UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

OCTUBRE 2019-MARZO 2020

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TITULO DE

INGENIERO EN SISTEMAS

TEMA:

Análisis del riesgo de las tics en el laboratorio de computo de la unidad educativa pueblo nuevo mediante la aplicación de la norma iso 27005.

EGRESADO:

Ronald Isidro Franco Cabrera

TUTOR:

ING. Jose Mejia Vitery, MSc.

AÑO 2020

INTRODUCCIÓN

En la actualidad las tecnologías de la información y la comunicación(TICs) están inmersas casi en la mayoría de entidades u organizaciones por el gran aporte que nos brindan para poder efectuar un sinfín de tareas en distintos campos ya sean laboral ,académicos ,o en nuestro diario vivir ,está en nosotros poder sacarle el mayor provecho posible y manejarlas de la manera más acertada posible ya que siempre están en constante actualización o cambios, debemos también tener una visión clara de los riesgos que estamos expuestos a una mala utilización de las tics o a una mala gestión de los mismo al no contar con niveles de seguridad aceptables .

En este estudio de caso se analizará los riesgos de las TICs (Tecnologías de Información y Comunicación) de la Unidad Educativa mediante la aplicación de la normativa International Standards Organization ISO 27005, con la ayuda de esta norma vamos a gestionar los riesgos de las TICs, como pueden ser programas o aplicaciones en ambientes vulnerables, tecnologías obsoletas, sistemas operativos sin actualizaciones.

Para la aplicación del análisis de riesgo partiremos desde la realización del inventario de activos y su área responsable además del personal inmerso, luego se llevará a cabo la valoración de los activos de acuerdo al nivel de confiabilidad, disponibilidad e integridad para el respectivo cálculo de la ocurrencia, valoración del riesgo a través de métodos cualitativos y cuantitativos y cálculo del riesgo.

La finalidad de esta investigación es que la Unidad Educativa Pueblo Nuevo pueda llevar a cabo sus tareas diarias de una manera óptima como son los métodos de enseñanza-aprendizaje a través de las TICs contando con un nivel aceptable de seguridad, disponibilidad, brindando confianza tanto para los docentes, personal administrativo y alumnos que puedan realizar sus trabajos sin tener complicaciones futuras en lo que respecta a los riesgos informáticos.

El desarrollo de este estudio de caso hace referencia a uno de sus campos de investigación de la carrera de ingeniería en sistemas que se centra en los procesos de transmisión de datos y telecomunicaciones.

DESARROLLO

La UEPN (Unidad Educativa Pueblo Nuevo) situada en Pueblo Nuevo, cantón Babahoyo Provincia de Los Ríos, es un establecimiento educativo con el objetivo de ofrecer una formación de calidad y calidez a seres humanos competentes, apegados a los valores y comprometidos con el medio ambiente.

Unidad Educativa Pueblo Nuevo tiene como misión ofrecer una educación de calidad a jóvenes, potencializando su formación integral en base al desarrollo del pensamiento crítico, lógico, creativo y emprendedor, la permanente innovación tecnológica y cultivo de principios éticos y ecológicos para que puedan desenvolverse en un mundo globalizado aplicando la filosofía del buen vivir. Formar e incorporar estudiantes que opten por el bachillerato en ciencias o técnico, basado en una educación centrada en los educandos que promueva el desarrollo académico, cultural, artístico y el cuidado de la naturaleza.

Actualmente la situación problemática que se logra evidenciar en la Unidad Educativa Pueblo Nuevo se centra en las vulnerabilidades o riesgos a los que se encuentran expuestas las TICs (Tecnologías de Información y Comunicación) del laboratorio de cómputo de la institución ,cabe mencionar debilidades tanto en la seguridad de sus activos ya sea física o lógica, falta de software de antivirus ,tecnologías obsoletas , poca ventilación, falta de mantenimiento a los activos, sin embargo , en la actualidad se pude mitigar o gestionar el riesgo para defender la integridad de las TICs en entidades con riesgos informáticos usuales.

Sin lugar a duda en la actualidad toda organización o entidad sea pública o privada cuenta con tecnologías de información y comunicación para lograr sus objetivos comunes o tareas diarias, por lo tanto, salvaguardarlas de personas malintencionadas o eventos que atenten contra la seguridad, integridad, disponibilidad o confidencialidad de los activos es una obligación , dicho esto se

tratara de instaurar los niveles adecuados de seguridad de las TICs mediante una metodología para la gestión del riesgo de la información y las tecnologías de la información y la comunicación para que la institución pueda llevar a cabo sus tareas diarias de una manera óptima como son los métodos de enseñanza-aprendizaje a través de las TICs contando con un nivel aceptable de seguridad, disponibilidad, brindando confianza tanto para los docentes, personal administrativo y alumnos que puedan realizar sus trabajos sin tener complicaciones futuras en lo que respecta a los riesgos informáticos.

El objetivo de este proyecto es analizar el riesgo de las tecnologías de información y comunicación (TICs) en el laboratorio de cómputo de la Unidad Educativa Pueblo Nuevo, es así como el diseño de estudio a utilizar en el presente estudio de caso está basada en la investigación descriptiva, cabe mencionar que se centra en la observación además de representar el comportamiento de nuestro objeto de estudio por lo cual nos basaremos en el método de investigación inductivo que nos ayudara a estudiar de una manera más a fondo el escenario, contexto y características de los hechos.

En consecuencia optaremos por las la técnica de investigación de campo tomando como herramientas la observación como se mencionó anteriormente y la entrevista para la respectiva recolección de la información y también nos apoyaremos en la normativa International Standards Organization ISO 27005 como instrumento de investigación, ya que con la ayuda de esta norma vamos a gestionar los riesgos de las TICs en el laboratorio de la Unidad Educativa Pueblo Nuevo, como pueden ser programas o aplicaciones en ambientes vulnerables, tecnologías obsoletas, sistemas operativos sin actualizaciones.

De acuerdo a ISO 27005 se establece un contexto en el que se indica un enfoque y criterios de evaluación, impacto y aceptación del riesgo, donde se definen alcances y límites, es importante tener en cuenta que el análisis de riesgo dentro de cualquier entidad ya sea pública o privada, es de vital importancia ya que nos permite instaurar los niveles convenientes de seguridad en nuestros activos para tener mayor eficiencia, confiabilidad, disponibilidad e integridad.

Sociedad de la información

El termino sociedad de la información ha sido bien adoptado desde hace mucho tiempo y hace énfasis al cambio, la transformación de la sociedad y va mucho más allá de centrarnos solo en términos de informática o tecnologías de información y comunicación, sino en los datos para convertirse en información y a través de estos se puede obtener conocimiento por ende esto es parte fundamental de cualquier entidad.

"En la sociedad de la información, el conocimiento se convierte en el combustible y la tecnología de la información y la comunicación en el motor." (Fuente, 2004, p.3)

Tecnologías de Información y Comunicación (TICs).

Sin lugar a duda alguna vez hemos escuchado la palabra TICs o hemos sido participe de ella consciente o inconscientemente, por lo tanto, las Tecnologías de la información y comunicación han sido definidas por muchos autores:

Las tecnologías de la información y comunicación giran en torno a tres medios básicos: la informática, la microelectrónica y las telecomunicaciones; pero giran, no solo de forma aislada, sino lo que es más significativo de manera interactiva e interconexionadas. (Cabero, 2001).

> Las TIC constituyen, por lo tanto, un pilar fundamental en las sociedades industrializadas actuales, como herramienta de acceso y transmisión de una información que, sometida a un proceso cognitivo adecuado, es susceptible de ser transformada en conocimiento. Y constituyen un elemento primordial el establecimiento de relaciones sociales en la red. Las TIC se conforman, de esa manera, como un elemento importante en el desarrollo científico y social de las sociedades. (Pozuelo & Fernández, 2014, p.2).

Cabe recalcar que mediante la ayuda de las tics se han desbloqueado un sinnúmero de posibilidades en donde estar al otro lado del mundo ya no es una barrera para estar en constante comunicación ,estas herramientas tecnológicas nos ayudan a mejorar la emisión ,recepción y transmisión de la información, comúnmente en los procesos de comunicaciones se centra en el mensaje, pero al hablar de las TICs hacemos referencia al conjunto de herramientas tecnológicas ya sean hardware o software , datos o instrucciones que viajan a través de un medio o canal que son enviados o recibidos por usuarios interconectados mediante la red.

Seguridad.

La seguridad de la información y todo el conjunto de herramientas o equipos de índole informático es de fundamental importancia en todas las empresas, instituciones gubernamentales, universidades, etc. Ya que en la actualidad todos quieren estar apegados a las últimas tecnologías por objetivos comunes como competitividad, efectividad en sus procesos, transmisión, almacenamiento o manipulación de datos, generación de conocimientos, en fin no es para menos que la

entidades opten por mantener sus activos o bienes tecnológicos con el mayor índice de seguridad posible, a continuación definimos algunos conceptos específicos.

Activos.

Un activo se define en general como los bienes , derechos y demás recursos con los que cuenta una entidad ya sea pública o privada para la consecución de sus objetivos, al hablar de activos en términos informáticos hacemos referencia o nos centramos en los datos, herramientas o dispositivos que se encuentran inmersos en las tareas apegadas con el manejo de la información y la comunicación como lo son los activos hardware :(Ordenadores, routers, switches, impresoras, etc.), activos software :(aplicaciones, sistemas de información.), Además de los activos mencionados anteriormente las personas inmersas en la organización también son considerados activos y por ultimo pero no menos importante los mueble y oficina .

En consecuencia, todos los activos siempre deben de estar salvaguardados de cualquier evento ilícito, daños, modificación, uso, hurto que dé como resultado pérdidas para cualquier entidad, entonces la seguridad informática tiene como fin observar y prevenir las amenazas que se encuentran expuestos todos y cada uno de los activos identificándolos y gestionando el nivel de riesgo a través de métodos o técnicas para precautelar su integridad, disponibilidad y confidencialidad.

Vulnerabilidad.

Se define a la vulnerabilidad desde el punto de vista informático a todas las debilidades o fallos que se puedan dar con respecto a las tecnologías informáticas que comprometan su trabajo, comúnmente las vulnerabilidades son originadas por falencias

en sistemas operativos, falta de antivirus, baja seguridad de acceso a los ordenadores o servidores, programas desactualizados, etc.

Según el autor (Aguilera, 2010, p.14) describe a las vulnerabilidades como las "Probabilidades que existen de que una amenaza se materialice contra un activo".

Amenaza.

Una amenaza comprende cualquier acción que infrinja o quebrante la labor de nuestros activos, podemos acotar que no todos los activos son sensibles a las mismas amenazas como ejemplo pongamos la información o datos, estos son vulnerables para las personas mal intencionadas es decir con intención de causar daños, en cambio una infraestructura eléctrica es vulnerable a un cortocircuito.

Riesgos.

Son todos aquellos eventos que atenten contra la seguridad de nuestros activos informáticos. No constituye riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe amenaza para la misma. (Aguilera, 2010).

Disponibilidad

La disponibilidad hace referencia a la habilidad de los usuarios para ingresar a diferentes programas o sistemas, realizar nuevos trabajos o tareas, actualizar o modificar tareas anteriores descargarlos o copiarlos.

Confidencialidad

La confidencialidad la define la Organización Internacional de Estandarización (ISO) en la norma ISO/IEC 27002 como "garantizar que la información es accesible sólo para aquellos autorizados a tener acceso.”

Integridad

La integridad hace referencia a salvaguardar la exactitud de la información, es decir, obtener o recuperar la información de manera completa y que no tenga fallas o errores.

Normativas UNE-ISO/IEC

Estas normativas constituyen los procedimientos, normas o directrices de regulación o normativización a nivel global, comprendidas por un conjunto de entidades participes en la elaboración de estas medidas universales, mediante personal técnico de las diferentes organizaciones con el objetivo de formalizar acuerdos en áreas concretas del campo técnico enfocadas en la gestión de las empresas.

En nuestro caso vamos a detallar algunas normas relacionadas con las tecnologías de la información, técnicas de seguridad y la gestión de la seguridad de la información.

Norma UNE-ISO/IEC 27001

La Norma UNE-ISO/IEC 27001 instaura los delineamientos o principios para establecer, implementar, conservar o perfeccionar los sistemas de gestión de la seguridad de la información.

Norma UNE-ISO/IEC 27002

La Norma UNE-ISO/IEC 27002 nos da un conjunto de lineamientos, controles para las buenas prácticas en la gestión de la seguridad de la información.

Norma UNE-ISO/IEC 27003

Esta normativa se centra en brindaros las directrices prácticas para el diseño e implementación de un sistema de gestión de la seguridad de la información y se apoya en la normativa UNE-ISO/IEC 27001.

Norma UNE-ISO/IEC 27004

Su objetivo principal se concentra en medir o evaluar la eficacia de los SGSI.

Norma UNE-ISO/IEC 27005

El objetivo de la normativa ISO 27005 es facilitar o darnos las pautas para la gestión de los riesgos de la seguridad de la información y las TICs. Esta norma es compatible o está relacionada con las nociones generales descritos en la normativa ISO 27001 y está delineado como ayuda o apoyo a la ejecución y satisfacción de la seguridad de la información direccionada a la gestión de los riesgos. La norma ISO 27005 no detalla ni recomienda alguna metodología específica de análisis de riesgos, aunque explica un proceso organizado, metódico y de rigor desde el análisis de los riesgos hasta la elaboración de un plan de mitigación del mismo.

¿Qué debe hacer una institución para aplicar la norma ISO 27005?

Al ser La Unidad Educativa Pueblo Nuevo una entidad pública es necesario tener presente lo que tipifican las Normas de Control Interno de la Contraloría General del Estado de la republica del Ecuador en el inciso 410-10 que corresponde a la Seguridad

de tecnología de información en donde se determina que la Unidad de Tecnología de Información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

Visión de la gestión y la evaluación del riesgo

Para la gestión y evaluación del riesgo de nuestros activos la norma **UNE-ISO/IEC 27005** nos proporciona la siguiente metodología como se logra apreciar en la figura 1.

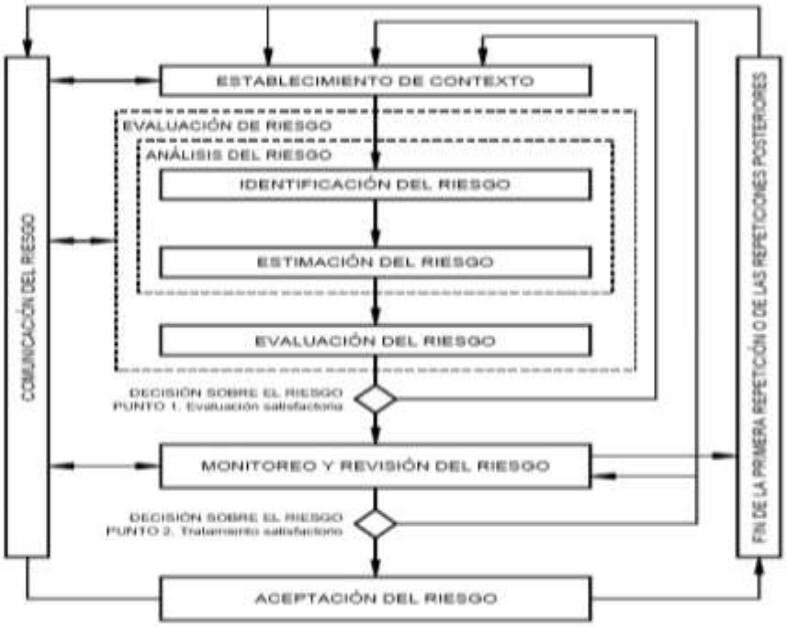

Figura 1: Metodología ISO para la evaluación de riesgo

Fuente: (UNE-ISO/IEC 27005, 2011)

Metodología propuesta

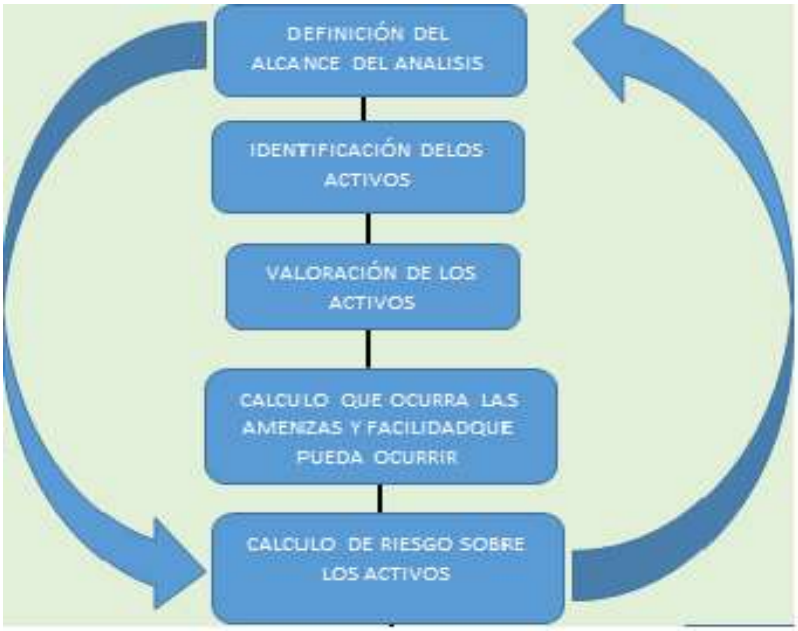

Figura 2: Metodología propuesta para la evaluación de riesgo

Fuente: (Mejia, 2017)

Como primer punto tenemos el establecimiento del análisis o contexto de nuestro objeto de estudio ,luego por la identificación de los activos y de la respectiva realización del inventario y su área responsable además del personal inmerso, es decir, clasificar nuestros activos donde esta información es relevante para la próxima gestión del riesgo ya que aquí delimitaremos conceptos como alcances y limites, luego se llevará a cabo la valoración de los activos de acuerdo al nivel de confiabilidad, disponibilidad e integridad identificando así los riesgos que se encuentra expuestos los activos para el respectivo cálculo de la ocurrencia y valoración del riesgo a través de métodos cualitativos y cuantitativos.

Metodología cualitativa para la estimación del riesgo.

Esta metodología se basa en 4 parámetros para la estimación del riesgo como son:

1. Amenazas
2. Vulnerabilidades
3. Impacto asociado a una amenaza si ésta llegara a materializarse
4. Controles preventivos o correctivos

Cabe mencionar que esta metodología es una de las más utilizadas gracias a que se centra en una escala de atributos calificativos muy fácil de manejar donde se detallan los hechos o consecuencia de los riesgos como puede ser Alto, Medio o Bajo.

Metodología cuantitativa para la estimación del riesgo.

Esta metodología se basa en 2 medidas para la estimación del riesgo

1. la probabilidad de ocurrencia de un evento
2. estimación del costo o las pérdidas en caso de que el evento sea positivo.

Mientras más exactos sean los valores cuantitativos que se le den a los activos, mayor es la probabilidad de éxito de este método:

La normativa (ISO 27005, 2008) nos dice que "Implica realizar una recolección de datos, cálculos complejos, técnicas de modelamiento, etc. Se utiliza una escala con valores numéricos, a diferencia de la anterior que utilizaba una escala descriptiva, tanto para la evaluación de probabilidades de ocurrencia como para sus consecuencias basándose en datos provenientes de varias fuentes".

CONCLUSIONES

Se concluye que las tecnologías de la información y la comunicación son de vital importancia dentro de las instituciones y salvaguardar cada de uno de nuestros activos de posibles eventos, amenazas, riesgos que afecten con su integridad, confidencialidad o disponibilidad es una tarea diaria para su eficaz desempeño u consecución de objetivos.

La aplicación de la norma ISO 27005 es crucial para el análisis de riesgos de los tics en las organizaciones ya que nos brinda los parámetros y la metodología a seguir o guiarse para su ejecución desde la valoración de activos hasta en cálculo de riesgo de los activos.

Según el estudio ejecutado las autoridades del plantel educativo deben realizar un procedimiento de tratamiento de los riesgos encontrados como se puntuaron en el **Plan de implementación de medidas propuesto** empezando por un mantenimiento preventivo y correctivo de las tecnologías de la información y la comunicación, desechar tecnologías obsoletas o dañadas que se encuentran el laboratorio aumentar la iluminación y dotar al laboratorio de una red de cableado estructurado de datos para mejorar la calidad de enseñanza-aprendizaje hacia los alumnos.

BIBLIOGRAFIA

Aguilera, P. (2010). *Seguridad Informatica.* Madrid: Editex S.A.

Cabero, J. (2001). *Tecnología educativa: diseño y utilización de medios en la enseñanza.* Barcelona: Paidós.

Fuente, F. G. (2004). *Los sistemas de información en la sociedad del conocimiento.* Madrid: ESIC EDITORIAL.

Gascó Gema, E. (2011). *Seguridad informática.* Madrid.

Gómez, F. L., & Andrés, Á. A. (2012). *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes.* Madrid. España: AENOR Ediciones (Asociación Española de Normalización).

Mejia, V. J. (2017). *Metodología para análisis de riesgo de información apoyado en ISO 27005 para las instituciones del Ecuador.* Babahoyo.

Pozuelo, E. J., & Fernández, M. S. (2014). *TIC en las aulas: luces y sombras.* Madrid.

UNE-ISO/IEC 27005. (2011). *UNE-ISO/IEC 27005.*

ANEXOS

Tabla 1: Inventario de activos

ACTIVOS DE SOPORTE	AREA RESPONSABLE
Equipos de escritorio	Personal docente del área informática.
Proyector	Personal docente del área informática.
Impresora	Personal docente del área informática.
Copiadora	Personal docente del área informática.
Pizarra digital	Personal docente del área informática.
Aires acondicionados	Personal docente del área informática.
Central eléctrico	Personal docente del área informática.
Sistema de iluminación	Personal docente del área informática.
Gabinetes Racks	Personal docente del área informática.

Parlantes	Personal docente del área informática.
Sistema operativo	Personal docente del área informática.
Aplicaciones de ofimática	Personal docente del área informática.
Aplicaciones de desarrollo	Personal docente del área informática.
Sistema gestor de base de datos MySql	Personal docente del área informática.
Router	Personal docente del área informática.
Muebles de oficina	Personal docente del área informática.
Portátil	Personal docente del área informática.
Antivirus	Personal docente del área informática.
Tarjetas inalámbricas (nics).	Personal docente del área informática.
Lcda. Milena Villala Velasco	Personal docente del área informática.

Elaboración propia: Ronald Franco

Escala de valoración de los activos

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

Figura 3: Escala de valoración de los activos

Fuente: (UNE-ISO/IEC 27005, 2011)

Tabla 2: Valoración de activos

ACTIVOS DEL LABORATORIO	ROL QUE CUMPLEN	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	MEDIA
EQUIPOS DE ESCRITORIO	Permite interactuar con las aplicaciones y navegar en internet.	3	5	5	4
PROYECTOR	Permite visualizar temas de estudio para impartir en las clases.	2	4	5	3
IMPRESORA	Permite imprimir documentos necesarios en el laboratorio.	2	4	5	3
COPIADORA	Permite imprimir, sacar copias y escanear documentos necesarios en el laboratorio.	2	4	5	3
PIZARRA DIGITAL	Permite controlar el ordenador mediante su superficie con un bolígrafo, con el dedo o en algunos casos con otros dispositivos como si se tratara de un ratón.	2	4	5	3
AIRES ACONDICIONADOS	Permite mantener un ambiente adecuado para los equipos.	1	5	5	3
CENTRAL ELECTRICO	Brinda energía eléctrica para el correcto funcionamiento de los TICs.	1	5	5	3

SISTEMA DE ILUMINACION	Brinda la iluminación adecuada al laboratorio	1	5	5	3
GABINETES RACKS	Permiten introducir una serie de dispositivos informáticos o de comunicaciones, así como electrónico de manera organizada.	1	4	4	3
PARLANTES	Permiten reproducción de sonidos	1	4	4	3
SISTEMA OPERATIVO	Permite gestionar recursos hardware, siendo este el software más importante del computador	3	5	5	4
APLICACIONES DE OFIMATICA	Permiten realizar trabajos, hojas de cálculo, crear pequeñas bases de datos.	2	5	5	4
APLICACIONES DE DESARROLLO (VISUAL STUDIO, JAVA, C++, DREAMWEAVER**)**	Permite la práctica y el desarrollo de aplicaciones informáticas como herramienta de estudio.	4	5	5	4
SISTEMA GESTOR DE BASE DE DATOS MYSQL	Permite la práctica y el desarrollo de base de datos como herramienta de estudio.	4	5	5	4
ROUTER	sirve para interconectar redes de ordenadores	4	5	5	4

MUEBLES DE OFICINA (SILLAS, MESAS, ARCHIVADORES**)**	Permiten facilitar los usos y actividades habituales en el laboratorio.	1	4	5	3
PORTATIL	Permite acceder los servicios como aplicaciones e internet, herramienta tecnológica para el desarrollo de las clases.	3	5	5	4
ANTIVIRUS	Permite proteger las computadoras contra softwares maliciosos y eliminar los virus que han infectado los ordenadores.	3	4	5	4
TARGETAS INALAMBRICAS	Nos permiten enviar y recibir datos sin la necesidad de utilizar un cableado estructurado.	3	5	5	4
LCDA. MILENA VILLALA VELASCO	Docente TICs Administradora del laboratorio 1.	2	5	5	4

Elaboración propia: Ronald Franco

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.

Figura 4: Probabilidad de ocurrencia de amenazas

Fuente: (UNE-ISO/IEC 27005, 2011)

Tabla 3: Calculo que ocurra la amenaza y facilidad con la que puede ocurrir

Activos	Amenazas	Vulnerabilidad	Nivel de ocurrencia	Facilidad de Explotación
EQUIPOS DE ESCRITORIO	Falta de mantenimiento preventivo o correctivo	El mantenimiento no es suficiente	Alta	Alta
	Hurto de documentos	Copias no controladas	Alta	Media
		Almacenamiento sin ningún tipo de protección		
	Errores de uso	Falta de control en las configuraciones	Media	Media
PROYECTOR	Inobservancia en el mantenimiento	El mantenimiento no es suficiente	Media	Media
	Deterioro de los activos a causa de polvo y corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.	Media	Media
IMPRESORA	Inobservancia en el mantenimiento	El mantenimiento no es suficiente	Media	Baja
COPIADORA	Inobservancia en el mantenimiento	El mantenimiento no es suficiente	Media	Baja
PIZARRA DIGITAL	Deterioro de los activos a causa de polvo y corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.	Media	Media
AIRES ACONDICIONADOS	Inobservancia en el mantenimiento	El mantenimiento no es suficiente - instalaciones fallidas	Alta	Media
CENTRAL ELECTRICO	Perdidas de abastecimiento de energía	Susceptibilidades a los cambios de tensión	Media	Alta
	Inobservancia en el mantenimiento	El mantenimiento no es suficiente - instalaciones	Media	Media

		fallidas		

Activos	Amenazas	Vulnerabilidad	Nivel De ocurrencia	Facilidad de Explotación
SISTEMA DE ILUMINACION	Inobservancia en el mantenimiento	El mantenimiento no es suficiente - instalaciones fallidas	Media	Media
GABINETES RACKS	Errores de uso	EL reemplazo no se torna periódico	Baja	Media
	Inobservancia en el mantenimiento	El mantenimiento no es suficiente	Baja	Baja
PARLANTES	Deterioro de los activos a causa de polvo y corrosión.	Exposición a la humedad, el polvo y la suciedad.	Baja	Media
SISTEMA OPERATIVO	Corrupción de los datos	Sistemas de comercialización amplia	Alta	Alta
	Errores de uso	La configuración no es correcta de los parámetros	Baja	Baja
	funcionamiento inadecuado	Falta de control eficaz del cambio	Alta	Alta
APLICACIONES DE OFIMATICA	Manejo de sistemas u aplicaciones	Falta de copias de respaldo.	Media	Media
APLICACIONES DE DESARROLLO	funcionamiento inadecuado del sistema	Falta de control eficaz del cambio	Alta	Alta
	Manipulación del sistema	Falta de copias de respaldo	Media	Media
	Corrupción de datos	Sistemas de comercialización extensa	Alta	Alta

SISTEMA GESTOR DE BASE DE DATOS MYSQL	Errores de uso	La configuración no es correcta de los parámetros	Baja	Baja
	Manipulación de sistemas	Inexistencias de copias de respaldo	Media	Media
Activos	Amenazas	Vulnerabilidad	nivel De ocurrencia	Facilidad de Explotación
ROUTER	Escucha sub-receptiva	Líneas de comunicaciones sin ninguna protección	Alta	Alta
	Inobservancia en el mantenimiento	El mantenimiento no es suficiente	Media	Media
	Uso no autorizado de los equipos	enlaces de red sin protecciones	Baja	Media
MUEBLES DE OFICINA	Deterioro de los activos a causa de polvo y corrosión.	El mantenimiento no es suficiente	Baja	Baja
PORTATIL	Falta de mantenimiento preventivo o correctivo	El mantenimiento no es suficiente	Alta	Alta
	Hurto de documentos	Copias no controladas	Alta	Media
		Almacenamiento sin ningún tipo de protección	Alta	Media
	Errores de uso	Falta de control en las configuraciones	Media	Media
ANTIVIRUS	Manipulación de software	Descargas y uso descontrolado de software	Baja	Baja
TARGETAS INALAMBRICAS	Escucha sub-receptiva	Líneas de comunicación desprotegidas	Alta	Alta
ADMINISTRADOR TICS	Inobservancia en la disponibilidad	Ausencia del personal	Media	Baja
	Hurto de documentos	El trabajo no es supervisado	Media	Media
	Errores de uso	Uso incorrecto de activos.	Baja	Baja

Elaboración propia: Ronald Franco

	Probabilidad de ocurrencia - Amenaza	Baja			Media			Alta		
	Facilidad de explotación	Baja	Media	Alta	Baja	Media	Alta	Baja	Media	Alta
VALORACION 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

Figura 5: Proceso de evaluación del riesgo

Fuente: (UNE-ISO/IEC 27005, 2011)

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

Figura 6: Nivel del riesgo

Fuente: (Mejia, 2017)

Tabal 4: Cálculo del riesgo sobre los activos

Activos	Amenazas	Vulnerabilidad	V/activos	Probabilidad de ocurrencia	Facilidad de Explotación	Riesgo
EQUIPOS DE ESCRITORIO	Falta de mantenimiento preventivo o correctivo	El mantenimiento no es suficiente	4	Alta	Alta	7
	Hurto de documentos	Copias no controladas	4	Alta	Media	6
		Almacenamiento sin ningún tipo de protección	4	Media	Media	5
	Errores de uso	Falta de control en las configuraciones	4	Media	Media	5
PROYECTOR	Inobservancia en el mantenimiento	El mantenimiento no es suficiente	3	Media	Media	4
	Deterioro de los activos a causa de polvo y corrosión.	susceptibilidad a la humedad, el polvo y la suciedad.	3	Media	Media	4
IMPRESORA	Inobservancia en el mantenimiento	El mantenimiento no es suficiente	3	Media	Baja	3
COPIADORA	Inobservancia en el mantenimiento	El mantenimiento no es suficiente	3	Media	Baja	3
PIZARRA DIGITAL	Deterioro de los activos a causa de polvo y corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.	3	Media	Media	4
AIRES ACONDICIONA	Inobservan	El	3	Alta	Media	5

DOS	cia en el mantenimiento	mantenimiento no es suficiente				
CENTRAL ELECTRICO	Inobservancia en el mantenimiento	El mantenimiento no es suficiente - instalaciones fallidas	3	Media	Alta	5
	Perdidas de abastecimiento de energía	Susceptibilidades a los cambios de tensión	3	Media	Media	4
SISTEMA DE ILUMINACION	Inobservancia en el mantenimiento	El mantenimiento no es suficiente - instalaciones fallidas	3	Media	Media	4
GABINETES RACKS	Errores de uso	EL reemplazo no se torna periódico	3	Baja	Media	3
	Inobservancia en el mantenimiento	El mantenimiento no es suficiente	3	Baja	Baja	2
PARLANTES	Deterioro de los activos a causa de polvo y corrosión.	Exposición a la humedad, el polvo y la suciedad.	3	Baja	Media	3
SISTEMA OPERATIVO	Corrupción de los datos	Sistemas de comercialización amplia	4	Alta	Alta	7
	Errores de uso	La configuración no es correcta de los parámetros	4	Baja	Baja	3
	funcionamiento inadecuado	Falta de control eficaz del cambio	4	Alta	Alta	7
APLICACIONES DE OFIMATICA	Manejo de sistemas u	Falta de copias de respaldo.	4	Media	Media	5

	aplicaciones					
APLICACIONES DE DESARROLLO	funcionamiento inadecuado del sistema	Falta de control eficaz del cambio	4	Alta	Alta	7
	Manipulación del sistema	Falta de copias de respaldo	4	Media	Media	7
	Corrupción de datos	Sistemas de comercialización extensa	4	Alta	Alta	7
SISTEMA GESTOR DE BASE DE DATOS MYSQL	Errores de uso	La configuración no es correcta de los parámetros	4	Baja	Baja	5
	Manipulación de sistemas	Inexistencias de copias de respaldo	4	Media	Media	6
ROUTER	Escucha subreceptiva	Líneas de comunicación sin protección	4	Alta	Alta	7
	Incumplimiento en el mantenimiento	Mantenimiento insuficiente	4	Media	Media	6
	Uso no autorizado del equipo	Conexiones de red pública sin protección	4	Baja	Media	4
MUEBLES DE OFICINA	Destrucción del equipo o los medios. Polvo y corrosión.	Mantenimiento insuficiente	3	Baja	Baja	2
PORTATIL	Incumplimiento en el mantenimiento	Mantenimiento insuficiente	4	Alta	Alta	7
	Hurto de medios o documentos	Copia o controlada	4	Alta	Media	6
		Almacenamiento sin protección	4	Alta	Media	6
	Error de uso	Falta de control de cambio en la configuración	4	Media	Media	5

ANTIVIRUS	Manipulación de software	Descarga y uso no controlado de software	4	Baja	Baja	3
TARGETAS INALAMBRICAS	Escucha subreceptiva	Líneas de comunicación sin protección	4	Alta	Alta	7
ADMINISTRADOR TICS	Incumplimiento en la disponibilidad	Ausencia del personal	4	Media	Baja	4
	Hurto de medios o documentos	Trabajo no supervisado	4	Media	Media	5
	Error de uso	Uso incorrecto de hardware, software y seguridad	4	Baja	Baja	3

Elaboración propia: Ronald Franco

Plan de implementación de medidas propuesto

En este apartado vamos a puntuar las acciones necesarias a efectuar en el laboratorio de cómputo de la Unidad Educativa Pueblo Nuevo para minimizar o mitigar el nivel de riesgo de los activos.

Tabla 5: Hardware

Situación actual	Situaciones correctivas
Falla de equipos se debe al poco mantenimiento y limpieza.	Efectuar mantenimiento preventivo por lo menos 2 veces al año (acción inmediata a efectuar).
Equipos en desuso por fallas, requieren remplazo de piezas.	Efectuar mantenimiento correctivo, (acción inmediata a efectuar).
Tecnologías obsoletas	Cambiar o actualizar equipos informáticos

Elaboración propia: Ronald Franco

Tabla 6: Software y utilitarios

Situación actual	Situaciones correctivas
Programas de desarrollo de software sin licencia	Instalar programas de desarrollo de software con sus respectivas licencias para poder impartir las clases de manera óptima.
Falta de software de antivirus	Instalar software de antivirus (acción inmediata a efectuar).

Inicio de sesión sin protección	Dotar a los ordenadores de respectivas credenciales de inicio de sesión.

Elaboración propia: Ronald Franco

Tabla 7: Personal

Situación actual	Situaciones correctivas
Errores involuntarios con respecto al manejo de activos hardware, software o de información.	Presentación de políticas informáticas, talleres, educación continua.

Elaboración propia: Ronald Franco

Tabla 8: Documentación

Situación actual	Situaciones correctivas
Archivos expuestos en el ordenador principal ya que no cuenta con inicio de sesión de administrador.	Dotar de credenciales a cada usuario para inicio de sesión segura.

Elaboración propia: Ronald Franco

Tabla 9: Suministro de energía

Situación actual	Situaciones correctivas
Abastecimiento insuficiente de luminarias	Existe poca iluminación, dotar al laboratorio de un sistema de iluminación óptimo.
En caso de incendio por cortocircuitos u otros eventos el laboratorio cuenta con	Si Cumple, como sugerencia realizar capacitaciones para el manejo de

extintores en perfecto estado para mitigar el fuego.	extintores y primeros auxilios.

Elaboración propia: Ronald Franco

Tabla 10: Suministro de internet

Situación actual	Situaciones correctivas
Suministro de internet Wireless, internet de baja velocidad (deficiente).	Aumentar la velocidad de transmisión de datos. (Recomendable).
Inexistencia de una red de cableado estructurado de transmisión de datos.	Implementar una red de cableado estructurado de transmisión de datos, (acción inmediata a efectuar).
Fallas en las tarjetas NICS en algunos ordenadores.	Remplazo de tarjetas NICS

Elaboración propia: Ronald Franco

Si no se tratan los riesgos a los que se encuentran expuestos los activos existirían daños que atenten contra la integridad, disponibilidad.

Tabla 11: posibles daños de activos susceptibles

Activos susceptibles a daños	posibles daños
Hardware	Deterioro o fallas (poco mantenimiento)
Software y utilitarios informáticos	perdida de información
Personal involucrado	Divulgación de información a terceros fuera de la institución, que atenten directa o indirectamente con los activos (robo de activos, hurto de medios o documentos)
Documentación	Perdida de documentos de importancia relacionados con el hardware, software o personal en el laboratorio de cómputo.
Suministro de energía	Abastecimiento insuficiente, fenómenos naturales (picos de voltaje, cortocircuitos).
Suministro de internet (wifi)	Abastecimiento insuficiente, perdida de datos, canales de comunicación inseguras, espionaje remoto.

Elaboración propia: Ronald Franco

UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
(F.A.F.I)

ESCUELA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Ingeniería En Sistemas

Entrevista realizada a la rectora de la Unidad Educativa Pueblo Nuevo

1. ¿Se realiza un presupuesto y se lo asigna al laboratorio de cómputo?

Si, existe un presupuesto de manera general, el cual se utiliza de manera estratégica en la entidad educativa en los campos que se requieran.

2. ¿Existen manuales de políticas internas para el personal que labora en el laboratorio de cómputo?

Si existen un manual de políticas para los docentes

3. ¿Existen medidas de seguridad para evitar la pérdida o hurto de los activos informáticos?

Existe seguridad física de las instalaciones (guardia)

4. ¿Existen extintores en el laboratorio como medida de seguridad en caso de una emergencia de incendio?

Si existen extintores en el laboratorio de cómputo, como en las demás oficinas

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
(F.A.F.I)

ESCUELA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Ingeniería En Sistemas

Entrevista realizada a la docente informático y encargada del laboratorio de la Unidad Educativa Pueblo Nuevo

5. ¿Cuentan con un plan de mantenimiento preventivo y correctivo para los activos del laboratorio de cómputo?

No existe un plan definido, pero se lo realiza en los inicios de periodo lectivo

6. ¿Con que frecuencia se lo efectúa?

Cada año

7. ¿Existen restricciones para ingerir alimentos, bebidas o fumar en el laboratorio de cómputo?

Si existen restricciones, y señaléticas de prohibido ingerir alimentos, bebidas o fumar en el laboratorio de cómputo

8. ¿Cree que el laboratorio cuenta un nivel mínimo de riesgos de las tecnologías de la información y la comunicación?

Al hablar de las tecnologías de la información y comunicación, por las constantes actualizaciones siempre va a existir un nivel mínimo de riesgos.

9. ¿Conoce sobre la normativa ISO (International Standarization Organization) 27005?

Si trata sobre los riesgos informáticos, pero no se ha trabajado con ella en ninguna ocasión.

Figura 7: solicitando permiso a la rectora de la unidad Educativa Pueblo Nuevo Lcda. Diana Delgado Coello

Elaboración propia: Ronald Franco

Figura 8: Entrevista a la Lcda. Milena Villala Velasco, docente informática encargada del

Figura 9: Pc principal del laboratorio de cómputo de la UEPN.

laboratorio de cómputo de la UEPN.

Elaboración propia: Ronald Franco

Elaboración propia: Ronald Franco