UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

ENERO – JUNIO 2017

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

Ingeniería en Sistemas

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS

TEMA:

Análisis de riesgo de la información en la infraestructura tecnológica para el Gobierno Autónomo Descentralizado del cantón Ventanas

EGRESADO:

Reyes Guerrero David Manuel

TUTOR:

Ing. Mejía Viteri José Teodoro

AÑO 2017

INTRODUCCIÓN

En la actualidad, muchas empresas tanto públicas como privadas, cuentan con implementos tecnológicos para el cumplimiento de ciertas tareas, denominados estos implementos como infraestructura tecnológica, siendo la infraestructura tecnológica parte fundamental en una empresa, ya que facilita el trabajo de los empleados que en ella laboran. La infraestructura tecnológica es muy necesaria, ya que las empresas cada vez trabajan con mayor volumen de información, y estas tecnologías minimizan el esfuerzo de los empleados, brindándoles facilidad y rapidez para la terminación de sus labores, posibilitando el compartimiento de información por medio de la red, permitiendo así, la comunicación entre los dispositivos de la empresa.

Muchas empresas dependen de la información, porque es un activo indispensable para seguir laborando, por esta razón las empresas afrontan múltiples inseguridades que las provee una variedad de fuentes, que los encargados de la seguridad en la empresa deben controlar, para que no se pierda la confidencialidad, integridad y disponibilidad en la infraestructura tecnológica de la empresa, ya que esto podría afectar el desempeño de las actividades de la empresa.

Hoy en día, los problemas de seguridad de la información, son uno de los más mencionados, ya que la pueden sufrir, desde las empresas más grandes, como hasta las más pequeñas, y más aún las que tengan información relacionada con ámbitos financieros.

El Gobierno Autónomo Descentralizado Municipal del cantón Ventanas, es una entidad pública, la cual trata con un alto volumen de información y de mucha importancia, por esta razón personas mal intencionadas la pueden hacer blanco de ataques informáticos.

El normal desempeño de los activos de la infraestructura tecnológica, es muy importante para la ejecución de las actividades, los cuales se pueden ver amenazados por la explotación de

vulnerabilidades que estos pueden tener, por esta razón, resulta de mucha relevancia, analizar y calcular los riesgos a los que están sometidos los activos, para poder contribuir con la gestión y minimización de los mismos, ya que pueden afectar a las actividades u operaciones del GADMCV.

El objetivo de este análisis de riesgo, es conocer las vulnerabilidades que los activos pueden tener y las posibles amenazas que podrían explotar aquellas vulnerabilidades, dando como resultado el nivel de riesgo a los que están sometidos cada uno de los activos del GADMCV.

Dentro del análisis de riesgo intervienen los siguientes pasos:

1. **Identificación de los activos**

   Proceso donde se dio lugar al análisis de campo, reconociendo así de esta manera los activos existentes en la empresa. Este proceso fue dirigido por los encargados del departamento TIC del GADMCV.

2. **Valoración de los activos**

   Este paso se lo realizó con la ayuda de una tabla de valoración, donde se establece como puntos principales, la dependencia de un activo para con otros, la integridad, confidencialidad y disponibilidad de cada activo.

3. **Cálculo de ocurrencia de amenazas y facilidad de explotación**

   Este proceso se lo realizó con la ayuda de una tabla de probabilidad, donde se establece el nivel de ocurrencia de amenazas, como también la facilidad de explotación sobre un activo.

4. **Cálculo de riesgo sobre los activos**

   Como último paso, se calculó el nivel de riesgo sobre los activos intervenidos, realizándolo con la ayuda de una tabla de estimación de riesgo, siendo esta tabla, analizada por el personal del departamento TIC del GADMCV.

DESARROLLO

El Gobierno Autónomo Descentralizado Municipal del cantón Ventanas, es una empresa pública, que formula y ejecuta planes, programas y proyectos, para garantizar el desarrollo social, económico y productivo del Cantón, además tiene otras actividades, como el cobro de patentes, matricula vehicular, catastro, etc.

El GADM del cantón Ventanas, posee mucha información y muy variada, por lo cual debería asegurarla, para que no se pierda, ya que es muy importante para la continuidad de sus labores.

Esta empresa pública, presenta algunas vulnerabilidades referentes a seguridad de la información, por lo que podría ser atacada, dando lugar a la perdida de información, lo cual afectaría a sus actividades, ya que muchas de estas dependen de la información que fluye en la empresa, por esta razón la información debería ser asegurada, así como también los activos de la infraestructura tecnológica, ya que por medio de estos activos fluye información importante que no se debería perder, por ello es necesario dar lugar a un análisis de riesgo, el cual determinará, el nivel de riesgo que está corriendo actualmente la empresa pública, las vulnerabilidades visibles que presenta, y también la identificación de nuevas vulnerabilidades, , lo cual se debería tomar en cuenta si no se quiere perder la información.

A continuación, se presenta el desarrollo del análisis de riesgo, el cual proporcionará información importante, como la valoración de los activos, lo cual especifica la influencia de los activos para la empresa, además se conocerá, las vulnerabilidades y posibles amenazas que pueden explotar las vulnerabilidades que tengan los activos y el nivel de riesgo que pueden tener cada uno de ellos, parte importante para hacer conciencia de que se debería asegurar de mejor manera, tanto la información, como los activos de la infraestructura tecnológica de la empresa.

Como primer paso se definió lo que es una vulnerabilidad, explicando de manera muy expresiva que una vulnerabilidad la puede tener cualquier activo presente en la empresa y definiéndola como, "Cualquier debilidad en los SI que pueda permitir a las amenazas causarles daños y producir pérdidas" (Ruiz Larrocha & Ruiz Virumbrales, 2012, pág. 89)

Luego de definir lo que es una vulnerabilidad, se trató el tema de las amenazas, las cuales podrían atacar a los activos, por la falta de seguridad que podría existir en la empresa con respecto a los activos que se emplean en la misma, definiendo la amenaza como, la "causa posible de incidente indeseado, que podría perjudicar a un sistema u organización" (de la Corte Ibáñez & Blanco Navarro, 2014)

Indagando un poco el campo de aplicación del análisis de riesgo, se notó que algunas de las oficinas corren riesgos de perder información por la falta de seguridad sobre sus activos, es decir por descuidar a los activos, conociendo que el riesgo es, "la probabilidad de que se cristalice o no una amenaza beneficiándose de una vulnerabilidad" (Aguilera López, 2011, pág. 14), teniendo esto claro, se puede concluir que el riesgo es visible en la empresa, por el descuido ante la información.

El riesgo en una empresa, se presenta muchas veces por la falta de concienciación por el personal operativo, de lo que podría ocurrir si se deja al descubierto la información con la que están trabajando, dando lugar, al riesgo de pérdida de información, ya que el riesgo se lo conoce también, como "la posibilidad de sufrir daño o pérdida a causa de la exposición a un evento sobre el cual se tiene incertidumbre" (Mantilla B, 2015) es decir, muchas veces el personal que labora en la empresa, es el creador del riesgo que se puede presentar en la misma, por la exposición que le dan a la información con la que estén trabajando, información de la cual depende la empresa. De esta manera la información queda con un alto grado de susceptibilidad.

La información es uno de los activos más importantes de toda la organización, por tanto requiere, junto a los procesos y sistemas que la tratan, ser protegidos, convenientemente frente a amenazas que puedan poner en peligro la continuidad de los niveles de competitividad, rentabilidad y conformidad legal, necesarios para alcanzar los objetivos de la organización (López Hermoso Agius, Medina Salgado, de Pablos Heredero, & Romo Romero, 2012, pág. 361)

Ya sea a nivel de empresa, de multinacional, de un usuario privado o incluso de un país, la seguridad de un sistema de información adquiere una importancia proporcional al valor de los datos que contiene.

En el despliegue de una red, no sólo hay que enfrentarse con el problema del aumento de la cantidad sino también, y, sobre todo, con la importancia de los datos que la recorren. (RAULT, y otros, 2015, pág. 25), por ello la importancia de la seguridad en la información, teniendo claro que "La seguridad de la información es la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento" (GARCÍA-CERVIGÓN HURTADO & ALEGRE RAMOS, 2011)

Este análisis de riesgo, interviene a los activos de la parte de la infraestructura tecnológica. Se basa en la identificación de los activos que contribuyen en las actividades de la empresa, analizando el valor de cada activo, las vulnerabilidades y cuáles son las posibles amenazas que podrían explotar las vulnerabilidades existentes. Luego de esto se realiza un cálculo de riesgo, el cual nos arroja el valor del riesgo que tiene cada activo en la empresa.

Existen normas que proveen reglas o protocolos, que deben ser respetados para ajustar ciertas conductas o actividades que deben ser mejoradas, también "establecen los requisitos y los

elementos mínimos que tienen que comprender los sistemas de calidad" (Gonzáles Ortiz & Arciniegas Ortiz, 2016)

La falta de seguridad en una empresa, puede suministrar una serie de consecuencias desagradables, por eso hay que tomar en cuenta las normas de seguridad, las cuales se definen como, "las reglas que resultan necesarias divulgar y vigilar su cumplimiento, con la anticipación necesaria, para de esta manera evitar los posibles daños que puedan derivarse de la ejecución de una actividad." (Del Prado, 2013)

"La norma ISO 27001 comprende un conjunto de normas o reglas relacionadas a la seguridad informática" (GARCÍA-CERVIGÓN HURTADO & ALEGRE RAMOS, 2011), "se ha promovido como alternativa en factor de seguridad de los sistemas de información, esencialmente para la aplicación de un sistema de gestión de la seguridad de la información" (CARPENTIER, 2016, pág. 34) el propósito de esta norma es "reducir la vulnerabilidad de una organización a riesgos de seguridad de la información mediante el uso de un Sistema de Gestión de la Seguridad de la Información" (Selm, 2006)

Existen otras normas complementarias como la ISO/IEC 27002: la cual "es un estándar para la seguridad de la información (también se considera una guía de buenas prácticas) en el que se incluyen los distintos objetivos de control y controles recomendados para mantener un nivel de seguridad de la información óptimo" (Tejada, 2015), y la norma ISO 27005, la cual es el estándar internacional que promueve la óptima gestión de riesgos de seguridad de la información en una organización. La norma proporciona las pautas para llevar a cabo la gestión de riesgos de seguridad de la información en una empresa, apoyando exclusivamente las exigencias del sistema de gestión de seguridad de la información definidos en ISO 27001. (ISOTools Excellence, 2014)

Siguiendo la metodología planteada por la norma ISO 27005, se debe definir el alcance del análisis de riesgo, el cual comprende, desde el departamento de Tecnologías de información y comunicación, hasta los racks que proporcionan los servicios a los ordenadores y los departamentos u oficinas que requieren estos servicios para laborar normalmente, en la cual encontramos los activos que hay que analizar.

Los activos, son los elementos que contribuyen al desarrollo de actividades en la empresa, son piezas fundamentales para el mismo, el cual es indispensable que se muestren disponibles en cualquier momento para su utilización, ya que de esa manera se garantiza la terminación de una determinada actividad.

Los activos se suelen clasificar en, software (aplicaciones informáticas), hardware (equipos informáticos, dispositivos de almacenamiento…), servicios (telefonía, informática), imagen, información y personas. (López Lemos, 2015)

Luego de definir el alcance del análisis de riesgo, como los activos que se pueden considerar o que podamos encontrar en la empresa, se procede a realizar una identificación de los activos.

La identificación de los activos, se la realiza aplicando la investigación de campo, es decir haciendo un recorrido por la empresa, específicamente en las áreas donde se trabaje con la tecnología, o en departamentos que laboren con información, ya que de esta manera se podrá realizar una categórica identificación de los activos. Además, se contó con la ayuda del personal del departamento TIC, los cuales detallaron a los activos en su área de trabajo, el cual se pudo constatar, fueron también la ayuda para hacer el recorrido, los cuales especificaban lo que existía en cada departamento, vital ayuda para la realización de la lista de activos, el cual es uno de los

pasos más importantes en el análisis de riesgo, ya que de esta manera se tiene claro con que tecnología cuenta la entidad a la que se le está aplicando el análisis de riesgo.

En la Tabla 1 se muestra los activos identificados en la empresa

Tabla 1: *Lista de activos del GADMCV*

LISTA DE ACTIVOS
ADMINISTRADOR DE RED
ANTIVIRUS
AXIS 4.0 – AGENCIA NACIONAL DE TRANSITO
CABLEADO ESTRUCTURADO
CENTRAL DE AIRE
CORREO ELECTRÓNICO
DISCOS DUROS DE SERVIDORES
DISCOS DUROS EXTERNOS
EQUIPOS DE ESCRITORIO
FACTURACIÓN ELECTRÓNICA
FIBRA ÓPTICA
INSTALACIÓN ELÉCTRICA
MÓDULO PARA TESORERÍA
MUNREN
PORTÁTIL
ROUTER
SERVIDOR
SIGAME
SISTEMA OPERATIVO WINDOWS
SISTEMA OPERATIVO WINDOWS SERVER
SOFTWARE DE CATASTRO
SWICH
TÉCNICO DE SOPORTE
UPS
WEB SITE

Fuente: Elaborada con la ayuda del personal del departamento TIC de la empresa.

En la Tabla 1, se muestra los activos con los que cuenta la empresa, paso importante para el análisis de riesgo, ya que de esta manera sabemos cuáles son los activos que debemos analizar.

Una vez identificados los activos de la empresa, se le debe asignar un valor, orientado a la confidencialidad, integridad y disponibilidad, ya que de esta manera se llega a conocer la importancia que tiene un activo para la empresa.

Para el siguiente paso, se realizará una escala de valoración de los activos.

Tabla 2: *Escala de valoración de los activos*

Valoración		Dependencia	Funcionalidad	Integridad, confidencialidad y disponibilidad
1	MUY BAJO	Este activo no contribuye con la transmisión o comunicación de servicios	Este activo cuenta con alcances tecnológicos muy básicos	La circulación, alteración y no disponibilidad de este activo o de la información que este tiene, puede afectar de manera muy baja la entrega de servicios
2	BAJO	Escasos activos dependen de este activo para la entrega de servicios	Este activo cuenta con alcances tecnológicos limitados	La circulación, alteración y no disponibilidad de este activo o de la información que este tiene, poco puede afectar en la entrega de servicios
3	MEDIO	Menos del 50% de los activos dependen de este activo para la entrega de servicios	Este activo cuenta con alcances tecnológicos un poco aceptables	La circulación, alteración y no disponibilidad de este activo o de la información que este tiene, puede afectar mucho, en la entrega de servicios
4	ALTO	Más del 50% de los activos dependen de este activo para la entrega de servicios	Este activo cuenta con alcances tecnológicos avanzados	La circulación, alteración y no disponibilidad de este activo o de la información que este tiene, puede afectar en gran manera la entrega de servicios
5	CRÍTICO	El 100% de los activos dependen de este activo para la entrega de servicios	Este activo cuenta con alcances tecnológicos modernos, de los más avanzados	La circulación, alteración y no disponibilidad de este activo o de la información que este tiene, puede arruinar la entrega de servicios

(Mejía Viteri, Gonzáles Valero, Campi Mayorga, Campi Mayorga, & España León, 2016)

Fuente: Elaborada con la ayuda del personal del departamento TIC de la empresa y con la ayuda de textos referenciados.

La Tabla 2, se la utiliza como ayuda para la asignación de valores a los activos intervenidos por el análisis de riesgo, siendo esta fundamental para el buen desarrollo de este proceso.

El impacto tecnológico, es el estudio de la intervención de la tecnología en las distintas sociedades, ya sea de carácter positivo, negativo o neutro, de esta forma también se conoce a la valoración de activos, ya que de esta manera se llega a saber, la importancia de un activo para la empresa.

En la Tabla 3, se realizó la descripción de las funciones de los activos, para lo cual se aplica la metodología cualitativa, donde se le estableció un valor de acuerdo a la escala elaborada, con respecto a la integridad, confidencialidad, y disponibilidad de las funciones que proporciona el activo.

Tabla 3: *Valoración de los activos*

Lista de activos	Funciones	Confidencialidad	Integridad	Disponibilidad	Promedio
Swich	Permite la interconexión de los equipos en la empresa	5	5	5	5
Router	Mantiene la conexión a internet sobre todos los dispositivos, restringiendo el acceso con clave a desconocidos	5	5	5	5
Cableado estructurado	Garantiza una buena conexión de internet, a los departamentos u oficinas de la empresa	5	5	5	5
Servidor	Activo con información de los servicios que provee la empresa y también con información de las configuraciones de los activos	5	5	5	5
Equipos de escritorio	Dispositivo que puede acceder a los servicios que dispone la red	4	4	4	4
Central de aire	Activo que mantiene acondicionado el ambiente, para los equipos.	4	4	4	4
Discos duros de servidores	Permite el almacenamiento de información y configuración de los servicios que ofrece la empresa	5	5	5	5

Sistema operativo windows server	Sistema base, que permite la ejecución de aplicativos y permite el acceso a los equipos en red a los servicios que ofrece como servidor.	5	5	5	5
Sigame	Sistema informático que facilita la automatización de las tareas de gestión y análisis de los Gobiernos Autónomos Descentralizados.	4	4	4	4
Facturación electrónica	Sistema informático que facilita la realización de facturación	4	4	4	4
Software de catastro	Sistema informático que facilita el cobro de catastro	4	4	4	4
Munren	Facilita la recaudación del dinero por servicios prestados a la ciudadanía como las patentes	4	4	4	4
Axis 4.0 – agencia nacional de transito	Sistema web que facilita la emisión de matrícula y cobro anual	4	4	4	4
Administrador de red	Personal encargado de la gestión de la red	4	4	4	4

Fuente: Elaborada con la ayuda de criterios del personal del departamento TIC de la empresa.

La valoración de activos reciente, es fundamental para el conocimiento de la importancia de cada activo para la empresa, teniendo presente las funciones que estos realizan, ya que también de esto depende la importancia del activo.

Luego de haber realizado la valoración a cada uno de los activos de la empresa, con la ayuda de las reuniones de trabajo, revisión de documentos bibliográficos e inspección física, se procedió a realizar la identificación de las vulnerabilidades, así como de las posibles amenazas que pueden afectar a cada uno de los activos que tengan vulnerabilidades.

En la Tabla 4, se muestra la valoración que se le asignó a la probabilidad de que una amenaza pueda explotar una vulnerabilidad, en base a la norma ISO 27005, y también con la ayuda de los responsables de los activos en el departamento de Tecnologías de información y comunicación de la empresa.

Tabla 4: *Probabilidad de ocurrencia de amenazas*

Probabilidad		Descripción
1	BAJA	Amenazas con baja probabilidad de atacar las vulnerabilidades existentes en un activo
2	MEDIA	Amenazas que a veces atacan las vulnerabilidades existentes en un activo
3	ALTA	Amenazas que comúnmente pueden atacar las vulnerabilidades existentes en un activo

Fuente: (ISO/IEC 27005, 2011)

Gracias a las entrevistas realizadas al personal responsable de los activos tecnológicos de la empresa, se logró la obtención de la información con respecto a las amenazas y vulnerabilidades que pueden intervenir en cada uno de los activos, información utilizada para la evaluación del riesgo sobre cada activo.

A continuación, se evaluó el riesgo, el cual es el análisis en la que se estima el nivel de exposición que puede tener un activo, dando lugar a que una amenaza se materialice sobre él, y pueda derivarse en otros activos, si de este dependen, causando de esta manera un grave daño a la empresa.

La fase de evaluación del riesgo, permite decidir sobre las acciones que la organización va a emprender, para tratar el riesgo, que van desde la ausencia de las mismas (en el caso de riesgos insignificantes) hasta la eliminación total de la actividad que genera el riesgo (en el caso riesgos intolerables) (López Lemos, 2015)

En la Tabla 5, se les asignaron valores a los niveles de riesgo, de la misma manera en reunión con los responsables del departamento de tecnologías de la información y comunicación.

Tabla 5: *Estimación del riesgo.*

Valores	Nivel de riesgo
8	ALTA
6-7	MEDIA ALTA
4-5	MEDIA
2-3	MEDIA BAJA
0-1	BAJA

Fuente: (Mejía Viteri, Gonzáles Valero, Campi Mayorga, Campi Mayorga, & España León, 2016)

La Tabla 5 fue obtenida de la fuente recientemente citada, y analizada conjuntamente con el personal del departamento TIC de la empresa.

El siguiente paso, fue calcular el riesgo que existe sobre cada activo, para lo cual utilizamos la Tabla 6, la cual es una combinación del valor del activo, la probabilidad de ocurrencia de una amenaza sobre el activo y la facilidad de explotación, que hace referencia al nivel de vulnerabilidad que existe sobre el activo que se esté calculando. Sacando un promedio de estos atributos, se generará como resultado el nivel de riesgo que corre un determinado activo.

Tabla 6: *Evaluación del riesgo*

	Probab. de que ocurra la amenaza	**Baja**			**Media**			**Alta**		
	Facilidad de explotación	Baja	Media	Alta	Baja	Media	Alta	Baja	Media	Alta
Valoración del activo	1	0	1	2	1	2	3	2	3	4
	2	1	2	3	2	3	4	3	4	5
	3	2	3	4	3	4	5	4	5	6
	4	3	4	5	4	5	6	5	6	7
	5	4	5	6	5	6	7	6	7	8

Fuente: (ISO/IEC 27005, 2011, pág. 87) (Mejía Viteri, Gonzáles Valero, Campi Mayorga, Campi Mayorga, & España León, 2016, pág. 13)

En la Tabla 7, se aplica un instrumento facilitado por la norma ISO 27005, donde se establece las posibles vulnerabilidades y amenazas que puede tener un activo, los cuales se reflejan en esta tabla, dependiendo el activo, será la valoración de la probabilidad de ocurrencia de amenazas, como también la facilidad de explotación, por las vulnerabilidades que puede tener el activo, y así de esta manera, utilizando la tabla de evaluación del riesgo, se logra obtener el nivel de riesgo que corre cada activo. Hay que tener en cuenta que la metodología aplicada para este proceso es la cuantitativa, ya que se entrevistó al personal operativo de la empresa, y de la misma manera es cualitativo, ya que cada uno de ellos especificaron las falencias presentadas por los activos.

Tabla 7: *Evaluación del riesgo sobre los activos.*

Activos	Vulnerabilidad	Amenazas	Valor – activo	Probab. de ocurrencia de amenaza	Facilidad de explotación	Riesgo
Swich Router Servidor	Falta de prueba del envío o la recepción de mensajes	Negación de acciones	5	BAJA	BAJA	4
	Líneas de comunicación sin protección (ISO/IEC 27005, 2011)	Escucha subrepticia	5	BAJA	MEDIA	5
	Tráfico sensible sin protección	Escucha subrepticia	5	BAJA	MEDIA	5
	Conexión deficiente de cables	Falla del equipo de telecomunicaciones	5	BAJA	MEDIA	5
	Arquitectura insegura de la red	Espionaje remoto	5	BAJA	MEDIA	4
	Transferencia de contraseñas autorizadas	Espionaje remoto	5	BAJA	ALTA	6
	Gestión inadecuada de la red (capacidad de recuperación del enrutamiento)	Saturación del sistema de información (ISO/IEC 27005, 2011)	5	BAJA	MEDIA	5
	Conexiones de red pública sin protección	Uso no autorizado del equipo	5	BAJA	ALTA	6

	Falta de esquemas de reemplazo periódico. Susceptibilidad a la humedad, el polvo y la suciedad	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento	5	MEDIA	MEDIA	6
	Sensibilidad a la radiación electromagnética	Radiación electromagnética	5	BAJA	BAJA	4
	Susceptibilidad a las variaciones de tensión	Pérdida del suministro de energía	5	BAJA	MEDIA	5
	configuración incorrecta de parámetros	Error en el uso	5	BAJA	MEDIA	5
Portátil Equipos de escritorio	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de información	4	BAJA	MEDIA	4
	Almacenamiento sin protección	Hurto de medios o documentos	4	BAJA	ALTA	5
	Falta de cuidado en la disposición final	Hurto de medios o documentos	4	BAJA	MEDIA	4
	Copia no controlada	Hurto de medios o documentos	4	MEDIA	MEDIA	5
	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de derechos	4	BAJA	ALTA	5
	Descarga y uso no controlados de software	Manipulación con software	4	ALTA	ALTA	7
Discos duros externos	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de derechos	3	BAJA	MEDIA	3
Ups	Susceptibilidad a las variaciones de tensión	Pérdida del suministro de energía	5	MEDIA	MEDIA	6
Administrador de red	Ausencia del personal	Incumplimiento en la disponibilidad del personal	4	BAJA	ALTA	5
Técnico de soporte	Entrenamiento insuficiente en seguridad	Error en el uso	4	BAJA	MEDIA	4
	Uso incorrecto de software y hardware	Error en el uso	4	BAJA	MEDIA	4
	Falta de políticas para el uso correcto de los medios	Uso no autorizado del equipo	4	MEDIA	MEDIA	5

	de telecomunicaciones y mensajería					
Personal en general	Trabajo no supervisado del personal externo o limpieza	Hurto de medios o documentos	4	BAJA	ALTA	5

Fuente: Departamento TIC de la empresa.

La Tabla 7, nos refleja el nivel de riesgo que tienen cada uno de los activos, de acuerdo a las vulnerabilidades presentes. Nos proporciona información importante, para tener en cuenta los activos que debemos de asegurar, conforme a las acciones que realicen, o a las actividades a las cuales contribuyan, para de esta manera poder tenerlos siempre disponibles.

La Tabla 8, describe el nivel de la necesidad, de mitigar los riesgos presentados, en el análisis de riesgo realizado.

Tabla 8: *Necesidad de tratamiento del riesgo*

Valores	Nivel de riesgo	Descripción del riesgo y acciones necesarias
8	ALTA	Requiere la rápida implementación de robustos controles y la monitorización del área de afectación, con los reportes correspondientes a los altos mandos
6-7	MEDIA ALTA	Gran necesidad de corrección o aplicabilidad de controles y la monitorización correspondiente con la divulgación a los altos mandos
4-5	MEDIA	Nivel de riesgo, que necesita la aplicabilidad de controles y la monitorización aplicada frecuentemente
2-3	MEDIA BAJA	Nivel de riesgo admirable, por los encargados del normal desempeño de los activos en la empresa, aplicando acciones para el normal desempeño de los activos
0-1	BAJA	El encargado del activo, se encarga del normal desempeño del mismo, con acciones comunicadas por el personal capacitado

(Mejía Viteri, Gonzáles Valero, Campi Mayorga, Campi Mayorga, & España León, 2016)

Fuente: Obtenida de la fuente recientemente citada y analizada por el personal del departamento TIC, modificado y adaptado a la necesidad de la empresa

La Tabla 8, nos ayuda a priorizar el aseguramiento de los activos con mayor nivel de riesgo, entendiendo que estos deben ser tratados con mayor énfasis por su actividad de aplicación, por lo cual su nivel de riesgo es muy alto, por tal razón se le debe poner mayor atención, teniendo en cuenta que en cualquier momento podría ser explotada alguna vulnerabilidad que este activo presente.

Con la información generada por el análisis de riesgo, el GADMCV, debería hacer conciencia del riesgo que está corriendo por la falta de atención sobre la información con la cual laboran en la empresa, ya que, si se pierde esta información, las actividades quedarían truncadas, porque la información es pieza fundamental para la continuidad de las actividades en una empresa, más aun, cuando se tiene implementadas las tecnologías de información y comunicación.

El tratamiento de los activos tecnológicos, se debe enfocar también, en la seguridad de la información, que puede fluir por ellos, y no solo al mantenimiento físico, que es lo que se acostumbra a hacer, ya que cada activo existente en la empresa, es fundamental para la continuidad de las actividades, por la información que provee, la cual se contrasta en las tablas de valoración de activos, por ello se debería poner más atención a estos activos, con respecto a la seguridad de la información sobre los activos.

El resultado del análisis de riesgo realizado a la empresa es temporal, es decir, es válido solo para una considerada temporada, ya que las amenazas que pueden afectar a los activos siguen evolucionando, también es temporal el análisis de riesgo por los nuevos activos que puede obtener la empresa, y esto representa nuevas amenazas a considerar. Por esta razón las empresas deben realizar continuamente análisis de riesgos, para mitigar todas las fallas que este presentando la empresa, con respecto a seguridad de la información, y así poder tener la información asegurada.

CONCLUSIONES

Entre las primordiales conclusiones que se pueden presentar tras haber realizado el análisis de riesgo se tienen las siguientes:

- Luego de haber realizado el análisis de riesgo en la infraestructura tecnológica del GADMCV, se pudo conocer, la importancia de los activos para la empresa, las vulnerabilidades que estos tienen y las amenazas que pueden afectarlos, por las vulnerabilidades que estos poseen.
- La metodología planteada por la norma ISO-27005, fue la que se aplicó en el análisis de riesgo, facilitando de esta manera, el proceso que se debía seguir para la obtención de los resultados esperados.
- El análisis de riesgo en el GADMCV, es de suma importancia, por la cantidad de información que fluye en la empresa y por las vulnerabilidades que tienen los activos, ya que en esta empresa no se aplica la adecuada seguridad sobre la información.
- Con los resultados obtenidos por el presente análisis, se conoció el nivel de riesgo que corren cada uno de los activos, por lo cual se sugiere aplicar los controles adecuados, para minimizar el riesgo a un nivel aceptable, y así poder tener asegurados los activos. Estos controles los facilita la norma ISO 27002, la cual define los Dominios que se deben tener en cuenta, Objetivos de Control y Controles que se deben implementar para optimizar el SGSI (Sistema de gestión de la seguridad de la información)

Referencias

(s.f.).

(s.f.).

Aguilera López, P. (2011). *Introducción a la seguridad informática (Seguridad informática).* Editex.

CARPENTIER, J.-F. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas.* Barcelona: ENI.

de la Corte Ibáñez, L., & Blanco Navarro, J. M. (2014). *Seguridad nacional, amenazas y respuestas.* Madrid: LID EDITORIAL.

Del Prado, J. (22 de 11 de 2013). *IMF Business School: Masters Oficiales Online y MBA. Becas*. Obtenido de Concepto de Norma de Seguridad: http://www.imf-formacion.com/blog/prevencion-riesgos-laborales/actualidad-laboral/concepto-de-norma-de-seguridad/

GARCÍA-CERVIGÓN HURTADO, A., & ALEGRE RAMOS, M. D. (2011). *SEGURIDAD INFORMÁTICA.* Madrid: Paraninfo.

Gonzáles Ortiz, Ó. C., & Arciniegas Ortiz, J. A. (2016). *Sistema de gestión de calidad.* Colombia: Ecoe Ediciones Ltda.

ISO/IEC 27005. (NTC-ISO 27005 de 2011). *ISO-27005 - español*. Obtenido de https://es.scribd.com/doc/124454177/ISO-27005-espanol

ISOTools Excellence. (31 de 01 de 2014). *PMG SSI - ISO 27001 - Chile SGSI Blog especializado en Sistemas de Gestión*. Obtenido de ISO/IEC 27005. Gestión de riesgos de la Seguridad la Información: www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/

López Hermoso Agius, J. J., Medina Salgado, S., de Pablos Heredero, C., & Romo Romero, S. (2012). *Organización y transformación de los sistemas de información en la empresa.* Madrid: ESIC Editorial.

López Lemos, P. (2015). *Novedades ISO 9001:2015.* Madrid: ESIC, 2016.

López Lemos, P. (2015). *Novedades ISO 9001:2015.* Madrid: ESIC, 2016.

Mantilla B, S. A. (2015). *Estándares/Normas Internacionales de Aseguramiento de la Información Financiera (ISA/NIA).* Ecoe Ediciones.

Mejía Viteri, J. T., Gonzáles Valero, M. I., Campi Mayorga, J. A., Campi Mayorga, I. I., & España León, Á. R. (2016). Análisis y Evaluación del Riesgo de la Información: Caso de Estudio Universidad Técnica de Babahoyo. *Revista de Ciencia, Tecnología e Innovación*, 12.

RAULT, R., SCHALKWIJK, L., ACISSI, AGÉ, M., CROCFER, N., CROCFER, R., . . . LASSON, S. (2015). *Seguridad informátiva - Hacking Ético.* Barcelona: Ediciones ENI.

Ruiz Larrocha, E., & Ruiz Virumbrales, J. L. (2012). *Sistemas de información de las organizaciones.* Madrid: Universitaria Ramón Areces.

Selm, L. (2006). *ISO/IEC 20000 Una Introducción.* Van Haren.

Tejada, E. (2015). *Gestión de servicios en el sistema informático. IFCT0609.* Málaga: IC Editorial.