas de información se puede mitigar el riesgo de una forma considerable para la institución.

Con la implementación de cualquier tipo de salvaguardas no existe la seguridad de eliminar totalmente la amenaza y por ende el riesgo que conlleva para los activos.

El Plan de contingencia servirá como una guía didáctica en caso de que se materialice una amenaza afectando el normal funcionamiento de la institución.

Estableciendo una manera ordenada de actividades que se deben de poner en práctica, el Municipio del cantón Bolívar contará con una herramienta muy importante la cual le permitirá recuperarse ante las posibles fallas y siniestros ocasionados por agentes internos o externos al mismo.

RECOMENDACIONES

No presentar resistencia al momento de invertir en seguridad informática y por ende de la institución.

Destinar recursos económicos para salvaguardar la información que tiene un alto valor y es de mucha relevancia.

Dar seguimiento al Plan de Contingencia, manteniéndolo actualizado en activos y en la disminución de los riesgos de acuerdo como se vayan implementando las salvaguardas en la institución.

A los encargados del departamento tecnológico, impartir capacitaciones al personal municipal, mismo que tendrá como objetivo concientizar y dar a conocer las bondades con que cuenta y ofrece el mencionado plan.

BIBLIOGRAFÍA

Arias, M. (2009). Percepción general de la virtualización de los recursos informáticos. Revista de las Sedes Regionales, (9), 152.

Amutio, M. (2015). Portal Administración Electrónica. Recuperado de http://administracionelectronica.gob.es/ctt/magerit#.VO4HNCuUeMI.

Gallardo, M. & Jácome, P. (2011). Análisis de Riesgo Informáticos y Elaboración de un plan de contingencia T.I. para la empresa eléctrica Quito S.A. (Tesis de pregrado). Escuela Politécnica Nacional, Quito. Recuperado de http://bibdigital.epn.edu.ec/bitstream/15000/3790/1/CD-3510.pdf.

García, A. (2010). Contingencias de aprendizaje sin refuerzo explícito. Psicothema, (22), 416-423.

Hernández, A. (2010). Auditoria Informática y Gestión de Tecnologías de Información y Comunicación. Compendiun, (13), 25.

Hernández, N., Yelandy, M. & Cuza, B. (2013). Modelos causales para la Gestión de Riesgos. CU. Revista Cubana de Ciencias Informáticas, (7), 4.

Morlanes, G. (2012). Seguridad Informática. Revista de Arquitectura e Ingeniería. (6) 1-14.

Velasco, A. (2008). El derecho informático y la gestión de seguridad de la información una perspectiva con base a la norma ISO 27001. Revista de Derecho, (29), 337- 341.