UNIVERSIDAD DE CIENCIAS COMERCIALES

UCC - CAMPUS LEÓN

COORDINACION DE INGENIERÍA EN SISTEMAS

TITULO: ANÁLISIS SITUACIONAL DE LAS ESTRATEGIAS Y METODOLOGÍAS IMPLEMENTADAS PARA PROMOVER LA CIBERSEGURIDAD EN LA UNIVERSIDAD DE CIENCIAS COMERCIALES CAMPUS LEÓN, EN EL PERÍODO COMPRENDIDO DE ENERO A JUNIO DE 2023.

ELABORADO POR:

Ing. Kelvin José Pineda Vargas.

Arq. Lennar Vanegas – Coautor

Asesor: MSc Constantino Portocarrero.

CAMPUS LEÓN, 28 DE AGOSTO DE 2023

Por nuestro Prestigio, Trayectoria y Calidad

¡Somos la Universidad de la Gente que Triunfa!

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

La seguridad de la red informática es un elemento crucial en las organizaciones contemporáneas que se apoyan en la tecnología de la información y las comunicaciones para llevar a cabo sus operaciones. En particular, en el contexto de las instituciones educativas, como la Universidad de Ciencias Comerciales Campus León, la protección de la información, sus equipos e infraestructura de red adquiere una importancia significativa, debido al constante tráfico de datos que sucede a diario en las distintas áreas de la comunidad educativa. En esta investigación, se detallan las políticas de gestión de seguridad existentes en campus León, sus actores directos y los factores que intervienen en la implementación o creación de las mismas. El proceso de investigación de estrategias existentes en materia de ciberseguridad se llevó a cabo durante un período de seis meses; Durante este intervalo, se realizaron entrevistas a las áreas que conforman el departamento TIC, encuesta a sujetos de interés para el estudio y análisis de documentos que evidencia la existencia de política de gestión de seguridad debidamente reglamentes y constituidas.

Palabras claves:

Ciber seguridad, estrategias, políticas, universidad, tecnología, información.

ABSTRACT

Computer network security is a crucial element in contemporary organizations that rely on information and communications technology to conduct their operations. In particular, in the context of educational institutions, such as the Universidad de Ciencias Comerciales Campus León, the protection of information, its equipment and network infrastructure acquires significant importance, due to the constant data traffic that happens daily in the different areas of the educational community. In this research, we detail the existing security management policies at the León campus, their direct actors and the factors that intervene in their implementation or creation. The process of researching existing cybersecurity strategies was carried out over a period of six months; During this interval, interviews were conducted with the areas that make up the ICT department, a survey of subjects of interest for the study and analysis of documents that evidence the existence of a duly regulated and constituted security management policy.

Keywords: Cybersecurity, strategies, policies, university, technology, information.

INTRODUCCION

La seguridad informática es un conjunto de prácticas orientadas a garantizar la integridad, confidencialidad y disponibilidad de los datos almacenados, dispositivos, sistemas informáticos, redes, servidores e infraestructura física en general, que tiene por objeto proteger dichas tecnologías contra amenazas, riesgos y vulnerabilidades que deriven en la pérdida parcial o total de la información a razón de malas prácticas de manipulación, infraestructura en mal estado o ataques de ciberdelincuente que buscan comprometer el funcionamiento, ganar acceso no autorizado, manipular, robar o destruir información confidencial.

La seguridad de la red informática es un elemento crucial en las organizaciones contemporáneas que se apoyan en la tecnología de la información y las comunicaciones para llevar a cabo sus operaciones. En particular, en el contexto de las instituciones educativas, como la Universidad de Ciencias Comerciales Campus León, la protección de la información, sus equipos e infraestructura de red adquiere una importancia significativa, debido al constante tráfico de datos que sucede a diario en las distintas áreas de la comunidad educativa.

El conocimiento de las políticas de ciberseguridad en la institución constituye un pilar fundamental para la implementación de buenas prácticas que garanticen el uso correcto, legítimo y adecuado de la información y recursos institucionales. En esta investigación, se detallan las políticas de gestión de seguridad existentes en campus León, sus actores directos y los factores que intervienen en la implementación o creación de las mismas.

El proceso de investigación de estrategias existentes en materia de ciberseguridad se llevó a cabo durante un período de seis meses, que comprende el tiempo transcurrido entre los meses de enero a junio 2023. Durante este intervalo, se realizaron entrevistas a las áreas que conforman el departamento TIC, encuesta a sujetos de interés para el estudio y análisis de documentos que evidencia la existencia de política de gestión de seguridad debidamente reglamentes y constituidas.

CAPÍTULO I: PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1 Antecedentes y Contexto del Problema

Con el cambio estrepitoso experimentado constantemente en materia de tecnología a nivel mundial, los avances tecnológicos en materia de comunicación y manejo del ciberespacio, surge la creciente necesidad de proteger la información que las empresas e instituciones contienen como estrategia fundamental en la buena gestión y administración de contenidos y datos. En el país, se ha venido considerando con mayor responsabilidad el uso, manejo y gestión de la información que de manera general contienen las empresas, muy específicamente aquellas que gestionan datos relacionados directamente con la privacidad de clientes. Esta creciente preocupación en el manejo de información de las personas responde a la vulneración y fraude que más constantemente perjudican a los usuarios cibernéticos y que ocurren con mayor frecuencia en los últimos años debido al poco interés en la seguridad cibernética de los datos manejados.

Este interés, ha trascendido a todos los ámbitos sociales y empresariales en el país, permeando en la administración de datos académicos que las Instituciones de Estudios Superiores manejan, con la única finalidad de asegurar la protección ante el quebrantamiento de los mismos.

1.1.1 Antecedentes documentados

Para el desarrollo de este trabajo de investigación se ha recurrido a antecedentes que abordan los procesos de seguridad cibernética desarrollado desde las IES tanto a nivel nacional como a nivel internacional.

1.1.2 Antecedentes internacionales

La primera consulta documental se realizó a trabajo desarrollado en grado de maestría, con el título: “Modelo dinámico de ciberseguridad basado en estándares ISO para IES Caso de estudio: Subproceso de gestión de recursos tecnológicos en Unimayor” (Montano Collazos, 2021).

El objetivo de la investigación anteriormente citada es proponer un modelo dinámico de ciberseguridad basado en estándares ISO (Organización Internacional de Normalización) para el Subproceso de Gestión de Recursos Tecnológicos en la Institución Universitaria Colegio Mayor del Cauca.

En la metodología propuesta se tuvieron en cuenta los aportes teóricos relacionados con la temática del estudio y se generaron una serie de actividades para construir el diseño de un modelo que podrá ser ajustado a las necesidades y requerimientos de las IES (Instituciones de Educación Superior). Finalmente se obtiene como resultado un modelo que contribuirá en el plan de mejoramiento de la seguridad de la información brindando su protección, confidencialidad, disponibilidad e integridad y así lograr prevenir los riesgos e identificar posibles amenazas de ciberseguridad, para salvaguardar la información.

Posteriormente se realizó consulta documental al texto que tiene por nombre: “Ciberseguridad y su aplicación en las Instituciones de Educación Superior”. (Carrillo, 2018) el propósito de esta investigación es conocer este aspecto de seguridad en los sistemas distribuidos, mediante la aplicación de la norma ISO 27032-2012, directrices en ciberseguridad en los dominios: seguridad de la información, de las aplicaciones y de las redes. Como complemento se utilizaron herramientas como Shodan, Nessus y Acunetix, que permitieron conocer y analizar posibles amenazas y defensas, en los niveles de seguridad de los sitios, sistemas o servicios webs. Además, con la metodología Análisis Modal de Fallos y Efectos (AMFE) se brindó soluciones de mitigación de riesgos. Finalmente, como medida de solución se efectuó un plan de acción para cada institución objeto de estudio, que le permita desarrollar medidas de control y estrategias de acciones.

Un tercer documento consultado es el que tiene por título: “La seguridad informática en las Instituciones de Educación Superior” (Mata, 2021) El propósito de este trabajo de investigación fue determinar el nivel de Ciberseguridad en las IES de México, con el fin de conocer los riesgos, amenazas y vulnerabilidades de los sistemas de gestión y manejo de información académica.

En la metodología desarrollada del trabajo de Mata (2021), se consideró los aportes teóricos relacionados con la temática del estudio, conceptos básicos y definiciones generales que aportan luces para el desarrollo de la investigación, generando una herramienta de diagnóstico básica para implementar en diversas IES del país considerando datos estadísticos actuales de la situación. Todo esto conlleva abordar responsablemente los temas de seguridad en los portales, sistemas o servicios web de las IES, de los cuales son formas de acceso a la información, y que deben ser monitoreadas o analizadas continuamente para su adecuada protección de los datos. Finalmente se obtiene como resultado una herramienta diagnostico que define criterios y lineamientos a seguir para abordar todo lo referente a seguridad de datos informáticos desde la academia, en las distintas universidades del país.

1.1.3 Antecedentes nacionales

El único documento encontrado en repositorios nacionales con énfasis integral en ciberseguridad corresponde a una tesis titulada: “Diagnóstico de la gestión de la seguridad de la información en la División de informática en la empresa Comercial S.A para la implementación de un SGSI norma ISO 27001” (Rodriguez, O & López , P., 2017), en este documento se elabora un diagnóstico para evaluar la posibilidad de implementar un sistema de gestión de seguridad de la información en la empresa Comercial S.A., y de esta manera optar a la certificación de la ISO 27001:2013. para mejorar el área de informática y toda la compañía con respecto a la seguridad de la información, con la entrega de pautas o recomendaciones que servirán para mejorar los puntos más vulnerables de esta área. El tipo de investigación es cualitativa, prospectiva, exploratoria y descriptiva, ya que, con la información obtenida, se determinó con mayor amplitud la situación actual de la división de informática de la empresa Comercial S.A. Como resultado obtenido de este diagnóstico se pudo identificar que las condiciones de la empresa Comercial S.A. se encuentran bajo un escenario ideal para implementar la ISO 27001:2013, debido que cuentan con una certificación ISO de calidad y tiene muchas actividades y procesos de TI implementados, no obstante, no están regulados ni implementados de manera formal.

En cuanto a los documentos del repositorio institucional, al momento en el que se redacta este acápite, se tiene conocimiento de otra investigación en curso que guarda estrecha relación con el tema de estudio, la cual lleva por título: “Evaluación del nivel de seguridad de la red informática de la universidad de ciencias comerciales UCC campus León, para identificación y mitigación de riesgos. En un período comprendido de enero a junio 2023” (Guevara Betanco, Hernández León, & López Pérez, 2023).

Este último es de potencial interés para investigaciones futuras que guarden relación con la ciberseguridad institucional, ya que, mientras que este estudio tiene por objeto detallar a nivel teórico las metodologías y estrategias existentes en materia de ciberseguridad, el estudio de Guevara Betanco, Hernández León, & López Pérez, buscar evaluarlas de forma práctica.

1.2 Objetivos

1.2.1 Objetivo General

Elaborar un análisis situacional de las estrategias implementadas en materia de ciberseguridad en la Universidad de Ciencias Comerciales Campus León, Nicaragua.

1.2.2 Objetivos Específicos

- Identificar los actores y factores que tienen incidencia en el desarrollo e implementación de estrategias para promover la ciberseguridad en la UCC campus León.
- Aplicar la matriz del análisis de Fortalezas, Oportunidades, Debilidades y Amenazas (FODA) en base a los factores que determinan el estado actual de las acciones a tomar ante ataques cibernéticos.
- Realizar el análisis de la situación actual de la UCC Campus León de cara al proceso de implementación de políticas, metodologías y sistemas que promuevan la ciberseguridad institucional.

1.3 Descripción del Problema y Preguntas de Investigación

Para iniciar un proceso de comprensión adecuada de las gestiones de seguridad de la información, es de suma importancia conocer el avance en materia de Ciberseguridad que se ha venido desarrollando en muchas de las instituciones del país, específicamente en algunas de las Instituciones de Estudios Superiores (IES). En Nicaragua se tiene existencia de tres leyes aprobadas en el año 2020 que están relacionados con la seguridad ciudadana, de las cuales una de ellas aborda directamente el delito de ciberseguridad, contemplado en el decreto presidencial 24 2020 sobre Estrategia Nacional de Ciberseguridad 2020-2025 (AMCHAM, 2020)

El objetivo principal de la antes mencionada legislación es el de garantizar el uso ciudadano y soberano, seguro y confiable del ciberespacio que permita el aprovechamiento de las Tecnologías de la Información y la Comunicación (TIC) como herramienta que contribuya a la paz, estabilidad, seguridad y desarrollo sostenible del país. (AMCHAM, 2020)

No obstante, aun con la existencia de un marco legal general para la implementación de acciones que promuevan la ciberseguridad en el país, las Instituciones de Educación Superior en el país no poseen avances significativos en este aspecto, por lo que siguen reproduciendo modelos obsoletos de resguardo de información que en muchas ocasiones no son del todo eficientes ni seguros.

Tal es el caso de la Universidad de Ciencias Comerciales UCC Campus León, que aun con la cantidad de información académica relevante como calificaciones, expedientes estudiantiles y procesos académico, no posee un adecuado sistema de gestión de la información y defensa ante ataques cibernéticos que puedan darse en perjuicio de la institución y los procesos académicos que en ella se desarrollan.

Esta vulnerabilidad identificada se ve agravada por el exiguo conocimiento que, en materia de metodología de respuesta ante ciberataques, poseen las instancias correspondientes de la salvaguarda de toda la información importante contenida en el Campus Universitario.

Las premisas antes expuestas contribuyen al planteamiento de las siguientes preguntas de investigación:

¿Por qué es relevante para la propia Universidad de Ciencias Comerciales el pleno conocimiento de las metodologías y estrategias implementadas para la gestión y salvaguarda de la información en campus León?

¿Las estrategias implementadas por el equipo responsable de ciberseguridad en sede León serían efectivas ante un escenario que pueda comprometer la seguridad de la información institucional?

¿Son conscientes docentes, estudiantes y personal administrativo de lo que implica la ciberseguridad y como estos conocimientos se encuentran encauzados a proteger la confidencialidad de los datos en sus dispositivos informáticos de uso cotidiano?

1.4 Justificación

El desarrollo de la presente investigación pretende constituirse como un documento base de referencia bibliográfica y de contextualización teórica que sea utilizada a futuro en el desarrollo de acciones o propuestas concretas en materia de ciberseguridad a ser implementadas en la Universidad de Ciencias Comerciales Campus León, así como herramienta técnica a considerar para el resto de sedes en las que tiene presencia la Universidad de Ciencias Comerciales.

1.5 Limitaciones

En todo proceso de investigación se debe considerar las posibles implicaciones y factores que pueden influir de manera negativa en el desarrolla de la misma.

Para el desarrollo de la presente investigación únicamente se tiene como limitante del investigador: la sinceridad de los participantes del estudio y la buena gestión del tiempo destinado para la recopilación y procesamiento de la información.

De igual forma, el acceso a información pertinente en el tiempo adecuado, supone una limitante que determina el nivel de involucramiento y cumplimiento de objetivos planteados por el investigador en el desarrollo de este trabajo investigativo.

1.6 Hipótesis

La implementación de métodos y estrategias de ciberseguridad esgrimidas por los departamentos de TIC de UCC Campus León aseguran la integridad de los datos y el empoderamiento de información de su comunidad educativa.

1.7 Variables

Variables Dependientes

Estrategias

Ciberseguridad

Análisis

Variables Independientes

Factores

Propuesta

Actores

CAPÍTULO II: MARCO REFERENCIAL

2.1 Estado del Arte

El estado del arte es el conjunto de saberes o el desarrollo que se ha conseguido en el área que se va a investigar. Su función entonces es la de reunir todas las fuentes de información que han versado sobre el tema a tratar, para así evitarle a un autor la repetición de juicios o investigaciones ya hechas. (Enciclopedia Online.com, s.f.)

Tabla 1
Bases de datos consultadas

Base de Datos Científicas Utilizadas	No. de publicaciones relacionadas con la investigación de acuerdo a la base de datos	No. de publicaciones con mayor reconocimiento científico	Tipos de publicaciones identificadas
Redalyc.Org	23,049	10	Artículo Científico
Dialnet	147	3	Investigación
Dialnet	2	1	Tesis de Grado
Scielo	4	1	Artículo Científico
Google Académico	7	3	Tesis de Grado

Fuente: Elaboración propia del autor

Tabla 2
Investigaciones encontradas en bases de datos consultadas

Autor(es) y año en orden cronológico	Principales Teorías y Aportes al Tema de Investigación

Troya Andrea, 2020	Teoría de Vulnerabilidad, Ciberseguridad, Ataques maliciosos, aporte de relevancia en conocimientos teóricos de redes informáticas.
Piza Dias Michell, 2019	Estudio de Amenazas y vulnerabilidad de la red informática, Identificación de tipos de vulnerabilidades, y escaneo de red mediante herramientas de seguridad.
Carlos E. Anchundia – Betancourt, 2017	Realiza una contextualización importante de la aplicación de acciones de seguridad cibernética en Universidades y cómo éstas deberían adaptarlas en todas sus estructuras organizativas.

Fuente: Elaboración propia del autor.

2.2 Teorías y Conceptualizaciones asumidas

2.2.1 Marco Teórico

Nube informática. Es un concepto abstracto, un paradigma tecnológico que empezó a popularizarse como modelo de arquitectura informático a finales del 2008. Según (Joyanes Aguilar, 2012) la nube, “puede ser infraestructura o software, es decir, puede ser una aplicación a la que se accede a través del escritorio y se ejecuta tras su descarga, o bien un servidor al que se invocará cuando se necesite”.

Seguridad de la información. La seguridad de la información es una disciplina asociada tradicionalmente a la gestión de TIC, cuyo propósito es mantener niveles aceptables de riesgo de la información organizacional y de los dispositivos tecnológicos que permiten su lectura y escritura. Ha sido definida por la norma ISO/IEC 27000 como la preservación de la confidencialidad, integridad y disponibilidad de la información (ISO/IEC, 2014). (Valencia-Duque, 2017)

Ciberseguridad. La ciberseguridad es la práctica de proteger los sistemas más importantes y la información confidencial ante ataques digitales. También conocida como seguridad de la tecnología de la información (TI), las medidas de ciberseguridad están diseñadas para combatir las amenazas a sistemas en red y aplicaciones, que se originan tanto desde dentro como desde fuera de una organización. (IBM, s.f.)

(Romero , M & Álava , J., 2018) afirman que; la seguridad siempre busca la gestión de riesgos, esto quiere decir que siempre una forma de evitarlo o prevenirlo y que se puedan realizar ciertas situaciones de la mejor forma, se definió que la seguridad puede ser catalogada como la ausencia de riesgos, la definición de este término involucra acciones que siempre están inmersas en cualquier asunto como:

- Prevención del riesgo
- Transferir el riesgo
- Mitigar el riesgo
- Aceptar el riesgo.

Defensa en profundidad (DiD). Es una metodología comúnmente asociada al término "seguridad por capas". Esta metodología "apunta a implementar varias medidas de seguridad con el objetivo de proteger un mismo activo. Es una táctica que utiliza varias capas, en la que cada una provee un nivel de protección adicional a las demás" (Portantier, 2012).

Las capas de control a las que hace referencia el texto citado, son en realidad un conjunto de tecnologías, estrategias, y mecanismos que se implementan a nivel físico y administrativo en una institución como estrategia principal de ciberseguridad para proteger los "activos" de la misma, estos activos pueden ser: equipos, datos, redes físicas o lógicas que funcionan como autopistas para el tráfico de información. Uno de los términos más relevantes en este sentido es la seguridad de red.

Seguridad de red. Conjunto de técnicas que combina varias capas de defensa perimetral. Cada capa implementa políticas y controles. Los usuarios autorizados tienen acceso a los recursos de red, mientras que se bloquea a los usuarios maliciosos para evitar que ataquen vulnerabilidades y amenacen la seguridad.

Vulnerabilidad, Riesgos y Amenazas. Una vulnerabilidad es un fallo o debilidad de un sistema de información que pone en riesgo la seguridad de la misma. Se trata de un "*agujero*" que puede ser producido por un error de configuración, una carencia de procedimientos o un fallo de diseño, según (Romero , M & Álava , J., 2018) las amenazas son sucesos que pueden dañar los procedimientos y los riesgos son probabilidades de que algo negativo suceda dañando los recursos tangibles o intangibles y por tanto impidiendo desarrollar la labor profesional.

Usuario. En informática, se entiende como usuario a un conjunto de permisos y de recursos asignados a un operador que accede a una red informática, generalmente un usuario suele estar asociado con algún identificador único y una contraseña.

Contraseña. Las contraseñas son secuencias de símbolos, generalmente asociadas a un nombre de usuario, que proporcionan un mecanismo para la identificación y la autenticación de un usuario en particular. En casi todos los servicios son los propios usuarios quienes eligen sus contraseñas, y con frecuencia eligen secuencias que no pueden ser consideradas seguras (por ejemplo, nombre de la pareja, nombre de hijo/hija, fechas de nacimiento, …) Como regla general, las contraseñas que son fáciles de recordar son también fáciles de adivinar.

Ataque Informático malicioso. Un ataque informático malicioso consiste en aprovechar alguna debilidad o falla en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; para obtener un beneficio, por lo general de condición económica, causando un efecto negativo en la seguridad del sistema, que luego pasa directamente en los activos de la organización.

Los ataques a las redes pueden ser definidos como diferentes tipos de actividades sistemáticas dirigidas a disminuir o corromper su seguridad. Desde este punto de vista, un ataque puede ser definido como una amenaza sistemática generada por una entidad de una manera artificial, deliberada e inteligente. (Soriano)

Las redes de ordenadores pueden ser vulnerables a muchas amenazas utilizando distintas formas de ataque, entre ellas se tienen los ataques más conocidos y utilizados.

a) **Ataques de denegación de servicio (DDoS).** Es un ataque que busca saturar un servidor o red con tráfico falso o inútil, de manera que no pueda procesar solicitudes legítimas y el servidor se vuelva inoperable. Este tipo de ataque es muy utilizado para interrumpir servicios web de empresas o instituciones.

b) **Ataques de fuerza bruta.** Un ataque de fuerza bruta es un intento automatizado por averiguar las credenciales de acceso de un usuario, la clave de acceso a una red cifrada, o la contraseña usada para el cifrado de un algún archivo con un enfoque de prueba y error. La tasa de éxito de estos tipos de ataques está condicionada por la capacidad de procesamiento de información del atacante y las vulnerabilidades en los protocolos de inicio de sesión de un sistema informático.

c) **Puntos wifi maliciosos.** Consisten en la creación de una red wifi falsa que parece ser legítima, pero que en realidad es controlada por un ciberdelincuente. Los usuarios que se conectan a esta red pueden estar expuestos a la captura de sus datos personales o al robo de información confidencial.

d) **Ingeniería social.** Es una técnica de manipulación psicológica que los atacantes utilizan para engañar a los usuarios y obtener información confidencial o acceso a sistemas. Puede llevarse a cabo a través de diversas formas, como la suplantación de identidad. Los términos más comunes asociados a la ingeniería social son:

- **Phishing**. Es un tipo de ingeniería social que consiste en enviar correos electrónicos que parecen provenir de entidades de confianza haciéndolos parecer legítimos, generalmente incluyen algún enlace a un sitio externo dentro del cuerpo del mensaje con el objetivo de engañar al usuario y hacer que proporcione información personal, como contraseñas, números de tarjetas de crédito o datos bancarios.
- **Smishing**: Variante de Phishing que utiliza los mensajes de textos como método de propagación para llevar a cabo estafas, suplantación de identidad e instalación de malware.
- **Vishing:** Es una técnica de phishing más sofisticada que involucra el uso de servicio telefónico por Internet conocido como VoIP (Voz sobre protocolo de Internet) para llevar a cabo su cometido, en lugar de usar correos electrónicos o servicios de mensajería de texto.

- **Whaling:** Es un método de suplantación de identidad más personalizado y dirigido, a diferencia del phishing que no posee un objetivo específico, el Whaling se enfoca en las personas influyentes dentro de la cadena de mando de una institución.

Malware. El término malware proviene del inglés “malicious software”, que en español significa código malicioso. Técnicamente, malware se refiere a programas que se instalan en los sistemas operativos de los equipos con desconocimiento de los usuarios. Estos programas esperan silenciosamente su ejecución con la intención de causar daños irreparables a los archivos informáticos o llevar a cabo un hurto de información. Existen diferentes tipos de software malicioso, se pueden clasificar por nivel de amenaza y propósito. Los más comunes son:

a) Virus. Un virus informático infecta los dispositivos viajando de manera autónoma entre ellos, normalmente, esperando a ser detonado por un usuario final. Suelen estar programados en un lenguaje específico con el objetivo de interferir con las tareas del sistema o entorpecer las acciones del usuario. Constituyen el nivel de amenaza de menor grado y suelen ser fácilmente detectados por los antivirus instalados en nuestros sistemas operativos.

b) Worm. Un gusano (traducción del término “Worm”) también es programado para viajar entre los dispositivos, pero este tipo de software sólo se instala una vez dentro del sistema, y posteriormente busca otro dispositivo para su infección. Algunos gusanos requieren de la interacción con usuarios, pero también existen algunos de ellos que logran infectar sin la necesidad de dicha interacción.

c) Troyano. Los troyanos (Trojans), por otro lado, hacen honor a la leyenda mítica griega “Caballo de Troya”, debido a que el software no aparenta ser mal intencionado, sino todo lo contrario, parece ser un software útil para el usuario. Los troyanos también pueden ser instalados sin la necesidad de ser descubiertos o detonados por un usuario, permitiéndose así el acceso al sistema sin aviso alguno. Estos son mejor conocidos como troyanos de puerta trasera (Trojans Backdoors). A diferencia de los virus y los gusanos, los troyanos dependen del acceso a Internet.

d) Spyware. Estos pretenden la obtención de información de los usuarios. Entre los datos más importantes que puede llegar a sustraer esta amenaza, se encuentran las contraseñas y números de tarjetas de crédito. (López-Chau, 2016)

e) Ransomware: Es un tipo de malware que cifra los archivos de la víctima y exige el pago de un rescate para su recuperación. Este tipo de ataque puede tener un impacto devastador en empresas, o en este caso la UCC, ya que pueden perder acceso a su información crítica o datos importantes como bases de datos. (Mc & Scambray J, 2012)

2.3 Marco Contextual

La Universidad de Ciencias Comerciales (UCC) inicio su funcionamiento como Instituto de Ciencias Comerciales, bajo la resolución No. 824 del Ministerio de Gobernación, con fecha trece de enero de 1964. Posteriormente cambió su nombre y adoptó el de Centro de Ciencias Comerciales (CCC) con personalidad Jurídica aprobada en Decreto Legislativo No. 627, publicado en La Gaceta, Diario Oficial, Número 193 del 13 de octubre de 1993.

El 20 de marzo de 1997, en sesión No. 08-97, el Consejo Nacional de Universidades, en uso de las facultades conferidas en el numeral 7 del artículo 58 de la Ley de Autonomía de las Instituciones de Educación Superior, Ley No. 89, autorizó el cambio de categoría académica de Centro de Educación Técnico Superior a Universidad de Ciencias Comerciales (UCC) por un periodo de cinco años de 1997 a 2001. (UNIVERSIDAD DE CIENCIAS COMERCIALES, 2016)

En el año 2001 se inaugura el Campus en la ciudad de León. Es una institución de educación superior ubicada en la ciudad de León, Nicaragua. Esta prestigiosa Alma Mater se dedica a ofrecer programas de Licenciaturas, Especializaciones en áreas como Administración de Empresas, Contabilidad, Marketing, Finanzas, Ingenierías entre otras. En la actualidad, como institución que se ocupa de la educación superior, maneja grandes volúmenes de información académica, reportes de calificaciones, información personal de estudiantes, planes de estudio y todo tipo de información administrativa, contable y académica relacionada al quehacer universitario.

De igual manera es importante mencionar que toda esta información pertenece a estudiantes matriculados activos e inactivos, personal docente fijo y docente horario, administrativos y personal académico, por lo que es imperativo asegurar una gestión adecuada de todos estos recursos informáticos, proveyendo un sistema de defensa eficaz ante los ataques maliciosos.

Asimismo, la buena gestión de la seguridad de información académica evita las posibles interrupciones en el funcionamiento administrativo ya que las universidades dependen cada vez más de la tecnología para llevar a cabo sus actividades diarias, desde la administración hasta la enseñanza y la investigación.

Los ciberataques pueden provocar interrupciones en el funcionamiento normal de la institución, lo que afectaría negativamente a estudiantes, profesores y empleados.

El análisis situacional de las estrategias y metodologías implementadas para promover la ciberseguridad en la Universidad de Ciencias Comerciales Campus León, permitirá identificar y diseñar herramientas adecuadas para minimizar o neutralizar la ocurrencia de ataques cibernéticos, asegurando la protección de la información de datos y la evaluación y mitigación de los riesgos asociados a la seguridad de la información.

2.3.1 Marco Legal

El Estado de Nicaragua tiene la obligación de proteger a la población y garantizar su seguridad, en el marco del respeto a los derechos humanos y las libertades fundamentales. Si se retoma esta premisa, se puede considerar que el Estado tiene la responsabilidad de crear el escenario adecuado para garantizar la seguridad cibernética de todos los ciudadanos del país, cumpliendo este deber con la creación de legislación vigente en materia de ciberseguridad. Dentro del ordenamiento jurídico actualmente se cuenta con las siguientes leyes:

- **Ley No. 1042, Ley Especial de Ciberdelitos.** Esta ley establece las normas para garantizar la ciberseguridad en Nicaragua, incluyendo la protección de la información, la prevención de ciberataques y la regulación del uso de las redes y sistemas de información. (Asamblea Nacional de la República de Nicaragua., 2015)

- **Ley No. 787, Ley de Protección de Datos Personales.** Publicada en La Gaceta, Diario Oficial 61 el 29 de marzo del 2012, tiene por objetivo la protección de la persona natural o jurídica frente al tratamiento, automatizado o no, de sus datos personales en ficheros de datos públicos y privados, a efecto de garantizar el derecho a la privacidad personal y familiar y el derecho a la autodeterminación informativa. (Asamblea Nacional de la República de Nicaragua, 2012) La investigación se centrará en los artículos:
    1. **Art. 11. Medidas de seguridad.** El responsable del fichero de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la integridad, confidencialidad y seguridad de los datos personales, para evitar su adulteración, pérdida, consulta, tratamiento, revelación, transferencia o divulgación no autorizada, y que permitan detectar desviaciones, intencionales o no, de información privada, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. Cuando los datos personales se refieran a los miembros de la Policía Nacional o del Ejército de Nicaragua y fallaren o se inobservaren las medidas de seguridad a las que se refiere el párrafo anterior, el responsable de fichero de datos deberá informar inmediatamente a la Institución afectada para lo de su cargo. (Asamblea Nacional de la República de Nicaragua, 2012)
    2. **Art. 12. Confidencialidad en el tratamiento de los datos.** El responsable del fichero de datos y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el responsable del fichero de datos. El titular de los datos personales tratados en ficheros de datos, tiene derecho a ser informado sobre las políticas de privacidad que adopta el responsable del fichero, y que se le notifique cualquier modificación de las mismas. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad nacional, defensa nacional, seguridad pública o la salud pública. (Asamblea Nacional de la República de Nicaragua, 2012)

- **Ley No. 1042, Ley Especial sobre Ciberdelitos.** Aprobada recientemente y que forma parte de nuestro ordenamiento Jurídico en su arto. 3. La presente Ley tiene por objeto la prevención, investigación, persecución y sanción de los delitos cometidos por medio de las Tecnologías de la Información y la Comunicación, en perjuicio de personas naturales o jurídicas, así como la protección integral de los sistemas que utilicen dichas tecnologías, su contenido y cualquiera de sus componentes, en los términos previstos en esta Ley. (Asamblea Nacional de la República de Nicaragua, 2020) El capítulo II trata de Delitos Relacionados con la Integridad de los Sistemas Informáticos el cual se basa en la investigación los siguientes artículos:

  1. **Art. 10. Daños a sistemas informáticos.** El que destruya, dañe, modifique, ejecute un programa o realice cualquier acto que altere el funcionamiento o inhabilite parcial o totalmente un sistema informático que utilice las Tecnologías de la Información y la Comunicación o cualquiera de los componentes físicos o lógicos que lo integran, será sancionado con prisión de tres a cinco años y trescientos a quinientos días multa.

     Si el delito previsto en el párrafo anterior se cometiere por imprudencia será sancionado con doscientos a quinientos días multa.

     Si el delito previsto en el presente artículo recayera en contra de cualquiera de los componentes de un sistema informático que utilicen las Tecnologías de la Información y la Comunicación, que estén destinadas a la prestación de servicios públicos o financieros, o que contengan datos personales, datos personales sensibles, información pública reservada, técnica o propia de personas naturales o jurídicas, la sanción de prisión será de cuatro a seis años y trescientos a seiscientos días multa.

     Si la acción prevista en el párrafo anterior se cometiere por imprudencia será sancionado con trescientos a seiscientos días multa. (Asamblea Nacional de la República de Nicaragua, 2020)

CAPÍTULO III: DISEÑO METODOLÓGICO

3.1 Tipo de Investigación

El estudio es de enfoque cuantitativo; mide y cuantifica a través del modelo DiD el grado de involucramiento que poseen los usuarios regulares de la intranet de sede León en materia de estrategias de ciberseguridad que son implementadas por los departamentos de tecnologías de información de sede León.

El estudio es también de tipo descriptivo, ya que, a través del mismo, se pretende obtener una comprensión detallada de los factores que inciden en la implementación de nuevas estrategias de ciberseguridad y cómo las ya existentes ayudan a las buenas prácticas del resguardo de la información. Asimismo, pretende establecer una base sólida de conocimientos para investigaciones futuras que profundicen en temáticas más especializadas sobre los ejes de la ciberseguridad.

Los instrumentos de recolección de información empleados para el alcance de los objetivos de investigación propuestos fueron:

- **Encuesta:** Instrumento de recolección de información de índole cuantitativa. Fue dirigida a estudiantes, docentes y personal administrativo para evaluar sus conocimientos en materia de ciberseguridad y estrategias aplicables en su entorno de trabajo.
- **Entrevista:** Instrumento de recolección de información de índole cualitativa. Aplicada al personal encargado de promover, coordinar y ejecutar estrategias de ciberseguridad y seguridad de la información en la institución.

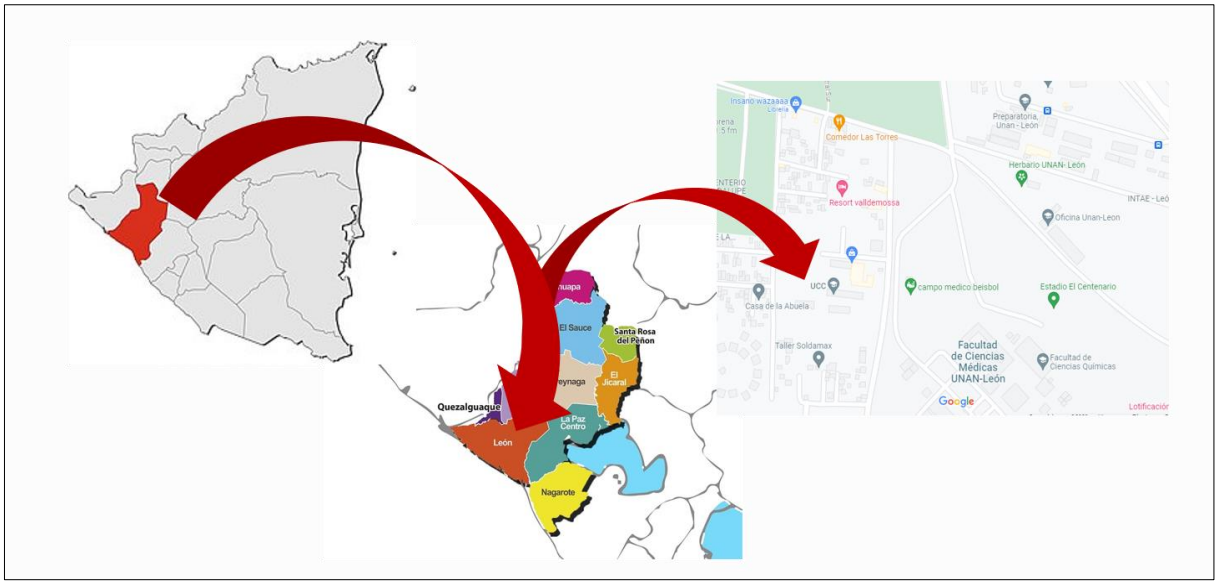
El estudio es de corte transversal, puesto que posee un marco temporal delimitado, comprendiendo los meses de enero a junio del año 2023.

El estudio se caracterizó por la no manipulación de las variables y la no injerencia del fenómeno observado, por lo tanto, es de tipo no experimental. En este mismo sentido, se ejerció la observación participativa como técnica de recolección de información, la cual permitió discernir con mayor certeza la veracidad de los datos presente en los instrumentos de recolección de información.

3.2 Área de estudio

El estudio se llevó a cabo en las instalaciones de la Universidad de Ciencias Comerciales Campus León, constituida legalmente como una institución de educación superior. Se encuentra ubicada al Sureste de la ciudad de León y referenciada en las coordenadas 12º41’88.0 N, -86º87’74.3 O. Limita hacia el Norte con el Cementerio de Guadalupe, al Sur con el parque infantil el Talchocote, al Este con el Anexo al Cementerio de Guadalupe y al Oeste con la facultad de Ciencias Médicas UNAN-León.

Figura 1
Mapa de macro y micro localización del área de estudio



Fuente: Elaboración propia del autor.

3.3 Unidades de Análisis: Población y Muestra: tamaño de la muestra y muestreo

3.3.1 Unidad de análisis

Se establece como unidad de análisis las estrategias y metodologías implementadas por los departamentos encargados de garantizar la seguridad e integridad de la información institucional. Esto implica validar la efectividad de las mismas a través del propio conocimiento adquirido por los usuarios, considerando que la desinformación constituye una de las principales amenazas potenciales en temas de ciberseguridad.

3.3.2 Población

La población se encuentra delimitada por los usuarios que acceden regularmente a la intranet de campus León.

3.3.3 Muestra

La población de usuarios puede segmentarse de acuerdo al rol que desempeñan en la comunidad educativa, por tanto, a fin de poder evaluar el grado de empoderamiento y el impacto de las estrategias implementadas para cada grupo de la población, se ha establecido un muestreo por conveniencia de:

- 15 docentes.
- 10 colaboradores del personal administrativo.
- 45 estudiantes de todas las coordinaciones de campus León del turno diurno.

La suma de los participantes que conforman la muestra es de 70 individuos.

Los criterios de inclusión y segmentación de la muestra se encuentran detallados en la tabla No. 3 “Criterios de inclusión para la recopilación de datos” presentados en la siguiente página.

Criterios de inclusión de la muestra.

Tabla 3
Criterios de inclusión para la recopilación de datos

Informantes	Criterios de inclusión	Criterios de exclusión	Tamaño de la muestra
Documentos	Formatos de reglamentación interna o de uso exclusivo en los departamentos de TIC.	Documentación no relacionada con los departamentos de TIC.	Bitácoras de asistencia. Formatos de inventario. Planes de estrategia.
Actores claves o grupos de interés	Estudiantes de todas las carreras servidas en turno diurno en campus León.	Estudiantes ajenos a sede León o del turno sabatino y dominical.	45 estudiantes.
	Personal administrativo con acceso de lectura o escritura a los sistemas de información.	Personal de otras áreas que no posean credencial de acceso a los sistemas de la institución.	10 miembros de personal administrativo.
	Docentes horarios o de plaza fija que hacen uso frecuente de la red o de los recursos institucionales.	Docentes horarios o de plaza fija que no hacen uso de recursos institucionales.	15 docentes.
Departamentos TIC	Personal encargado de la implementación de estrategias de ciberseguridad.	Personal externo o de otras sedes fuera de campus León.	2 coordinadores de área.

Fuente: Elaboración propia del autor

3.4 Técnicas e instrumentos de recolección de datos

Para la recolección de datos se utilizó las siguientes técnicas de recolección de datos.

3.4.1 Técnicas de fuentes Primarias

Encuesta.

"El objetivo de la encuesta es obtener información relativa a las características predominantes de una población mediante la aplicación de procesos de interrogación y registro de datos". (García Córdoba, 2004) En este sentido particular, la encuesta aplicada mediante cuestionario permite obtener información de los participantes del estudio de manera sistemática y ordenada. A partir de los cuestionarios aplicados a cada segmento de la muestra (Ver anexos 1 y 2) se pretende:

1. Medir el grado de conocimiento de los encuestados a través de preguntas de control en relación a los conceptos básicos de ciberseguridad y las principales amenazas de ingeniería social a la que se encuentran expuestos.
2. Conocer la forma en que los usuarios practican la autoprotección ante los posibles ataques de ingeniería social.
3. Conocer el uso medio de los recursos informáticos.
4. Identificar las posibles amenazas de red proveniente del tráfico de contenido consumido por los usuarios.

Entrevista.

"La entrevista es una forma oral de comunicación interpersonal, que tiene como finalidad obtener información en relación a un objetivo" (López M. & Acevedo Ibañéz, 2004). A través de este instrumento de recolección de información aplicado al personal especializado en las áreas de las tecnologías de la información en los departamentos de sistemas, soporte técnico y ciberseguridad, se pretendía identificar a los actores responsables de establecer, coordinación, ejecutar y dar seguimiento a políticas, métodos y estrategias en materia de ciberseguridad en la institución.

3.4.2 Fuentes secundarias

Son fuentes de información secundaria para este estudio:

- Estudios monográficos citados a lo largo del documento.
- Libros consultados para la contextualización de la investigación.
- Documentos proporcionados por lo departamentos participantes del estudio que enriquezcan la información proporcionada por las fuentes primarias.

3.5 Confiabilidad y Validez de los Instrumentos

La confiabilidad de los instrumentos se evaluó utilizando el coeficiente de alfa de Cronbach por el método de varianza de los ítems. Como resultado, se obtuvo un valor de 0.8 que indica una alta consistencia y fiabilidad de los resultados obtenidos a través de los instrumentos de recolección de datos.

3.6 Procesamientos de Datos y Análisis de la Información

La recolección de datos se llevó a cabo a través de la red, haciendo uso de formularios de Google con el objetivo de poder brindarles a los docentes, estudiantes y personal administrativo, la posibilidad de analizar la información solicitada sin límite de tiempo en horas no comprometidas.

El procesamiento de datos numéricos y estadísticos se llevó a cabo en el software de Microsoft Excel 2019 por su alta versatilidad y amplio número de funciones que permiten la clasificación, filtrado, evaluación y consolidación de la información que se obtiene de los procesos de entrevista y cuestionarios aplicados a las fuentes primarias.

La toma de notas y levantado de texto se realizó a través de la herramienta Microsoft Word 2019.

3.7 Operacionalización de las Variables

Tabla 4
Operacionalización de las variables

Objetivo	Variable	Tipo de Variable	Definición Conceptual	Dimensión Operacional	Técnicas e instrumentos de recolección de datos
Identificar los actores y factores que tienen incidencia en el desarrollo e implementación de estrategias para promover la ciberseguridad en UCC campus León.	Actores y factores	Independiente	**Actor:** Persona que tiene un papel de responsabilidad en uno o más procesos o actividad. **Factor:** Elemento, circunstancia o influencia que contribuye a producir un resultado.		Entrevista Encuesta
Aplicar la matriz de análisis (FODA) en base a los factores que inciden en la toma de acciones ante los ataques cibernéticos	Ataques cibernéticos	Independiente	**Ataque cibernético:** Actividades que se dirigen a sistemas de información para vulnerar o corromper su seguridad.	Acceso a la intranet	Entrevista Encuesta
Realizar un análisis situacional de los procesos de implementación que promuevan la ciberseguridad	Estrategias de ciberseguridad	Dependiente	Decisiones basadas en la ocurrencia de riesgos que permiten desarrollar metas de seguridad realistas.	Capacitaciones. Acceso a la intranet. Acceso a equipos.	Entrevista Encuesta

Fuente: Elaboración propia del autor

CAPITULO IV: ANALISIS DE RESULTADOS

4.1 Estrategias de ciberseguridad implementadas en la institución

Se detallan a continuación las metodologías de ciberseguridad implementadas por los departamentos de TI bajo el modelo DiD a partir del análisis de la información presente en los instrumentos de recolección de datos.

Figura 2
Modelo de capas DiD

Fuente: (Portantier, pág. 21)

4.1.1 Capacitación

Actualmente no existe un plan de capacitación activo dirigido a la población de estudio, no obstante, la coordinación de ciberseguridad si tiene contemplado incluir en el corto plazo (próximo inicio de cuatrimestre) la programación de capacitaciones dirigidas a todos los segmentos de la muestra como parte de su plan de actividades.

4.1.2 Políticas y Procedimientos

De los departamentos de tecnología de información consultados en sede León, sólo soporte técnico posee formatos físicos que permiten establecer una trazabilidad de actividades y equipos, en cuanto a las políticas y reglamentos internos, las áreas de sistemas y ciberseguridad manifestaron encontrarse bajo gerencia directa de sede Managua, por lo que no se encontró evidencia física de los manuales operativos y fichas de procesos.

En el orden de ideas anteriores, la documentación pertinente a sede Managua no fue consultada durante el ejercicio de esta investigación por formar parte de los criterios de exclusión de la muestra.

4.1.3 Perímetro

Los departamentos de soporte técnico y sistemas son los responsables de establecer conjuntamente el perímetro de operación de los equipos informáticos que utilizan los colaboradores. Esto se logra implementando las siguientes estrategias:

- Los equipos informáticos se encuentran inventariados.
- La trazabilidad de los equipos es posible gracias a la existencia y aplicación de formatos para la requisa y solicitud de los mismos.
- Los equipos informáticos son asignados a segmentos de red específicos.

4.1.4 Red

Se identificó la existencia de un firewall físico capaz de monitorear y denegar el tráfico de datos que ocurre en la intranet de campus León. Estas acciones se llevan a cabo en el área de soporte técnico bajo la coordinación y autorización de sede Managua. Adicionalmente, se toman otras medidas de seguridad para restringir el acceso a la red tales como:

- Claves cifradas en puntos de acceso wifi.
- Segmentación de redes virtuales.

4.1.5 Servidores (Hosts)

No existen servidores físicos en sede León. La lectura y escritura de información de los sistemas institucionales se logra a través del enrutamiento lógico de los datos a cargo del área de soporte técnico. La logística operativa y estructural de los servidores es competencia exclusiva de sede Managua, por lo que trasciende el área de estudio de esta investigación.

4.1.6 Aplicaciones

El área de sistemas, a través de las directrices de sede Managua, es el responsable de gestionar las credenciales de acceso a los sistemas de información en sede León.

Como estrategia de ciberseguridad, la información de los sistemas institucionales solo es accesible a los usuarios una vez que el servidor central ha logrado identificar correctamente sus credenciales de acceso, concediéndole permisos de lectura o escritura a la información solicitada en función de su rol.

4.1.7 Datos

La permanencia e integridad de la información es tarea exclusiva del área de soporte técnico. Esto se logra implementando las siguientes estrategias:

- Respaldo periódico de la información en medio físico y nube institucional.
- Protección de los sistemas operativos administrada por antivirus y actualizaciones de seguridad.
- Protección de voltaje proporcionadas por sistemas de alimentación ininterrumpida.

4.1.8 Factores que inciden en la implementación de estrategias

De acuerdo con Msc. Aguinaga, responsable de la coordinación de ciberseguridad en sede León, uno de los principales factores que han impactado de forma negativa en la implementación de estrategias, es la falta de personal que existe en el resto de áreas TIC producto de los recientes casos de dimisión que tuvieron lugar durante los primeros meses de operación de la coordinación, asimismo, durante el ejercicio de la observación participativa, se logró identificar que la creación o implementación de estas estrategias también se encuentra ligado a:

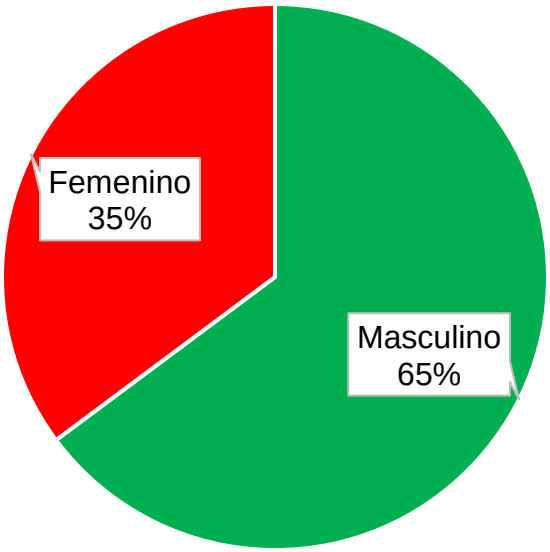
- Requerimientos institucionales establecidos por la alta gerencia.
- Disponibilidad del personal de las áreas TIC para llevarlas a cabo.
- Autorización centralizada de los procedimientos requeridos.
- Viabilidad logística, temporal y económica de las estrategias.
- Disponibilidad inmediata de recursos y equipos especializados.

4.2 Análisis de encuestas

Para una mejor comprensión e interpretación del lector, se han agrupado los gráficos de acuerdo a la capa de seguridad en la que se sitúa el propósito de las preguntas en el modelo DiD y no de acuerdo al orden pre establecido en las encuestas.

4.2.1 Perímetros de operación y datos demográficos

Figura No. 3
Género de los encuestados



Fuente: Elaboración propia del autor

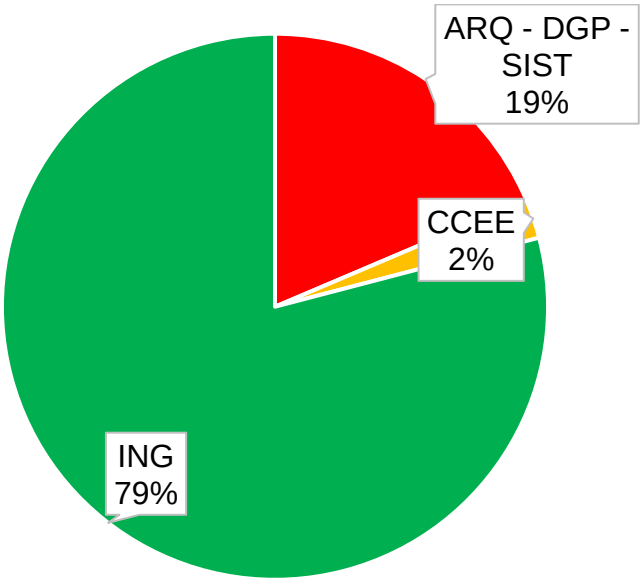
El género predominante de los participantes del estudio es el Masculino, con una diferencia que ronda el 30% respecto al género femenino. La distribución exacta de los participantes de acuerdo a su género se expone en la siguiente tabla.

Tabla 5
Matriz de datos de gráfico 1

Genero	Estudiantes	Personal	Recuento	Porcentaje
Masculino	28	7	35	64.81 %
Femenino	15	4	19	35.19 %
Totales	43	11	54	100 %

Fuente: Elaboración propia del autor

Figura No. 4
Coordinación a la que pertenecen los estudiantes encuestados



Fuente: Elaboración propia del autor

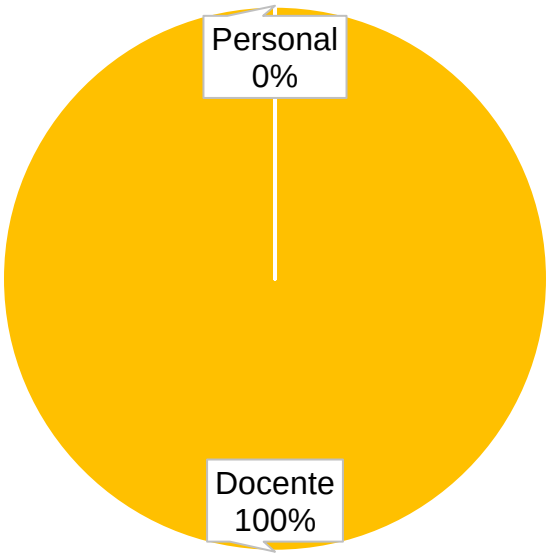
Destaca la participación representativa de los estudiantes de las coordinaciones de ingeniería y Diseño gráfico publicitario, arquitectura e Ingeniería en sistemas como segmentos de la población de estudio. La coordinación de ingeniería se compone de las carreras: Ing. Industrial, Ing. civil e Ing. agronómica con mención en agroindustrias. Los perfiles técnicos de todas estas carreras involucran el uso constate de TI en sus campos académicos y laborales, por lo que aportarán una opinión relevante en el resto de preguntas orientadas al análisis de los conceptos del modelo DiD. La distribución exacta de los estudiantes por coordinación se especifica en la siguiente tabla.

Tabla 6
Matriz de datos de gráfico 2

Coordinación	Recuento	Porcentaje
ARQ – DGP – SIST	8	18.60 %
CCEE	1	2.33 %
ING	34	79.07 %
Totales	43	100 %

Fuente: Elaboración propia del autor

Figura No. 5
Distribución de personal docente y administrativo



Fuente: Elaboración propia del autor

En cuanto a la encuesta aplicada a docentes y personal administrativo, el 100% de los encuestados se identificaron como docentes de la institución. Por razones ajenas al investigador, el personal administrativo no participó del proceso investigativo.

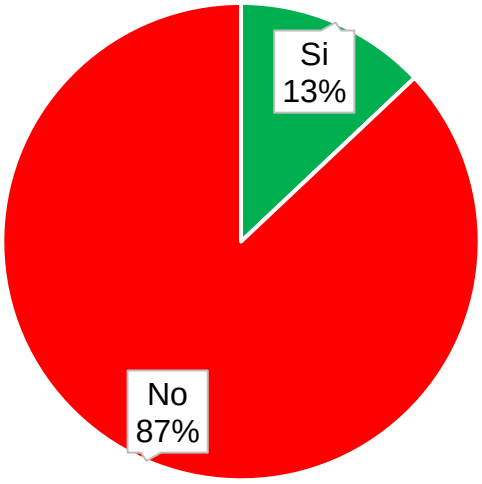
Tabla 7
Matriz de datos de gráfico 3

Variable	Recuento	Porcentaje
Docentes	11	100 %
Personal administrativo	0	0%
Totales	11	100 %

Fuente: Elaboración propia del autor

4.2.2 Capacitación

Figura No. 6
Encuestados que han recibido capacitación



Fuente: Elaboración propia del autor

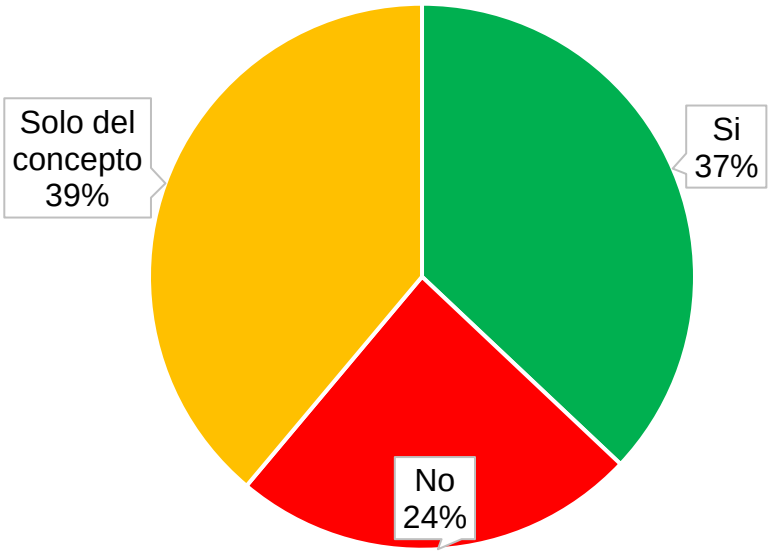
En conjunto, el 87% de los encuestados indicó no haber recibido capacitación para correcto uso de equipos informáticos, esto refleja un gran contraste con respecto al número de participantes que aseguraron conocer las implicaciones del concepto de ciberseguridad, esto podría implicar que han adquirido dichos conocimientos de forma empírica o mediante autoaprendizaje. De manera individual, el 12% de los estudiantes (todos ellos estudiantes de la coordinación de ingeniería) y el 18% de los docentes indicaron haber recibido algún tipo de capacitación, por tanto, el 88% de estudiantes y 82% de docentes restantes indicaron no haber recibido ningún tipo de capacitación.

Tabla 8
Matriz de datos de gráfico 4

Respuesta	Estudiantes	Docentes	Recuento	Porcentaje
Si	5	2	7	12.96 %
No	38	9	47	87.04 %
Totales	43	11	54	100 %

Fuente: Elaboración propia del autor

Figura No. 7
Conocimientos básicos en materia de ciberseguridad de los encuestados



Fuente: Elaboración propia del autor

En conjunto, el 75% de los encuestados indicaron tener conocimientos del concepto de ciberseguridad, pero solamente el 37% conocen sus implicaciones. De manera segmentada, el 90% de los docentes y el 72% de los alumnos indicaron conocer sólo el concepto, mientras que el 32% de los estudiantes y el 54% de los docentes conocen sus implicaciones.

El número tan elevado de estudiantes con desconocimientos puede deberse a un factor no medido dentro de las variables del perímetro demográfico: el año de estudio que cursa. De acuerdo con lo dicho por Msc. Aguinaga, la información proporcionada en materia de ciberseguridad se ha dado a conocer en talleres de inducción a inicio de ciclo, en donde, de acuerdo al calendario académico, el inicio de ciclo corresponde a la apertura de un nuevo año lectivo, mientras que los talleres de inducción, son impartidos sólo a los primeros años de todas las carreras. Otro de los factores que inciden en tan alto número de estudiantes desinformados, es la ausencia de planes de capacitación que se encuentran en fase de revisión y aprobación por diversos factores ya explicados en el acápite 4.1.8.

La distribución exacta de participantes para este ítem se encuentra detallada en la siguiente tabla.

Tabla 9
Matriz de datos de gráfico 5

Respuesta	Estudiantes	Docentes	Recuento	Porcentaje
Si	14	6	20	37.04 %
No	12	1	13	24.07 %
Del concepto	17	4	21	38.89 %
Totales	43	11	54	100 %

Fuente: Elaboración propia del autor

En la siguiente tabla, se expresa una correlación entre las coordinaciones y el número de respuestas marcadas para cada ítem.

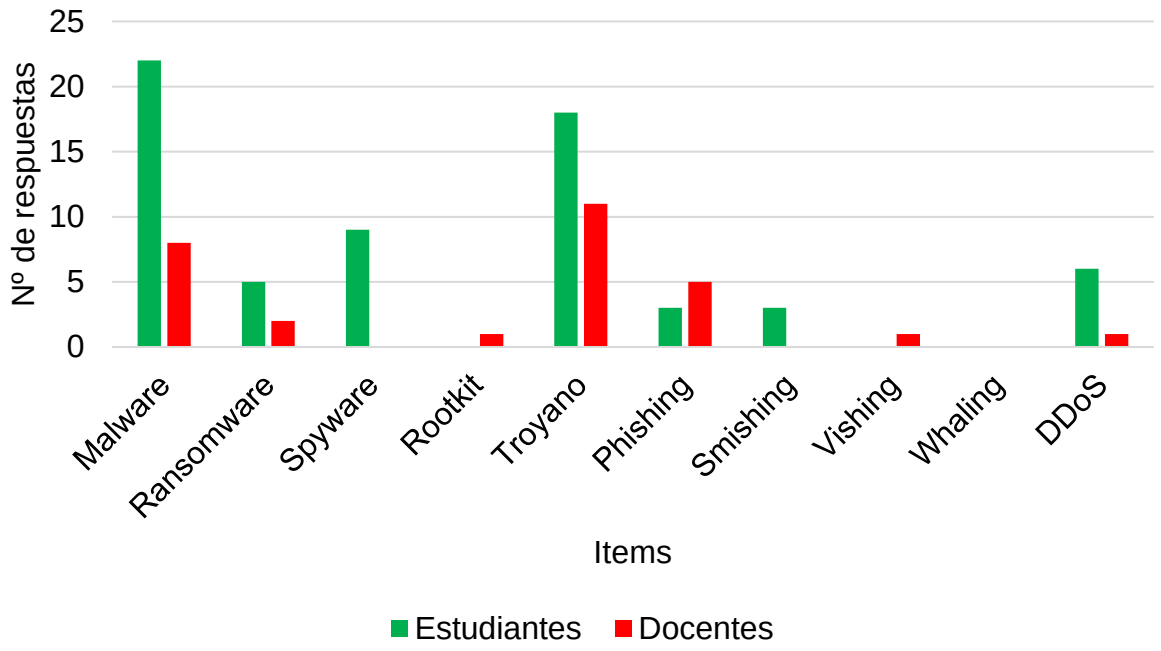
Tabla 10
Correlación entre los estudiantes de las coordinaciones y su grado específico de conocimiento en materia de ciberseguridad

Respuesta	ARQ – DGP – SIST	CCEE	ING	Recuento
Si	2	1	11	14
No	2	0	10	12
Del concepto	4	0	13	17
Totales	8	1	34	43

Fuente: Elaboración propia del autor

De la tabla anterior se puede inferir que: la coordinación de ciencias económicas posee el mayor número de estudiantes bien informados en materia de ciberseguridad (1/1 estudiante), seguida de la coordinación de ingeniería con el 32% de los encuestados (11/34 estudiantes), finalizando con la coordinación de arquitectura, diseño gráfico e ingeniería de sistemas con el 25% de los encuestados (2/8 encuestados).

Figura No. 8
Conocimiento de los encuestados de las amenazas más conocidas en ciberseguridad



Fuente: Elaboración propia del autor

Tabla 11
Matriz de datos de gráfico 6

Ítem	Estudiantes	Docentes	Recuento
Malware	22	8	30
Ransomware	5	2	7
Spyware	9	N/A	9
Rootkit	0	1	1
Troyano	18	11	29
Phishing	3	5	8
Smishing	3	0	3
Vishing	0	1	1
Whaling	0	0	0
DDoS	6	1	7

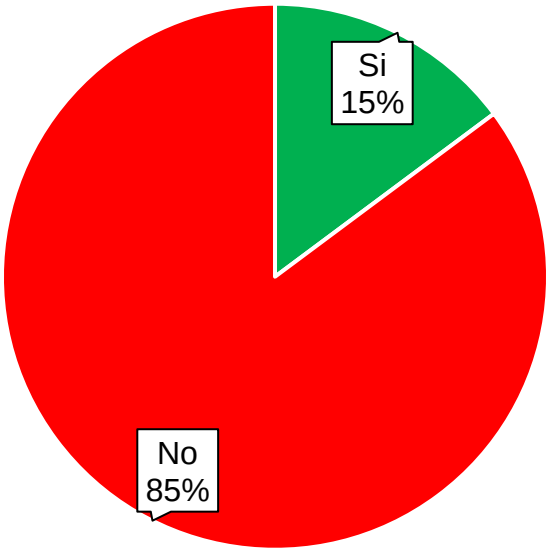
Fuente: Elaboración propia del autor

La información de la tabla anterior refleja que los términos más conocidos son Malware y Troyano, ambas variantes de virus informáticos de moderado grado de amenaza. En cuanto a las técnicas de ingeniería social, el Phishing y el Smishing resaltan como las más conocidas.

Al promediar el número de respuestas obtenidas basado en el tamaño de la muestra, se obtiene como resultado que el 18% de los encuestados conocen al menos un tipo de amenaza de ciberseguridad de las que se encuentran enlistadas, esto contrasta con el 37% de participantes que indicaron conocer las implicaciones de la ciberseguridad y su concepto. No obstante, si tomamos como referencia la respuesta con mayor número de aciertos, obtenemos que el 55% de los encuestados tienen conocimientos de la misma. De cualquier modo, estos índices de desconocimiento resultan alarmantes y constituyen una grave amenaza de ciberseguridad para el uso de equipos informáticos institucionales y los propios usuarios, ya que estas estrategias están diseñadas para extraer información de cualquier índole, dado que los virus informáticos no se encuentran programados para clasificar la información según la pertinencia de su contenido, sino que tienen por objeto el hurto, daño o encriptación de los datos y sus dispositivos.

Continuando con el análisis, ningún encuestado indicó conocer la técnica de ingeniería social denominada Whaling, una variante más sofisticada del phishing que consiste en la suplantación de identidad para generar confianza dentro de las altas cadenas de mando y así obtener cantidades masivas de información sensible como los números de cuentas bancarias asociadas a cada uno de los colaboradores en nómina de una organización. De igual manera, resulta preocupante que la mayoría de encuestados desconozcan que el phishing es la técnica de ingeniería social más común de engaño empleada por los ciberdelincuentes, lo que podría facilitar la propagación e infección de los dispositivos conectados en red de un software con código malicioso que se valga de este método.

Figura No. 9
Identificación de un ataque de ciberseguridad



Fuente: Elaboración propia del autor

Al consultar a los participantes si habían notado la presencia de algún correo electrónico en su carpeta de spam que parecía provenir de una fuente fiable en alguna de las redes de UCC sede León, el 85% de los encuestados indicaron no haber identificado ningún correo electrónico con dichas características. De forma particular, los docentes registraron el menor número de casos posibles para esta pregunta con una sola respuesta, equivalente al 9% de su segmento, mientras que 7 estudiantes, equivalentes al 16% de su segmento y 14% de los encuestados totales indicaron haber identificado un correo electrónico con estas características.

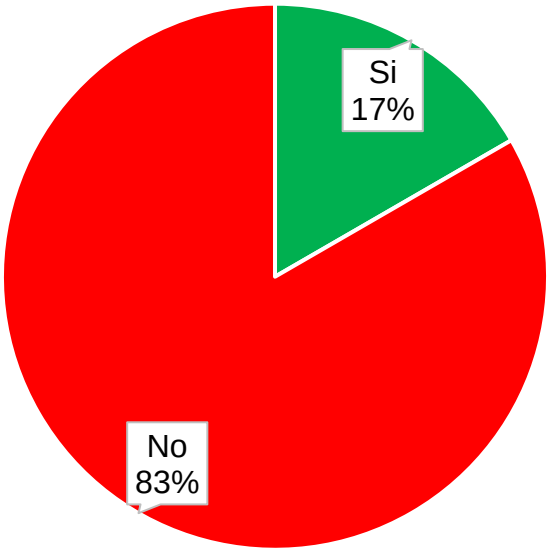
Tabla 12
Matriz de datos de gráfico 7

Respuesta	Estudiantes	Docentes	Recuento	Porcentaje
Si	7	1	8	14.81 %
No	36	10	46	83.72 %
Totales	43	11	54	100 %

Fuente: Elaboración propia del autor

4.2.3 Políticas y procedimientos

Figura No. 10
Conocimiento de los encuestados acerca de la localidad y existencia de la coordinación de ciberseguridad



Fuente: Elaboración propia del autor

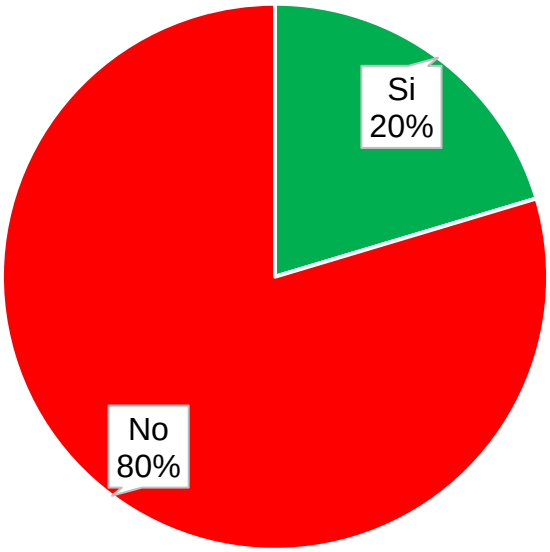
Del total de encuestados, el 83% indicó no conocer la ubicación de la coordinación de ciberseguridad de campus León. De manera individual, el 91% de los estudiantes y el 55% de los docentes marcaron no como respuesta a esta pregunta, mientras que el 9% de los estudiantes (todos ellos pertenecientes a la coordinación de ingeniería) y el 45% de los docentes indicaron si conocer su ubicación. Durante el ejercicio de la observación participativa, se constató que el área no está rotulada, lo que podría incidir de forma significativa en el alto índice de desinformación reflejado en esta pregunta.

Tabla 13
Matriz de datos de gráfico 8

Respuesta	Estudiantes	Docentes	Recuento	Porcentaje
Si	4	5	9	16.67 %
No	39	6	45	83.33 %
Totales	43	11	54	100 %

Fuente: Elaboración propia del autor

Figura No. 11
Conocimiento de los encuestados del responsable de ciberseguridad



Fuente: Elaboración propia del autor

Del total de encuestados, el 80% indicó no haber identificado al personal responsable de brindarle asistencia ante situaciones de emergencia en materia de ciberseguridad, la distribución por segmentos está dada de la siguiente forma: 16% de los estudiantes (5 de la coordinación de ingeniería, 1 de la coordinación de ciencias económicas y 1 de la coordinación de arquitectura, diseño gráfico e ingeniería en sistemas) y 36% de los docentes respondieron afirmativamente a esta pregunta. En este contexto particular, el alto índice de desinformación estudiantil representa una grave amenaza a la seguridad institucional, pues aun cuando el estudiante sea capaz de reconocer un ataque, riesgo, amenaza o vulnerabilidad, no sabrá a quien reportarlo.

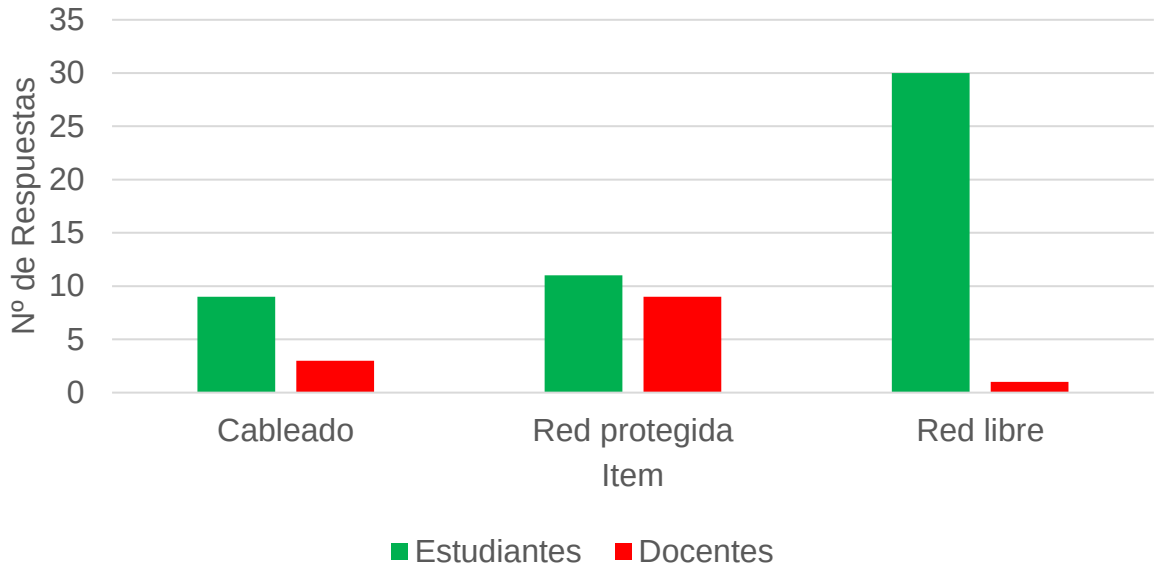
Tabla 14
Matriz de datos de gráfico 9

Respuesta	Estudiantes	Docentes	Recuento	Porcentaje
Si	7	4	11	20.37 %
No	36	7	43	79.63 %
Totales	43	11	54	100 %

Fuente: Elaboración propia del autor

4.2.4 Red

Figura No. 12
Métodos de acceso a la red usados por los usuarios



Fuente: Elaboración propia del autor

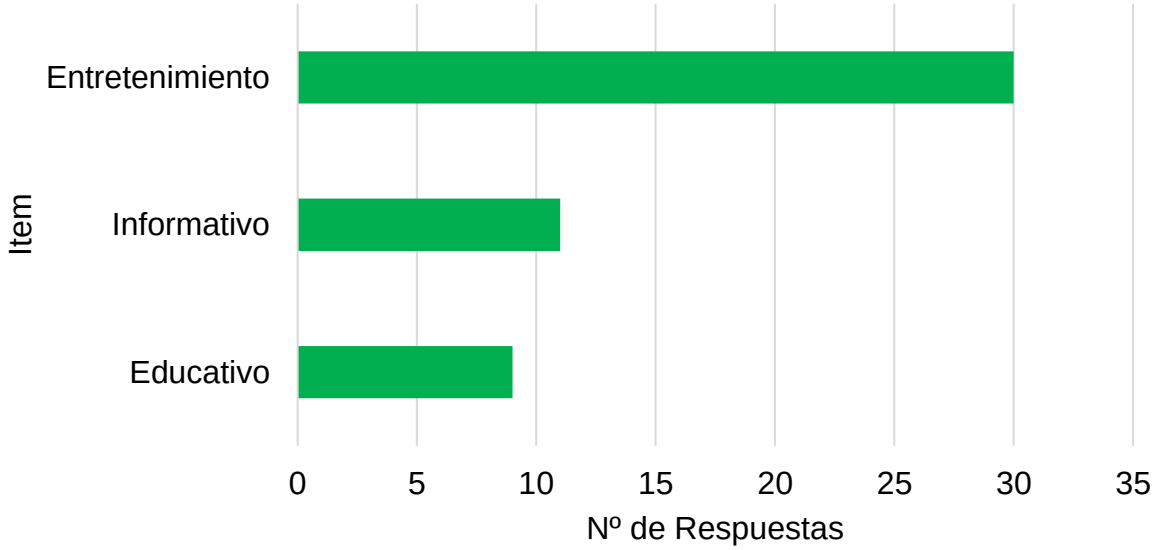
Tabla 15
Matriz de datos de gráfico 10

Respuesta	Estudiantes	Docentes	Recuento
Cableado	9	3	12
Red libre	30	1	20
Red protegida	11	9	31

Fuente: Elaboración propia del autor

La información presente en la tabla anterior indica que al menos 7 individuos se conectan por más de un medio a la intranet de sede León, asimismo, existen dos escenarios posibles en los que estos datos pueden ser considerado como válidos: intrusión a las redes protegidas o fuga no intencionada de información. Las redes protegidas por cifrado y contraseña son exclusivas para uso del personal docente y administrativo, por lo que un estudiante de cualquier coordinación no debería poder tener acceso a la intranet del campus a través de dicho medio de conexión.

Figura No. 13
Propósito de uso de las redes institucionales de los estudiantes



Fuente: Elaboración propia del autor

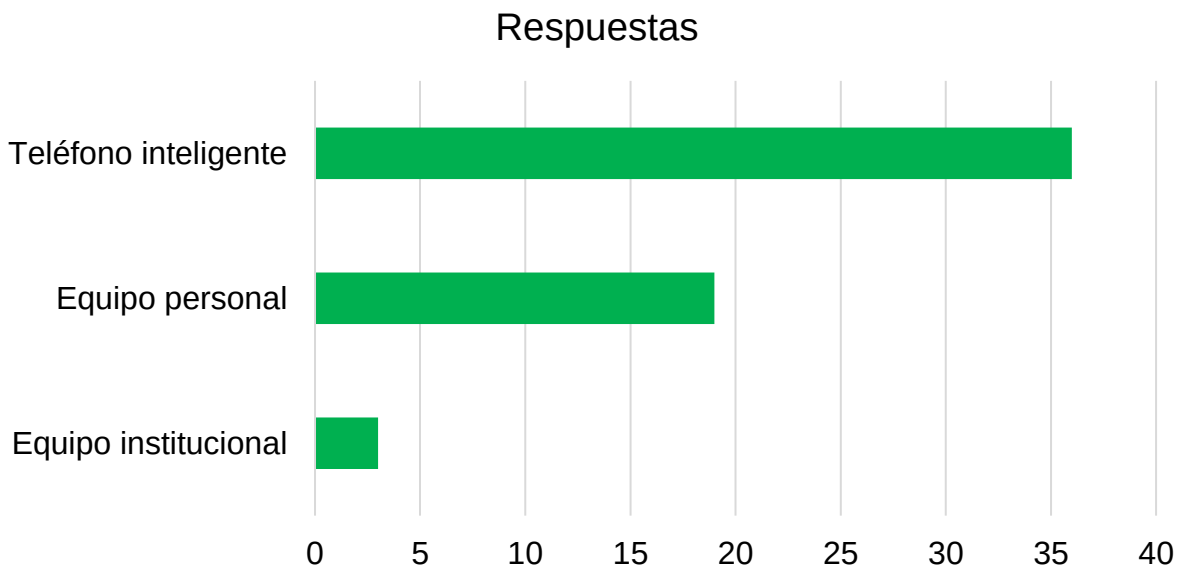
Tabla 16
Matriz de datos de gráfico 11

Respuesta	Estudiantes
Educativo	9
Entretenimiento	30
Informativo	11

Fuente: Elaboración propia del autor

La información presente en la tabla anterior indica que al menos 7 estudiantes utilizan la red con más de un propósito. El mayor número de respuestas está dado por los estudiantes que utilizan la red con fines de entretenimiento, en ese sentido, se requiere de la inclusión de nuevas variables que permitan identificar el nivel de amenaza que esto representa para la institución, ya que la visita a ciertas páginas con certificados de seguridad como YouTube no representarían un riesgo potencial de infección de malware o ataque de red.

Figura No. 14
Equipos informáticos mediante los cuales los estudiantes acceden a la intranet



Fuente: Elaboración propia del autor

Tabla 17
Matriz de datos de gráfico 12

Respuesta	Estudiantes
Equipo institucional	3
Equipo personal	19
Teléfono inteligente	36

Fuente: Elaboración propia del autor

A partir de la información anterior se pude inferir que al menos 15 usuarios acceden a las redes de UCC León haciendo uso de más de un tipo de dispositivo informático. Del mismo modo en que se especificó en el gráfico No.11, este comportamiento de los usuarios por sí mismo no representan un alto nivel de amenaza, a menos que generen perturbaciones en la red que disparen los mecanismos de seguridad basados en el monitoreo de información y tráfico de datos, sin embargo, si establecen un precedente a considerar: el tráfico de red producido por lo estudiantes no se encuentra regulado, normado o controlado.

En cuanto al resto de preguntas relacionadas con el resto de capas del modelo DiD cabe señalar que:

- El 100% de los docentes nunca han compartido sus credenciales de inicio de sesión.
- El 23% de los estudiantes si han compartido sus credenciales de inicio de sesión de correos electrónicos o de acceso a la plataforma institucional de UCC Virtual.
- El 67% de los estudiantes si practican medidas de autoprotección como la autenticación de dos pasos.
- El 63% de los estudiantes ha permitido el acceso vinculado a sus cuentas de correo electrónico u otra red social con el objetivo de acceder a contenido exclusivo en páginas de baja fiabilidad.
- Los sistemas operativos que tienen mayor presencia en las redes institucionales son distribuciones basadas en arquitectura Windows o Android.
- La mayoría de los sistemas operativos usados por personal docente si ejecuta Windows 10, tal como indicaba el Ing. Renzo Calderón en su entrevista.
- Tanto docente como estudiantes, renuevan su contraseña de acceso a sistemas institucionales, correos electrónicos y redes sociales con muy frecuencia, siendo las opciones más marcadas nunca (en ambos segmentos de la muestra), 1 vez cada trimestre (marcada mayormente por docentes) y 1 vez al año (marcada mayormente por alumnos).
- Más de un 30% de los encuestados indicaron poseer una contraseña segura. En el caso de los docentes, el 45% indicó poseer contraseñas débiles en base a los criterios mínimo de seguridad establecidos, mientras que 39% de los estudiantes indicaron poseer una contraseña con buen grado de seguridad. Estos datos corresponden a su segunda opción más marcada.

4.3 Análisis FODA

FORTALEZAS	OPORTUNIDADES DE MEJORA
• Propuesta de un sistema de gestión de seguridad basado en estándares internacionales (Norma ISO 27001). • Redes segmentadas. • Redes protegidas por contraseñas. • Redes protegidas por firewall. • Respaldos periódicos de información. • Equipos protegidos con antivirus. • Los equipos cuentan con sistemas operativos relativamente modernos y actualizados. • Equipos protegidos ante cambios abruptos de voltaje. • Módulos de autenticación de acceso a sistemas institucionales. • Todos los colaboradores poseen cuenta institucional.	• Infraestructura de red mejorable. • Cifrado de contraseñas mejorable. • Oportunidad de migración a sistemas operativos más modernos. • Oportunidad de implementación de arquitectura de nube. • Promoción, difusión y publicación de las políticas de ciberseguridad. • Programas de capacitación en todas las áreas institucionales. • Fichas de procesos mejorables.
DEBILIDADES	**AMENAZAS**
• Segmentos de red desprotegidos. • Poca frecuencia de actualización de sistemas operativos institucionales. • Cifrado débil en las claves de acceso de los puntos de red. • La comunidad educativa posee poca información al respecto. • Las políticas de ciberseguridad no se encuentran visibles.	• Siempre existen amenazas internas a considerar en temas relativos a la ciberseguridad. • La poca información que posee la comunidad educativa constituye una fuerte amenaza para la institución. • El cifrado actual de las contraseñas es vulnerable a intrusiones en la red.

CAPITULO V: CONCLUSIONES Y FUTURAS LÍNEAS DE INVESTIGACIÓN

5.1 Conclusiones

Se identificaron dos actores directos de implementar estrategias de ciberseguridad en sede León. Se identificaron los principales factores que incidencia en el desarrollo e implementación de estas estrategias, destacando como principales factores.

- Carga de trabajo de los responsables de área.
- Asignación de recursos disponibles para la implementación de las estrategias.
- Autorización transversal de las metodologías y políticas de acción.

Se aplicó la matriz de análisis FODA con base al estado de las estrategias que se implementan actualmente en sede León, destacando como mayor fortaleza la propuesta de un sistema de gestión normado, de la misma manera, se destaca como mayor debilidad la poca información que posee la comunidad educativa en materia de conceptos de ciberseguridad.

Se realizó el análisis situacional de los procesos y políticas existentes en los departamentos TIC de sede León, concluyendo que, por motivos de exclusión de muestra, solo se tuvo acceso a los planes de trabajo y fichas de procesos del área de soporte técnico, la cual goza de cierta autonomía en relación a las demás áreas del departamento TIC.

Se niega la hipótesis planteada en el acápite 1.6 de esta investigación. Las estrategias de ciberseguridad existentes si garantizan en cierta medida la integridad de los datos, pero no aseguran el empoderamiento de la información a la comunidad educativa, ya que muchas de las políticas que rigen estas estrategias se encuentran en proceso de aprobación o revisión.

En lo que respecta a las preguntas de investigación, la relevancia de este estudio radica en su carácter exploratorio, ya que previo a la realización de esta investigación, no existían estudios relacionados con el ámbito de la ciberseguridad institucional dentro de los repositorios locales o nacionales.

Las estrategias existentes sí podrían ser efectiva contra ciertos escenarios que plantean vulnerabilidades de seguridad de la información.

La comunidad educativa goza de ciertos conocimientos de autoprotección en materia de ciberseguridad como la autenticación de dos pasos, no obstante, existen múltiples factores de riesgo a los que la comunidad educativa se encuentra expuesto por el limitado conocimiento que poseen en esta materia.

5.2 Futuras Líneas De Investigación

Políticas de gestión ante amenazas conocidas. La coordinación de ciberseguridad debe documentar las políticas de gestión de seguridad y protocolos de acción a aplicarse en caso de identificar ciberataques o intento de ciberataques a través de métodos conocidos, por tanto, se requiere de un estudio que identifique, detalle y categorice estas amenazas, proporcionando además las medidas de mitigación y contingencias necesarias que permitan establecer las bases de la política de ciberseguridad de la coordinación.

Evaluación de la efectividad de las medidas de seguridad existentes. El presente estudio pretendía detallar las estrategias de ciberseguridad existente en un contexto teórico. Se requiere de un estudio que evalué de forma práctica y experimental la efectividad de las mismas a través de escenarios de simulaciones controladas.

Migración de los sistemas de información a la nube. Considerando que una arquitectura de red basada en servidores (como la que opera actualmente en UCC) incurre en altos costos operativos debido a la gran cantidad de recursos hardware y software que estos requieren para su óptimo funcionamiento, se propone la realización de un estudio de viabilidad para la implementación o migración de un sistema de gestión de información basado en la arquitectura de nube.

CAPITULO VI: RECOMENDACIONES

- Iniciar con el plan de capacitación a la comunidad educativa a la brevedad posible, dado el alarmante índice de desinformación reflejado por las encuestas.
- Programar auditorias en las áreas TIC de todas las sedes en búsqueda de vulnerabilidades de ciberseguridad.
- Incorporar dentro del organigrama institucional a la coordinación de ciberseguridad.
- Establecer un programa de pasantías a estudiantes internos o externos que permita una mejor distribución en la carga de trabajo de las áreas TIC dados el reciente número de dimisiones.
- Centralizar la operación del departamento de ciberseguridad o en su defecto, conceder privilegios de autonomía y súper administrador con el objetivo de poder brindar asistencia a áreas afectadas por ciberataques cuando sea requerido.
- Renovar periódicamente las contraseñas de los enrutadores que poseen puntos de acceso cifrado.
- Implementar un portal cautivo para las redes de uso estudiantil, o en su defecto, implementar restricciones de acceso a contenido basado en el tráfico y filtrado de lista blanca de dominios de internet.
- Monitorear permanente las redes institucionales a fin de poder prevenir o detener ataques de ciberseguridad que tengan lugar en tiempo real.
- Instalar actualizaciones periódicas de los parches de seguridad en todos los dispositivos informáticos de uso institucional para evitar vulnerabilidades de día cero.

REFERENCIAS BIBLIOGRÁFICAS

, Iván; , Orlando;. (s.f.). *Repositorio Institucional, Universidad Técnica de Cotopaxi.* Obtenido de http://repositorio.utc.edu.ec/handle/27000/5323

Alvarado, O. & Changoluisa, I. (2019). *"ANÁLISIS DE LA CIBERSEGURIDAD A LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI".* "Proyecto de Investigación para optar al titulo de Ingeniería Informática¨, Latacunga, Ecuador. Recuperado el 10 de Febrero de 2023, de http://repositorio.utc.edu.ec/handle/27000/5323

AMCHAM. (8 de Octubre de 2020). *amcham.org.ni*. Obtenido de https://www.amcham.org.ni/recientes-propuestas-de-leyes-en-nicaragua/

Asamblea. (s.f.). *Constitución Politica*. Recuperado el 19 de Marzo de 2023

Asamblea Nacional de la República de Nicaragua. (s.f.). Recuperado el 21 de Marzo de 2023, de Ley No 845 Ley de Telecomunicaciones: https://www.asamblea.gob.ni/actos-legislativos/ley-no-845-ley-de-telecomunicaciones/

Asamblea Nacional de la República de Nicaragua. (21 de Marzo de 2012). *Normas Jurídicas de Nicaragua*. Recuperado el 20 de Abril de 2023, de http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/e5d37e9b4827fc06062579ed0076ce1d

Asamblea Nacional de la República de Nicaragua. (27 de Octubre de 2020). *Normas Jurídicas de Nicaragua*. Recuperado el 01 de Mayo de 2023, de http://legislacion.asamblea.gob.ni/normaweb.nsf/($All)/803E7C7FBCF44D7706258611007C6D87#:~:text=Quien%20a%20sabiendas%20que%20un,a%20cuatro%20a%C3%B1os%20de%20prisi%C3%B3n.

Asamblea Nacional de la República de Nicaragua, Gaceta. (21 de Marzo de 2023). Obtenido de Ley No. 787, Ley de Protección de Datos Personales:

http://legislacion.asamblea.gob.ni/Normaweb.nsf/($All)/40EA25DB712AA86D06257A3F006F8D9F?OpenDocument

Asamblea Nacional de la República de Nicaragua. (2012). Recuperado el 22 de Marzo de 2023, de Ley No. 787, Ley de Protección de Datos Personales.: https://www.asamblea.gob.ni/actos-legislativos/ley-no-787-ley-de-proteccion-de-datos-personales/

Asamblea Nacional de la República de Nicaragua. (2015). Recuperado el 21 de Marzo de 2023, de Ley Especial de Ciberdelitos, Ley No. 1042.: http://legislacion.asamblea.gob.ni/normaweb.nsf/($All)/21F1873C39EAF7F106257E9300647179?OpenDocument

Asamblea Nacional de Nicaragua. (s.f.). Recuperado el 21 de Marzo de 2023, de Ley 977 de Delitos Informáticos.: http://legislacion.asamblea.gob.ni/Normaweb.nsf/($All)/AB8295D5FED88A7806257C9E006BB66A?OpenDocument&Highlight=0,ley,977

Astudillo, K. (2021). *Hacking Ético 101: Cómo hackear profesionalmente en 21 días o menos.*

Barcos, M. C. (Abril de 2016). *Scielo.sld.cu.* Obtenido de http://scielo.sld.cu/pdf/rus/v8n1/rus20116.pdf

Camino, E & Puente, E.;. (2020). *ANÁLISIS Y EVALUACIÓN DE LA SEGURIDAD EN LA RED DE LA UNIDAD EDUCATIVA SALESIANA CARDENAL SPELLMAN,.* Tesis de Titulo de Grado, Universidad de Salesiana , Quito. Recuperado el 29 de marzo de 2023

Camino, Edison; Puente, Edwin;. (s.f.). ANÁLISIS Y EVALUACIÓN DE LA SEGURIDAD EN LA RED DE LA UNIDAD EDUCATIVA SALESIANA CARDENAL SPELLMAN,UTILIZANDO HERRAMIENTAS DE INGENIERÍA SOCIAL, YRECOMENDAR MEDIDAS PREVENTIVAS.

Carrillo, J. J. (Diciembre de 2018). Google Académico. *Revista Ibérica de Sistemas e Tecnologias de Informacion* , 438-448. Obtenido de

https://media.proquest.com/media/hms/PFT/1/Pc6LC?_s=52SuKqhrn0nWuouhYRBT1xenjeQ%3D

Chiticariu, L.& Radu, C.;. (2014). *Análisis de tráfico en redes: Uso y aplicación de herramientas para examinar el tráfico de red.*

Constitución Politica Asamblea de Nicargua. (2012). *Normas Jurídicas de Nicaragua*. Recuperado el 30 de Marzo de 2023, de http://legislacion.asamblea.gob.ni/normaweb.nsf/b92aaea87dac762406257265005d21f7/7bf684022fc4a2b406257ab70059d10f?OpenDocument

Enciclopedia Online.com. (s.f.). Recuperado el 19 de Marzo de 2023, de https://enciclopediaonline.com/es/estado-del-arte/

Fernandez S. (2016). *ISO 27001: Análisis y gestión de riesgos de la información. Editorial: RA-MA.*

García Córdoba, F. (2004). *El cuestionario: Recomendaciones metodológicas para el diseño de un cuestionario.* México D.F., México: Limusa.

Green Globe. (s.f.). *Green Globe Sostenibilidad y proyectos ambientales.* Recuperado el Mayo de 10 de 2023, de https://www.greenglobe.es/los-objetivos-desarrollo-sostenible-ods-la-agenda-2030/#

Guevara Betanco, E. M., Hernández León, E. R., & López Pérez, G. M. (2023). *Evaluación del nivel de seguridad de la red informática de la universidad de ciencias comerciales UCC campus León, para identificación y mitigación de riesgos. En un periodo comprendido de enero a junio 2023.* León, Nicaragua.

Hernández , R. Fernández , C., Baptista, M.;. (2010). Metodología de la Investigación. México, México: C.P. 01376, México D.F. Recuperado el 19 de Marzo de 2023, de https://drive.google.com/file/d/1OzAyRwb_hGWHFOuhs6iWpFv8bstIXLfs/view

Huamán R. (2008). *“Evaluación de la seguridad informática en el área de sistemas de la Municipalidad Distrital de Nuevo Chimbote”.* "Tesis para Optar a título de Ingenieria en Informática", Universidad San Pedro, Chimbote, Perú.

Recuperado el 10 de Febrero de 2023, de https://renati.sunedu.gob.pe/handle/sunedu/2693740

IBM. (s.f.). *¿QUE ES LA CIBERSEGURIDAD?* Recuperado el 19 de Marzo de 2023, de https://www.ibm.com/es-es/topics/cybersecurity

Joyanes Aguilar, L. (2012). *Computación en la Nube. Estrategias de Cloud Computing en lasEmpresas.* (Primera ed.). México, D.F., México: Alfaomega.

Kaspersky. (2021). *Ciberamenaza,Mapa en tiempo Real.* Recuperado el 15 de Marzo de 2023, de https://cybermap.kaspersky.com/es/stats#country=82&type=oas&period=m

Kennedy , D.;Gorman, J.&Aharoni, M.;. (2012). *Metasploit para Pentesters: Guía de uso y aplicaciones del framework Metasploit.*

LAWI. (2021). (D. y. © 2023 Plataforma Digital de Economía, Productor) Recuperado el 19 de Marzo de 2023, de Historia de la Ciberaeguridad: https://leyderecho.org/historia-de-la-ciberseguridad/

López M., A. F., & Acevedo Ibañéz, A. (2004). *El proceso de la entrevista: Conceptos y modelos* (Cuarta ed.). México: Limusa.

López-Chau, L. A. (2016). *Propagación de malware: propuesta de modelo.* Ciudad de México: Instituto Politécnico Nacional, Escuela Superior de Ingeniería Mecánica y Eléctrica.

Managua, Gaceta. (s.f.). Recuperado el 21 de Marzo de 2023, de Constitución Política de la República de Nicaragua.: https://www.asamblea.gob.ni/assets/constitucion.pdf

Mata, J. S. (2021). La seguridad informática en las Instituciones de Educación Superior. *TECTZAPIC*.

Mc, S., & Scambray J, K. G. (2012). *Hacking Exposed 7, Ntworl security secrets and solutions.*

Mieres E. (2015). *Virus Informáticos: Prevención, detección y eliminación.*

Montano Collazos, F. A. (2021). *Google Académico.* Obtenido de Tecnológico de Antioquia - Institución Universitaria: https://dspace.tdea.edu.co/handle/tdea/1402

NACIONES UNIDAS. (2023). Recuperado el 15 de Mayo de 2023, de Objetivos de Desarrollo Sostenible (ODS): https://www.cepal.org/es/temas/agenda-2030-desarrollo-sostenible/objetivos-desarrollo-sostenible-ods

Portantier, F. (2012). *Seguridad informática* (Primera ed.). Buenos Aires, Argentina: RedUSERS.

Repositorio SCIELO. (s.f.). Herramientas Fundamentales para el Hacking Ético. Recuperado el 19 de Marzo de 2023, de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1684-18592020000100116

Rodriguez, O & López , P. (2017). *"Diagnóstico de la gestión de la seguridad de la información en la División de informática en la empresa Comercial S.A para la implementación de un SGSI norma ISO 27001",.* "Tesis de Grado", Managua , Nicaragua. Recuperado el 10 de Febrero de 2023, de http://repositorio.uca.edu.sv/jspui/

Romero , M & Álava , J. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y ANÁLISIS DE VULNERABILIDADES.* Área de Innovación y Desarrollo. Recuperado el 19 de Marzo de 2023

Sánchez, R. (2007). *"Análisis de riesgos en seguridad informática caso UNSMS".* Universidad Nacional Mayor de San Marcos , Lima, Perú. Recuperado el 10 de Febrero de 2023, de https://renati.sunedu.gob.pe/handle/sunedu/2693740

Sant Leo University. (s.f.). *¿Cuál es la Historia de la Ciberseguridad?* Recuperado el 19 de Marzo de 2023, de https://worldcampus.saintleo.edu/noticias/historia-de-la-ciberseguridad

Servitux. (2023). *Servitux*. Recuperado el 20 de Abril de 2023, de https://www.servitux.es/2018/03/22/ponentes-de-seguridad-informatica-en-el-i-congreso-transformacion-digital-en-los-despachos-de-abogados/

Soriano, M. (s.f.). *Seguridad en redes y seguridad de la información .* Praga, República Checa: IMPROVET, České vysoké učení technické v Praze.

Universidad de Ciencias Comerciales. (23 de 05 de 2023). *UCC*. Obtenido de https://ucc.edu.ni/historia/page/2/

UNIVERSIDAD DE CIENCIAS COMERCIALES, U. (2016). *MODELO EDUCATIVO UCC.* MANAGUA: UCC.

Valencia-Duque, F. J. (01 de Mayo de 2017). Metodología para la implementación de un Sistema. *Revista Ibérica de Sistemas y Tecnologías de Información*, pág. 16.

ZAMBRANO, N. V. (2019). *CIBERSEGURIDAD Y SU APLICACIÓN EN LAS IES PUBLICAS DE MANABI.* Calceta, Ecuador.

ANEXOS O APENDICES

Anexo 1: Cuestionario de encuesta dirigido a docentes

A partir de la última década, el uso y desarrollo de aplicaciones con arquitectura de nube ha incrementado drásticamente. Esto ha despertado especial interés en todas las organizaciones a nivel mundial debido a los riesgos de ciberseguridad que ello conlleva. A través del presente formulario, se pretende identificar el grado de involucramiento de los colaboradores de UCC campus León en materia de estrategias de ciberseguridad implementadas por la propia institución.

1. Indique su genero.

   ○ Masculino. ○ Femenino.

2. ¿Qué rol desempeña en la institución?

   ○ Docente. ○ Personal administrativo.

3. ¿Tiene conocimientos del concepto de ciberseguridad y sus aplicaciones?

   ○ Si. ○ No. ○ Sólo del concepto.

4. ¿Conoce la ubicación del departamento de ciberseguridad en campus León?

   ○ Si. ○ No.

5. ¿Ha identificado al personal responsable de brindarle asistencia ante situaciones de emergencia en materia de ciberseguridad?

   ○ Si. ○ No.

6. ¿Ha sido capacitado, instruido o informado de directrices para el uso correcto de equipos informáticos en materia de ciberseguridad?

   ○ Si. ○ No.

7. Los ciberdelincuentes suelen emplear distintos métodos de ataque para tratar de extraer información de sus victimas. Algunos de estos métodos se basan en el engaño, no obstante, existen métodos más complejos que explotan las vulnerabilidades de los sistemas y los infectan con código malicioso. Indique cuál de los siguientes métodos conoce.

   ☐ Phishing. ☐ Smishing. ☐ Vishing. ☐ Whaling. ☐ DDoS.

   ☐ Malware. ☐ Rootkit. ☐ Troyano. ☐ Ransomware.

8. ¿Le ha sido asignada una cuenta de correo institucional?

   ○ Si. ○ No.

9. Una de las estrategias más comunes empleadas por los ciberdelincuentes es la que se conoce como ataque de fuerza bruta. Este método intenta descifrar las credenciales de acceso (id, nombre o contraseña) de un usuario mediante un proceso automatizado de prueba y error. Para que una contraseña se considere completamente segura debe cumplir con ciertos criterios: ser única e independiente para cada cuenta o servicio, y, contar con un mínimo de 10 caracteres alternando entre números, mayúsculas, minúsculas, y símbolos de forma aleatoria. Basado en la información anterior, ¿Cómo calificaría el nivel de seguridad de sus contraseñas?

   ○ Débil. ○ Buena. ○ Segura. ○ Muy segura.

10. ¿Posee acceso a alguno de los sistemas institucionales?

    ○ Si. ○ No.

11. En caso afirmativo a la pregunta anterior, ¿Con qué frecuencia renueva o solicita renovación de sus credenciales de acceso a los sistemas institucionales?

    ○ 1 vez al mes. ○ 1 vez al año.

    ○ 1 vez cada semestre. ○ 1 vez cada trimestre.

    ○ Nunca.

12. ¿Qué metodo utiliza para acceder a la red institucional en los equipos informáticos?

    ☐ Punto de red (cableado).

    ☐ Red Wifi - Sin contraseña.

    ☐ Red Wifi - Con contraseña.

13. ¿Ha experimentado algún incidente relacionado con ataques de ciberseguridad al hacer uso de la red institucional en el pasado? Por ejemplo: correos electrónicos en su carpeta de spam que parecen provenir de fuentes institucionales o fuentes personales confiables.

    ○ Si. ○ No.

14. En caso afirmativo a la pregunta anterior, Indique el grado de frecuencia con la que ocurrían estos acontecimientos.

○ Baja. ○ Regular. ○ Alta.

15. Indique la frecuencia con la que se actualizan los sistemas operativos de los equipos informáticos de uso institucional en su área.

○ No lo sé. ○ Nunca.

○ Al menos 1 vez al mes. ○ Al menos 1 vez cada semestre.

○ Al menos 1 vez al año. ○ Al menos 1 vez cada trimestre.

16. ¿Los ordenadores de su área poseen antivirus?

○ Si. ○ No.

17. ¿Los ordenadores de su área están protegidos con contraseña de inicio de sesión o control de usuario?

○ Si. ○ No.

18. ¿Qué sistema operativo utilizan los ordenadores de su área?

○ Windows XP. ○ Windows 8.

○ Windows 7. ○ Windows 11.

○ Windows 11.

19. ¿Alguna vez ha compartido sus credenciales de inicio de sesión (correos, usuarios, contraseñas) con otros colaboradores de la institución?

○ Si. ○ No.

Fuente: Elaboración propia del autor

Anexo 2: Cuestionario de encuesta dirigido a estudiantes del turno diurno

A partir de la última década, el uso y desarrollo de aplicaciones con arquitectura de nube ha incrementado drásticamente. Este tipo de arquitectura nos permite interactuar con cantidades masivas de información desde cualquier punto remoto con conexión abierta a internet, por lo anterior, la ciberseguridad es un tema que ha cobrado gran relevancia debido al creciente número de fraudes y ciberataques que suceden a diario a través de los distintos canales de información general. Por medio del presente formulario se pretende conocer el grado de involucramiento que poseen los estudiantes de UCC campus León en materia de estrategias de ciberseguridad.

1. Indique su género.
   ○ Masculino. ○ Femenino.
2. Indique la coordinación a la que pertenece su carrera.
   ○ ING. ○ CCEE. ○ ARQ - SIST - DGP.
3. ¿Tiene conocimientos del concepto de ciberseguridad y sus aplicaciones?
   ○ Si. ○ No. ○ Sólo del concepto.
4. ¿Conoce la ubicación del departamento de ciberseguridad en campus León?
   ○ Si. ○ No.
5. ¿Ha identificado al personal responsable de brindarle asistencia ante situaciones de emergencia en materia de ciberseguridad?
   ○ Si. ○ No.
6. ¿Ha sido capacitado, instruido o informado de directrices para el uso correcto de equipos informáticos en materia de ciberseguridad?
   ○ Si. ○ No.
7. Los ciberdelincuentes suelen emplear distintos métodos de ataques para tratar de extraer información de sus víctimas. Algunos de estos métodos se basan en el engaño, no obstante, existen métodos más complejos que explotan las vulnerabilidades de los sistemas informáticos o de los dispositivos conectados en red, infectándolos con código malicioso. Indique cuál de los siguientes métodos conoce.
   ☐ Malware. ☐ Spyware. ☐ Rootkits. ☐ Troyanos. ☐ Ransomware.
   ☐ Phishing. ☐ Smishing. ☐ Vishing. ☐ Whaling. ☐ DDoS.

8. Una de las estrategias más comunes empleadas por los ciberdelincuentes es la que se conoce como ataque de fuerza bruta. Este método intenta descifrar las credenciales de acceso (id, nombre o contraseña) de un usuario mediante un proceso automatizado de prueba y error. Para que una contraseña se considere completamente segura debe cumplir con ciertos criterios: ser única e independiente para cada cuenta o servicio (Ejemplo: La contraseña de su correo electrónico y la de su cuenta de Instagram son diferentes entre sí), y, contar con un mínimo de 10 caracteres alternando entre números, mayúsculas, minúsculas, y símbolos de forma aleatoria. Basado en la información anterior, ¿Cómo calificaría el nivel de seguridad de sus contraseñas?
   ○ Débil. ○ Buena. ○ Segura. ○ Muy segura.
9. ¿Con qué frecuencia renueva sus contraseñas?
   ○ 1 vez al mes. ○ 1 vez cada semestre. ○ Nunca.
   ○ 1 vez al alño. ○ 1 vez cada trimestre.
10. ¿Utiliza algún otro método de seguridad para la autenticación de sus credenciales? Ejemplo: Autenticación de dos pasos. (Donde se requiere de un código de inicio de sesión adicional al usuario y contraseña para validarla)
   ○ Si. ○ No.
11. ¿Alguna vez ha compartido sus credenciales de inicio de sesión (correos, usuarios contraseñas) con otro compañero en la institución?
   ○ ING. ○ CCEE. ○ ARQ - SIST - DGP.
12. En ocasiones, algunas páginas web con cierto grado de confiabilidad nos soliciten identificarnos como usuarios para poder acceder a su contenido ¿De qué manera realiza este procedimiento?
   ○ Manual: Relleno los datos de registro/inicio de sesión en un formulario.
   ○ Vinculado: Inicio sesión vinculando la página a mi cuenta de Google, Facebook, Twitter, etc.
   ○ Lo omito: No suelo registrarme en páginas.
13. ¿Qué metodo utiliza para acceder a la red institucional en los equipos informáticos?
   ☐ Punto de red (Cableado).
   ☐ Red Wifi - Sin contraseña.
   ☐ Red Wifi - Con contraseña.

14. ¿Ha experimentado o detectado algún incidente relacionado con ataques de ciberseguridad al hacer uso de la red institucional en el pasado? Por ejemplo: correos electrónicos en su carpeta de spam que parecen provenir de fuentes institucionales o fuentes personales confiables.
    ○ Si. ○ No.
15. En caso afirmativo a la pregunta interior, indique con que grado de frecuencia ocurrían estos acontecimientos.
    ○ Baja. ○ Regular. ○ Alta.
16. ¿Alguna vez ha instalado en su dispositivo un software/aplicación de dudosa reputación de forma deliberada o por desconocimiento haciendo uso de los recursos institucionales?
    ○ Si. ○ No.
17. ¿Qué contenido suele buscar mientras navega en las redes institucionales?.
    ☐ Educativo: Repositorios de información, revistas/artículos científicos.
    ☐ Informativo: Portales de noticias, foros, blogs, wikis.
    ☐ Entretenimiento: Redes sociales, música, videojuegos.
    ☐ Otros.
18. ¿A través de que tipo de dispositivos informáticos suele conectarse a las redes institucionales?
    ☐ Ordenador institucional.
    ☐ Ordenador personal.
    ☐ Teléfono inteligente.
19. ¿En que arquitectura de sistema/distribución se basa el sistema operativo de los dispositivos con los cuales accede a las redes institucionales?
    ☐ Windows.
    ☐ Linux.
    ☐ MacOs.
    ☐ Android.
    ☐ iOs.
    ☐ Otro.

Fuente: Elaboración propia del autor

Anexo 3: Entrevista realizada a coordinadora de ciberseguridad.

Entrevista realizada a Msc. Martha Elizabeth Aguinaga el día 22 de junio del año 2023, docente colaboradora de sede León desde el año 2017, actual coordinadora del departamento de ciberseguridad en campus León. Las abreviaturas corresponden a:

KP = Kelvin Pineda (Entrevistador). **MA** = Martha Aguinaga (Entrevistado).

KP: Buenas tardes, soy el Ing. Kelvin Pineda, docente fijo adscrito a la coordinación de ARQ – DGP – SIST. Actualmente estoy llevando a cabo una investigación en materia de ciberseguridad en campus León. Me han indicado que usted es la coordinadora del departamento de ciberseguridad en sede León. ¿Es correcto?

MA: Si. ¿En qué puedo ayudarle?

KP: Perfecto, la investigación que estoy realizando tiene por objeto identificar los actores y factores que inciden en la implementación de estrategias de ciberseguridad en la intranet del campus, por lo que he preparado una entrevista semiestructurada con 10 preguntas que me ayudarán a alcanzar este objetivo, sin embargo, dicho número podría incrementar en la medida en la que sus respuestas den lugar a otras preguntas de interés para el contexto de la investigación.

MA: Entiendo. Le proporcionaré toda la información que esté a mi alcance.

KP: Se lo agradezco. Antes de profundizar a cabalidad sobre las estrategias implementadas en torno a los ejes de la ciberseguridad, me gustaría conocer un poco más acerca de su coordinación. ¿De qué manera surge este departamento? ¿Qué motivó a su creación?

MA: Es una coordinación relativamente nueva, surge como una propuesta de rectoría general de UCC, en respuesta a la necesidad de garantizar la confidencialidad de los datos y la seguridad de la información, así mismo, surge como reconocimiento a las potencialidades de los colaboradores en el área de las tecnologías de información. Como campus León, somos la única sede a nivel institucional que cuenta con una coordinación especializada en dicha área.

KP: ¿Cuánto tiempo tomó materializar la idea? Es decir, ¿Es una coordinación debidamente constituida al día de hoy con reglamento interno y roles definidos? ¿En qué nivel del esquema organizacional se encuentra ubicado? ¿Es completamente independiente de otras áreas?

MA: Como idea, surge en julio del 2022, como coordinación, se encuentra operativo desde octubre del 2022. En cuanto a su jerarquía, se rige por las directrices establecidas por la Dirección de Tecnologías de la Información y Comunicación de sede central Managua a cargo de MBa. Ulises Rivera. En el organigrama de sede León, se encuentra ubicado en el mismo nivel que los departamentos de Sistemas y Soporte Técnico, aunque en su conjunto conforman el departamento de Tecnologías de la Información y Comunicación, son áreas independientes entre sí y con roles establecidos.

KP: Anterior a la creación del departamento, ¿existían protocolos de acción o medidas de mitigación frente a los ciberataques?

MA: No. Desde sus propias competencias, los departamentos de Sistemas y Soporte Técnico han establecido configuraciones básicas que funcionan en cierto modo como medidas de contingencia, pero no existían protocolos o estrategias de mitigación.

KP: ¿Cuáles han sido los mayores logros del departamento de ciberseguridad desde su creación hasta el día de hoy?

MA: Destaco 3. El mayor logro corresponde a la elaboración de una propuesta de implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma internacional ISO/IEC 27001, como segundo logro, destacó el análisis exhaustivo realizado a la intranet del campus y la actualización al diseño de la infraestructura basado en su topología de red, y por último, he coordinado con el departamento de soporte técnico la actualización de inventario de activos informáticos que posee sede León.

KP: ¿A qué obstáculos se ha enfrentado en calidad de coordinadora para el ejercicio pleno de sus funciones? ¿Cuáles considera que son los mayores retos del departamento?

MA: Han sido dos grandes obstáculos. Desde que el departamento se encuentra constituido, he asumido mayor carga horaria de docencia sumado a la coordinación de otras áreas de la institución debido al inesperado número de dimisiones que ha ocurrido en el personal docente y personal de los departamentos de las tecnologías de información en tiempos recientes, esto me ha impedido focalizarme en estrategias y metodologías de ciberseguridad que garanticen la integridad de la información en todos los niveles, por otra parte, existe carencia de equipo especializado que me ayude a identificar y diagnosticar con mayor eficiencia las vulnerabilidades, amenazas y factores de riesgos dentro de la intranet del campus León. En cuanto a los retos, considero que la planificación de actividades será uno de ellos, puesto que se ha planteado la posibilidad de que este departamento brinde asistencia permanente a nivel físico y remoto en el resto de sedes de la Universidad de Ciencias Comerciales.

KP: Un usuario bien informado, es un usuario menos vulnerable a ataques de ingeniería social, en este sentido ¿De qué manera planea instruir a la comunidad educativa de las implicaciones de la ciberseguridad?

MA: Planeo integrar a mi plan de actividades capacitaciones regulares servidas a modo de conferencias magistrales o estratificadas de acuerdo al nivel de amenaza interna que representen los usuarios. Abordaré las buenas prácticas para el manejo de la información, el reconocimiento de amenazas y riesgos, tipos de ataques y tipos de hackers a los que se exponen como usuario de una red pública o privada. Por ahora, estos temas se presentan solo en talleres de inducción en cada inicio de ciclo.

KP: Entrando en temáticas más específicas de la ciberseguridad, ¿Existen protocolos establecidos o estrategias de defensa que permitan detectar, detener y mitigar un ciberataque? ¿Emplea mecanismos como la criptografía, bloqueo de tráfico basado en lista blanca o acceso controlado para disminuir estos riesgos de intrusión?

MA: Actualmente no. En el mediano plazo se pretende implementar un sistema de control de acceso a usuarios, portal cautivo, monitoreo y filtrado de red, mejora a la infraestructura de los puntos de acceso expuestos, reforzar el cifrados de los routers, etc.

MA: Aunque no todos son aspectos negativos, actualmente los servidores cuentan con firewall que brinda una protección estándar a la red del campus, además, esta se encuentra segmentada en redes virtuales que brindan acceso a características únicas de los sistemas en función del bloque al que pertenecen, por lo que de producirse un ciberataque éste quedaría aislado del resto de redes virtuales y podría controlarse de forma segura.

KP: En vista de que existe un departamento encargado de brindar asistencia y soporte técnico a los equipos informáticos ¿De qué manera coordinan estrategias conjuntas que garanticen el correcto resguardo físico y digital de la información?

MA: Precisamente como le comentaba, una de las acciones conjuntas que hemos llevado a cabo es el levantamiento de inventario de los equipos físicos del campus, así mismo, hemos recorrido todas las instalaciones en búsqueda de infraestructura dañada que comprometa el resguardo de la información, por ejemplo, recientemente reportamos a las autoridades competentes el hallazgo de una gotera localizada en el área de registro académico, en este sentido, le despliego orientaciones que ayuden a reforzar las estrategias del departamento para de esta forma poder alcanzar los estándares mínimos de ciberseguridad, de igual manera, doy seguimiento a la implementación y cumplimiento de dichas políticas. Sin embargo, le recomiendo realizar una entrevista al encargado de soporte técnico, ya que, al ser un área constituida, tiene autoridad para operar de forma independiente y autónoma.

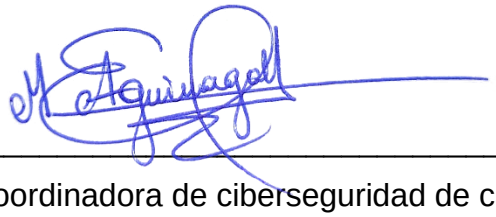
KP: En cuanto a la confidencialidad de los datos ¿Qué estrategias ha implementado para garantizar la integridad de la información en los sistemas institucionales?

MA: Bueno, actualmente, también soy la encargada de brindar asistencia al personal docente y administrativo en lo relativo a los sistemas de información, esto debido a las dimisiones del área, pero, si bien tengo acceso de escritura en los sistemas de información gracias a mi rol de administrador, no tengo acceso a todas las configuraciones y código fuentes de los mismos en calidad de super administrador, esa es una competencia que se le ha adjudicado exclusivamente a sede central Managua.

MA: No obstante, si pretendo programar dentro de mi plan de actividades auditorias periódicas a los sistemas de información, tanto web como de escritorio, que ejecutan los equipos informáticos; en ese sentido, deberé coordinar con sede Managua la logística de las estrategias en caso de que las herramientas requeridas para llevar a cabo los análisis comprometan la operatividad de los sistemas, un ejemplo de esto sería una simulación de ataque DDoS.

MA: Por ahora de la única medida de la que tengo conocimiento, es la de acceso controlado a la información basado en roles.

KP: Le agradezco toda la información que me ha proporcionado, realizaré la transcripción de la entrevista y le solicitaré su firma para que conste en acta como garantía sobre la veracidad de lo aquí expuesto. Sin más a que hacerle mención, le agradezco una vez más su tiempo y aporte elocuente para el desarrollo de la investigación.



Firma de la coordinadora de ciberseguridad de campus León.

Msc. Martha Elizabeth Aguinaga.

Fuente: Elaboración propia del autor

Anexo 4: Entrevista realizada a jefe de soporte técnico.

Entrevista realizada a Ing. Renzo Javier Calderón Lezama el día 23 de junio del año 2023, jefe del departamento de soporte técnico desde julio 2023 en campus León. Las abreviaturas del escrito hacen referencia a:

KP = Kelvin Pineda (Entrevistador). **RC** = Renzo Calderón (Entrevistado).

KP: Buenas días Ing. Calderón, le saluda el Ing. Kelvin Pineda, docente fijo anexo a la coordinación de ARQ – DGP – SIST. En esta oportunidad lo visito con fines académicos, le brindo el contexto…

KP: La tarde de ayer me encontraba entrevistando a Msc. Aguinaga, coordinadora de ciberseguridad del campus, y es que actualmente estoy llevando a cabo una investigación que recopila actores y factores que inciden en la implementación de estrategias de ciberseguridad, entonces, al consultarle a la coordinadora de qué manera llevaba a cabo acciones conjuntas con su área, me indicó ciertas pautas y remitió a su persona en calidad de representante para conocer a profundidad estas estrategias.

RC: Entiendo. ¿De qué manera puedo apoyarle?

KP: Correcto, he preparado una entrevista semiestructurada con 5 preguntas que guardan relación con las competencias de su área, puede desarrollar sus respuestas tanto como guste. Iniciaré con la primera pregunta: ¿Qué funciones específicas posee esta área?

RC: Brindamos soporte técnico en el sentido amplio del concepto a todas las áreas de la institución, esto incluye el mantenimiento preventivo y correctivo de ordenadores de escritorio, laptops, impresoras, entre otros equipos informáticos de uso institucional; realizamos instalación de paquetes software, formateo de sistemas operativos, respaldo total o parcial de información, instalación de puntos de red y velamos por el óptimo funcionamiento de los equipos informáticos presentes en laboratorios, áreas de docencia y el resto de departamentos administrativos.

KP: ¿Tiene acceso a algún módulo del sistema que le permita establecer un plan de actividades programadas o inventariar los equipos informáticos?

RC: No. He asumido hace poco más de un mes el cargo y según lo que se me orientó, se realizan dos mantenimientos preventivos anuales que inician en fechas preestablecidas. Antes de proceder a realizar el mantenimiento, debo notificar por correo electrónico a las áreas afectadas con al menos una semana de anticipación, para de esta manera poder alcanzar un mutuo acuerdo que ayude a establecer el calendario de afectaciones, este consenso se lleva a cabo con el objetivo de que las áreas afectadas tomen medidas que le permitan suplir su carga de trabajo mientras los equipos asignados se encuentran en el departamento de soporte técnico.

RC: En cuanto el levantamiento de inventario, lo realizo mediante un formato físico que luego remito a las autoridades competentes en archivos de Excel, por ejemplo, cuando un equipo ha finalizado su vida útil, éste es remitido a bodega con una ficha que aporta datos relevantes como modelo, características y procedencia.

RC: En lo personal, he propuesto la implementación de un sistema de etiquetado para equipos informáticos en coordinación con el departamento de bodega y otras áreas pertinentes, esto permitirá tener un mayor control sobre los equipos existentes y poder separarlos de los equipos de uso personal que ingresan a diario por parte de docentes y estudiantes en el campus, ya que, si bien existen formatos de solicitud de equipos, y de remisión de salida, dichos formatos solo permiten establecer características muy básicas que podrían desencadenar ambigüedades de control.

KP: Ya que ha mencionado el embodegado de los equipos ¿Qué tratamiento se le da a la información de estos equipos? ¿Existen estrategias para asegurar la permanencia de la información a largo plazo?

RC: Cuando un equipo es llevado a bodega lo que sucede en la práctica es que ha se le da de baja definitiva, ya que muchos de sus componentes ya no son operativos o se encuentran en muy mal estado, en ese sentido, cuando un equipo sufre una afectación, se realiza un diagnóstico para evaluar la gravedad del problema y encontrar las posibles soluciones, yo personalmente he logrado poner en marcha dos equipos de escritorio y un rúter que la previa administración había considerado para almacenar en bodega. Todas las acciones llevadas a cabo por el personal de soporte técnico son registradas en un formato de bitácora.

RC: En cuanto al respaldo de la información, si el disco duro aún contiene datos legibles de forma innata o recuperable a través de software especializados, se procede a realizar la extracción de la información en un disco duro externo exclusivo para este propósito, luego, este respaldo es subido a un drive ligado a la cuenta oficial de la nube institucional. Este procedimiento también es aplicable a dos casos con ciertas variantes: cuando se realizan los mantenimientos programados y cuando un colaborador deja de laborar para la institución…

RC: En caso de que el respaldo se ejecute por mantenimiento programado, también se realiza el formateo y la actualización del sistema operativo, por lo que la información solo será restablecida al colaborador con previa autorización, en cambio, cuando se realiza por recepción de equipo, está información solo es respaldada más no destruida, por lo que la reasignación del equipo y las medidas posteriores quedan sujetas a las indicaciones de recursos humanos.

KP: Para finalizar, ¿Ha logrado identificar si los sistemas operativos de los equipos informáticos son legítimos y se encuentran actualizados?, ¿Poseen antivirus?, ¿Se encuentran protegidos por control de usuario o contraseñas de acceso?

RC: Si. Los equipos del campus operan con una variante del sistema operativo Windows 10 Enterprise que recibe actualizaciones de seguridad en segundo plano, más no admite actualizaciones de versión, esto debido a una serie de conflictos relacionados con el firewall presente en versiones posteriores, lo que impide la correcta configuración y segmentación de los bloques de red y las impresoras de red.

RC: La mayoría de estos equipos si poseen antivirus, y desde mi conocimiento, al menos en las áreas sensibles como registro académico, caja, contabilidad, entre otras, si requieren de logeo por contraseña, independientemente de que estos equipos sean asignados a un único usuario.

KP: Sólo me restra agradecerle por su tiempo y participación de este proceso investigativo, transcribiré la entrevista y le solicitaré su firma para que conste en acta como muestra de buena fe de que lo que aquí se ha expresado, es información veraz.

Firma del jefe de soporte técnico de campus León.
Ing. Renzo Javier Calderón Lezama.

Fuente: Elaboración propia del autor

Anexo 5: Formato de remisión de salidas de materiales y equipos.

UNIVERSIDAD DE CIENCIAS COMERCIALES

SEDE-LEÓN.

REMISION DE SALIDA DE MATERIALES Y EQUIPOS

A: VIGILANCIA FECHA: _____ DEPARTAMENTO: _____

SOLICITANTE: _____

DESTINO: _____

JUSTIFICACION: _____

CANTIDAD	DESCRIPCION DEL MATERIAL O EQUIPO

RECIBI CONFORME: _____ ENTREGUE CONFORME: _____

AUTORIZADO: _____

Fuente: Ing. Renzo Calderón, jefe de soporte técnico.

Anexo 6: Formato de bitácora de asistencias técnicas.

Universidad de Ciencias Comerciales

UCC – LEÓN

Bitácora de Soporte Técnico Asistido

Fecha	Nombre y apellido	Área	Descripción	Firma

Fuente: Ing. Renzo Calderón, jefe de soporte técnico.

Anexo 7: Formato de solicitud de equipos.

UNIVERSIDAD DE CIENCIAS COMERCIALES

UCC – LEON

Fecha	Nombre y apellido	No. Data	Extensión	Regleta	Hora salida	Hora devolución	Firma ST	Firma al entregar

¡Listado de Solicitudes de Equipos!

Fuente: Ing. Renzo Calderón, jefe de soporte técnico.

UNIVERSIDAD DE CIENCIAS COMERCIALES

UCC-CAMPUS LEON.

UCC

COORDINACIÓN DE ARQUITECTURA, DISEÑO GRAFICO Y PUBLICITARIO E INGENIERIA DE SISTEMAS

Relación de Autores

Elaborado por:

Ing. Kelvin José Pineda - Docente

Arq. Lennar Vanegas Urey – Coordinador de Carrera ARQ DGP IS

Revisado por:

MSc. Constantino Portocarrero – Coordinador de Investigación

Autorizado por:

Dra. Fabiola Somarriba – Vice Rectoría Académica