Análisis y Evaluación del Riesgo de la Información: Caso de Estudio Universidad Técnica de Babahoyo

Analysis and Risk Assessment of Information: Case Study Universidad Técnica de Babahoyo.

José Teodoro Mejía Viteri
dyhack@hotmail.com
Universidad Técnica de Babahoyo
María Isabel Gonzáles Valero
mery_2523@hotmail.com
Universidad Técnica de Babahoyo
Julieta América Campi Mayorga
julietacampi@hotmail.com
Universidad Técnica de Babahoyo y UNANDES
Ida Ivette Campi Mayorga
idacampimayorga@hotmail.com
Universidad Técnica de Babahoyo y UNANDES
Ángel Rafael España León
arel_setnet@hotmail.com
Universidad Técnica de Babahoyo

RESUMEN

Esta investigación propone identificar las debilidades y fortalezas que están sometidos los activos de la dirección de TIC de la Universidad Técnica de Babahoyo ubicada en la Provincia de Los Ríos, con el fin de establecer los objetivos, dominios y controles para minimizar la ocurrencia de las amenazas que puedan explotar vulnerabilidades en la infraestructura tecnológica. Este estudio permitió recoger información a través de instrumentos de recolección de datos, como entrevistas, reuniones de trabajo y revisión bibliográfica, además se realizó visitas a las instalaciones de la Universidad Técnica de Babahoyo, revisando aspectos de seguridad física previstos en las Normas ISO 27001-2013. Se realiza un levantamiento de los dispositivos hardware , software y de información, para luego realizar una valoración a los mismos de acuerdo a su incidencia en la integridad, confidencialidad y disponibilidad, también se realiza una asignación de las amenazas más significativas que pueden causar daño al activo y afectar su actividad, para luego realizar una valoración del riesgo. Se concluye que los activos del departamento de TIC se consideraron de mucha importancia para la Universidad Técnica de Babahoyo, siendo necesario la aplicación de controles de las Normas ISO 27002-2013.

PALABRAS CLAVE: Seguridad Informática, Tecnología de la Información, ISO 27005, Análisis de Riesgo.

ABSTRACT

This research aims to identify the strengths and weaknesses that are under active ICT direction of the Technical University of Babahoyo located in the province of Los Rios, in order to suggest strategies to minimize the occurrence of threats that can exploit

Recibido: Marzo 2016. **Aceptado:** Mayo 2016

vulnerabilities in technological infrastructure. This study allowed to collect information through data collection tools such as interviews, meetings and literature review also visits were made to the premises of the Technical University of Babahoyo, reviewing aspects of physical security set forth in the ISO Standards 27001- 2013. An uprising of the hardware, software and information devices is performed, and then make an assessment to them according to their impact on the integrity, confidentiality and availability, allocation of the most significant threats that can damage is also done to active and affect its activity, and then make an assessment of riesgo.Seconcludes that the assets of the ICT department considered very important for the Technical University of Babahoyo, the application of some controls being necessary ISO 27002-2013.
KEYWORDS: Computer Security, Information Technology, ISO 27005, Risk Analysis

INTRODUCCIÓN

En la actualidad las TIC(Tecnología de la Información y Comunicación), es la columna vertebral de las empresas públicas y privadas, es crítico tener un departamento que se encargue de la Gestión de los servicios de TIC, tales como páginas web, control en los accesos a la información, y software que funcionen a nivel LAN y WAN, esto implica asegurar la disponibilidad y la seguridad de la misma, tanto así que el bien más cotizado en la actualidad por las empresas es la información; hoy en día se escucha mucho que los hackers se apropian de la información de los clientes de las empresas, solicitando cuantiosas cantidades de dinero por esta razón, se hace necesario implementar una infraestructura que cumpla con estándares en cuanto a seguridad, integridad y confidencialidad.

Las Empresas se enfrentan en la actualidad a un número muy alto de inseguridades que proceden de una amplia variedad de fuentes, que los CEO (Director General) y CIO (Director de Informática) deben controlar a través de políticas de seguridad y mecanismos que ayuden a disminuir la posibilidad de que ocurra un incidente que afecte al desempeño de actividades de la empresa.

Para Carlos Manuel Fernández, 2012; “La información es como el aparato circulatorio para las organizaciones y requiere que se proteja ante cualquier amenaza que pueda poner en peligro las empresas tanto públicas como privadas, pues en otro caso podría dañarse la salud empresarial”.

Los problemas de seguridad de la información alcanzan a todas las empresas, más aun a las Universidades que forman personal en el área informática, que tiene alto volumen de información relacionada con ámbitos financieros y académico, por esta variedad e importancia la hacen blanco de posibles ataques.

La Universidad Técnica de Babahoyo es una institución pública de Educación Superior, ubicada en Babahoyo, provincia de Los Ríos, actualmente cuenta con 6250 estudiantes, profesores contratados 435, titulares y 72 empleados contratados 36, y 225 empleados titulares.

La Dirección de TI (Tecnología de la Información) es el departamento encargado de resguardar los servidores de las distintas aplicaciones que manejan elevados volúmenes de información, de los servicios de Aulas Virtuales, Sistema Académico, Páginas Web, Servidor de Gestión financiera, y dispositivos de servicios de Intranet e

Recibido: Marzo 2016. **Aceptado:** Mayo 2016

Internet. Estos activos son importantes para la ejecución de actividades. Por lo tanto es necesario analizar y calcular el riesgo que están sometidos los activos para gestionarlos y minimizar las consecuencias en las operaciones.

DESARROLLO

El presente estudio pretendió, evaluar los riesgos que están sometidos los activos del departamento de TI desarrollado en tres fases: la primera consistió en una investigación bibliográfica, la segunda una investigación de campo y la tercera un cálculo, análisis y tratamiento del riesgo de los activos del departamento de TI.

La investigación bibliográfica porque permitió el análisis y fundamentación científica, para ampliar el conocimiento sobre el problema y las soluciones con el apoyo de textos, trabajos previos distribuidos por medio impreso o electrónico.

La investigación de campo porque permitió describir todos los hechos observados dentro de la Universidad Técnica de Babahoyo y de su infraestructura tecnológica y cómo está actualmente llevando la gestión de la seguridad, con el propósito de describirlos, interpretarlos y entender su naturaleza, así como sus causas y efectos que estos problemas pueden conducir, haciendo uso métodos técnicas e instrumentos de los enfoques de investigación conocidos.

La población está conformada por el personal administrativo encargado de uso y control de los servicios del departamento de TI.

El levantamiento de la información se llevó a cabo a través de entrevistas, cuestionarios y reuniones de trabajo.

La entrevista se la realizó al director de TIC y al personal que labora en el departamento para obtener información sobre sus conocimientos, y procedimientos a seguir en caso de falla y pérdida de la información en la infraestructura tecnológica.

El cuestionario se utilizó porque permitió obtener información necesaria, sobre la existencia de políticas, normas y procedimientos de seguridad de la información, la cual se obtuvo con la colaboración de los empleados de la Universidad Técnica de Babahoyo.
La reunión de trabajo se utilizó para la elaboración de la valoración de los activos, y el análisis de las vulnerabilidades que podían actuar en cada uno de los activos del departamento de tecnologías de la información y comunicación.

Una vez obtenidos los datos e información de los diferentes departamentos involucrados a través de visitas, se precedió al análisis e interpretación del cuestionario y que se utilizó preguntas con métricas cuantitativas y cualitativas, como la de Likert, de razón, de orden, dicotómicas.

Análisis del Riesgo

“El riesgo es definido como la probabilidad que una amenaza pueda explotar una vulnerabilidad en particular” (Peltier, 2001).

El proceso de aseguramiento de la información es un proceso que para establecer medidas de seguridad en una empresa se convierte en una práctica ardua, por lo que es necesario realizar un análisis de riesgo para facilitar este proceso.

Recibido: Marzo 2016. **Aceptado:** Mayo 2016
Universidad Regional Autónoma de los Andes UNIANDES

Este análisis de riesgo a que están sometidos los activos es crucial para poder gestionarlos, está basado en una identificación de los activos y todas las dependencias jerárquicas de estos y las amenazas que pueden afectarlos, luego se realiza una estimación de impactos y se obtiene el riesgo de la organización.

El diagnóstico de análisis de riesgo de la empresa es válido solo para ese momento y se debe dar el seguimiento respectivo a las políticas de seguridad de la información implementadas para disminuir el riesgo, esto se debe porque a través del tiempo se hacen adquisiciones de nuevos activos por lo tanto existen nuevas amenazas que pueden afectarlos. Entonces la empresa debe continuamente realizar un nuevo análisis de riesgo para mitigarlos y tener su información asegurada.

Existen varias metodologías y estándares para gestionar la seguridad de la información entre ellos podemos mencionar los principales ISO, ITIL y COBIT entre otros. Estás normas y estándares hay que adaptarlos al contexto particular de las empresas.

Las Normas ISO 27001-2013 especifican los requisitos para la implantación del SGSI (Sistemas de Gestión de la Seguridad de la Información). Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos, existen otras normas complementarias como ISO 27002-2013 que especifica los Dominios, Objetivos de Control y Controles que se deben implementar para mejora del SGSI y la Norma ISO 27005 que surgió en el 2009, proporciona directrices para la gestión del riesgo en la seguridad de la información, dando soporte a los SGSI.

Gestión de riesgo

"El análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, controla todas las actividades. La fase de tratamiento estructura las acciones a realizar en materia de seguridad para anular las amenazas detectadas por el análisis" (Amutio, 2013).

Objetivo de evaluar el riesgo

Después de realizar un análisis de las metodologías y métodos se propone el siguiente esquema para análisis y evaluación del riesgo.

Figura 1: Metodología de Análisis de Riesgo. **Fuente:** Elaboración propia

Recibido: Marzo 2016. **Aceptado:** Mayo 2016

Análisis del Riesgo.

Definición del Alcance.

Este es el primer paso de la metodología planteada esta investigación comprende el departamento de Tecnologías de la Información y todos los equipos de la parte administrativa de la Universidad Técnica de Babahoyo es decir los equipos desplazados desde el centro de datos hasta los racks que proveen los servicios a los computadores de los laboratorios y oficinas de cada una de las cuatro facultades.

Identificación de los Activos.

Una vez definidos los alcances se procede a realizar una identificación de los activos del departamento de TIC, según ISO 27005 estos pueden ser:

- Activos Primarios**.** Son aquellos que implican procesos del negocio.
- Información. Son considerados manuales de usuario entre otros
- Activos de Soporte .Estos dependen los elementos primarios del alcance, de todos los tipos: hardware, software, redes, personal, sitio, estructura de la organización.

En la **Tabla 1** se muestra una parte los activos identificados del departamento de TIC y sus áreas responsables.

ACTIVOS DE SOPORTE	AREA RESPONSABLE DEL BIEN
UTM SOPHOS	REDES Y TELECOMUNICACIONES
SWICH	REDES Y TELECOMUNICACIONES
TRANSEIVER	REDES Y TELECOMUNICACIONES
FIBRA OPTICA	REDES Y TELECOMUNICACIONES
ROUTER INALAMBRICO	REDES Y TELECOMUNICACIONES
ROUTERS	REDES Y TELECOMUNICACIONES
ARMARIO RACKEABLE	REDES Y TELECOMUNICACIONES
ORGANIZADORES DE CABLE	REDES Y TELECOMUNICACIONES
CABLEADO ESTRUCTURADO	REDES Y TELECOMUNICACIONES
SERVIDOR	MANTENIMIENTO Y SOPORTE
PORTATIL	MANTENIMIENTO Y SOPORTE
EQUIPOS DE ESCRITORIO	MANTENIMIENTO Y SOPORTE
INSTALACION ELECTRICA	MANTENIMIENTO Y SOPORTE
CENTRAL DE AIRE	MANTENIMIENTO Y SOPORTE
DISCOS DUROS EXTERNOS	MANTENIMIENTO Y SOPORTE
DISCOS DUROS DE SERVIDORES	MANTENIMIENTO Y SOPORTE

Recibido: Marzo 2016. **Aceptado:** Mayo 2016
Universidad Regional Autónoma de los Andes UNIANDES

UPS	MANTENIMIENTO Y SOPORTE
SISTEMA OPERATIVO WINDOWS SERVER	MANTENIMIENTO Y SOPORTE
SISTEMA OPERATIVO LINUX CENTOS	MANTENIMIENTO Y SOPORTE
ANTIVIRUS	MANTENIMIENTO Y SOPORTE
CORREO ELECTRONICO	DESARROLLO
DSPACE	DESARROLLO
MOODLE	DESARROLLO
WEB SITE	DESARROLLO
ERP	DESARROLLO
EKUBIBLIO	DESARROLLO
SEGUIMIENTO GRADUADOS	DESARROLLO
HELPDESK	DESARROLLO
OLIMPO INVENTARIOS Y ACTIVOS FIJOS	DESARROLLO
SEGUIMIENTOS DE DOCUMENTOS	DESARROLLO
URKUND	DESARROLLO
ADMINISTRADOR DE RED	REDES Y TELECOMUNICACIONES
DESARROLLADOR	DESARROLLO

ACTIVOS DE INFORMACIÓN	
LICENCIA DE USO DE UTM SOPHOS	REDES Y TELECOMUNICACIONES
LICENCIA DE MICROSOFT WINDOWS SERVER 2008 R2	MANTENIMIENTO Y SOPORTE
GARANTIAS DE SERVIDORES	MANTENIMIENTO Y SOPORTE
GARANTIAS DE ROUTER Y SWICH CISCO	REDES Y TELECOMUNICACIONES
GARANTIAS DE SWICH HP	REDES Y TELECOMUNICACIONES
TECNICO DE SOPORTE	MANTENIMIENTO Y SOPORTE

Tabla 2: Activos de la Unidad de TI. **Fuente:** Elaboración propia

Valoración de Activos.

Esta es una de las partes más importantes dentro de la fase de Análisis de Riesgo, se lo realiza con el objetivo de establecer el valor de afectación de este activo en cuanto a la utilidad de los servicios y procesos de negocio de la empresa. La base para la valoración de los activos del departamento de TIC es el costo en que se incurre debido a la perdida de la confidencialidad, integridad y disponibilidad como resultado de un incidente. Esta valoración proporcionará las dimensiones que tienen los elementos

Recibido: Marzo 2016. **Aceptado:** Mayo 2016
Universidad Regional Autónoma de los Andes UNIANDES

importantes para el valor del activo. Para este proceso se realiza una escala de valoración que se detalla en la **tabla 3.**

PARAMETROS/VALORACION		DEPENDENCIA	FUNCIONALIDAD	INTEGRIDAD , CONFIDENCIALIDAD Y DISPONIBILIDAD
1	MUY BAJO	Ningún otro activo depende de este para la entrega de servicios	Activo con capacidades tecnológicas muy limitadas	La divulgación, modificación y no disponibilidad de su archivo de configuración puede afectar de forma insignificante la entrega de servicios
2	BAJO	Pocos activos dependen de este para la entrega de servicios	Activo con capacidades tecnológicas limitadas	La divulgación, modificación y no disponibilidad de su archivo de configuración podría afectar en parte la entrega de servicios
3	MEDIO	Una mínima cantidad de activos dependen de este para la entrega de servicios	Activo con capacidades tecnológicas avanzadas	La divulgación, modificación y no disponibilidad de su archivo de configuración podría afectar significativamente la entrega de servicios
4	ALTO	Un número considerable de activos dependen de éste para la entrega de servicios	Activo con capacidades tecnológicas muy avanzadas.	La divulgación, modificación y no disponibilidad de su archivo de configuración podría afectar gravemente la entrega de servicios.
5	CRITICO	Todos los activos dependen de éste para la entrega de servicios	Activo con capacidades tecnológicas de última generación	La divulgación, modificación y no disponibilidad de su archivo de configuración podría afectar totalmente la entrega de servicios

Tabla 3: Escala de valoración de los activos. **Fuente:** Elaboración propia

La tabla de la valoración de activos se la obtuvo en las reuniones de trabajo con los miembros del departamento de tecnologías realizando un análisis de la dependencia de entrega de servicios del activo, si del activo dependen otros, la funcionalidad en

Recibido: Marzo 2016. **Aceptado:** Mayo 2016
Universidad Regional Autónoma de los Andes UNIANDES

cuanto a las capacidades y la afectación del activo en caso de falla sobre la integridad de la confidencialidad y disponibilidad de los servicios.

A continuación se realizó la identificación de las funciones del activo y se le asigna un valor de acuerdo a la escala realizada de la pérdida de confidencialidad, integridad y disponibilidad de las funciones que provee al suscitarse algún incidente. Este proceso se encuentra detallado en la **tabla 4**.

ACTIVOS DE SOPORTE	Funciones	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	PROMEDIO
UTM SOPHOS	Core núcleo de la red recibe las conexiones de internet de los proveedores y controla las conexiones hacia todas las instalaciones de la UTB	5	4	5	5
SWICH	controla conectividades hacia los equipos de los empleados y laboratorios si existe una falla se puede cambiar pero se pierde el servicio	2	4	2	3
TRANSEIVER	realiza funciones de recepción de una comunicación, que permite un procesamiento para también realizar la Transmisión de esta información	2	2	5	3
FIBRA OPTICA	provee la conexión de servicios de internet de los proveedores y hacia las diferentes dependencias de la Universidad	2	3	5	3
ROUTER INALAMBRICO	provee de servicios de internet al campus universitario	4	5	5	5
ROUTERS	poseen configuradas las redes de las diferentes dependencias y unidades de la UTB	4	5	5	5
ARMARIO RACKEABLE	mantiene organizado y estable toda la parte física de la infraestructura tecnológica	2	2	2	2
ORGANIZADORES DE CABLE	mantiene organizados los cables de la UTB identificados a quienes les provee conectividad	2	2	2	2
CABLEADO ESTRUCTURADO	provee de conectividad a las estaciones de trabajo y dispositivos	2	2	3	2
SERVIDOR	contiene la configuración de los software y servicios de la Universidad y tienen	4	4	5	4

Recibido: Marzo 2016. **Aceptado:** Mayo 2016
Universidad Regional Autónoma de los Andes UNIANDES

	alojada base de datos				
PORTATIL	permite acceder a los servicios y acceso a las redes	5	5	4	5
EQUIPOS DE ESCRITORIO	permite acceder a los servicios y acceso a las redes	5	5	4	5
INSTALACION ELECTRICA	da energía a todos los equipos de la universidad	2	2	5	3
CENTRAL DE AIRE	mantiene en clima apropiado a los dispositivos del data center para evitar daños por calentamiento	2	2	5	3
DISCOS DUROS EXTERNOS	permite almacenar información	5	4	5	5
DISCOS DUROS DE SERVIDORES	mantiene la información de la configuración e información de los software de la universidad	4	3	5	4
UPS	mantiene energía de reserva hasta por seis hora en caso de fallas eléctricas	2	2	5	3
SISTEMA OPERATIVO WINDOWS SERVER	permite ejecutar las aplicaciones y accesos a los equipos de escritorio a estos servicios	4	4	5	4
SISTEMA OPERATIVO LINUX CENTOS	permite ejecutar las aplicaciones y accesos a los equipos de escritorio a estos servicios	4	4	5	4
ANTIVIRUS	permite mantener alertas y limpieza de amenazas en los equipos de escritorio	2	2	2	2
CORREO ELECTRONICO	permite enviar y recibir correo electrónico	2	2	2	2
DSPACE	repositorio de documentos y tesis de la universidad	4	4	5	4
MOODLE	Entorno virtual de aprendizaje	4	4	5	4
WEB SITE	espacio de información a la comunidad universitaria hacia el público en general	4	5	4	4
ERP	aplicación para dar seguimiento a plan de mejoras de la universidad y plan de desarrollo institucional	3	4	5	4
EKUBIBLIO	aplicación para el manejo de la bibliotecas de la Universidad	3	3	5	4
SEGUIMIENTO GRADUADOS	aplicación para la gestión y realización de encuestas a los graduados de la universidad	2	2	3	2

Recibido: Marzo 2016. **Aceptado:** Mayo 2016

HELPDESK	aplicación de soporte a los usuarios de la universidad se atiende todos los requerimientos al departamento de sistemas	4	4	5	4
OLIMPO INVENTARIOS Y ACTIVOS FIJOS	software que permite gestión de todos los activos de la Universidad así como los egresos e ingresos	5	5	5	5
SEGUIMIENTOS DE DOCUMENTOS	aplicación que permite gestionar el flujo de los procesos de la Universidad	3	3	5	4
URKUND	software anti plagio de investigaciones de la Universidad	2	2	2	2
ADMINISTRADOR DE RED	persona que esta cargo y tiene conocimiento sobre la gestión y configuración de la red	5	4	5	5
DESARROLLADOR	persona que realiza y actualiza las aplicaciones de la Universidad	5	2	4	4
TECNICO DE SOPORTE	persona que se encarga de dar mantenimiento y soporte a las fallas de la infraestructura tecnológica	5	4	3	4
ACTIVOS DE INFORMACIÓN					
LICENCIA DE USO DE UTM SOPHOS	documento que otorga el serial para la activación del software del equipo	5	4	4	4
LICENCIA DE MICROSOFT WINDOWS SERVER 2008 R2	documento que otorga el serial para la activación del software del equipo	5	4	4	4
GARANTIAS DE SERVIDORES	documento que establece criterios y tiempo de garantía de los equipos	5	4	4	4
GARANTIAS DE ROUTER Y SWICH CISCO	documento que establece criterios y tiempo de garantía de los equipos	5	4	4	4
GARANTIAS DE SWICH HP	documento que establece criterios y tiempo de garantía de los equipos	5	4	4	4

Tabla 4: Valoración de los activos. **Fuente:** Elaboración propia

Cálculo de ocurrencia de las amenazas y facilidad de explotación.

Una vez realizada la valoración de los Activos del departamento de TIC a través de reuniones de trabajo, inspección física y revisión de documentos. A continuación se realizó la identificación de las amenazas, vulnerabilidades que afectan a cada uno de los activos. “Una amenaza es una acción que trata de aprovechar una vulnerabilidad de un sistema informático para provocar un impacto sobre él tomar el control del mismo. Trata de acciones tanto intencionadas como fortuitas que pueden llegar a poner en riesgo un sistema” (Roa, 2013).

Recibido: Marzo 2016. **Aceptado:** Mayo 2016

El listado de ejemplos de vulnerabilidades con sus respectivas amenazas se encuentra en la norma ISO 27005 y detallado en la **tabla 5**.

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información
	Falta de esquemas de reemplazo periódico. Susceptibilidad a la humedad, el polvo y la suciedad	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Falta de control de cambio con configuración eficiente	Error en el uso
	Susceptibilidad a las variaciones de tensión	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurto de medios o documentos
	Falta de cuidado en la disposición final	Hurto de medios o documentos
	Copia no controlada	Hurto de medios o documentos

Tabla 5: Ejemplo de vulnerabilidades y amenazas. **Fuente:** ISO 27005

En la **tabla 6** se realizó a través de reuniones de trabajo con los responsables de los activos una escala de valoración para las amenazas y probabilidad de ocurrencia de explotar vulnerabilidades con las bases especificadas en la norma ISO 27005.

PARAMETROS/VALORACION		DESCRIPCIÓN
1	BAJO	Amenazas cuya probabilidad de explotar vulnerabilidades es muy baja.
2	MEDIO	Amenazas que con poca frecuencia explotan vulnerabilidades.
3	ALTO	Amenazas que frecuentemente explotan vulnerabilidades.

Tabla 6: Probabilidad que ocurra la amenaza. **Fuente:** ISO 27005

En la **Tabla 7** se muestra el resultado que se obtuvo a través de la observación y reuniones trabajo para obtener las amenazas y vulnerabilidades que influyen en cada uno de los activos esto constituye la base para realizar el cálculo de la ocurrencia de la amenaza y la facilidad que puede ser explotada.

Recibido: Marzo 2016. **Aceptado:** Mayo 2016
Universidad Regional Autónoma de los Andes UNIANDES

ACTIVOS	AMENAZAS	VULNERABILIDAD	PROBABILIDAD OCURRA LA AMENZA	Facilidad de explotación
PORTATIL	INCUMPLIMIENTO EN EL MANTENIMIENTO	MANTENIMIENTO INSUFICIENTE	ALTA	ALTA
	HURTO DE MEDIOS O DOCUMENTOS	ALMACENAMIENTO SIN PROTECCIÓN	MEDIA	MEDIA
EQUIPOS DE ESCRITORIO	INCUMPLIMIENTO EN EL MANTENIMIENTO	MANTENIMIENTO INSUFICIENTE	ALTA	ALTA
	HURTO DE MEDIOS O DOCUMENTOS	COPIA NO CONTROLADA	ALTA	ALTA
		ALMACENAMIENTO SIN PROTECCIÓN	ALTA	ALTA
	ERROR DE USO	FALTA DE CONTROL DE CAMBIO EN LA CONFIGURACION	MEDIA	MEDIA

Tabla 7: Cálculo que ocurra la amenaza y facilidad con la que puede ocurrir sobre los activos**.**
Fuente: Elaboración propia

Evaluación del Riesgo.

"Es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente" (Roa, 2013).

Esta evaluación del riesgo se la realizó por una combinación de los valores de los activos y los niveles de seguridad requeridos, para evitar que las amenazas exploten las vulnerabilidades.

Estimación del riesgo.

En esta etapa se asignan valores a la probabilidad y a las consecuencias de un riesgo (ISO 27005, 2009). Esta escala se detalla en la **tabla 8.**

Valores	Nivel de riego
8	ALTO
6-7	MEDIO ALTO
4-5	MEDIO
2-3	MEDIO BAJO
0-1	BAJO

Tabla 8: Estimación del riesgo. **Fuente:** Elaboración Propia

Cálculo de Riesgo sobre los Activos.

La siguiente actividad fue la determinación de cada tipo de amenaza, para cada agrupación de activos con los cuales se relaciona el tipo de amenaza, con el fin de habilitar la evaluación de los niveles de amenazas (probabilidad de ocurrencia) y niveles de vulnerabilidades (facilidad de explotación por parte de las amenazas para causar consecuencias adversas). Cada respuesta a un interrogante suscita un puntaje. Estos puntajes se acumulan a través de una base de conocimientos y se compara con los rangos (ISO 27005,2009).Esto identifica los niveles de amenaza en

Recibido: Marzo 2016. **Aceptado:** Mayo 2016
Universidad Regional Autónoma de los Andes UNIANDES

una escala de alto a bajo y los niveles de vulnerabilidad de manera similar, tal como se presenta en la **tabla 9**, diferenciando entre los tipos de consecuencias según sea pertinente.

	Probab. de ocurrencia – 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**

Tabla 9: Evaluación del Riesgo**. Fuente:** ISO 27005

Los valores del activo, los niveles de amenaza y vulnerabilidad, pertinentes para cada tipo de consecuencias se contrastan en una matriz con el fin de identificar para cada combinación la medida pertinente de riesgo en una escala de 0 a 8. Los valores se ubican en la matriz de manera estructurada. En la **tabla 10** se muestra los activos, amenazas y la vulnerabilidad que presenta el activo su valoración la probabilidad de ocurrencia y facilidad de explotación.

Activos	**Amenazas**	**Vulnerabilidad**	**Valor activo**	**Probab. que ocurra la amenaza**	**Facilidad de explotación**	**Riesgo**
Portátil	Incumplimiento en el mantenimiento	Mantenimiento insuficiente	5	ALTA	ALTA	8
	Hurto de medios o documentos	Almacenamiento sin protección	5	MEDIA	MEDIA	6
Equipos de escritorio	Incumplimiento en el mantenimiento	Mantenimiento insuficiente	5	ALTA	ALTA	8
	Hurto de medios o documentos	Copia no controlada	5	ALTA	ALTA	8
		Almacenamiento sin protección	5	ALTA	ALTA	8
	Error de uso	Falta de control de cambio en la configuración	5	MEDIA	MEDIA	6

Tabla 10: Evaluación del Riesgo. **Fuente:** Elaboración Propia

Gestión del Riesgo.

"La gestión del riesgo es un proceso separado que utiliza los resultados del análisis de riesgos para seleccionar e implantar las medidas de seguridad (salvaguardas) adecuadas para controlar los riesgos identificados."(Heredero, 2006).

Recibido: Marzo 2016. **Aceptado:** Mayo 2016

Tratamiento del Riesgo.

El tratamiento de riesgo se lo define como el conjunto de decisiones tomadas con cada activo de información. "ISO lo establece como el proceso de selección e implementación de medidas para modificar el Riesgo" (ISO, 2013). Como resultado de las reuniones de trabajo con el departamento de TIC se estableció cada uno de los criterios de descripción del riesgo y las acciones necesarias para mitigarlo.

Los criterios de aceptación de riesgo demandados por la Universidad Técnica de Babahoyo y el departamento de TIC, establece que riesgos de niveles "Alto" y "Medio Alto" se consideran inaceptables y deben ser tratados de forma inmediata con los recursos necesarios requeridos. Así mismo, para los niveles "Medio" y "Bajo" se requiere de un registro en el cual la gerencia demuestre que se acepta el riesgo asociado a estos activos. Este tratamiento del riesgo se encuentra detallado en la **tabla 10.**

Valores	Nivel de riego	Descripción del riesgo y acciones necesarias
8	ALTO	Requiere fuertes medidas correctivas. Planes de tratamiento implementados en corto tiempo, reportados y controlados con atención directa de alta dirección
6-7	MEDIO ALTO	Requiere vigilancia de alta dirección con planes de tratamiento implementados y reportados a los gerentes de UTB
4-5	MEDIO	Se requieren acciones correctivas controladas por grupos de manejo de incidentes en período de tiempo razonable
2-3	MEDIO BAJO	Riego aceptable-Administrado por los grupos de incidentes bajo procedimientos normales de control
0-1	BAJO	El propietario del activo lo administra con procedimientos rutinarios o decide aceptar el riesgo

Tabla 11: Tratamiento del riesgo. **Fuente:** Elaboración Propia

Aplicabilidad de Controles.

A continuación se plantean los controles que pueden ser implementados, una vez identificados y evaluados los procesos de tratamiento del riesgo, se determina qué objetivos de control y controles se van a implementar.

La declaración de aplicabilidad incluye los objetivos de control y controles que serán aplicados y los que serán excluidos. La declaración de aplicabilidad da la oportunidad

Recibido: Marzo 2016. **Aceptado:** Mayo 2016
Universidad Regional Autónoma de los Andes UNIANDES

a la empresa de que asegure que no se ha omitido algún control.

En la **tabla 12** se presenta el enunciado de aplicabilidad tomando en cuenta los Dominios, Objetivos de Control y controles de la Norma ISO 27002.

CONTROL ISO 27002	CONTROLES	Aplicable SI	NO
5. POLÍTICA DE SEGURIDAD.	5.1 Política de seguridad de la información.		
	5.1.1 Documento de política de seguridad de la información.		
	5.1.2 Revisión de la política de seguridad de la información.	X	
		X	
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.	6.1 Organización interna.		
	6.1.1 Compromiso de la Dirección con la seguridad de la información.		
	6.1.2 Coordinación de la seguridad de la información.	X	
	6.1.5 Acuerdos de confidencialidad.	X	
	6.1.6 Contacto con las autoridades.	X	
	6.1.7 Contacto con grupos de especial interés.	X	
	6.1.8 Revisión independiente de la seguridad de la información.	X	
		X	
7. GESTIÓN DE ACTIVOS.	7.1 Responsabilidad sobre los activos.		
	7.1.1 Inventario de activos.		
	7.1.2 Propiedad de los activos.	X	
	7.1.3 Uso aceptable de los activos.	X	
	7.2 Clasificación de la información.	X	
	7.2.1 Directrices de clasificación.		
	7.2.2 Etiquetado y manipulado de la información.	X	
8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.			
9. SEGURIDAD FÍSICA Y DEL ENTORNO.	**9.2 Seguridad de los equipos.**		
	9.2.1 Emplazamiento y protección de equipos.		
	9.2.4 Mantenimiento de los equipos.	X	
	10.1 Responsabilidades y procedimientos de operación.	X	

Recibido: Marzo 2016. **Aceptado:** Mayo 2016
Universidad Regional Autónoma de los Andes UNIANDES

	10.1.2 Gestión de cambios.		
	10.5 Copias de seguridad.	X	
	10.5.1 Copias de seguridad de la información.		
	10.6 Gestión de la seguridad de las redes.	X	
	10.6.1 Controles de red.		
	10.6.2 Seguridad de los servicios de red.	X	
	10.7 Manipulación de los soportes.	X	
	10.7.1 Gestión de soportes extraíbles.		
	10.7.2 Retirada de soportes.	X	
	10.7.3 Procedimientos de manipulación de la información.	X	
	10.7.4 Seguridad de la documentación del sistema.	X	
	10.8 Intercambio de información.	X	
	10.9 Servicios de comercio electrónico.		
	10.9.1 Comercio electrónico.		
	10.9.2 Transacciones en línea.		
	10.9.3 Información públicamente disponible.		
	10.10 Supervisión.		
	10.10.1 Registros de auditoría.		
	10.10.2 Supervisión del uso del sistema.	X	
	10.10.5 Registro de fallos.	X	
		X	
11. CONTROL DE ACCESO.	**11.1 Requisitos de negocio para el control de acceso.**		
	11.1.1 Política de control de acceso.		
	11.2 Gestión de acceso de usuario.	X	
	11.2.1 Registro de usuario.		
	11.2.2 Gestión de privilegios.	X	
	11.2.3 Gestión de contraseñas de usuario.	X	
	11.3 Responsabilidades de usuario.	X	
	11.3.1 Uso de contraseñas.		
	11.3.2 Equipo de usuario	X	

Recibido: Marzo 2016. **Aceptado:** Mayo 2016

	desatendido.		
	11.3.3 Política de puesto de trabajo despejado y pantalla limpia.	X	
	11.4 Control de acceso a la red.	X	
	11.4.3 Identificación de los equipos en las redes.		
	11.4.4 Protección de los puertos de diagnóstico y configuración remotos.	X	
	11.4.5 Segregación de las redes.	X	
	11.4.6 Control de la conexión a la red.	X	
	11.4.7 Control de encaminamiento (routing) de red.	X	
	11.5 Control de acceso al sistema operativo.	X	
	11.5.1 Procedimientos seguros de inicio de sesión.		
	11.5.2 Identificación y autenticación de usuario.	X	
	11.5.3 Sistema de gestión de contraseñas.	X	
	11.5.4 Uso de los recursos del sistema.	X	
	11.5.5 Desconexión automática de sesión.	X	
	11.5.6 Limitación del tiempo de conexión.	X	
		X	
12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFO.	**12.1 Requisitos de seguridad de los sistemas de información.**		
	12.2 Tratamiento correcto de las aplicaciones.		
	12.2.1 Validación de los datos de entrada.		
	12.2.2 Control del procesamiento interno.	X	
	12.2.3 Integridad de los mensajes.	X	
	12.2.4 Validación de los datos de salida.		
	12.3 Controles criptográficos.		
	12.3.1 Política de uso de los controles criptográficos.		
	12.3.2 Gestión de claves.		
	12.4 Seguridad de los archivos de sistema.	X	
	12.4.3 Control de acceso al código		

Recibido: Marzo 2016. **Aceptado:** Mayo 2016
Universidad Regional Autónoma de los Andes UNIANDES

	fuente de los programas.		
	12.5 Seguridad en los procesos de desarrollo y soporte.	x	
	12.5.1 Procedimientos de control de cambios.		
	12.6 Gestión de la vulnerabilidad técnica.	X	
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.			
14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	14.1.4 Marco de referencia para la planificación de la continuidad del negocio.		
		X	
15. CUMPLIMIENTO.	15.1.3 Protección de los documentos de la organización.		
		X	

Tabla 12: Aplicabilidad de Controles. **Fuente:** ISO 27002

La **tabla 12** presenta los objetivos, dominios y controles que se deben aplicar proporcionados por la Norma ISO 27002 y esta selección se justificó sobre la base de la evaluación de riesgo y su tratamiento.

CONCLUSIONES

Entre las principales conclusiones que se pueden obtener de esta investigación tenemos:

- Los activos que se encuentran en custodia del departamento de TIC manejan datos críticos de la Universidad Técnica de Babahoyo, de allí la importancia de protegerlos.
- En la metodología planteada para el análisis, evaluación y gestión del riesgo toma como base la norma ISO-27005 y luego de un análisis está adaptada al contexto de la Universidad Técnica de Babahoyo.
- Para realizar la aplicabilidad de controles es necesario tener en cuenta las actualizaciones que se realizan en la Norma ISO 27002, porque se incorporan nuevos controles a las tecnologías.
- Una vez realizado el proceso de evaluación del riesgo y la aplicabilidad de controles, se debe realizar en ciertos periodos de tiempo un análisis y evaluación del riesgo nuevamente para establecer que controles se deben mejorar e incorporar, por que continuamente el departamento de TIC incorpora nuevos servicios.
- La evaluación del riesgo es identificar y ponderar los riesgos que están expuestos los activos de la empresa estos pueden ser software, hardware, documentación y servicios, para finalizar con una selección de controles que ayudan a mitigar el riesgo.

Recibido: Marzo 2016. **Aceptado:** Mayo 2016
Universidad Regional Autónoma de los Andes UNIANDES

REFERENCIAS.

AENOR (2009). ISO 27005. Gestión del Riesgo en la seguridad de la información. España: AENOR

Amutio, A. (2013). MAGERIT versión 3.0 Metodología de Análisis y gestión de Riesgo de los Sistemas de Información: España. Ministerio de Hacienda y administración Pública.

Bernard, P. (2011): Foundations of ITIL®. Ed. Van Haren Publishing.

Díaz, G., Alzórriz, I., & Castro, M. (2014).Procesos y Herramientas para la seguridad de redes. España: Publicaciones UNED.

Fernández, C., & Piattini, M. (2012).Modelo para el Gobierno de las TIC basado en las normas ISO. España: AENOR.

Helat, A. (2003): Remembrance of Data Passed: A Study of Disk Sanization Practices: IEEE Security & Privacy: IEEE Computer Society.

Heredero, C. (2006).Dirección y gestión de los sistemas de información en la empresa una visión integradora. España: ESIC Editorial.

Roa, J. (2013).Seguridad Informática. España: McGraw-Hill.

Recibido: Marzo 2016. **Aceptado:** Mayo 2016
Universidad Regional Autónoma de los Andes UNIANDES