BLUEFIELDS INDIAN & CARIBBEAN UNIVERSITY
BICU

FACULTAD DE CIENCIAS DE LA EDUCACIÓN Y HUMANIDADES
FACEYH

ESCUELA DE INFORMÁTICA

INGENIERÍA EN SISTEMAS

Monografía para Optar al título de Ingeniero de Sistemas

Política de seguridad informática para la Bluefields Indian & Caribbean University (BICU), sede central, 2021

Autores:

Br. Jenifer Tamara Hurtado Martínez

Br. Cesar Augusto Ocampo Núñez

Tutor:

Msc. Jhonny Francisco Mendoza

Bluefields, RACCS, Nicaragua

Agosto, 2022

“La educación es la mejor opción para el desarrollo de los pueblos”

ÍNDICE DE CONTENIDO

ÍNDICE DE GRÁFICOS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

RESUMEN

La investigación monográfica que lleva por título **"Política de seguridad informática para la Bluefields Indian & Caribbean University (BICU)"** tiene como objetivo principal diseñar políticas de seguridad informática para el resguardo de los datos y equipos informáticos, gestionados por la universidad y sus diferentes instancias. Para alcanzar dicho objetivo primeramente se deben identificar las vulnerabilidades de los datos de la universidad. Dicha identificación servirá como base para minimizar los riesgos como dispersión de datos, pérdida de tiempo y demás sobre los recursos TIC (Tecnologías de la información y telecomunicaciones) que posee la institución, además se propuso una estructura organizativa que se encargue de velar por las políticas de seguridad informática.

Las políticas de seguridad plasmadas en este documento son una herramienta fundamental para el resguardo de los recursos TIC de la universidad además busca el desarrollo del conocimiento tecnológico del capital humano que es esencial para el buen funcionamiento y aprovechamiento de dichos bienes.

Esta investigación fue descriptiva ya que se describieron características y cualidades de las variables con un corte transversal, también se apuntó a un tiempo definido, la población de estudio estuvo constituida por 9 trabajadores permanentes 3 pasantes y 6 monitores, como resultados tenemos un total de 18, la medición se hizo a través de los instrumentos entrevista y encuestas, los instrumentos se aplicaron después de informar el propósito.

Los resultados obtenidos arrojaron que no existe en el recinto un documento donde se plasmen las políticas de seguridad necesarias para el resguardo de los recursos TICS por lo cual se hizo una propuesta de ello.

Palabra claves: Políticas, Seguridad, Informática, TIC

ABSTRACT

The main objective of the monographic research entitled "Computer Security Policy for the Bluefields Indian & Caribbean University (BICU)" is to design computer security policies for the protection of data and computer equipment, managed by the university and its different instances. To achieve this objective, the vulnerabilities of the university's data must first be identified. Said identification will serve as a basis to minimize risks such as data dispersion, loss of time and others on the ICT resources (Information and Telecommunications Technologies) that the institution possesses, in addition, an organizational structure is determined that is responsible for ensuring the policies computer security.

The security policies embodied in this document are a fundamental tool for the protection of the ICT resources of the university, it also seeks the development of the technological knowledge of human capital that is essential for the proper functioning and use of said assets.

This research was descriptive since the characteristics and qualities of the variables were described with a cross section, it was also pointed out at a defined time, the study population consisted of 9 permanent workers, 3 interns and 6 monitors, as results we have a total of 18, the measurement was made through the instruments and surveys, the instruments were applied after informing the purpose.

The results obtained showed that there is no document on the premises where the security policies necessary for the protection of ICT resources are reflected, for which a proposal was made.

Keywords: Politics, Security, Informatic, ITC

I. INTRODUCCION

La información es uno de los activos más valiosos que tiene toda organización, esta facilita la toma de decisiones y permite el desarrollo de las actividades cotidianas. La Bluefields Indian & Caribbean University, a través de sus diferentes áreas o departamentos, genera gran cantidad de datos que se almacenan en servidores o en computadoras personales. Departamentos como Administración, Contabilidad, Recursos Humanos, Registro Académico, entre otras, manejan información de estudiantes, colaboradores, empleados y demás; la seguridad informática juega un papel imprescindible en la institución, pero ¿qué tan efectivos son los métodos que se utilizan? La seguridad está dividida en diversos aspectos como la disponibilidad, confidencialidad, integridad que buscan un bien común, el correcto funcionamiento de todo el entorno informático.

Las políticas de seguridad informática para el uso y aprovechamiento de los recursos TIC, en la Bluefields Indian & Caribbean University (BICU), son la base para alcanzar la protección, el resguardo físico, lógico de los datos y equipos tecnológicos de las diferentes áreas de la universidad con el fin que funcionen como directrices que permitan garantizar los tres principios básicos de la seguridad informática que son confidencialidad, la integridad y la disponibilidad y así contribuir al crecimiento y desarrollo tecnológico de los recursos TIC con los que cuenta esta casa de estudios. Esta investigación se realizó en el segundo semestre del año 2021.

Con la puesta en marcha de esta investigación se buscó identificar las amenazas y vulnerabilidades de los datos e información de la universidad para la formulación pertinente de las políticas de seguridad, seguidamente se describieron las claves necesarias para minimizar los riesgos sobre los recursos TIC, garantizando la continuidad de las operaciones de la organización al tiempo que se administra ese riesgo y finalmente se hizo la propuesta de una estructura organizativa. Este estudio, tuvo un enfoque mixto ya que fue el que mejor se adaptó a las necesidades y características de la misma y fue investigación descriptiva porque se trabajó con aspectos fundamentales de la problemática planteada.

1.1 Antecedentes

Definir políticas de seguridad es una necesidad que toda institución debe de cumplir. Es por ello que, para fortalecer el trabajo de investigación, se realizo una búsqueda de otras investigaciónes que dieran sustento al presente documento investigativo.

A nivel internacional se encontraron las siguientes investigaciones:

Tulmo Checa (2019) realizó una tesis para la obtención del titulo de ingeniero en informática y sistemas computacionales que tuvo por titulo, *diseño de un modelo de políticas de seguridad informática* para la Universidad Tecnica de COTOPAXI. El objetivo principal de la investigación fue diseñar un modelo de Políticas de Seguridad Informática para la Universidad Técnica de Cotopaxi basada en la norma ISO/IEC. Las metodologías utilizadas para la recopilación de información son las investigaciones de campos y bibliografías, las técnicas utilizadas fueron observación y la entrevistas. Las conclusiones obtuvieron con el desarrollo de la tesis son:

- Poseer conocimientos sobre metodologías y mecanismos de seguridad informática es de suma importancia ya que las tecnologías de la información y comunicación avanzan a pasos agigantados y es sustancial para la institución contar con elementos que ayuden a resguardar la información de forma adecuada, confiable y segura.
- La Universidad Técnica de Cotopaxi al contar con el diseño de políticas de seguridad informática, podrá contar con una guía para contrarrestar los riesgos a los cuales se encuentra expuesta y además sirven como pauta para la utilización correcta de los recursos informáticos con los que cuentan la institución.
- El diseño de las políticas de seguridad informática tuvo como base la utilización de la norma ISO/IEC 27001:2013, la cual tiene como propósito el aseguramiento, la confidencialidad e integridad de la información y de los sistemas que la procesan.

En el protocolo presentado por Galeano y Alzete (2013) *titulado Modelo protocolo de políticas de seguridad informática* para las Universidades de Risalda. El objetivo principal de dicha investigación fue proponer un protocolo que marque unas pautas claras al momento de implementar la seguridad en las instituciones de educación superior proporcionando una orientación y unas recomendaciones en la elección de herramientas para así garantizar el correcto funcionamiento de los sistemas y al momento de un posible ataque o desastre natural que conlleve a perdida de información o sistemas informáticos, saber cómo actuar para mitigar el problema

tomando los correctivos apropiados . Las metodologías utilizadas para el desarrollo de esta investigación, consta de un estudio basado en sondeos a estudiantes de diferentes universidades y distintos programas y entrevistas a los encargados del área de sistemas, por lo que eligieron el tamaño de la muestra de acuerdo a la necesidad utilizando estadística no probabilística. Los principales resultados obtenidos con la investigación fueron que no hay unas buenas prácticas implementadas de seguridad informática y poco conocimiento e importancia por la parte académica y administrativa. Puede concluir que la seguridad informática juega un papel muy importante en las universidades, por lo cual, es importante realizar unas buenas prácticas de seguridad, para así mantener un alto estándar de protección de la información.

En un escrito presentado por Puris y Viteri (2014) *mencionan en un escrito para la obtención del título de ingeniera en sistemas* tuvo como objetivo definir políticas de seguridad informáticas en la UTEQ que conlleven a un mejor uso de los activos tecnológicos y la información, la cual busca definir políticas de seguridad informática en la unidad de Tics, en beneficio de la Universidad Técnica Estatal de Quevedo para que de esta manera se conlleven a un mejor uso de los activos tecnológicos y la información buscando establecer en el interior de la Institución una cultura de calidad operando en una forma confiable.

El problema que se abordó para el desarrollo de este proyecto es el hecho de que en esta institución académica se maneja información transcendental de estudiantes, finanzas e investigaciones, dicha información debe ser protegida de ataques informáticos, lo mismos que pueden ocasionar serios problemas a sus bienes, servicios y operaciones. Por tal razón se definirán políticas de seguridad informática para prevenir riesgos y amenazas que pongan en peligro la disponibilidad, integridad y confidencialidad de las tecnologías de información y comunicación. Las metodologías utilizadas para la recopilación de información son las investigaciones de campos y bibliografías y las técnicas que se utilizaron fueron el Método Descriptivo-Analítico y las entrevistas. Las conclusiones obtenidas con el desarrollo de este proyecto son:

Definición de políticas de seguridad informática en esta sección del documento se presenta una propuesta de políticas de seguridad, como un recurso para mitigar los riesgos a los que la universidad técnica estatal de Quevedo se ve expuesta.

- Políticas de seguridad del personal.
- Políticas de seguridad física y ambiental.

- Políticas generales de seguridad.
- Políticas del departamento de tics.

Mollocondo (2019*)* presentó la tesis *Análisis de riesgo y políticas de seguridad de información de la Oficina de Tecnologías de información (OTI)- UNA Puno,* para optar el grado académico de: magister scientiae en informática con mención gerencia de tecnologías de la información y comunicaciones, que tenía como objetivo el poder elaborar políticas de seguridad de la información para salvaguardar la información y que estas políticas, puedan dar fortaleza a los tres principios de seguridad de la información: confidencialidad, integridad y disponibilidad, llegando a presentar la propuesta de políticas de seguridad de la información El problema que se aborda es que no se ha iniciado con un Sistema de Gestión de Seguridad de la Información (SGSI), ni mucho menos con implementar políticas de seguridad de la información, el cual es la base del SGSI.

Las metodologías utilizadas para el desarrollo de esta investigación, es de corte positivista, teniendo mayor preocupación en procedimientos analíticos, es decir, por la fragmentación y el estudio de las partes que constituyen el todo social. Para desarrollar el alcance y los objetivos propuestos en el proyecto, la metodología a implementar enmarca las fases de inicio, análisis y propuesta. Los principales resultados obtenidos con dicha investigación son de acuerdo al resultado de análisis de riesgo de la seguridad de la información respecto a los activos primordiales de la Oficina de Tecnologías de Información de la Universidad Nacional Del Altiplano (UNA) PUNO, existen 12 riesgo de nivel alto, 28 riesgos de nivel medio y 151 riesgos de nivel bajo, siendo varios los criterios respecto a las amenazas que puedan vulnerar la información que administra la OTI, que permite delimitar el su estructura, siendo hoy en día la información en todas sus formas un activo primordial, al cual debe garantizarse su confidencialidad, integridad y disponibilidad.

A nivel nacional se encontraron las siguientes investigaciones

(García y Malespín, 2014) realizaron una tesis titulada *Propuesta de políticas informáticas para el uso y aprovechamiento de los recursos tic en las alcaldías de Boaco*. El objetivo principal de la investigación fue contribuir al crecimiento y desarrollo tecnológico ordenado de los recursos TIC, en las Alcaldías del Departamento de Boaco, mediante la formulación de Políticas Informáticas, que sirvan de base para la optimización de los recursos, procesos y operaciones municipales. La metodología aplicada al trabajo se basó en los métodos deductivos, inductivo y el analítico,

implementando las principales técnicas para la recopilación de datos tales como encuestas y entrevistas al personal operativo e informático de cada Alcaldía de Boaco; de igual forma se hace uso de la observación para conocer los diferentes procesos que se llevan a cabo. El resultado obtenido fue la creación de las políticas informáticas seguido de las recomendaciones dirigidas a las Alcaldías y futuros egresados de la carrera.

A nivel regional no se encontraron antecedentes.

1.2 Justificación

La seguridad informática es el proceso por medio del cual se protegen los activos informáticos. Se debe tener en cuenta que, en la actualidad, la información juega un papel muy importante y es considerado el activo más valioso en las organizaciones, lo cual ha generado que se le dé mayor atención a la disponibilidad, confidencialidad e integridad de los datos para garantizar una fluidez segura y protegida.

La Bluefields Indians & Caribbean University (BICU), sede central, Región Autónoma de la Costa Caribe Sur de Nicaragua, es una institución educativa de educación superior que requiere de gran control en este aspecto, como también contar, con los documentos de políticas de seguridad bien establecidas en todo lo que concierne al manejo de información, de datos y de usuarios, para que sean protegidas a la hora de permitir el acceso mediante las tecnologías de información y comunicación.

Por tanto, se hace necesario contar con estrategias y procedimientos para implementar la seguridad informática y garantizar el correcto funcionamiento de los sistemas para estar preparados al momento de un posible ataque o desastre natural que conlleve a pérdida de información o de tecnología informática y de comunicación, saber cómo actuar para mitigar el problema tomando los correctivos apropiados, por esa razón, esta investigación es de gran importancia y muy necesaria su realización.

Así mismo, las políticas de Seguridad informática funcionan como herramientas permiten identificar necesidades como las de capacitación al personal de una institución. Cabe resaltar que esta investigación juega un papel muy importante dentro de la dinámica operativa de la BICU ya que ayudad en la adquisición de los equipos informáticos bajo lineamientos de calidad y seguridad. Con este proyecto monográfico se presenta la oportunidad de proponer lineamientos Informáticos que ayuden al uso y aprovechamiento eficiente de los recursos TIC.

Como es de esperarse, los beneficiarios directos de este trabajo, será toda la comunidad académica y administrativa de BICU. De manera indirecta, toda la población de Bluefields y sus alrededores que viene a la institución a solicitar algún tipo de servicio. Por último, es importante resaltar que la puesta en marcha de este trabajo investigativo viable, pues se tuvo acceso al área geográfica de

la institución y a la población y muestra tomada en cuenta para el estudio. Financieramente esta investigación no requirió de grandes gastos, por ende, fue puesto en marcha con los recursos monetarios propios de los investigadores. Para finalizar, con la ejecución de esta investigación no se alteró ni se causó ningún daño a un individuo o comunidad.

1.3 Planteamiento del problema

En la actualidad, las políticas de seguridad informática juegan un papel vital en la protección de información y recursos tecnológicos en una institución. Estas surgen para minimizar los riesgos a los que están expuestos los sistemas, resguardando la privacidad de la información y evitando que personas no autorizadas accedan a esta, manteniendo la integridad de los datos cuando ocurren fallos de soportes o se borran por accidente. Es así, que las políticas de seguridad informática son una herramienta fundamental para toda institución, ya que sirven para generar conciencia entre el personal y educarlo en materia informática.

La Bluefields Indian & Caribean University es una institución profesional con reconocimiento nacional e internacional en materia educativa. Su sede central está ubicada en la ciudad de Bluefields, RACCS, Nicaragua y, a pesar de contar con 31 años de fundación, se ha constatado por medio de la aplicación de entrevistas, encuestas, experiencia personal y una investigación exhaustiva que en la universidad, no se cuenta con políticas de seguridad informáticas para garantizar la integridad de los datos y la protección de los equipos de informática con los que se cuenta en esta casa de estudio, lo cual podría ocasionar serías repercusiones debido a las vulnerabilidades que existen hoy en día y que hasta podría comprometer gravemente la actividad diaria como una institución profesional.

Ante esta situación, para el desarrollo de la presente investigación, se plantea la siguiente interrogante.

¿Qué medidas toma la unidad de soporte informático para garantizar la integridad de los datos y equipos y por qué, hasta la fecha, la universidad no ha definido o establecido sus Políticas de Seguridad Informática?

II. OBJETIVOS

2.1 General

Diseñar políticas de seguridad informática para el resguardo de los datos, la información y equipos informáticos, gestionados por la universidad y sus diferentes instancias.

2.2 Específicos

- Identificar las amenazas y vulnerabilidades de los datos e información de la universidad para la formulación pertinente de políticas de seguridad informática que contribuyan al buen funcionamiento de la institución.
- Describir las Políticas de Seguridad Informática necesarias para minimizar los riesgos sobre los recursos TIC, garantizando la continuidad de las operaciones de la organización al tiempo que se administra ese riesgo informático.
- Proponer una estructura organizativa del departamento de informática que se encargue de velar por las políticas de seguridad informática.

III. MARCO TEORICO

3.1 Marco Conceptual

3.1.1 Seguridad informática

La seguridad informática como el proceso de prevenir y detectar amenazas en los sistemas informáticos que puedan poner en riesgo, sobre todo, la data. Esta rama de la ciber seguridad se encarga de mantener lejos de las manos de intrusos todos los recursos informáticos y de data, que suelen ser vulnerados con el objetivo de cometer fraude, hacer extorsiones o vender la información.

Se compone de una serie específica de procesos que abarcan desde software antivirus, firewalls y otras medidas especializadas acorde al sistema informático en cuestión, qué recursos de red tenemos y otras particularidades. La idea es que mediante un plan de acción puedas abarcar problemas de confidencialidad, autorizaciones, disponibilidad y autenticación sin correr el riesgo de que tus datos sean modificados, borrados o robados por una brecha de seguridad. (CompuEducacion, 2019).

3.1.2 Amenazas

Las amenazas consisten en la fuente o causa potencial de eventos o incidentes no deseados que pueden resultar en daño a los insumos informáticos de la organización y ulteriormente a ella misma. Entre ellas, identificamos como las principales:

- El advenimiento y proliferación de "malware" o " software malicioso", programas cuyo objetivo es el de infiltrase en los sistemas sin conocimiento de su dueño, con objeto de causar daño o perjuicio al comportamiento del sistema y por tanto de la organización.
- La pérdida, destrucción, alteración, o sustracción de información por parte de personal de la organización debido a negligencia, dolo, mala capacitación, falta de responsabilidad laboral, mal uso, ignorancia, apagado o elusión de dispositivos de seguridad y/o buenas prácticas.
- La pérdida, destrucción, alteración, sustracción, consulta y divulgación de información por parte de personas o grupos externos malintencionados.
- El acceso no autorizado a conjuntos de información.
- La pérdida, destrucción o sustracción de información debida a vandalismo.
- Los ataques de negación de servicio o de intrusión a los sistemas de la organización por parte de ciber–criminales: personas o grupos malintencionados quienes apoyan o

realizan actividades criminales y que usan estos ataques o amenazan con usarlos, como medios de presión o extorsión.

- La pérdida o destrucción de información debida a accidentes y fallas del equipo: fallas de energía, fallas debidas a calentamiento, aterramiento, desmagnetización, ralladura o descompostura de dispositivos de almacenamiento, etcétera.
- La pérdida o destrucción de información debida a catástrofes naturales: inundaciones, tormentas, incendios, sismos, etc. Quiroz & Macias (2017) citado por Granger (2009)

3.1.3 Riesgos

El riesgo es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza. (Quiroz & Macias, 2017) citado por Santana Roldan C. (2012).

Voutssas (2010) define el riesgo como la probabilidad de que un evento nocivo ocurra combinado con su impacto o efecto nocivo en la organización. Se materializa cuando una amenaza actúa sobre una vulnerabilidad y causa un impacto.

3.1.4 Vulnerabilidades

Probabilidades que existen de que una amenaza se materialice contra un activo. No todos los activos son vulnerables a las mismas amenazas. Por ejemplo, los datos son vulnerables a la acción de los hackers, mientras que una instalación eléctrica es vulnerable a un cortocircuito. Al hacer el análisis de riesgos hay que tener en cuenta la vulnerabilidad de cada activo.

Las vulnerabilidades de un sistema son una puerta abierta para posibles ataques, de ahí que sea tan importante tenerlas en cuenta; en cualquier momento podrían ser aprovechadas. Podemos diferenciar tres tipos de vulnerabilidades según cómo afectan a nuestro sistema.

Vulnerabilidades ya conocidas sobre aplicaciones o sistemas instalados.

- Vulnerabilidades de las que ya tienen conocimiento las empresas que desarrollan el programa al que afecta y para las cuales ya existe una solución, que se publica en forma de parche. Existen listas de correo relacionadas con las noticias oficiales de seguridad que informan de la detección de esas vulnerabilidades y las publicaciones de los parches a las que podemos suscribirnos.

- Vulnerabilidades conocidas sobre aplicaciones no instaladas. Estas vulnerabilidades también son conocidas por las empresas desarrolladores de la aplicación, pero puesto que nosotros no tenemos dicha aplicación instalada no tendremos que actuar.
- Vulnerabilidades aún no conocidas. Estas vulnerabilidades aún no han sido detectadas por la empresa que desarrolla el programa, por lo que, si otra persona ajena a dicha empresa detectara alguna, podría utilizarla contra todos los equipos que tienen instalado este programa. Lograr que los sistemas y redes operen con seguridad resulta primordial para cualquier empresa y organismo. (Aguilera, 2010)

3.1.5 Impactos

Los impactos son los efectos nocivos contra la información de la organización al materializarse una amenaza informática. Al suceder incidentes contra la seguridad informática pueden devenir en:

- Disrupción en las rutinas y procesos de la organización con posibles consecuencias a su capacidad operativa.
- Pérdida de la credibilidad y reputación de la organización por parte del consejo directivo de la organización, público en general, medios de información, etcétera.
- Costo político y social derivado de la divulgación de incidentes en la seguridad informática.
- Violación por parte de la organización a la normatividad acerca de confidencialidad y privacidad de datos de las personas.
- Multas, sanciones o fincado de responsabilidades por violaciones a normatividad de Confidencialidad.
- Pérdida de la privacidad en registros y documentos de personas.
- Pérdida de confianza en las tecnologías de información por parte del personal de la Organización y del público en general
- Incremento sensible y no programado en gastos emergentes de seguridad.

Costos de reemplazo de equipos, programas, y otros activos informáticos dañados, Robados, perdidos o corrompidos en incidentes de seguridad. Voutssas (2010)

3.1.6 Principios de la seguridad

La seguridad informática de la información, conocemos como los principios fundamentales la disponibilidad, confidencialidad e integridad. El menor o mayor nivel de aplicación de estos 3 principios dependerá del tipo de empresa u organización en la que nos encontremos.

3.1.6.1 Confidencialidad

Respecto a la confidencialidad este principio se encarga de prevenir la divulgación de los datos a personas que no estén autorizadas, en resumen, este principio se encarga de qué de forma intencional o accidental se divulgue información sensible ante personas que no estén autorizadas a conocer los datos

3.1.6.2 Integridad

El principio de integridad garantiza la confiabilidad esto significa que el contenido debe permanecer inalterado a no ser que sea modificado por un usuario autorizado. Un fallo de integridad puede darse por ejemplo por un virus informático o por un atacante que realiza una modificación en los datos.

3.1.6.3 Disponibilidad

Este tercer principio fundamental de la seguridad informática es la disponibilidad, esto es que los datos permanezcan siempre disponibles para ser utilizados por usuarios autorizados. Una amenaza que afecta a este principio puede ser un fallo en el hardware debido a por ejemplo las condiciones del entorno como puede ser la humedad electricidad estática, etc. Para combatir los efectos de estas amenazas se implementan medidas tanto de recuperación, contingencia y resguardo de la información. Pc-Solucion (2017)

3.1.7 Políticas de seguridad

Las políticas de seguridad informática consisten en una serie de normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afectan

La definición de una política de seguridad debe estar basada en una identificación y análisis previo de los riesgos a los que está expuesta la información y debe incluir todos los procesos, sistemas y personal de la organización. Además, tiene que haber sido aprobada por la dirección de la organización y comunicada a todo el personal. Unir (2020)

6.1.7.1 Grupos de políticas de seguridad informática

Según Carisio (2018) dentro de las políticas de seguridad informática se pueden distinguir dos grupos:

- Las políticas que indican lo que se debe evitar.
- Las que definen qué es lo que siempre se debe hacer.

En la primera, se incluyen los comportamientos y prácticas que pueden poner en riesgo los sistemas y la información, como, por ejemplo: abrir archivos o enlaces sospechosos, compartir contraseñas, utilizar redes Wi-Fi abiertas, descargar archivos de páginas poco confiables, etc.

Por su parte, en el segundo grupo se definen las acciones para garantizar la seguridad, como realizar copias de seguridad, usar contraseñas seguras, usar VPN, instalar software de antivirus y antimalware, cifrar archivos con mayor vulnerabilidad, entre otras acciones.

3.1.8 Etapas de desarrollo de una política

Las etapas en el desarrollo de políticas de seguridad son:

6.1.8.1 Redacción

Escribir las políticas requiere utilizar un lenguaje conciso y fácil de comprender, a través de la selección de un enfoque que puede ser permisivo o restrictivo, así como evitar enunciados escritos en sentido negativo. En esta etapa ya deben estar definidos los temas a abordar en los documentos, como la legislación aplicable, información sensible, clasificación de la información, entre muchos otros.

6.1.8.2 Revisión

Luego de contar con la versión preliminar de los documentos, es necesario analizar el contenido para verificar que está alineado con los intereses de la organización, el sentido de la redacción y la funcionalidad de lo descrito en los enunciados, es decir, mantener el equilibrio entre la protección y operación. En esta fase, la retroalimentación es una actividad muy importante para comprobar que se emiten políticas que pueden ser cumplidas.

6.1.8.3 Aprobación

Después de llevar a cabo la revisión y de calificar el contenido como apropiado, las políticas deben ser ratificadas para su publicación. Como una actividad para el desarrollo del gobierno de la

seguridad de la información, es conveniente que los niveles jerárquicos más elevados dentro de la organización otorguen el visto bueno y promuevan la aplicación de las mismas.

3.1.8.4 Publicación

Una actividad de gran importancia en este ciclo consiste en dar a conocer las políticas entre las audiencias a las cuales están dirigidas. Es necesario contar con estrategias que permitan difundir el contenido entre los miembros de la organización, así como evaluar el conocimiento del personal con relación a estos documentos. Asumir que las políticas se leen y se cumplen sólo por mandato es una equivocación.

3.1.8.5 Actualización

Como ya se mencionó, la seguridad debe ser vista como un proceso de mejora continua, en donde los controles de seguridad se pueden mantener, corregir o cambiar en función de los resultados obtenidos y de los parámetros de medición establecidos.

La siguiente imagen muestra cada una de las etapas consideradas dentro de un proceso cíclico:

Ilustración 1: El ciclo de vida de las políticas de seguridad

Fuente: Welivesecurity (2014)

De esta manera, las etapas definen el ciclo de vida de las políticas de seguridad, como una tarea permanente dentro de las actividades de gestión de seguridad de la información. Welivesecurity (2014)

3.1.9 Seguridad física

La seguridad física es la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial.

Entonces, el buen estudio de la infraestructura tecnológica que se va a instalar en un edificio y el análisis del entorno físico son partes fundamentales para que se soporten las aplicaciones o sistemas de hardware y software; todo este estudio es para llevar a cabo la minimización de riesgos y generar una continuidad de operación en las organizaciones.

Revisando las principales amenazas, vulnerabilidades, ataques, se establece un esquema de prevención, donde se establece una detección y así mismo se realizan las medidas establecidas por las políticas de seguridad.

Las medidas de detección que se recomiendan son:

- Mantener las máquinas actualizadas y seguras físicamente
- Mantener personal especializado en cuestiones de seguridad
- Los administradores de red deben configurar en forma adecuada.
- Mantenerse informado constantemente sobre cada una de las vulnerabilidades
- Control de acceso, la restricción de los derechos de acceso a las redes, sistemas, aplicaciones, funciones, edificios y datos
- Seguridad de la información de manejo de incidentes, anticipar y responder adecuadamente a las violaciones de la seguridad de información
- Gestión de la continuidad, proteger, mantener y recuperar los procesos críticos de negocio y Sistemas
- Cumplimiento, garantizar la conformidad con las políticas de seguridad de la información, normas, leyes y reglamentos. Guzman (2018)

3.1.9.1 Prevención

En el momento que se requiera ser preventivos se debe de empezar con los diferentes roles de los recursos humanos, realizando una estructura organizacional con grados de responsabilidad y desarrollo de la custodia de la información; no se debe de olvidar que la buena clasificación de procesos y recursos nos lleva a generar protocolos de seguridad como lo pueden ser una buena gestión de alertas y así mismo puedan dar respuesta con reacción inmediata a una contingencia ocasionada al momento de la operación. Guzman (2018)

3.1.9.2 Detección

Hoy día, la detección ha evolucionado, partiendo de procedimientos tradicionalistas como innovadores, entonces para realizar una buena custodia de la información, se propone empezar por implementar una física reactiva; esto es, poner barreras físicas que son recursos humanos operando como vigilantes, o bien, usar la tendencia de la electrónica lógica como lo son los CCTV, sensores, firewall que en la actualidad se encuentra en verdadero auge, si se desea estar con líneas innovadoras, existe el desarrollo de la tecnología mediante la seguridad inteligente, que utiliza la biometría, análisis de imágenes, sistemas inteligentes de seguridad, sensores, sistemas blindados, etc.

Es importante evaluar y controlar la seguridad de las instalaciones con base en la integración de una función primordial, manteniendo controlado un ambiente que ayude a disminuir siniestros y así trabajar con una sensación de seguridad, basado en el descarte de falsas hipótesis que dieran origen a incidentes.

Podemos decir que, si contamos con una buena seguridad física tanto de infraestructura, instalaciones y que además incluya la seguridad del personal manteniendo una vigilancia y estableciendo controles, ayudará a minimizar los riesgos de las organizaciones, lo anterior se denomina arquitectura de seguridad de la información, ya que durante la operación se administran las amenazas, vulnerabilidades, procesos, entre otros, que ayudan a tomar decisiones en la generación de políticas de seguridad mediante el cumplimiento de normas. Guzman (2018)

3.1.10 Seguridad lógica

La seguridad lógica informática es una referencia a la protección por el uso de software en una organización, e incluye identificación de usuarios y contraseñas de acceso, autenticación, derechos

de acceso y niveles de autoridad. Estas medidas son para asegurar que sólo los usuarios autorizados son capaces de realizar acciones o acceder a información en una red o un equipo concreto.

La seguridad lógica incluye entre otros lo siguiente:

- Los virus
- Programas no testeados
- Errores de usuario
- Error del operador
- Mal uso del ordenador
- Fraude informático
- Investigación de accesos no autorizados internos
- Accesos no autorizados externos

Uno de los problemas con cualquier violación de la seguridad lógica informática es que el daño es invisible y su extensión es desconocida. El coste de investigación es muy probable que sea alto. Equipo de expertos de la universidad internacional de Valencia, (2016)

3.2 Marco Referencial

3.2.1 Contexto Histórico

La preocupación a la seguridad de la información, trasladada a la tecnología, data de 1980 cuando james P. Anderson, redacto el documento titulado "Computer Security Threat Monitoring and Surveillance" en donde se desarrollan los primeros conceptos de amenazas informática (Vargas & Lopez, 2014)

Los ataques informáticos son cada día más habituales, y son imposibles de evitar, dada la apertura de las redes actuales, la conexión de todo tipo de dispositivo a Internet y la creciente sofisticación de las amenazas avanzadas. Los ciberataques ya no son cuestión de "si" van a suceder, sino "cuándo". (Centro Nacional de respuestas a incidentes de seguridad informática, 2020).

3.2.2 Objetivos de las políticas de seguridad informática

Los principales objetivos de la seguridad informática podríamos destacar los siguientes:

- Minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad

- Garantizar la adecuada utilización de los recursos y de la aplicación del sistema
- Limitar las pérdidas y conseguir la adecuada recuperación de sistemas en caso de un incidente de seguridad
- Cumplir con el marco legal y con los requisitos impuestos por los clientes en sus contratos

Para cumplir con estos objetivos una organización debe contemplar cuatro planos de actuación

- Técnico: Tanto a nivel físico como a nivel lógico
- Legal: Algunos países obligan por ley a que en determinados sectores se implanten unas series de medidas de seguridad (Sector de servicios financieros y sector sanitario en estados unidos, protección de datos personales en todos los estados miembros de la unión europea, etc.
- Humano: Sensibilización y formación de empleados y directivos, definición de funciones y obligaciones de la persona.
- Organizativo: Definición e implantación de políticas de seguridad, planes, normas, procedimientos y buenas prácticas de actuación. (Gomez, Vieites, 2006)

3.2.3 Importancia de la seguridad informática

La importancia de la seguridad informática tiene como premisa principal la conservación de la integridad de la información y el equipo en sí. Piense en los virus como algo dañino que puede dañar tu sistema operativo y dejar tu ordenador colgado o muy lento, sin dejar trabajar con él. También, en el peor de los casos, podemos perder parte o todos los datos de nuestro ordenador y ello sería un desastre para nuestra productividad personal o profesional.

Otra cuestión a tener en cuenta es el valor de la información en sí, los datos importantes como tus cuentas bancarias, tus fotos y hasta tus gustos, todo ello es importante y debe ser protegido, porque cabe la posibilidad de que alguien externo haga mal uso de ello.

Hay que tener en cuenta que el factor más importante en el mantenimiento informático y la seguridad informática, es el usuario, muy por encima de los factores técnicos. De nada sirve tener una puerta acorazada si se deja abierta. (Informaticos.co, 2021)

3.2.4 Funciones de la seguridad informática

Las funciones que se refieren a la seguridad informática son:

- Planear y establecer estrategias de seguridad informática de acuerdo a lineamientos principios y necesidades institucionales.
- Contar con un sistema de información estadístico para dar seguimiento a los proyectos y planes de acción con el fin de garantizar dentro de la institución su implantación control y seguimiento.
- Definir, elaborar, liberar, difundir y actualizar políticas y normas de seguridad informática que permitan a las áreas de la organización implantar y fortalecer mecanismos de protección de la información.
- Realizar campañas de capacitación, difusión y concientización que eleven el nivel de recepción, entendimiento y conocimiento del personal en general sobre la materia.
- Realizar diagnósticos y evaluaciones de seguridad informática para identificar y minimizar los riesgos en los diferentes niveles funcionales, operativos y de sistema.
- Mantener la actualización sobre los avances tecnológicos en este campo, con el fin fortalecer esquemas de protección en la organización". Galeano & Alzete, 2013 citado por Mediavilla Manuel (1998, p 102, 103)

3.2.5 Características de una PSI

En el 2013, Galeano & Alzete resaltaron que siempre se debe tener en cuenta cuáles son las expectativas de la organización frente a las PSI, qué es lo que espera de ellas en cuanto a seguridad y eficacia.

Siempre que se redacten, las PSI deben permanecer libres de tecnicismos que dificulten su comprensión por parte de cualquier persona de la organización.

Cada política redactada, debe explicar por qué se toma dicha decisión y por qué se protegen esos servicios o conocimientos particulares.

Toda PSI debe ser vigilada por un ente, una autoridad, que la haga cumplir y apique los correctivos necesarios. Sin embargo, no debe confundirse una PSI con una ley, y no debe verse como tal.

Así como las características y elementos de una empresa cambian, también deben hacerlo las PSI, por lo que debe tenerse en cuenta, al redactarlas, que deben establecer un esquema de actualización constante, que dependa de las características de la organización.

No hay nada obvio. Se debe ser explícito y concreto en cuanto a los alcances y propuestas de seguridad. Esto evita gran cantidad de malos entendidos, y abre el camino para el establecimiento de la política de seguridad específica.

3.2.6 Requisitos Para Implementar Políticas De Seguridad Informática

Para la puesta en marcha de una serie de leyes, normas, estándares y prácticas que garanticen la seguridad, confidencialidad y disponibilidad de la información.

- Por un lado, se han de identificar las necesidades de seguridad y los posibles riesgos informáticos que enfrenta.
- Igualmente, se ha de proporcionar una perspectiva general de las propias reglas y procedimientos que deben implementarse para afrontar los diferentes riesgos identificados en los distintos departamentos de la organización.
- La siguiente etapa consiste en controlar y detectar las vulnerabilidades del propio sistema de información y mantenerse al tanto de los fallos presentes en las aplicaciones y materiales usados.
- Finalmente, has de definir las acciones previstas y las personas con las que contactarás en caso de amenaza. Hungria)2019).

3.2.7 Mecanismos preventivos de seguridad informática

Los mecanismos preventivos en la seguridad informática son los más olvidados, los cuales son vistos como una pérdida de tiempo, la parte administrativa en la mayoría de los casos lo ve como un costo extra, es algo parecido como por ejemplo, con los seguros médicos o seguros de vehículos, se puede pagar 10 años el seguro de un carro y nunca tener un accidente, en primera instancia se podrá analizar que es algo muy bueno, pero después en algún momento se podrá pensar que es un desperdicio haber pagado una cantidad 10 años y sin usarla.

La mayoría de los ataques informáticos se pueden evitar o por lo menos disminuir el impacto, si se hiciera utilizando mecanismos preventivos, deficiencia de sistemas y otros problemas podrían encontrarse, evitarse y resolverse gracias a un buen trabajo durante esta etapa. La barrera más fuerte a la que se enfrenta una empresa al querer aplicar los mecanismos preventivos es la

aceptación y el compromiso de todos los involucrados, hacer entender que no es una carga, es parte de los procesos y de lo que se debe hacer bien en la organización.

Entre los elementos que se pueden aplicar en los mecanismos preventivos se puede mencionar a:

• El respaldo de información: Las empresas entienden que los problemas con información son muy costosos, parece muy fácil, pero seleccionar los mecanismos de respaldo no es tan sencillo como se analizar, se tiene que considerar los siguientes factores: Qué formatos de archivo se tienen, por ejemplo, MP3, archivos de texto, bases de datos y otros, las imágenes y vídeos, por ejemplo, son archivos que normalmente necesitan atención especial.

• Horario de respaldo: Otro reto es a qué hora se puede hacer el respaldo, es común seleccionar las horas de menos tráfico.

• Control de los medios: El tener acceso a respaldos es algo de alto riesgo, se puede robar la información, manipular, perder, así que, el respaldo es una solución, pero también es otro problema que se debe resolver.

• La comprensión de la información: No toda la información se puede comprimir, pero existe alguna que, sí lo necesita, así que se deben hacer las valoraciones respectivas.

Estos son sólo algunos de los puntos que se deben considerar, solamente para el mantenimiento y respaldo de la información. Otros ejemplos de proceso que se tienen en el mecanismo preventivo son:

• Actualización de sistemas.

• Antivirus.

• Firewall.

• Navegación por internet.

• Contraseñas.

• Accesos remotos.

Estos son sólo algunos de los procesos, pero la organización puede personalizar lo que quiere considerar en los mecanismos preventivos (Romero, Figueroa, Vera, Álava, Parrales, Álava, Murillo & Castillo, 2018).

3.2.8 Mecanismos correctivos en seguridad informática

Los mecanismos correctivos tienen una gran diferencia en tiempo con los mecanismos preventivos, estos se aplican cuando, después de que algo sucedió y la función principal es corregir las consecuencias. Entre las características que tienen los mecanismos correctivos normalmente son muy caros, esto se debe a que el problema ya se lo tiene encima y no se puede tenerlo durante mucho tiempo, así que, contratar expertos para resolver el problema o el tiempo que le dedicara a el equipo de trabajo siempre va a costar mucho, en un porcentaje muy alto se acaban pagando servicios de solución a otras empresas, adquiriendo soluciones o comprando software y parches de actualización que logran resolver el problema.

Otra característica de los mecanismos correctivos es que el tiempo es limitado, así que el tiempo se vuelve algo muy apreciado en estos casos, pero también es muy escaso. Probablemente la empresa o la persona puede poder obtener dinero, pero tiempo es casi imposible. Dentro de los mecanismos de corrección se tienen diferentes pasos de ejecución para enfrentar este problema serio en los que se puede mencionar:

- Catalogación y asignación de problemas: En este paso se hace un catálogo de los problemas a los que se pueden enfrentar, detectar y clasificar es algo muy recurrente en todo lo relacionado con la seguridad informática, ya que es una forma para poder saber cómo abordar las situaciones y buscar alguna respuesta o solución a lo que se presenta.
- Análisis del problema: En este paso es muy evidente que la actividad que se hace es analizar el problema que se ha presentado, en muchos casos esta parte se realiza por los expertos, ya no, por las personas involucradas en el problema.
- Análisis de la solución: Antes de intentar solucionar el problema se debe de analizar la propuesta de la solución, se ha cometido un error, puede ser que no de forma directa, pero es un error, el impacto no va a ser más o menos, si es culpa del usuario o de un tercero, así que la solución tiene que estar bien planteada y ejecutada.

La documentación: Este componente es vital, ya que los cambios que se hacen probablemente son algo que se hizo con un tiempo limitado, rápido y que involucraron muchos recursos, así que la documentación es muy importante, ya que puede ser que por las velocidades no se recuerden todos los pasos y cambios que se han realizado. (Romero Castro, y otros, 2018).

3.2.9 Consecuencias de la falta de seguridad

A la hora de analizar las posibles consecuencias de la ausencia o de unas medidas deficientes de seguridad informática, el impacto total para una organización puede resultar bastante difícil de evaluar, ya que además de los posibles daños ocasionados a la información almacenada y a los equipos y dispositivos de red, deberíamos tener en cuenta otros importantes perjuicios para la organización:

- Horas de trabajo invertidas en las reparaciones y reconfiguraciones de los equipos y redes
- Pérdidas ocasionadas por la indisponibilidad de diversas aplicaciones y servicios informáticos: coste de oportunidad por no poder utilizar estos recursos.
- Robo de información confidencial y su posible revelación a terceros no autorizados: fórmulas, diseños de productos, estrategias comerciales, programas informáticos...
- Filtración de datos personales de usuarios registrados en el sistema: empleados, clientes, proveedores, contactos comerciales o candidatos de empleo, con las consecuencias que se derivan del incumplimiento de la legislación en materia de protección de datos personales vigentes en toda la Unión Europea y en muchos otros países.
- Posible impacto en la imagen de la empresa ante terceros: pérdida de credibilidad en los mercados, daño a la reputación de la empresa, pérdida de confianza por parte de los clientes y los proveedores.
- Retrasos en los procesos de producción, pérdida de pedidos, impacto en la calidad del servicio, pérdida de oportunidades de negocio.
- Posibles daños a la salud de las personas, con pérdidas de vidas humanas en los casos más graves.
- Pago de indemnizaciones por daños y perjuicios a terceros, teniendo que afrontar además posibles responsabilidades legales y la imposición de sanciones administrativas.

De hecho, es necesario contemplar otros posibles problemas que se podrían derivar del compromiso o toma de control de algunos de los equipos de una organización:

- Utilización de los equipos y redes de una organización para llevar a cabo ataques contra las redes de otra empresa
- Almacenamiento de contenidos ilegales en los equipos comprometidos, con la posibilidad de instalar un servidor FTP (o similar) sin la autorización del legítimo propietario de éstos.
- Utilización de los equipos de una organización para realizar envíos masivos de correo no solicitado (spam) (Leal, 2012).

IV. PREGUNTAS DIRECTRICES

1. ¿Cuáles son las amenazas y vulnerabilidades que pueden comprometer la integridad de los datos y la información de la comunidad universitaria en la BICU?
2. ¿Cuáles serían las políticas de seguridad informática idóneas para minimizar los riesgos en los recursos TIC y que garanticen la continuidad de las operaciones de la organización al tiempo que se administra ese riesgo informático?
3. ¿Cuál es la importancia de contar con una estructura organizativa dentro del departamento de informática que se encargue de velar por las políticas de seguridad informática?

V. DISEÑO METODOLÓGICO

5.1 Área de estudio

El área de estudio de esta investigación fue la Bluefields Indian and Caribbean University (BICU), en su recinto Bluefields de la Región Autónoma Costa Caribe Sur de Nicaragua.

5.2Tipo de estudio

La presente investigación tuvo un enfoque mixto, puesto que fue el que mejor se adaptó a las características y necesidades del trabajo, de este enfoque se tomó la técnica de la entrevista para describir políticas de seguridad informática necesarias para minimizar los riesgos sobre los recursos TIC, así como una encuesta para la opinión de la población de estudio en cuanto a la necesidad de políticas de seguridad formalmente establecidas para la institución.

El tipo de estudio aplicado fue descriptivo ya que se desarrollaron políticas de seguridad informática necesarias y de corte transversal debido a que se apuntó a un tiempo definido y se aplicó solo una vez, este trabajo investigativo fue de campo.

5.3 Población

La población estuvo conformada por todo el personal que está directamente relacionado con los temas de informática, tanto a nivel formativo como administrativo. De este modo, para la población se tomó en cuenta al personal del Departamento de Informática y la Escuela de Informática. En total, fueron 18 individuos.

5.4 Muestra

Dado que la población de estudio correspondió a un número pequeño y manejable de individuos, la muestra para esta investigación estuvo conformada por el total de la población, la cual corresponde a 18 trabajadores, compuesta por trabajadores administrativos, pasantes y monitores, los cuales están distribuidos en el departamento y escuela de informática.

El detalle de la muestra y distribución de la misma, se presenta en la **Tabla 1**, la cual se comparte a continuación.

Tabla 1: Muestra

Trabajadores permanentes	
Descripción	Cantidad
Directores de áreas	2
Redes	1
Escuela de informática	1
Sistemas	4
Soporte técnico	1
Pasantes	
Soporte técnico	2
Redes	1
Monitores	
Laboratorios de informática	6
Total	18

5.5 Tipo de Muestreo y muestra

Para la elaboración de la investigación el tipo de muestra fue no probabilístico con un muestreo por conveniencia, debido a que la población era pequeña y de fácil acceso para aplicar los instrumentos a los involucrados. De esta forma, se logró garantizar que toda la información brindada fuera confiable para efectos de análisis de los resultados, tomando en cuenta los siguientes criterios:

- Criterios de inclusión: Se incluyeron una parte de los trabajadores de la Universidad BICU específicamente del área y escuela de informática, pasantes de las diferentes áreas de informática y monitores de los laboratorios de informática porque ello son la población que más se relaciona con la seguridad informática.
- Criterios de exclusión: Se excluyeron a los demás trabajadores y pasantes de áreas no relacionadas estrechamente a la informática.

Se exceptuó autoridades (rectoría) debido a que estás no están estrechamente relacionadas a la temática en estudio y, de igual modo, al resto de población debido a que estos solo tendrían que cumplir con las disposiciones expresadas en las Políticas de Seguridad establecidas.

5.6 Técnicas e instrumentos de recolección de información

Para la obtención de datos que sirvieron como base de información se aplicó una entrevista y una encuesta a través de contacto directo e indirecto con los individuos en estudio que permitió recopilar de manera precisa y sistemática los datos de interés para esta investigación

-Entrevista a jefes de área y personal permanente del Departamento de Informática, Escuela de Informática y Redes del recinto d BICU en Bluefields.

-Encuesta a personal permanente de Sistemas, Soporte Técnico, monitores de laboratorios de informática y pasantes de Soporte Técnico y Redes

5.7 Fuentes de información

- **Primaria:** La constituyeron los individuos que forman parte del estudio mediante los instrumentos aplicados en esta investigación.
- **Secundaria:** Fue la información obtenida de libros, protocolos, y monografías académicas de las cuales se revisaron a detalle para poder obtener información que resulte de interés para el presente estudio. Y las fuentes de interés consultadas en sitios web.

5.8 Procesamiento de la información

El levantamiento y creación de textos, elaboración del protocolo e informe investigativo, fue elaborado de manera digital a través Microsoft Office Word 2016; la tabulación de los datos se realizó a través de matrices, para luego realizar el procesamiento y el análisis de los datos en el programa Microsoft Office Excel 2016 y para la presentación final del trabajo investigativo se utilizó Microsoft Office PowerPoint 2016.

5.9 Aspecto técnico

Se solicitó el permiso correspondiente al jefe del departamento de informática para dicha investigación de igual forma se solicitó el permiso a monitores, trabajadores permanentes y pasantes. De igual forma se les informo que los resultados de este estudio solo servirán para efectos de esta investigación.

5.10 Operacionalización de las variables

Tabla 2 Operalización de las variables

Objetivos Específicos	Variable	Definición	Indicador	Técnica	Destinatario
Identificar las amenazas y vulnerabilidades de los datos e información de la universidad para la formulación pertinente de políticas de seguridad informática que contribuyan al buen funcionamiento de la institución.	Vulnerabilidades	Una vulnerabilidad (en términos de informática) es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible.	Registro de actividades de terceros Control de personal que accede a los equipos	Encuesta Entrevista	Pasantes Monitores Trabajadores

		INCIBE, (2017)			
Describir las Políticas de Seguridad Informática necesarias para minimizar los riesgos sobre los recursos TIC, garantizando la continuidad de las operaciones de la organización al tiempo que se administra ese riesgo informático	Mecanismos de seguridad informática	Un mecanismo de seguridad informática es una técnica o herramienta que se utiliza para fortalecer la confidencialidad, la integridad y/o la disponibilidad de un sistema informático. Rios, (2010)	Elaboración de políticas	Encuesta Entrevista	Pasantes Monitores Trabajadores
Proponer una estructura organizativa del departamento de informática que se encargue de	Políticas de seguridad informática	La definición de una política de seguridad debe estar basada en una identificación y análisis previo de los	Seguimiento a políticas de seguridad informática	Encuesta Entrevista	Pasantes Monitores Trabajadores

velar por las políticas de seguridad informática	riesgos a los que está expuesta la información y debe incluir todos los procesos, sistemas y personal de la organización. Además, tiene que haber sido aprobada por la dirección de la organización y comunicada a todo el personal. Unir, (2020)

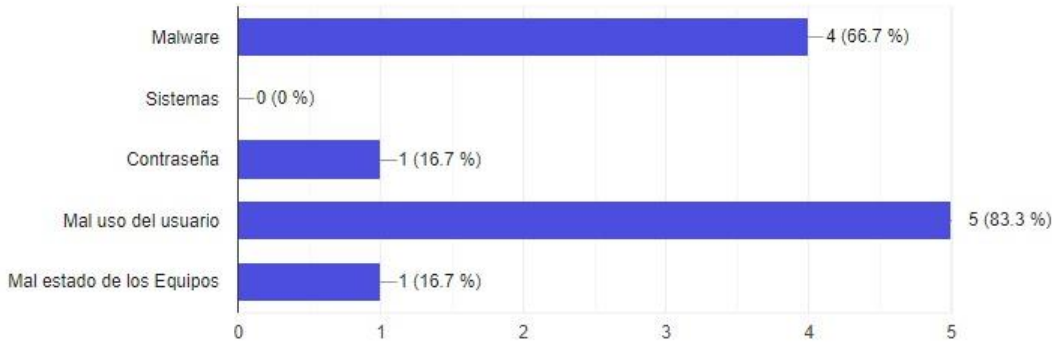
VI. RESULTADOS Y DISCUSIONES

Los resultados que se presentan a continuación son el producto obtenido mediante la aplicación de los instrumentos de investigación seleccionados para el presente trabajo monográfico. La aplicación de estos instrumentos se realizó entre enero y marzo del 2022. Los datos obtenidos permitieron diseñar los gráficos necesarios para representar los resultados.

Los resultados se presentan en relación al orden de los objetivos específicos elaborados para la investigación. Posterior a ello, se realiza la debida interpretación de los mismos.

6.1 Identificación de las amenazas y vulnerabilidades de la seguridad de los datos e información de la universidad

Gráfico 1. Amenazas y vulnerabilidades de los datos e información detectadas en la universidad



Encuesta aplicada por Jenifer Hurtado y Cesar Ocampo, marzo 2022

- En orden de porcentaje la mayoría de los encuestados resaltan que el mal uso de los usuarios (83.3%) representa una seria amenaza para los equipos, ya que no se respetan los reglamentos relacionados a los recursos TICS o hacen caso omiso de estos, un ejemplo claro de esto es el hecho de que, aunque exista un reglamento en los laboratorios de informática en donde se especifica claramente que no se deben ingresar alimentos y bebidas no es siempre respetado lo que provoca un deterior a largo o corto plazo de los dispositivos.

  Otro ejemplo puede ser la eliminación de archivos necesarios para el equipo. Muchos estudiantes, trabajadores, docentes piensan que por haber leído trucos sobre computadoras

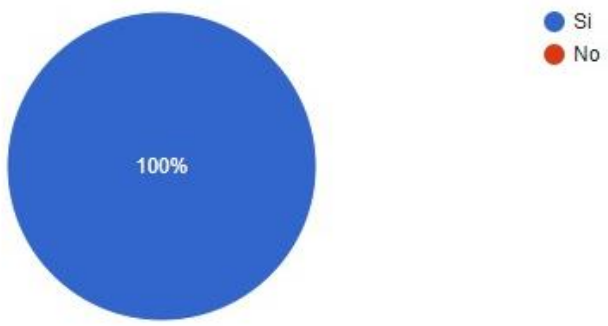
son unos técnicos en informática y cuando el dispositivo se está quedando sin almacenamiento empiezan a borrar todo lo posible y eliminan archivos vitales y en vez de ahorrarles trabajo a trabajadores, monitores y pasantes se lo duplican.

- De igual modo tenemos a los malware (66.7%) que son la consecuencia de un uso incorrecto que se le da a la tecnología, pueden generar muchos daños como perdida de información, robo de datos, errores de hardware, redes computacionales de sistemas inutilizables, los malware surgen en muchos casos por acceder a páginas web no recomendables e inseguras.
- Las malas contraseñas (16.7%) convierten a los usuarios más vulnerables a hackeos, robos, modificación de información, las contraseñas son intransferibles y no deben estar relacionadas a datos personales.
- Si bien el mal estado de los equipos (16.7%) está bastante relacionado con el intento de alargar exageradamente la vida útil de los equipos, también esta vinculado al trato que se le da

El mal uso que el usuario le da a los recursos tics del recinto es la amenaza que tiene mayor impacto porque es la que está relacionada a todas las demás vulnerabilidades y amenazas, los malware en los equipos surgen como consecuencia de que el usuario accediera paginas inseguras que representan una amenaza a la integridad de los datos, de las redes y hardware. Las contraseñas son vulnerables por razones como que el usuario tiene pereza de escribir contraseñas largas y complejas, se le olvidan o transfieren esa información privada a terceros. El mal estado del equipo si bien está relacionado a la antigüedad de los dispositivos también está conectado al trato que se le da.

Así también se evaluó si los encuestados manejaban herramientas para facilitar la protección física y lógica de los equipos informáticos.

Gráfico 2. Conocimiento de la población de estudio sobre herramientas que faciliten la protección física y lógico de equipos informáticos



Encuesta aplicada por Jenifer Hurtado y Cesar Ocampo, marzo 2022

Según estos resultados todos y cada uno de los encuestados conocen de herramientas que ayudan en la protección de su información por herramientas que facilitan la seguridad física y lógica se entiende planes de contingencia, controles de acceso a programas y archivos, respaldos.

También se analizó si la población de estudio ha sufrido o sufrió pérdidas de información o fue víctima de algún delito informático**,** los casos más claros son intentos de hacking a los servicios de puntos locales y de afuera, también porque la mayoría de los equipos son crackeados o mejor dicho que en la universidad no se compran licencia para el equipamiento y ha habido varios casos de perdidas por no poseer licencias activadas y no tener antivirus, lo que representa una vulnerabilidad para los sistemas operativos. Una particularidad interesante es la falta de comunicación entre áreas, las áreas más relacionadas con la informática si conocían de diferentes casos de delitos informáticos en el recinto y la parte menos relacionada a la informática no, esto puede ocurrir por razones como la falta de comunicación como ya se mencionaba, el poco interés a temas no relacionado a sus áreas por parte del personal.

Gráfico 3. Casos de perdida de información por ataques de virus o dispositivos dañados

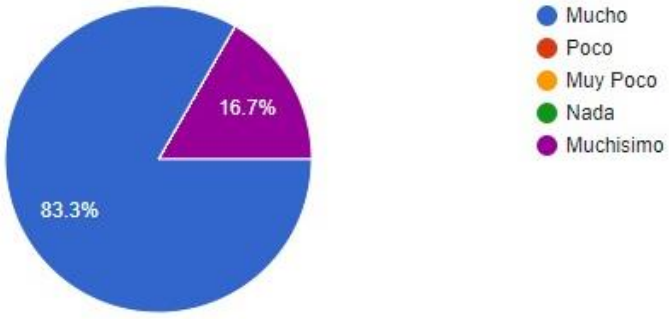
Encuesta aplicada por Jenifer Hurtado y Cesar Ocampo, marzo 2022

Como podemos observar en esta grafica el 50% de las personas encuestadas en algún momento ha perdido y talvez nunca recuperó la información gracias a un virus o daños físicos que han sufrido en equipos. Existe una gran probabilidad de que esto pueda deberse al desconocimiento de las políticas de seguridad que existen en la institución o deberse a la falta de capacitación acerca de normas o directivas de seguridad informática con las que se puedan prevenir estas pérdidas y un 50% de los individuos nunca han tenido este problema o inconveniente pero no cuentan con la garantía que no les pasara en un futuro ya que la mayoría de ellos desconocen el hecho de saber si hay o no políticas de seguridad informática que los ayude a seguir los lineamientos adecuados para evitar a largo plazo una pérdida de información.

6.2 Políticas de Seguridad Informática necesarias para minimizar los riesgos sobre los recursos TIC.

Para poder desarrollar políticas de seguridad se encuestó y entrevistó a la población. En primera instancia se evaluó que importancia tiene la seguridad informática en la institución para los individuos.

Gráfico 4. Importancia de la seguridad informática en la institución.



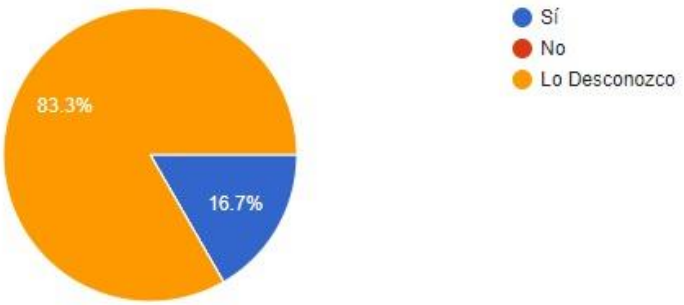
Encuesta aplicada por Jenifer Hurtado y Cesar Ocampo, marzo 2022

Los datos presentados en esta gráfica, acerca de cuán importante es la seguridad informática para una institución revela que el 83.3 % considera que la seguridad informática es muy importante y el 16.7% lo considera un pilar fundamental.

En este caso la población encuestada está de acuerdo en que la seguridad informática es vital para la institución con el fin de prevenir todo tipo de amenazas y vulnerabilidades y en caso de que los recursos TICS fueran víctimas de alguna falla de seguridad informática lógica o física se pueden seguir los lineamientos correctos para dar una solución de forma eficaz.

También se examinó el conocimiento de los encuestados sobre si la universidad contaba con políticas de seguridad.

Gráfico 5. Conocimiento respecto a si la universidad cuenta con políticas de seguridad



Encuesta aplicada por Jenifer Hurtado y Cesar Ocampo, marzo 2022

Según los resultados obtenidos un 83.3% desconoce si en su ambiente laboral cuentan con políticas de seguridad lo cual no está muy alejado de las realidad porque aunque en el recinto se sigan normas de seguridad no hay nada formal y un pequeño grupo del 16.7 % si tiene conocimiento de que hay políticas de seguridad informática considerando que el personal que está más relacionado es el de soporte técnico, resaltando así que no todos los involucrados tienen acceso o conocen en verdad acerca de que si cuentan con políticas de seguridad. Aunque se sigan lineamientos para garantizar la seguridad de sus recursos, no existe un documento formal donde se detallen.

En el caso de la población entrevistada hubo una particularidad interesante la mayoría de los entrevistados se centraban más en la seguridad lógica, navegación, software, redes y dejaban de lado la seguridad física; también se pudo observar que toda la responsabilidad cae sobre una sola persona, y aunque hay opciones de respuestas preventivo para la seguridad de los sistemas, como el accesos no autorizados a aplicaciones que llevan malware , configuraciones de equipos VLAN, y mantenimiento, respaldo y topología de red. No hay nada aprobado, a través de las opiniones de los entrevistados y encuestados se resaltó la necesidad de una política que sea del conocimiento autorizado y aprobada por las autoridades pertinentes de la universidad.

Se valoró la importancia de contar con políticas de seguridad, los resultados obtenidos fueron los posteriores:

Gráfico 6. La importancia de que la universidad disponga de una serie de pasos y reglas para implementar la seguridad informática

Encuesta aplicada por Jenifer Hurtado y Cesar Ocampo, marzo 2022

Los resultados indican una clara preocupación de los individuos para que se cuente en la universidad BICU con políticas de seguridad informática que garanticen en todo momento la correcta utilización de los recursos físicos y lógicos, también en casos de emergencia se seguirían normativas que resguarden la información y sean utilizadas las herramientas de protección que ya muchos conocen, de esta forma aprovechar el conocimiento previo que poseen como una base para agilizar la reducción de los riesgos a lo cual se expone la información.

Según el 100% de los entrevistados resalta que es altamente importante **que la universidad cuente con Políticas de Seguridad Informática,** por diferentes razones que la hacen valida, para resguardar la información evitar hackeos en los sistemas de inventarios, académicos, contables así evitando el robo de información y el fraude. También para regular los accesos a los canales adecuados para el acceso a la información, y darle una garantía a los encargados de sistemas de cómo proceder ante X situaciones, cabe resaltar que la mayoría de los entrevistados en este punto se centraron únicamente en la parte lógica de la seguridad informática y dejaron de lado la seguridad física esto puede ocurrir por diversas razones, que el área en el que están no está muy relacionado a la seguridad física o que le prestan poca importancia a ella .

También consultamos con la población que temas/ áreas/ puntos deberían ser garantizados dentro de las políticas de seguridad.

Toda la población entrevistada está de acuerdo en que todos los puntos deben ser garantizados en una política de seguridad, pero especificándose más nos dicen que todo servicio que esté disponible en la red, todo lo que este anclado bajo el dominio.bicu.edu.ni,, también que cualquier aplicación o software que se esté haciendo o exista en la universidad para que agentes externos no puedan acceder, como se puede analizar de nuevo se muestra poco interés por la seguridad física de los equipos en el recinto, aunque ambas deberían ir de la mano para así garantizar un servicio de calidad a los usuarios de la universidad.

Gráfico 7. Seguridad física o lógica ¿cuál trabajar a lo inmediato?

Encuesta aplicada por Jenifer Hurtado y Cesar Ocampo, marzo 2022

Ocurre algo interesante en las encuestas ya que la población considera que se deben de desarrollar políticas de seguridad tanto la parte física sin descuidar también la parte lógica ambas partes deben ser trabajadas por igual buscando de esta manera maximizar la seguridad en la institución minimizando los peligros que cada día se debe de enfrentar.

Los resultados obtenidos de los encuestados y entrevistados fueron fundamentales para el desarrollo de las políticas de seguridad informática ya que en ellos se brindó información sobre qué temas, puntos áreas trabajar, y que tan importante seria.

6.2.1 Políticas de seguridad

De acuerdo a los datos e información obtenida por la población se describieron políticas de seguridad informática que garantizaran la continuidad de las operaciones de la organización al tiempo que se administra el riesgo informático.

La revisión de la documentación, los datos recopilados en el recinto y la metodología encontrada para el desarrollo de políticas, fue el punto de partid permitieron para la elaboración de políticas de seguridad informática que logren salvaguardar los bienes físicos y lógicos de la institución.

Las presente Políticas de Seguridad de la Información, tiene como objetivo fundamental instaurar el marco operativo para la seguridad de los datos y activos en la Universidad BICU. Dichas normativas serán de vigilancia constante para todos los relacionados en el funcionamiento de los activos, en donde se engloban todos los recursos de la institución que representan un costo y que

además son vitales para la continuidad de las operaciones de la misma, de igual forma para todos los individuos que formen parte de la comunidad académica y que hagan uso de recursos TIC.

6.2.1.1 Políticas de Seguridad Física y de los espacios

Con el fin de garantizar la integridad de todos los activos físicos y de los espacios ante fenómenos naturales (inundaciones, tormentas, terremotos) o daños humanos (sabotajes, actos vandálicos o involuntarios) se presentan las siguientes Políticas de Seguridad Informática.

A. Áreas Resguardadas

1. Todas las oficinas o áreas que son reconocidas como zonas restringidas en la cual se maneja información sensible de la universidad y en las cuales hay recursos Tics del recinto (Laboratorios informáticos) deben ser resguardadas contra el acceso no autorizado, utilizando herramientas tecnológicas o un control de ingresos en formatos previamente definidos por cada área u oficina.
2. Todos los trabajadores, pasantes o estudiantes que tengan acceso a los lugares donde se encuentran los sistemas de información o equipos informáticos deben llevar su carnet de estudiante o identificación de trabajador obligatoriamente visible.
3. Todo individuo que ingrese a zonas restringidas debe registrase obligatoriamente y detallar la hora de entrada, hora de salida y el detalla de su visita.
4. Los trabajadores y estudiantes no deben consumir líquidos dentro de los centros de cómputos o zonas restringidas de la universidad.
5. La universidad debe contar con extintores de incendio en los lugares donde existan equipos, se procese información, debido a que se debe contar con la capacidad de mitigar los daños que pueden ser causados por un posible incendio.
6. Los suministros de papelería deben estar ubicados a una distancia considerable de los equipos en donde se procesa y almacena información para evitar daños en estos.

B. Seguridad de los equipos

1. Todos los equipos informáticos que proveen información a la universidad como centro de datos, servidores, equipos de área de sistemas deben tener energía eléctrica sin interrupciones.

2. Realizar mantenimientos periódicos del cableado estructurado de la universidad para prevenir daños en el ambiente o robo o intercepción de datos.
3. El cableado estructurado debe estar codificado de forma clara, para que así sea más fácil identificar la estructura de conexión entre los sitios de la universidad.
4. Llevar registros del mantenimiento preventivo y correctivo de los equipos de cómputo en el recinto.
5. Realizar planificaciones anualmente de mantenimiento de equipos en toda la universidad, también deben ser en horarios que no afecte el funcionamiento operativo del personal
6. Queda terminantemente prohibido mover, instalar, reubicar los equipos y retirar los sellos de seguridad de todos los aparatos.
7. Al terminar la jornada laboral de los recursos informáticos, el usuario tiene la responsabilidad de apagar equipos informáticos.
8. Los equipos no deben estar en el piso para evitar daños provocado por el polvo, cortocircuitos o desastres ambientales como inundaciones
9. Instalar cámaras de vigilancia en áreas sensibles (acceso a servidores, laboratorios de informática).
10. Implementación de los certificados de seguridad SSL / TLS en todas las tecnologías de información de la universidad.

6.2.1.2 Políticas de respaldo de la información

Con el objetivo de tener un plan de contingencia en caso de daños o pérdidas de información, se exponen las siguientes medidas:

1- Definir los tipos de dispositivos que servirán como herramientas para las copias de seguridad, ejemplos discos duros externos, en la nube, cintas magnéticas y demás.
2- Tener registros de los respaldos de datos que se han realizado detallados fecha de inicio y el contenido de los respaldos.
3- Al momento de crear los respaldos de información se debe garantizar que el equipo esté conectado a un SAI (Sistema de Alimentación Ininterrumpida) para disponer de tiempo extra.
4- Las copias de seguridad se deben guardar fuera del recinto por casos como problemas ambientales, incendios, robos etc. El área donde se resguarde las copias de seguridad debe tener las condiciones necesarias para afrontar las condiciones que se le puedan presentar.

5- Los dispositivos de respaldo deben estar correctamente etiquetados con sus contenidos y el nivel de seguridad.
6- Se deben garantizar los backups automatizados (en tareas programadas de Windows) diariamente.
7- Las copias de seguridad de la información deben ser resguardadas en unidades de almacenamiento en discos duros extraíbles en buen estado.
8- Cuando las unidades de almacenamiento extraíble se encuentren en mal estado se realizará un proceso de eliminación de forma segura y luego dar de baja esos activos.

6.2.1.3 Políticas de control de acceso.

Con la finalidad de impedir el acceso no autorizado a la información se deben tomar en cuenta las siguientes normas, para un mejor control de los accesos, sistemas datos y los servicios de información.

A. Requerimientos para controlar accesos

1. Se debe proporcionar manuales de usuarios para la correcta utilización y manejo de sistemas que brinda el área de sistemas hacia las demás áreas.
2. Se debe obligar a los empleados a cambiar las claves que son de carácter temporal la primera vez que acceden a un sistema asignado.
3. No mostrar contraseñas en pantalla cuando se está ingresando a los sistemas.
4. Utilizar contraseñas seguras, las cuales deben cumplir los siguientes requisitos.
   Mínimo 8 caracteres, máximo 16.
   Usar letras mayúsculas.
   Usar caracteres especiales.
   Usar números.
5. Las contraseñas deben ser cambiadas en periodos establecidos de tiempo.
6. No se deben utilizar contraseñas relacionadas con fechas de nacimiento, nombres, apellidos o fechas de matrimonio.
7. No se deben proporcionar las contraseñas a nadie.

B. **Gestión de accesos de usuarios**.

1. Se debe informar de forma inmediata la baja de algún empleado para procesos de inactivación de usuarios en los sistemas de información.
2. Se debe mantener y establecer mecanismos de accesos físicos y lógicos para los usuarios que accedan a los sistemas informáticos.
3. La asignación de privilegios a usuarios en los sistemas informáticos se realizará con una previa autorización del jefe correspondiente., con un documento firmado o un correo de autorización
4. Se debe revocar inmediatamente los privilegios de los usuarios que cambiaron de puesto con las respectivas obligaciones, también se revoca los accesos a usuarios que fueron autorizados por la universidad.

C. Responsabilidades de los usuarios

1. Ningún usuario debe permitir que se accedan a los sistemas y aplicaciones informáticas de la universidad utilizando las credenciales de terceros. Para esto, se sugiere utilizar el servicio de verificación de dos pasos mediante el uso del teléfono celular del propietario de la cuenta con lector de huellas o facial, de esta forma habrá un control más eficiente en el acceso a las cuentas.
2. Los usuarios son los únicos responsables de todas las actividades y procesos realizados con sus cuentas y contraseñas.
3. Las contraseñas, claves de acceso a las cuentas de los usuarios no deben ni pueden ser almacenados en dispositivos que no estén cifrados, tampoco deben ser guardados o escritos en lugares de fácil acceso como por ejemplo escritorios, cuadernos monitores.
4. Los usuarios tienen la obligación inmediata de informa sobre daños, fallas o amenazas detectadas en las aplicaciones y equipos informáticos.
5. El departamento de informática y sus demás instancias no responden sobre el mal uso que se les dé a las cuentas de correos electrónicos que son otorgadas a usuarios.
6. Las cuentas de estudiantes o personal que termine una relación con la universidad deben ser desactivadas de forma inmediata.

D. Control de accesos para sistemas y aplicaciones

1. Se deben restringir los accesos a los sistemas y que los usuarios solamente tengan acceso únicamente a la información que está relacionada con sus tareas para cumplir las actividades que tiene a cargo.
2. Absolutamente todos los dispositivos de cómputo que tengan acceso a los sistemas de información, base de datos, reportes, etc., deben contar con mecanismos de autenticación y privilegios de usuario convenientes, que dependan del tipo de información que manipula el usuario.
3. Todas las contraseñas que vengan por defecto en servidores, base de datos sistemas informáticos, aplicaciones, Routers, Switch, Acces Point deben de cambiarse antes de su utilización.
4. El departamento de informática de la Universidad BICU será el encargado de generar usuarios y contraseñas, el primer acceso se realizará con los datos otorgados por el departamento luego los usuarios se encargarán de efectuar un cambio en estos datos.
5. Los usuarios podrán cambiar sus contraseñas cuando consideren necesario o cuando se le exija hacerlo.

6.2.1.4 Políticas de seguridad en las telecomunicaciones

La seguridad en las telecomunicaciones es fundamental cuando se manejan datos confidenciales de personas o información interna, el no contar con dichas políticas pone en riesgo información ya que puede ser robada, manipulada o interceptada por terceros, por las razones expuestas anteriormente se plantean las siguientes pautas con el fin de garantizar seguridad y privacidad en las telecomunicaciones

1. El departamento de informática es el único encargado de los permisos y administración de los accesos de los usuarios que necesiten ingresar a la red, siempre y cuando estos permisos sean autorizados para el personal a cargo y se para fines académicos o laborales.
2. Los usuarios que fueron autorizados por el personal encargado deberán acercarse al departamento de Informática con su equipo para el registro de MAC y asignación de ip estática.
3. El departamento de informática debe implementar herramientas para gestionar y monitorear permanentemente la red de datos de toda la universidad.

4. El control de acceso a la red de datos de la Universidad se realizará cuando se detecte que el usuario está navegando en páginas con contenido pornográfico, comunidades de hackers o está accediendo a datos no autorizados de la institución.
5. Establecer los acuerdos de niveles de servicios cuando sea requerido contratar servicios de terceros.
6. Mantener una bitácora de respaldo (backups) de las configuraciones de routers, firewall, switch de core y otros dispositivos de red, de manera mensual o cuando se ejecuten cambios significativos.
7. La red se debe mantener segmentada dependiendo de los grupos como personal, estudiantes, red de enlaces y ubicación geográfica.
8. Se debe establecer cláusulas en los contratos:
    - Acuerdos de confidencialidad.
    - Acuerdos de intercambio de información.
    - Acuerdos de divulgación para evitar problemas relacionados con la información.

6.2.1.5 Políticas de adquisición mantenimiento y desarrollo de sistemas de información.

Estas medidas se implementan para integrar seguridad a los sistemas de información (propios o de terceros) y a las actualizaciones que se le agreguen.

A. Requerimientos de seguridad de los sistemas de información

1. Es obligatorio implementar controles de seguridad antes, durante y después de la implementación o mantenimientos de sistemas de información.
2. Todo sistema, software o aplicación que se instale en las computadoras de la universidad deberá contar con su respectiva licencia y la instalación debe ser realizada por personal del departamento de informática.
3. Queda terminantemente prohibido que los usuarios realicen instalación de cualquier tipo en las computadoras del recinto, en el caso de que necesite algún software se deberá hablar con el personal del departamento Informática o en los casos de los laboratorios. de informática con los monitores.

B. Seguridad en los procesos de desarrollo y soporte

1. El departamento de informática está en la obligación de velar por el desarrollo de sistemas informáticos que cumplan con los requisitos de seguridad y buenas prácticas en el desarrollo como las que se mencionara a continuación:
2. Metodologías para realizar pruebas de certificación y seguridad a los softwares desarrollados.
3. El departamento de Informática es el único autorizado para realizar copias de seguridad de códigos fuentes.
4. Debe haber áreas de desarrollo, certificación y control de las versiones para posterior actualización en producción.
5. Los cambios en los sistemas y aplicaciones informáticos desarrollados por el departamento de informática deben ser requeridos bajo solicitudes formales.
6. Se deberán poner a prueba los nuevos desarrollos y las áreas que solicitaron deben certificar con documentos formales.

6.2.1.6 Políticas para el manejo de incidentes en la seguridad de la información

La finalidad de las políticas para el manejo de incidentes en la seguridad de la información es garantizar una respuesta rápida eficaz y de forma sistemática a los incidentes relacionados a la seguridad.

1. Todos los trabajadores, estudiantes de la universidad tienen la obligación de reportar eventos en donde se ha puesto en peligro la seguridad de la información que observe en las distintas áreas del recinto y también debe informar fallas en los sistemas informáticos.
2. Se debe asignar personal que sea encargado de investigar bajo los lineamientos adecuados los incidentes de seguridad que se hayan reportado y brindar una respectiva solución.

6.2.1.7 Políticas de capacitación

Capacitar a los recursos humanos es importante para optimizar el uso de los recursos TIC. El desarrollo de programas de capacitación contribuye significativamente a la optimalización de los procesos y mejor utilización de los recursos.

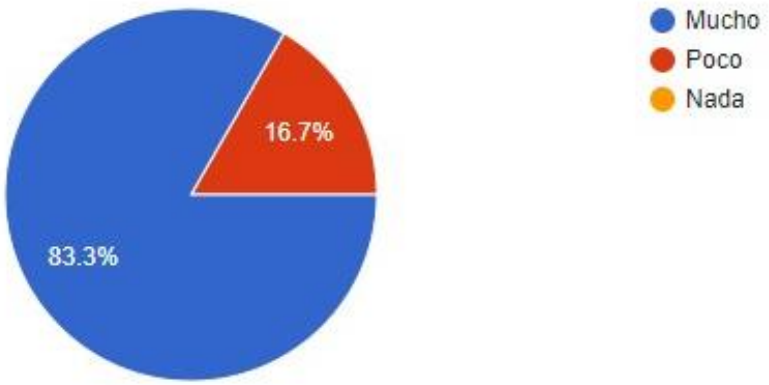
1. Organizar y aplicar de manera constante programas de capacitación dirigidos al personal informático, en base a las necesidades reales que existan para que de esta forma estén actualizados con las nuevas tecnologías.

2. El jefe encargado de cada área es el responsable directo de definir las necesidades de capacitación en TICS del área que está bajo su resguardo para alcanzar los objetivos y metas planteados.
3. El departamento de informática debe crear, mantener, actualizar y ejecutar planes de capacitación para todos los usuarios que utilicen los recursos TICS como el manejo de sistemas de información, seguridad y office.
4. Los programas de capacitación deben tener claramente establecido el contenido de temas, horas, materiales, y documentación, después de los programas se deben realizar evaluaciones.
5. Realizar cronogramas de actividades para las capacitaciones y cumplirlos al pie de la letra.
6. Ejecutar investigaciones y revisiones de las necesidades de capacitación del personal en todas las áreas del recinto con la finalidad de establecer escala de prioridades.

6.3 Propuesta de estructura organizativa del departamento de informática que se encargue de velar por las políticas de seguridad informática.

Para el debido desarrollo de una nueva estructura del departamento de informática se comenzó evaluando la familiarización de los encuestados con la frase Políticas de seguridad Informática, los resultados obtenidos fueron los siguientes:

Gráfico 8. Familiarización con la frase Políticas de Seguridad Informática

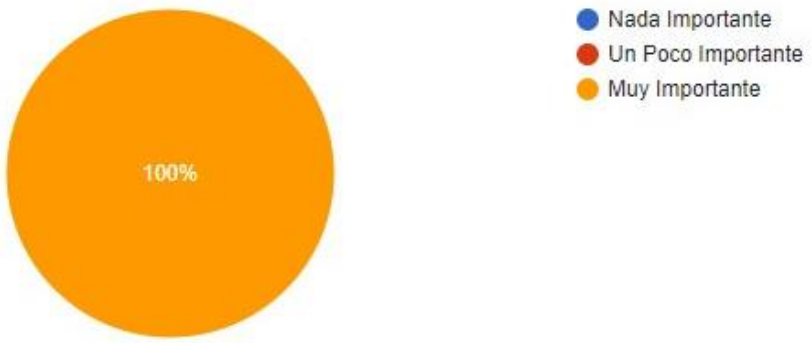


Encuesta aplicada por Jenifer Hurtado y Cesar Ocampo, marzo 2022

Los resultados presentados en el gráfico permiten establecer un acercamiento significativo al conocimiento que tienen los encuestados con el significado de Políticas de Seguridad Informática. El hecho de que la mayoría de ellos, 83.3%, exprese estar familiarizado con este concepto, permite decir que se cuenta con personal altamente calificado o, al menos informado, sobre la base teórica de esta temática. Esto es algo valioso para la institución, pues indica que hay personal con los conocimientos necesarios para asegurar la integridad de todos los componentes informáticos de la universidad. Sin embargo, es importante que este conocimiento sea transferido a todo el personal, pues, aunque es un porcentaje pequeño, 16.7%, es importante que todos los involucrados tengan la información y las herramientas para garantizar el correcto funcionamiento de todo el sistema informático de la universidad.

Después se consultó con los encuestados la importancia de que la comunidad académica sea educada en temas de seguridad.

Gráfico 9. La importancia de educar a la comunidad académica en temas de seguridad informática



Encuesta aplicada por Jenifer Hurtado y Cesar Ocampo, marzo 2022

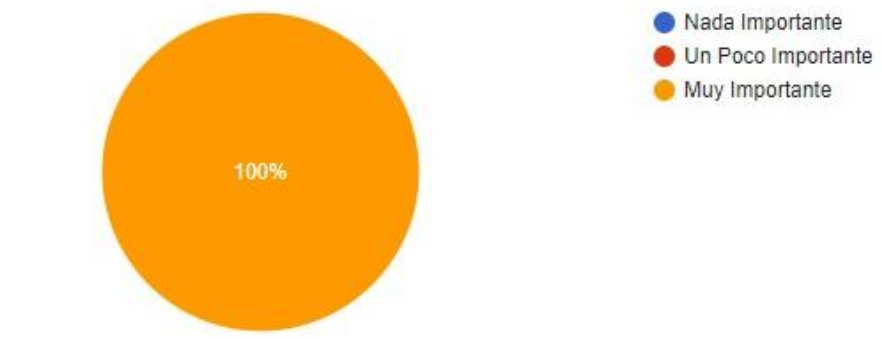
La comunidad académica juega un papel fundamental dentro del recinto, docentes, trabajadores de planta, estudiantes, todos deben ser educados sobre la políticas de seguridad para que así ellos por su propia cuenta puedan garantizar el buen funcionamiento físico y lógico de los equipos, en los gráficos anteriores se pudo evidenciar que el 100% de los encuestados conocen herramientas de seguridad informática pero que no todos saben si se implementa estas herramientas, de tal forma que se debe instar a cada departamento de esta organización a que adopten medidas de seguridad

que son beneficiosas para ellos mismo y para garantizar la confidencial e integridad de datos y el buen estado de los recursos tecnológicos.

Al consultarles sobre la aprobación de una Política de Seguridad Informática y que si consideraban necesario capacitar al personal, los entrevistados opinaron que no se debe capacitar a todo el personal, sino que hay que enfocarse en el personal de primera línea, trabajadores que tienen contacto directo con los sistemas, redes, recursos TIC, aquellos que modifican, actualizan y dan mantenimiento, pero también coinciden en que se debe informar a los trabajadores del recinto que tienen contacto con computadoras y necesitan conocer acerca de las políticas y como proceden para no estar en la ignorancia.

En relación a la existencia en el recinto de alguna comisión o personal encargado de velar por la seguridad informática de la universidad, los entrevistados respondieron que no existe una comisión o persona como tal, pero si~~n~~ concordaron en que esta responsabilidad se delega a una sola área en específico, en este caso, el área de redes. Contrario a esto, los encuestados desconocen los procedimientos y como se administra los procesos de seguridad y es agobiante que todas las responsabilidades recaigan sobre un solo individuo.

Gráfico 10. La importancia de una comisión que vele por mantener la seguridad informática en el recinto



Encuesta aplicada por Jenifer Hurtado y Cesar Ocampo, marzo 2022

Según la opinión de los encuestados reflejada en este grafico podemos darnos cuenta del deseo y preocupación que existe en la universidad para que este protegida y que cuente lo antes posible con parámetros de seguridad que ayuden al desarrollo y seguridad de la universidad y que lo antes posible cuente con procesos de contingencia para su debida implementación en casos inesperados o de emergencia.

Aunque se pudo confirmar que los trabajadores del recinto hacen una excelente labor por mantener protegidos los recursos de la institución, que todas las responsabilidades recaigan sobre 2 0 3 individuos es agotador por lo cual se puede deducir que una comisión que vele por el buen funcionamiento y seguridad de los recursos es imprescindible.

6.3.1Estructura del departamento de informática

Se propuso una nueva estructura del departamento de informática que diera soluciones a las necesidades expresadas por los encuestados y entrevistados.

6.3.1.1 Situación actual

Actualmente en la Bluefields Indian & Caribbean University (BICU) la gestión de seguridad en la información se encuentra principalmente en el departamento de informática, dividida entre las áreas de soporte técnico, el área de redes y el área de sistemas. Las labores de seguridad son realizadas según la acción a realizar por cada una de las unidades de acuerdo a las características de las mismas. Las acciones por unidad se detallan a continuación.

Soporte Técnico

- Mantenimiento y reparación de Hardware.
- Instalación de sistemas operativos y aplicaciones de escritorio.
- Respaldo de Información.
- Instalación de equipos Tecnológicos.

Área de Redes

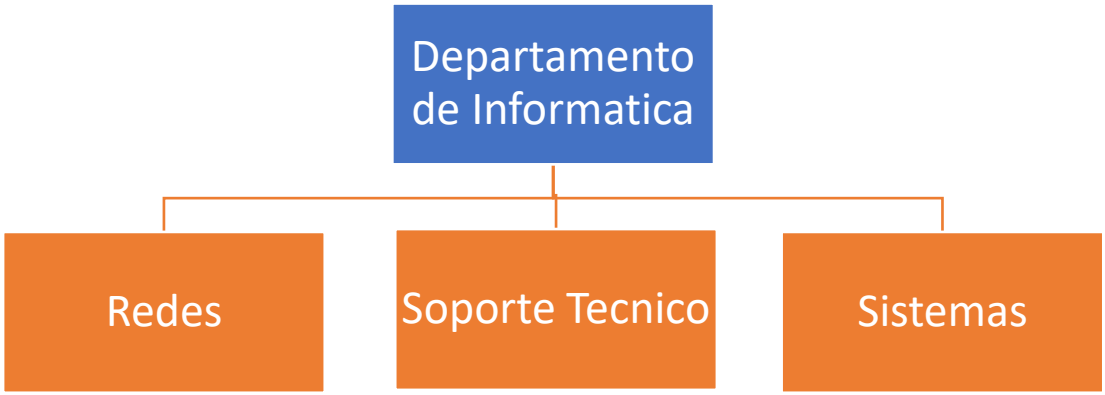
- Control de red.
- Creación y eliminación de usuarios.
- Administración del firewall.
- Administración de accesos a servidores.

Equipo de Sistemas

- Desarrollo de Sistemas de información conforme las necesidades de la universidad.
- Administración de los sistemas de información de la universidad.
-Soporte Técnico a los Sistemas de información.

Las funciones de desarrollo y mantenimiento de políticas y estándares de seguridad no están definidas dentro de los roles de la institución a su vez carece de una estructura organizativa informática completa que se encargue de velar por la seguridad informática y de monitorear constantemente los procesos informáticos de la institución, no hay especialistas, que se dediquen especialmente a la seguridad informática, para el monitoreo de los servidores, no hay personal para cableado técnico, ni para la radiofrecuencia entre otras necesidades.
Se presenta a continuación la estructura actual organizativa del departamento de informática y sus divisiones.

Ilustración 2: Estructura actual



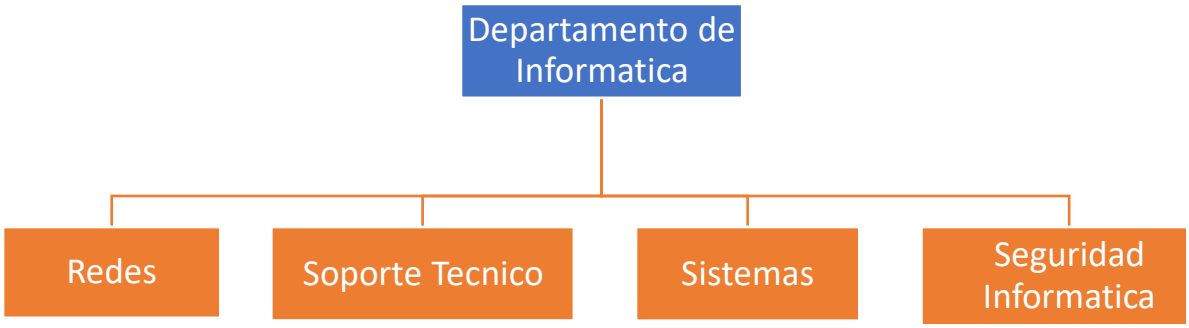
6.3.1.2 Propuesta de nueva estructura organizativa

Basados en el análisis de la información recopilada tanto de las encuestas como entrevistas se propone una nueva estructura organizacional donde se crea el Área de Seguridad Informática encargada de la administración de seguridad de información y tecnologías, dando soporte los objetivos de seguridad de información de la institución. Dentro de algunas de sus

responsabilidades se encuentran la gestión del plan de seguridad de información, así como la coordinación de esfuerzos entre el personal de sistemas, Soporte Técnico, Redes y las demás áreas de la institución, Asimismo, es responsable de promover la seguridad de información y tecnologías a lo largo de la organización.

.

Ilustración 3: Propuesta de nueva estructura



Con esta propuesta, es importante recalcar que la aprobación de la nueva estructura en el departamento de informática como producto de las políticas de seguridad informática y tecnológicas, deberán ser aprobadas por el Consejo Universitario quien es la máxima autoridad, para después ponerlas en marcha en la universidad, resaltando así que debe ser un trabajo conjunto de toda la organización donde abarque a todos sus trabajadores en todos los niveles , a los docentes, los alumnos pero principalmente el departamento de informática quien se encarga de la información y tecnología dentro de la universidad y sus recintos.

Para poner en marchar la nueva estructura organizativa del departamento de informática propuesta y con ella la implementación de las políticas de seguridad informática la institución tiene tres opciones:

1. Hacer por Consultoría el proceso de validación el cual, dentro del mercado de consultoría, tiene costo estimado de U$ 20.00 la hora.

2. Realizar una promoción laboral, tomando en cuenta los trabajadores del área, promoviendo así, una competencia sana y validando la experiencia y conocimiento de cada trabajador. En este caso,

los costos se establecerían según la tabla de planilla correspondiente y de la cual hace uso la universidad para establecer la tabla salarial.

3. En tercer lugar, está la opción de contratar a personal nuevo y fijo para la institución bajo las normas administrativas que establezca la universidad.

En todo caso, es meritorio mencionar que la universidad deberá tomar las medidas que más convengan a la institución, tomando en cuenta el costo beneficio que pueda generar cualquiera opción que se tome en cuenta.

VII. CONCLUSIONES

1. A través de una exhaustiva revisión a los procesos de seguridad de la Bluefields Indian & Caribbean University se diseñaron políticas de seguridad informática para el resguardo de los datos, información y equipos gestionados por la institución y sus diferentes instancias en el desarrollo de esta propuesta se tuvo como base los 3 principios fundamentales de la seguridad (integridad, disponibilidad y confidencialidad).
2. Las amenazas y vulnerabilidades identificadas en la universidad BICU están bastante relacionadas primeramente al mal uso que el usuario les da a los equipos no respetando reglamentos o haciendo caso omiso de ellos. También los malware que son una consecuencia muy grave del uso incorrecto de la red pueden generar muchos daños como pérdida de información, robo de datos, errores de hardware, redes computacionales de sistemas inutilizables. Las malas contraseñas convierten a los usuarios vulnerables a hackeos, robos, modificación de información, las contraseñas son intransferibles y no deben estar relacionadas a datos personales. Además, el mal estados de los equipos ya sea por su antigüedad o falta de manteamiento y cuidado.
3. Se describieron políticas de seguridad informática necesarias para minimizar los riesgos sobre los recursos TIC, dichas políticas fueron descritas en el acápite anterior. En ella se abarcan puntos fundamentas desde la seguridad física y de los espacios, respaldo de la información, control de acceso seguridad en las telecomunicaciones, en la adquisición desarrollo y mantenimiento de sistemas, manejo de incidentes y capacitaciones. Con el fin de garantizar el buen funcionamiento de la institución.
4. Se logra la presentación de una nueva estructura organizacional en donde se añade una nueva extensión que sería el área de seguridad informática, dentro de las responsabilidades de dicha área se encuentran el monitoreo de servidores, cableado estructurado radiofrecuencia además la gestión del plan de seguridad de información, así como la coordinación de esfuerzos entre el personal de Sistemas, Soporte Técnico, Redes y demás áreas de la institución, Así mismo tiene como responsabilidad promover la seguridad de información y tecnologías a lo largo de la organización e instruir a docentes y estudiantes en temas de seguridad física y lógica.

VIII. RECOMENDACIONES

Al Consejo Universitario de la Bluefields Indian and Caribbean University

→ Hacer una revisión detallada de las políticas de seguridad y la estructura del departamento de informática establecido en la presente investigación para su correspondiente aprobación e implementación en la universidad.

Al Departamento de Informática

→ Realizar seguimientos y actualizaciones anuales de las políticas de seguridad informática con la finalidad de mantener la confidencialidad, integridad y disponibilidad de la información en el recinto.

→ Hacer un plan de divulgación dentro de la universidad con la finalidad de que toda la comunidad académica se mantenga al tanto de las políticas de seguridad y puedan adoptar buenas prácticas de seguridad.

A los trabajadores, estudiantes y comunidad universitaria en general

→ Fortalecer el compromiso de resguardar los activos de la universidad respetando y acatando las políticas de seguridad, siguiendo cada uno de los lineamientos establecidos.

→ Acercarse a las unidades correspondientes cuando tengan algún problema relacionado con el uso de los recursos TIC de la institución.

A la Escuela de Informática

→ Promover en los estudiantes la realización de investigaciones relacionadas a la seguridad informática del recinto debido a que es un tema extenso que posee pocos estudios y necesita ser más analizado.

→ Fomentar en los docentes un mayor apoyo hacia los estudiantes de la carrera de Ingeniera de Sistemas para que de manera colectiva puedan realizar investigaciones relacionadas a las TIC y la ciberseguridad, así como el resguardo y protección de los equipos físicos.

IX. REFERENCIAS

Carisio, Emanuele;. (2018). Políticas de seguridad informática y su aplicación en la empresa. Obtenido de https://blog.mdcloud.es/politicas-de-seguridad-informatica-y-su-aplicacion-en-la-empresa/

Centro Nacional de respuestas a incidentes de seguridad informatica . (23 de 11 de 2020). Urugay.

CompuEducacion. (2019). Seguridad informática: ¿en qué consiste? Obtenido de https://compueducacion.mx/blog/seguridad-informatica-en-que-consiste/

Disete. (2020). QUÉ SON LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA Y POR QUÉ TU EMPRESA DEBE TENER UNA. Obtenido de https://disete.com/que-son-las-politicas-de-seguridad-informatica-y-por-que-tu-empresa-debe-tener-una/

Equipo de expertos. (2016). Conceptos sobre seguridad lógica informática. Universidad Internacional de Valencia. Recuperado el 06 de Junio de 2021, de https://www.universidadviu.com/int/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme

Equipo de expertos. (2018). ¿Qué es la seguridad informática y cómo puede ayudarme? Universidad Internacional de Valencia. Obtenido de https://www.universidadviu.com/int/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme

Figueroa, J. (15 de septiembre de 2018). *centro europeo de posgrado*. Obtenido de https://mbauruguay.uy/cuales-son-las-ventajas-de-la-seguridad-informatica/

Galeano Villa, Jorge Luis; Alzete Castañeda, Crisitan Camilo. (2013). PROTOCOLO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA LAS UNIVERSIDADES DE RISARALD. Pereira, Colombia: Univerrsidad Catolica de Pereira.

García Peña, Nidia del Socorro ; Malespín López, Jania Geomara ;. (Mayo de 2014). “Propuesta de Políticas Informáticas para el uso y aprovechamiento de los recursos TIC en las Alcaldías de Boaco. Managua, Nicaragua. Obtenido de https://ribuni.uni.edu.ni/1145/1/40017.pdf

Gomez, Vieites, A. (2006). Enciclopedia de la Seguridad Informática. 2ª Edición. España: RA-MA. Obtenido de https://www.ra-ma.es/libro/enciclopedia-de-la-seguridad-informatica-2a-edicion_48115/

Guzman, Mercado , Ruben Bernardo;. (2018). Seguridad Física de TI. Obtenido de https://www.rberny.com/2018/08/15/seguridad-fisica-de-ti/

Hungria, David. (2019). *prakmatic*. Obtenido de https://www.prakmatic.com/como-implementar-una-politica-de-seguridad-ti/

INCIBE;. (2017). Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? Obtenido de https://www.incibe.es/en/node/5224

Informaticos.co. (2021). La importancia de la seguridad informática. Obtenido de https://informaticos.co/la-importancia-de-la-seguridad-informatica/

ISOToolsExcellence;. (2017). Seguridad informática o seguridad de la información? Obtenido de https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

Leal, Mila;. (2012). Principiosde la seguridad informatica. Obtenido de https://1library.co/document/qoppn3kz-principios-de-la-seguridad-informatica-mila-leal-asir.html

Lopez, Amparo;. (2017). Seguridad informática: qué es y por qué es importante.

Machicao Mollocondo, Saulo Gustavo;. (2019). ANÁLISIS DE RIESGO Y POLÍTICAS DE SEGURIDAD DE. Puno, Peru: UNIVERSIDAD NACIONAL DEL ALTIPLANO.

Ministerio de educasion ,cultura y deporte del gobierno de españa. (12 de 07 de 2017). Recuperado el 12 de Julio de 2021, de http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestin_de_seguridad_de_la_informacin.html

Ministerio de Tecnologías de la informacion y las comunicaciones. (2016). Seguridad y Privacidad de la informacion., (pág. 20). colombia.

Pc-Solucion. (2017). Principios fundamentales de la seguridad informática. Obtenido de https://pc-solucion.es/2017/06/16/aspectos-principios-fundamentales-la-seguridad-informatica/

Puris Caceres , Amilkar Yudier; Viteri Jimenez, Mayra Johana;. (2014). Políticas de seguridad informática en el departamento de tecnologías de la información y comunicación en beneficio de la Universidad Técnica Estatal de Quevedo. manual de procedimientos 2014. Quevedo, Ecuador: Quevedo: UTEQ.

Quiroz Zambrano, S. M., & Macias Valencia, D. G. (2017). Seguridad en informática. Manabi, Bolivia: Universidad Laica Eloy Alfaro de Manabí. Obtenido de file:///C:/Users/Admin4/Downloads/Dialnet-SeguridadEnInformatica-6137824.pdf

Quiroz, Zambrano, Silvia M; Macias, Valencia, David G;. (2017). Seguriad Informatica: Consideraciones. Manabi, Bolivia: Universidad Laica Eloy Alfaro de Manabi. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=6137824

Rios, J. (2010). *Monografas.com.* Obtenido de https://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.shtml

Romero Castro, M. I., Figueroa Moràn, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Murillo Quimiz, Á. L., & Castillo Merino, M. A. (2018). INTRODUCCIÓN A LA SEGURIDAD. (Editorial Área de Innovación y

Desarrollo,S.L.). Obtenido de https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Tulmo Checa, D. W. (Julio de 2019). DISEÑO DE UN MODELO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA LA UNIVERSIDAD TÉCNICA DE COTOPAXI". Latacunga, Ecuador. Obtenido de http://repositorio.utc.edu.ec/handle/27000/5338

Tuyu Technology. (2017). ¿Por qué es tan importante la Seguridad Informática? Obtenido de https://www.tuyu.es/importancia-seguridad-informatica/

Unir. (2020). Claves de las políticas de seguridad informática. Obtenido de https://www.unir.net/ingenieria/revista/politicas-seguridad-informatica/

Vargas, Jenny; Lopez, Pablo;. (2014). Seguridad informatica, Importancia desde la perspectiva del recurso humano. Bogota, Colombia. Obtenido de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2841/00001616.pdf?sequence=1

Voutssas M. J. ;. (2010). Preservación documental digital y seguridad informática. Ciudad de Mexico, Mexico. Obtenido de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008

Welivesecurity. (2014). El ciclo de vida de las políticas de seguridad. Obtenido de https://www.welivesecurity.com/la-es/2014/08/18/ciclo-de-vida-de-las-politicas-de-seguridad/

X. ANEXOS

Anexo 1: Encuesta a pasantes y monitores

BLUELFIELDS INDIAN & CARIBBEAN UNIVERSITY

BICU

Encuesta a personal y pasantes

Como estudiantes de la carrera de ingeniería de sistemas estamos realizando esta encuesta para efectos investigativos dentro del proyecto "Propuesta de políticas de seguridad informática para la Bluefields Indian and Caribbean University", por ello solicitamos amablemente que nos respondas las cuestiones a continuación.

I. Circula la respuesta correcta.

1. **¿Te es familiar la frase Políticas de Seguridad Informática?**

   Mucho Un Poco Nada

2. **¿Qué importancia tiene la seguridad informática en una institución?**

   Nada Muy Poco Poco Mucho Muchísimo

3. **¿Cuenta la universidad con un Política de Seguridad Informática?**

   Si No No sé Lo desconozco

4. **¿Alguna vez has perdido información por ataque de virus o daño a tus dispositivos de almacenamiento?**

   Nunca Algunas veces Muchas Veces

5. **¿Cuáles son las principales amenazas y vulnerabilidades que usted ha detectado en el ámbito informático**

   Malware Sistema Contraseña Mal uso del usuario

6. **¿Conoce algunas herramientas que faciliten la protección física y lógica de equipos informáticos?**

   Si No

Mencione alguna: _____

7. **Que la universidad BICU disponga con una serie de pasos y/o reglamentos para la implementación de la seguridad informática es:**

   Nada Importante Un Poco Importante Muy Importante

8. **De las siguientes opciones, ¿cuál crees que es la que debe de trabajarse a lo inmediato?**

   Seguridad lógica Seguridad física Ambas

9. **¿Qué tan importante es que la universidad cuente con una comisión que vele por mantener la seguridad informática en el recinto?**

   Nada Importante Un Poco Importante Muy Importante

10. **¿Qué tan importante es educar a la comunidad académica en temas de seguridad informática?**

    Nada Importante Un Poco Importante Muy Importante

Anexo 2: Entrevista al personal permanente

BLUELFIELDS INDIAN & CARIBBEAN UNIVERSITY

BICU

Entrevista a jefes de área y personal de la escuela de informática

Como estudiantes de la carrera de ingeniería de sistemas estamos realizando esta entrevista para efectos investigativos dentro del proyecto "Propuesta de políticas de seguridad informática para la Bluefields Indian and Caribbean University", por ello solicitamos amablemente que nos respondas las cuestiones a continuación.

1. En la actualidad, ¿posee la universidad algún tipo de mecanismo preventivo relacionado con el tema de seguridad informática?
2. Para el área que usted gestiona, ¿qué tan importante es que la universidad cuente una Política de Seguridad Informática?
3. ¿Puedes decirnos si en la universidad han ocurrido casos de perdida de información o delito informático?
4. Desde su criterio, ¿Qué beneficios traería a la universidad contar con Políticas de Seguridad Informática?
5. ¿Cuáles deberían de ser los puntos/temas/áreas que deberían ser garantizados dentro de estas Políticas de Seguridad Informática?
6. Hasta el momento, ¿podrías decirnos de qué manera se lleva a cabo las medidas de seguridad informática en la universidad?
7. Al aprobarse una Política de Seguridad Informática, ¿consideras necesario capacitar a todo el personal? ¿Por qué?
8. ¿Existe en el recinto alguna comisión o personal encargado de velar por la seguridad informática de la universidad?

Anexo 3: Cronograma De Actividades

Tabla 3 Cronograma de actividades

Año	2021												2022							
	E	F	M	A	M	J	J	A	S	O	N	D	E	F	M	A	M	J	J
Actividades (Mes)																				
Elaboración del protocolo				X	X	X														
Presentación del protocolo				X		X	X	X				X								
Correcciones del protocolo				X	X	X	X	X	X	X	X									
Procesamiento de la información												X	X	X	X	X	X	X	X	
Análisis de los resultados												X	X	X	X	X	X	X	X	
Finales																				
Conclusiones y Recomendaciones												X	X	X	X	X	X	X	X	
Presentación del trabajo final																				X

Anexo 4: Presupuestos

Tabla 4 Presupuestos

No	Descripción	Costo unitario C$	Costo total	Costo total en dólares
50	Horas de internet	10	500	14.22 $
150	Impresiones	2	300	8.53 $
50	Páginas blancas	1	50	1.42 $
300	Fotocopias	1	300	8.53 $
9	Encolochados	30	270	7.68 $
2	Lapiceros	10	20	0.57 $
20	Gasto de transporte de movilización	12	240	6.83 $
24	Impresiones de las encuestas	2	48	1.37 $
1	Tutoría	4,395.00	4,395.00	125 $
2	Borradores(impresiones)	130	260	7.39 $
Total			6383	181.54