UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ELABORACIÓN DE UNA GUÍA DE SEGURIDAD INFORMÁTICA PARA ESTUDIANTES DE LA UTMACH USANDO LA METODOLOGÍA COBIT 5

JIMENEZ RAMIREZ MARITZA DANILA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2020

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ELABORACIÓN DE UNA GUÍA DE SEGURIDAD INFORMÁTICA PARA ESTUDIANTES DE LA UTMACH USANDO LA METODOLOGÍA COBIT 5

JIMENEZ RAMIREZ MARITZA DANILA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2020

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

ELABORACIÓN DE UNA GUÍA DE SEGURIDAD INFORMÁTICA PARA ESTUDIANTES DE LA UTMACH USANDO LA METODOLOGÍA COBIT 5

JIMENEZ RAMIREZ MARITZA DANILA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

GONZALEZ SANCHEZ JORGE LUIS

MACHALA, 21 DE FEBRERO DE 2020

MACHALA
21 de febrero de 2020

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado ELABORACIÓN DE UNA GUÍA DE SEGURIDAD INFORMÁTICA PARA ESTUDIANTES DE LA UTMACH USANDO LA METODOLOGÍA COBIT 5, hacemos constar que luego de haber revisado el manuscrito del precitado trabajo, consideramos que reúne las condiciones académicas para continuar con la fase de evaluación correspondiente.

GONZALEZ SANCHEZ JORGE LUIS
0703333898
TUTOR - ESPECIALISTA 1

PARRA OCHOA EUDORO BENITO
0701063406
ESPECIALISTA 2

OCHOA CAICEDO HECKLER ROTHWELL
0702681917
ESPECIALISTA 3

Fecha de impresión: viernes 21 de febrero de 2020 - 10:19

ELABORACIÓN DE UNA GUÍA DE SEGURIDAD INFORMÁTICA PARA ESTUDIANTES DE LA UTMACH USANDO LA METODOLOGÍA COBIT 5

por Maritza Danila Jimenez Ramirez

Fecha de entrega: 09-feb-2020 10:59p.m. (UTC-0500)
Identificador de la entrega: 1254441306
Nombre del archivo: MARITZA_DANILA_JIMENEZ_RAMIREZ.pdf (405.58K)
Total de palabras: 3644
Total de caracteres: 20654

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

La que suscribe, JIMENEZ RAMIREZ MARITZA DANILA, en calidad de autora del siguiente trabajo escrito titulado ELABORACIÓN DE UNA GUÍA DE SEGURIDAD INFORMÁTICA PARA ESTUDIANTES DE LA UTMACH USANDO LA METODOLOGÍA COBIT 5, otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

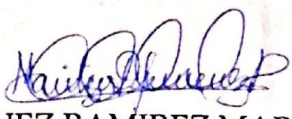
La autora declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

La autora como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 21 de febrero de 2020



JIMENEZ RAMIREZ MARITZA DANILA
0705169779

RESUMEN

El avance tecnológico tiene impacto en todo el mundo y sobre todo en muchos sectores económicos de la sociedad, empresas dedicadas a la producción, industria, comercio, educación, etc. incluyen a las tecnologías de comunicación e informaciòn como herramientas para la ejecución de sus actividades. Específicamente en las instituciones educativas se han adoptado las TIC`s como instrumentos de ayuda, pues se emplean tanto en su parte administrativa como académica. La utilización de herramientas tangibles como los equipos de cómputo y de intangibles como los programas y aplicaciones, son utilizados para optimizar el trabajo, reducir el esfuerzo y garantizar los mismos resultados; en las universidades particularmente se emplean plataformas con las que es posible ejecutar varios procesos, por ejemplo: realizar seguimiento a la asistencia, consultar calificaciones, realizar evaluaciones a los docentes, descargar un plan académico (syllabus), entre otras cosas. El presente documento aborda la problemática de la gestión de seguridad informática, dirimir criterios sobre las adversidades y riesgos latentes en las prestaciones de las tecnologías de comunicación e informaciòn, especialmente en aquellas afines a los procesos académicos. El objetivo del escrito es elaborar una guía de seguridad informática enfocada a los estudiantes de la Universidad Técnica de Machala (Utmach) mediante la metodología Cobit 5 para mejorar la gestión de riesgos en sus datos personales. Los resultados expresan los controles aplicables por los estudiantes al reforzar la seguridad informática de sus dispositivos, cuentas institucionales y datos personales en contraste con las vulnerabilidades más comunes encontradas en el contexto institucional de la Utmach.

PALABRAS CLAVE: Seguridad informática, auditoria, Cobit 5, estudiantes, guía.

ABSTRACT

Technological progress has an impact throughout the world and especially in many economic sectors of society, companies engaged in production, industry, commerce, education, etc. It includes communication and information technologies as tools for the execution of its activities. Specifically, in educational institutions, ICTs have been adopted as aid instruments, since they are used both administratively and academically. The use of tangible tools such as computer equipment and intangibles such as programs and applications are used to adapt the work, reduce effort and detect the same results; In the universities included, platforms with which it is possible to execute various processes are used, for example: follow up on attendance, consult grades, perform evaluations of teachers, download an academic plan (curriculum), among other things. This document addresses the problem of computer security management, set criteria on adversities and latent risks in the provision of communication and information technologies, especially in threats related to academic processes. The objective of the paper is to develop a computer security guide focused on students of the Technical University of Machala (Utmach) using the Cobit 5 methodology to improve risk management in their personal data. The results express the controls applicable by students by modifying the computer security of their devices, institutional accounts and personal data in contrast to the most common vulnerabilities found in the institutional context of the Utmach.

KEYWORDS: Computer security, audit, Cobit 5, students, guide.

ÍNDICE DE CONTENIDOS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE CUADROS

1. INTRODUCCIÓN

Debido al avance tecnológico y desarrollo de nuevas Tecnologías de Información la mayoría de las empresas las utilizan para desarrollar sus actividades, mediante la cuales han podido optimizar trabajos, rentabilizándolos debido al ahorro de tiempo y los beneficios que se obtienen. El uso de la tecnología también ha sido acogido para el manejo de los datos y la información de la entidad, tal es el caso que los registros de clientes, suministros, inventarios y ventas, que anteriormente se llevaban a mano, hoy por hoy pueden ser registrarse en un documento digital al cual se puede acceder desde cualquier lugar; de alguna manera puede decirse que el uso de las TIC`s facilitan el trabajo para el ser humano.

Esto sin duda beneficia a muchos sectores incluyendo al sector educativo, en este aspecto se conoce que las instituciones de educación superior especialmente, han adoptado tecnologías que aportan efectivamente al proceso enseñanza – aprendizaje con las que no solo facilitan el trabajo de los docentes al procesar calificaciones y enviar tareas, sino que también existen plataformas con las que el docente puede interactuar desde cualquier sitio en tiempo real con los estudiantes.

La carrera de contabilidad y auditoría es un conjunto de saberes interdisciplinarios que abarcan desde las cuestiones financieras hasta la gestión de riesgos en una empresa, particularmente la auditoria es supervisar, analizar e inferir medidas tanto preventivas como correctivas al mejorar las cualidades de una organización.

Hoy en día sin duda alguna las infraestructuras informáticas son parte nominal de la sociedad, solventando cualquier necesidad referente al procesamiento o almacenamiento de datos, además potencian funcionalidades como comunicación, interacción, entretenimiento y educación en virtud de las capacidades de sus usuarios.

La auditoría informática es un campo de acción enfocado en identificar vulnerabilidades para proponer medidas de seguridad que conserven la integridad de los activos digitales en forma continua, debido al auge de la tecnológica y su relevancia se ha convertido en toda una filosófica tanto a nivel profesional como personal.

El problema a solucionar es la necesidad de mejorar la cultura en seguridad informática en los estudiantes de la Utmach, se evidencia la falta de una guía para saber qué hacer, cómo actuar y cuales medidas deben aplicarse al resguardar los datos e informaciòn personal.

EL objetivo principal es Elaborar una guía de seguridad informática enfocada a estudiantes dela UTMACH mediante la metodóloga COBIT 5 para mejorar la gestión de riesgos en los datos personales.

Los objetivos específicos que delinean el trabajo son:

- Caracterizar los criterios teóricos de una guía de seguridad mediante una revisión literaria para estructurar la guía de seguridad
- Identificar las vulnerabilidades informáticas en el tratamiento de datos personales mediante un análisis comparativo para idear medidas de seguridad
- Elaborar una guía de seguridad informática mediante la metodología Cobit 5 para mejorar la gestión de riesgos en los datos personales de los estudiantes de la Utmach

El alcance del proyecto es la propuesta de una guía de seguridad, no compete su implementación ni socialización; pero si da consejos prácticos a los estudiantes desde la perspectiva de la auditoria informática al mejorar la gestión de riesgos referentes a sus datos personales.

2. DESARROLLO:

En esta sección se especifica la fundamentación teórica ordenada sistemáticamente, de tal manera que permita entender la temática planteada. Se exponen temas relacionados al ámbito de estudio que han sido extraídos de distintos artículos de revistas científicas que pueden avalar la investigación realizada.

2.1 Marco Teórico

Comprende un conjunto de criterios y concepciones epistemológicas del estudio fundamentando la postura del autor en base a informaciòn documentada.

2.1.1 Seguridad informática en instituciones educativas.

Sin duda las instituciones educativas han aprovechado de forma increíble el uso de las Tecnologías de Información y Comunicación; implementándolas en su sistema educativo han encontrado la manera de mejorar la calidad de la educación tanto en la capacitación docente como en el proceso de enseñanza – aprendizaje del cuerpo estudiantil.

El uso de estas tecnologías prácticamente obliga a las instituciones a llevar un estricto control sobre su manejo, pues debido a la enorme cantidad de ventajas que ofrecen es posible que surjan riesgos debido a la vulnerabilidad del sistema informático. En este aspecto se debe prestar especial consideración a la seguridad informática, que no es otra cosa que el control del buen estado de la información y de los equipos que la albergan.

Es importante saber que existen varios procesos que pueden gestionarse para enfrentar estos riesgos, siempre y cuando se tenga en cuenta que deben ejecutarse como medida preventiva, pues esto ayudará a reducir las vulnerabilidades del sistema y por ende minimizará los riesgos. Logrando con esto evitar pérdidas de información ya sea por negligencia operativa o por intrusos de la red (Corda, Viñas, & Coria, 2017).

Para que exista un sistema informático seguro se debe tener las siguientes características:

Cuadro 1. Características de la seguridad informática.

Características de un sistema informático seguro	
Integridad	Sólo puede modificarse por el autor de la misma
Confidencialidad	Los datos solo pueden ser leídos por los interesados
Disponibilidad	La información debe estar a disposición en todo momento
Irrefutabilidad	La información debe conservar la autoría probada

Fuente: (Corda, Viñas, & Coria, 2017)

La seguridad informática es un tema del que gran parte de las organizaciones hoy en día se fijan debido al incremento en el uso de internet para realizar sus actividades; pues el internet es un medio que permite comunicar e intercambiar información desde un sitio a otro por más remoto que este sea. La seguridad informática trata de proteger equipos, información y usuarios; esto se logra con la correcta capacitación sobre medidas preventivas y análisis de riesgos.

Roque & Juárez (2018), explican que se puede aumentar la seguridad informática a medida que el personal se capacite y tenga conocimiento de los riesgos del sistema informático y de la forma adecuada para protegerse de ellos. Además, menciona que el personal debe saber el significado de ciertos términos como hackers, virus informáticos, phishing, respaldo informático, etc., para entender mejor sobre lo que se trata.

Es así que la aparición de las TIC en el mundo gestiona un pronunciado cambio del sistema de información, pues con ayuda de estas se puede dar solución a problemas complejos intercomunicando redes comunes y sustituyéndolas por servidores con cada vez mayor capacidad de procesamiento de datos (Quiroz & Macías, 2017).

En torno al tema de seguridad informática, es importante mencionar que se debe conocer las siguientes terminologías básicas:

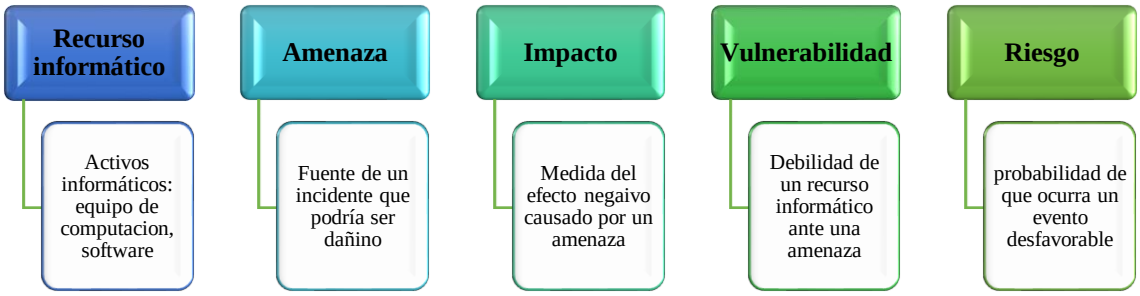


Ilustración 1. Conceptos básicos de la seguridad informática.

Fuente: (Quiroz & Macías, 2017)

2.1.2 Influencia de avances tecnológicos en universidades.

La innovación tecnológica aportada por las grandes potencias mundiales ha causado gran impacto en la sociedad, tanto así que hoy en día es casi imposible encontrar personas sin utilizar algún artefacto tecnológico. Las empresas productoras y comerciales y de servicios han incluido dentro de su organización, un sinnúmero de maquinarias con los que se les facilita ejecutar sus actividades, proporcionándoles resultados de rentabilidad y eficiencia.

Pero estas no son las únicas que se ven beneficiadas por la evolución de la tecnología; el sector educativo ha incorporado a su sistema educacional una variedad de programas y aplicaciones que le ayudan a optimizar el proceso de enseñanza – aprendizaje, mismos que junto a la implementación de equipos de cómputo logran una educación influyente que provoca ascendencia de nivel al sistema educativo del país.

Las TIC nacen con el afán de contribuir al desarrollo del conocimiento y facilitar el proceso de la información, ayudando a la satisfacción de las necesidades de un determinado grupo de personas. Las TIC implementadas en el sector educativo, aportan al proceso de enseñanza – aprendizaje y contribuyen a la gestión de la educación (Gómez, Contreras, & Gutiérrez, 2016).

Al mencionar la influencia de las TIC en el ámbito educativo, se debe saber que representa no solamente las herramientas como servidores y programas, sino que constituyen la oportunidad de analizar la forma en la que se maneja el sistema educativo. En base a esto se conoce que su implementación trae consigo un conjunto de ventajas y desventajas en el sector educativo. Estas se detallan en el siguiente cuadro:

Cuadro 2. Ventajas y Desventajas de la implementación de TIC en universidades.

VENTAJAS	DESVENTAJAS
Mejor aprovechamiento del tiempo	Poca capacitación docente para su manejo
Facilidad para trabajar en grupo	Desinterés académico por parte de alumnos
Motivación para realizar tareas	Desvinculación profesor – alumno
Facilidad de acceder a la información	Tráfico de información
Rapidez en el procesamiento de información	Distracción por parte de los alumnos
Variedad de canales de comunicación	Falta de inclusión
Eliminación de barreras espacio – tiempo	Educación poco humanística
Retroalimentación de conocimientos	Aprendizaje superfluo
Autonomía personal y desarrollo de trabajo colaborativo	Tiende a anular la capacidad de crítica
Optimización de organización	Cansancio visual y otros problemas
Agilidad en actividades administrativas y gestión	Poca memoria a corto plazo

Fuente: (Gómez, Contreras, & Gutiérrez, 2016)

Las TIC han generado gran impacto en el sector educativo, constituyen no solo un conjunto de herramientas utilizadas en la ejecución de actividades, sino que contribuyen a la formación académica y a la búsqueda de un modelo constructor de aprendizaje basado en la tecnología y el uso del conocimiento pedagógico. Hernández (2017), sostiene que los cambios experimentados por las TIC las han convertido en verdaderos instrumentos

formadores de estudiantes, que con su aplicación mejoran las condiciones de enseñanza y revolucionan la manera en que se obtiene y procesa la información.

Los países de la región, actualmente están adoptando as las TIC en las instituciones de educación superior (Universidades), pero debido a que este es un proceso lento aún se encuentran en la primera etapa, un poco lejos de alcanzar todo el potencial que ofrecen (Tapasco & Giraldo, 2017).

2.1.3 Metodología COBIT 5.

Dentro de los procesos de auditoria informática se emplea el uso de varias herramientas con las se posibilita distinguir rápidamente los riesgos y amenaza presentes en el medio digital.

Entre las herramientas utilizadas está COBIT 5 que consiste en una metodología utilizada con el fin de controlar la ejecución de proyectos, la cantidad de información procesada y los riesgos a los que expone. Su principal objetivo es el desarrollo investigativo presentando a su vez un plan de gestión de las tecnologías de información que pueda ser adoptado por grandes empresas a nivel mundial (Caiza & Bolaños, 2014).

Características	Objetivos
Orientado a negocios.	Proporciona la información que la organización requiere para alcanzar los objetivos.
Orientado a procesos.	Ofrece un modelo de procesos y un lenguaje común para todas las personas que integran la organización.
Basado en controles.	Proveen de un conjunto de requerimientos de alto nivel, que son considerados por la alta gerencia para un efectivo control.
Impulsado por mediciones.	Comprender el estado de los sistemas de TI que tienen en la actualidad.

Ilustración 2. Características de COBIT 5

Fuente (Caiza & Bolaños, 2014)

La metodología COBIT 5 se encarga de unir 5 principios que contribuyen a la buena administración de una organización, optimizando el uso de la tecnología para beneficiar a los interesados. Estos principios antes mencionados son muy utilizados por las empresas, sin distinción de tamaño o tipo.

COBIT 5 se basa en varios principios y habilidades que le permiten ser una herramienta de gestión y administración de proyectos, que muestra acciones a manera de ejemplo de sus características (De la Cruz, 2017). Los principios se detallan a continuación:

1. Satisfacer necesidades de los clientes (partes interesadas)

2. Cubrir la organización de forma completa
3. Emplear un marco integrado
4. Permitir un enfoque holístico
5. Dividir al gobierno de la administración

En cuanto a las habilidades, se las puede encontrar en la siguiente ilustración:

Ilustración 3. Habilidades de COBIT 5.

Fuente: *(De la Cruz, 2017)*

El Control Objetives for Information Technology (COBIT) es un gestor de las Tecnologías de Información, su última versión lanzada al mercado en el 2012 (COBIT 5) es un marco libre que enuncia la mejor manera de gestionar y administrar las Tecnologías de Información; puede ser utilizado en la administración de cualquier empresa. Este gestor ayuda a crear rentabilidad o valor utilizando las TI y llevando un balance entre riesgos, beneficios y recursos empleados (Yrigoyen, 2016).

2.1.4 Guía de seguridad informática.

En torno a la evolución tecnológica surgen nuevos riesgos que varían en tipo e intensidad dependiendo el origen de los mismos. En este punto se hace válido entender el concepto de seguridad informática que trata sobre la agrupación de medidas que deben usarse con el fin de garantizar una navegación segura en la red y que de alguna manera podrían minimizar los riegos a los que se expone constantemente el sistema informático de la organización.

Para ello es indispensable establecer un conjunto de reglas y normativas con las que se pueda prevenir, minimizar y combatir aquellos riesgos que aparecen debido a las vulnerabilidades del sistema informático. Existen muchas herramientas que suelen usarse como programas, aplicaciones, antivirus, enfoques de análisis tanto estático como

dinámico y otras formas de detección de problemas informáticos; para proporcionar una revisión sistemática y completa (Hernández & Mejia, 2015).

2.2 Caso Práctico

Compete la resolución de la problemática, aplicar los saberes afines al ejercicio profesional de la carrera al elaborar la guía de seguridad conjugando los criterios versados de la auditoria Informàtica.

2.2.1 Aplicación de metodología COBIT 5 en el sistema informático de universidades.

La metodología COBIT 5 como se enunció anteriormente constituye un marco libre que trata de conseguir valores utilizando las Tecnologias de Informacion, tomando en cuenta los factores externos como los riegos y beneficios. Actualmente las instituciones educativas de nivel superior han adoptado tecnologías con las cuales busca mejorar la calidad de la educación (Zambrano & Molina, 2017).

Con la aplicación de esta metodología se obtiene un conjunto de normativas que basadas en ciertas organizaciones y comisiones ayudan a cuantificar el desempeño que tienen las empresas al momento de gestionar la información. Certificando que se cumplan los objetivos marcados, respondiendo siempre a los modelos estándar señalados.

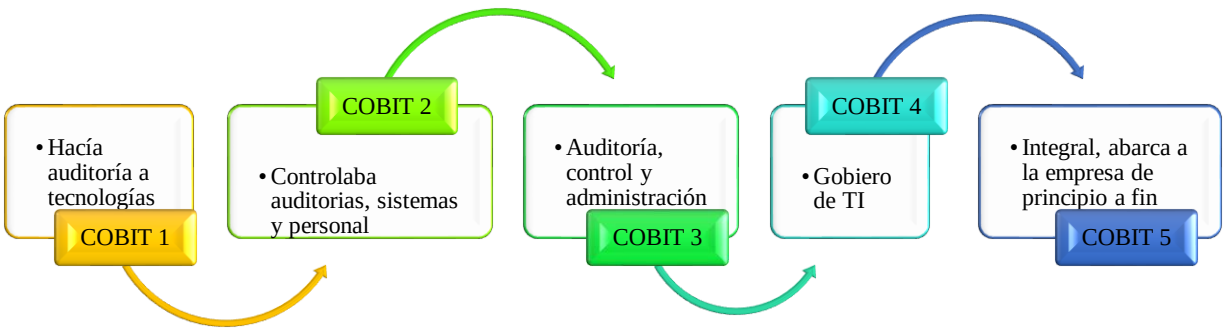


Ilustración 4. Evolución de la metodología COBIT.

Fuente: *(Zambrano & Molina, 2017)*

Arcentales & Caycedo (2017), señalan que COBIT permite desarrollar habilidades de manejo de las TIC en las instituciones, tratando de conseguir un aumento en el valor empresarial a través de la utilización de tecnologías de la información cumpliendo con

las normativas establecidas, básicamente esta metodología trata de trabajar con la institución como un todo sin individualizar.

2.2.2 Vulnerabilidades informáticas en el campus Utmach.

Debido a que se enfatiza en el tratamiento de datos personales, es necesario entrevistar a los estudiantes para analizar su perspectiva e identificar sus conductas entorno a los activos digitales.

Cuadro 3. Debilidades en los campos de acción de los estudiantes

CAMPO DE ACCIÒN	DEBILIDADES	Riesgos
Smartphone	No se tiene un antivirus para celulares, ni procesos o protocolos de seguridad	Pérdida del equipo, avería, pérdida de acceso al dispositivo, daño o corrupción de datos
Redes sociales	No se tienen contraseñas fuertes, ni cierre automático, están vinculadas entre sí (ordenador, celular, correo)	Exponer informaciòn sensibles, chantajes, acosos o problemas legales por fotografías y comentarios
Correo electrónico institucional	Poca versatilidad, su uso es restringido y no se hace a consciencia	Pérdida de acceso, daño de archivos o documentos referentes a las clases
Redes e internet (estudiante y docente)	La red WLAN falla constantemente, es muy lenta ocasionando molestias	Dejar abiertas redes sociales en ordenadores de ciber, perder acceso a plataformas virtuales o no enviar trabajos a tiempo
Políticas de seguridad	No son muy difundidas, no se han actualizado ni retroalimentado	Las amenazas actuales sobrepasan a las previstas, no es aplicada por los estudiantes ni socializada por autoridades
Servicios y plataformas virtuales Utmach	Fallos en el sistema, confusiones entre estudiantes, poca agilidad en procesos, lenta respuesta de las plataformas.	Daños en la informaciòn de los estudiantes, exposición de datos sensibles, no registrar notas.

Fuente: Elaboración Propia

Algunos estudiantes manifiestan que el sistema suele confundir su identidad, errores en los registros de notas, asistencia a clases; además muchos de ellos publican abiertamente su informaciòn personal como ubicación, actividad y hora, siendo un blanco fácil porque

sin notarlo están vulnerando su espacio privado; también que usan contraseñas débiles sin seguir las recomendaciones de la dirección de TIC`s, mismas que no son socializadas correctamente.

En lo referente a redes e internet, existe un descontento general sobre la lentitud, saturación del WIFI, dificultando uso de ordenadores en tareas e investigaciones académicas.

Es aconsejable que el sistema informático codifique y encripte la informaciòn protegiéndola por sí sola, porque los alumnos no presentan preocupación por cuidar sus respectivos datos, esto indica que el problema sea de carácter cultural.

2.2.3 Controles de seguridad aplicables.

En base a una exhaustiva revisión literaria, observaciones y entrevista a estudiantes se deducen las conjeturas del *cuadro 4.*

Cuadro 4. Controles aplicables al entorno institucional de la Utmach

CAMPO DE ACCIÒN	**MEDIDAS DE SEGURIDAD**
Smartphone	Contraseñas periódicas por software, bloqueo y eliminación de datos remoto, así como respaldo en drive
Redes sociales	Autentificación en dos pasos, no exponer informaciòn sensible como números, correos, direcciones de viviendas, contraseñas fuertes.
Correo electrónico institucional	Contraseña fuerte y verificación de identidad, ser usado únicamente en procesos académicos
Redes e internet (estudiante y docente)	Mejorar el ancho de banda, incrementar velocidad y renovar infraestructura de internet
Políticas de seguridad	Socializarlas, actualizarlas e implementarlas, ser llevadas a la práctica es el paso principal en la seguridad
Servicios y plataformas virtuales Utmach	Potenciar los servidores, usar prestaciones cloud computing, monitorear el tráfico de la red e implementar configuraciones seguras

Fuente: Elaboración Propia

Según la metodología COBIT 5, la empresa debe analizarse en su totalidad, pero es necesario hackeos éticos, juicio de expertos e inferencias pragmáticas para proponer una guía holística; por lo tanto, respetando sus lineamientos se enfocan en los procesos de seguridad aplicables por lo estudiantes y proponer las medidas competentes a la universidad.

2.2.4 Descripción de la guía de seguridad informática.

En una guía de seguridad informática constan las herramientas y los procesos que se siguen para garantizar que tanto los equipos como la información se encuentren en buen estado y con el mínimo riesgo posible.

Herramientas:

Los instrumentos evidentemente son físicos y lógicos; los discos duros externos, celulares con huella digital, tecnologías de acceso remoto (bloqueo y eliminación de datos); activos digitales como antivirus, cortafuegos, software de análisis, alertas y matriz de riesgos para valorar e identificar conductas de vulnerabilidad.

La matriz debe ser pro activa, acorde al contexto local por ende se propone lo siguiente:

Cuadro 5. Matriz de acciones contra riesgos detectados

RIESGO	**NIVEL DE PELIGRO**	**ACCIONES**
Pérdida de dispositivos	ALTO	Respaldar datos e informaciòn
Olvidar claves	MEDIO	Recuperar datos, reforzar seguridad y usar contraseñas periódicas
Acoso o chantajes	ALTO	Denunciar, documentarse y tomar acciones legales
Errores o fallos en el sistema	BAJO	Comunicar a docentes y autoridades

Fuente: Elaboración Propia

En forma paralela se debe minimizar los riesgos, evitando paginas o contenidos inapropiados, puesto que es posible que un virus de ordenador infectado en un ciber se vincule a todas las cuentas personales.

Procesos:

Los procedimientos deben ser sistemáticos, realizar actividades constantes al mantener la seguridad en los datos sensibles.

- Prevenir riesgos y amenazas informáticas
- Identificar peligros o riesgos
- Tomar acciones correctivas
- Revisar la seguridad de sus dispositivos e informaciòn
- Repetir el proceso semanalmente

Políticas:

Se propone lo siguiente:

1. Respaldar datos e informaciòn tanto físicamente como virtualmente (nube)
2. Usar contraseñas fuertes y software de encriptado
3. Mantener vigilancia sobre el estado de sus cuentas
4. No exponer datos sensibles como ubicación, informaciòn personal o actividades diarias
5. Comunicar cualquier irregularidad a las autoridades y docentes competentes
6. Evitar contenidos inapropiados y computadores ajenos
7. No dar ni compartir claves a terceros o dejar teléfono a terceros

Cultura:

Es el aspecto principal de la seguridad, debido a que el desconocimiento, malas conductas e ignorar los peligros conducen a las vulnerabilidades detectadas; un punto fuerte de la metodología COBIT 5 es el personal, debe capacitarse, empoderarse y desarrollar por sí mismo criterios de eficiencia en cuestiones de seguridad.

Se aconseja socializar las políticas de la dirección de TIC`s, coordinar y gestionar charlas en el auditoria sobre seguridad informática, concientizar al cuerpo estudiantil e integrar procesos normados para promover una participación más dinámica en lo relacionado riesgos informáticos.

Aplicación:

Su aplicación debe ser sistemática, docentes, estudiantes, negocios dentro del campus, personal en general e inclusive visitantes o terceros para evitar cualquier riesgo dentro y fuera de la institución.

El principal problema no es el acatamiento, sino el desconocimiento y poca participación de las autoridades que no le dan la debida importancia, por ello es imperioso dar a conocer los riesgos, instrumentos y medidas para que los propios estudiantes sean responsables de cuidar sus datos personales.

3. CONCLUSIONES:

La guía de seguridad es una serie de policías, herramientas y procesos claves en la gestión de riesgos informáticos, aunque no se hayan registrado daños o ataques consumados es mejor prevenir, renovar la infraestructura e integrar una cultura en la protección de datos tanto personales como institucionales.

El mayor riesgo encontrado es la falta de implementación de las políticas de seguridad, poca tecnificación en procesos de diagnóstico de fallas y una cultura ambigua en términos de protección de informaciòn; puesto que por sí mismos cometen actos que viabilizan amenazas como dejar redes sociales abiertas, exponer informaciòn sensible, no respaldar datos o simplemente ignorar los peligros.

Posterior a la investigación realizada se ha podido evidenciar que a medida que crece y se desarrolla la tecnología, se incrementan también los riesgos informáticos y se debe estar preparado para enfrentarlos por ello es importante tener el conocimiento necesario para utilizar las herramientas y metodologías correctas con las que se garantice la confidencialidad de la información y el buen estado de los equipos.

Los riesgos no opacan las bondades de las TIC`s; pero ya es tiempo de potenciar la seguridad y formalizar una metodología de gestión como COBIT 5 que se adapta fácilmente a los requerimientos de la Utmach.

4. REFERENCIAS BIBLIOGRÁFICAS

Arcentales, D., & Caycedo, X. (2017). Auditoría informática: un enfoque efectivo. *Dominio de las ciencias*, 157-173.

Caiza, M., & Bolaños, F. (2014). Las implementaciones de las normas de seguridad de la información: estudio de caso la Sociedad de Lucha Contra el Cáncer del Ecuador. *Revista electrónica de Computación, Informática, Biomédica y Electrónica*, 2-22.

Corda, M., Viñas, M., & Coria, M. (2017). Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje. *Palabra Clave (La Plata)*, 1-18.

De la Cruz, P. (2017). Capital Intelectual, Gestión del Conocimiento en la Interacción Gobierno y Gestión de las Tecnologías de la Información desde Perspectiva COBIT 5. *Hamut´ay*, 30-44.

Gómez Collado, M., Contreras Orozco, L., & Gutiérrez Linares, D. (2016). El impacto de las tecnologías de la información y la comunicación en estudiantes de ciencias

sociales: un estudio comparativo de dos universidades públicas. *Innovación Educativa*, 61-80.

Hernández , A., & Mejia, J. (2015). Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web. *Revista electrónica de Computación, Informática Biomédica y Electrónica*, 2-18.

Hernández, R. (2017). Impacto de las TIC en la educación: Retos y Perspectivas. *Propósitos y Representaciones*, 325 - 347.

Quiroz, S., & Macías, D. (2017). Seguridad en informática: consideraciones. *Dominio de las ciencias*, 676-688.

Roque, R., & Juárez, C. (2018). Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios. *Paakat: Revista de Tecnología y Sociedad*, 1-13.

Tapasco, O., & Giraldo, J. (2017). Estudio Comparativo sobre Percepción y uso de las TIC entre Profesores de Universidades Públicas y Privada. *Estudio Comparativo sobre*, 3-12.

Yrigoyen, M. (2016). Modelo de referencia de gobierno de las tecnologías de la información para instituciones universitarias. *INTERFASES*, 87-115.

Zambrano, M., & Molina, L. (2017). Diagnóstico situacional del Gobierno de las Tecnologías de Información. Caso Universidad Laica Eloy Alfaro de Manabí. *Revista Ciencia UNEMI*, 111 - 122.