UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE COMPUTACIÓN

Tema: "Plan de contingencia para el Data Center de la Universidad Politécnica Estatal del Carchi".

Trabajo de Integración Curricular previo a la obtención del Título de Ingenieros en Ciencias de la Computación

AUTORES: Fuel Piarpuezán Alexis Fernando
López Mosquera Willian Alejandro
TUTOR: Ing. Yandún Velastegui Marco A, MSc.

Tulcán, 2023

CERTIFICADO DEL TUTOR

Certifico que los estudiantes: Fuel Piarpuezán Alexis Fernando con el número de cédula 040174774-6 y López Mosquera Willian Alejandro con el número de cédula 040195186-8 respectivamente han elaborado bajo mi dirección el TIC titulado: "Plan de contingencia para el Data Center de la Universidad Politécnica Estatal del Carchi".

Este trabajo se sujeta a las normas y metodologías dispuestas en el Reglamento de la Unidad de Integración Curricular, Titulación e Incorporación, por lo tanto, autorizo la sustentación de la presentación para la calificación respectiva.

Firmado electrónicamente por:
MARCO ANTONIO
YANDUN VELASTEGUI

_____

Ing. Yandún Velastegui Marco Antonio MSc.

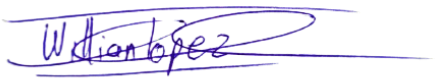
TUTOR

Tulcán, diciembre del 2023

AUTORÍA DE TRABAJO

El presente TIC constituye un requisito previo para la obtención del título de Ingenieros en la Carrera de Computación de la Facultad de Industrias Agropecuarias y Ciencias Ambientales.

Nosotros, Fuel Piarpuezán Alexis Fernando con el número de cédula 040174774-6 y López Mosquera Willian Alejandro con el número de cédula 040195186-8 respectivamente declaramos que la investigación es absolutamente original, auténtica, personal y los resultados y conclusiones a los que hemos llegado son de nuestra absoluta responsabilidad.



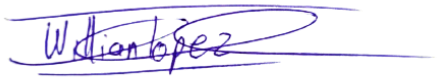
López Mosquera Willian Alejandro
AUTOR

Fuel Piarpuezán Alexis Fernando
AUTOR

Tulcán, diciembre del 2023

ACTA DE CESIÓN DE DERECHOS DEL TIC

Nosotros, Fuel Piarpuezán Alexis Fernando con el número de cédula 040174774-6 y López Mosquera Willian Alejandro con el número de cédula 040195186-8 respectivamente declaramos ser autores de los criterios emitidos en el TIC: "Plan de contingencia para el Data Center de la Universidad Politécnica Estatal del Carchi" y se exime expresamente a la Universidad Politécnica Estatal del Carchi y a sus representantes legales de posibles reclamos o acciones legales.



López Mosquera Willian Alejandro
AUTOR

Fuel Piarpuezán Alexis Fernando
AUTOR

Tulcán, diciembre del 2023

AGRADECIMIENTO

Me gustaría expresar mi más sincero agradecimiento a todas las personas que han contribuido de manera significativa en la realización de este trabajo de integración curricular.

En primer lugar, quiero agradecer a mis profesores y asesores académicos, cuyo conocimiento y orientación ha sido fundamental en cada etapa de este proceso. Su apoyo y dedicación han sido inspiradores, y su guía ha sido invaluable para llevar a cabo esta investigación.

No puedo pasar por alto el apoyo y comprensión brindados por mis familiares y seres queridos. Su aliento constante, paciencia y amor incondicional han sido un motor fundamental para mi perseverancia y éxito en este proyecto.

Además, quiero expresar mi gratitud a las instituciones y organizaciones que me han brindado acceso a recursos, datos e información relevante para la investigación. Su apoyo ha sido fundamental para llevar a cabo un estudio completo y riguroso.

Fuel Piarpuezán Alexis Fernando

Quiero expresar mi sincero agradecimiento a todas las personas que hicieron posible la realización de esta tesis. En primer lugar, agradezco a mi Tutor, por su orientación experta y apoyo constante. Su guía fue esencial para dar forma a este trabajo. También agradezco a mis profesores y amigos, cuyas contribuciones fueron invaluables. A mi familia, les agradezco por su amor y aliento incondicional. Agradezco a todas las personas que, de alguna manera, aportaron a este proyecto. Este logro no habría sido posible sin su ayuda y respaldo. Gracias por ser parte de este viaje académico.

López Mosquera Willian Alejandro

DEDICATORIA

Este trabajo de integración curricular está dedicado a todas aquellas personas que han contribuido de manera directa e indirecta en su desarrollo y culminación.

A mis profesores, quienes han compartido su conocimiento y experiencia, guiándome en este proceso de aprendizaje y brindando las herramientas necesarias para llevar a cabo esta investigación.

A mi familia, por su amor, paciencia y comprensión, alentándome en cada paso y siendo un pilar de apoyo incondicional en este camino académico.

A las instituciones y organizaciones que nos han brindado su apoyo y facilitado el acceso a recursos, información y datos necesarios para llevar a cabo esta investigación.

Fuel Piarpuezán Alexis Fernando

A mi amada familia, cuyo apoyo incondicional ha sido mi mayor fortaleza. A mi madre y mi padre, quienes siempre creyeron en mis sueños y me inspiraron con su ejemplo de dedicación y perseverancia. A mi hermano, por ser mi confidente y cómplice en cada etapa de esta travesía.

A mis queridos amigos, quienes compartieron risas, desafíos y momentos inolvidables a lo largo de estos años. Su amistad ha sido un faro en los días oscuros y una celebración en los días de triunfo. A todos mis profesores, gracias por su guía y sabiduría que han moldeado mi pensamiento y enriquecido mi aprendizaje.

Esta tesis está dedicada a cada persona que ha sido parte de mi vida, aportando su amor, apoyo y sabiduría. Cada uno de ustedes ha dejado una huella imborrable en este viaje académico.

López Mosquera Willian Alejandro

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

Este proyecto de investigación se realizó con el fin de evidenciar la problemática que posee el data center, el cual debe contar con la documentación necesaria para mantenerse funcionando de manera óptima e ininterrumpida. Sin embargo, el creciente desarrollo de la Universidad ha generado que este tipo de documentación quede completamente obsoleta, dado que fue diseñada y estructurada para el año 2017, para poder llevar a cabo este proyecto se aplicó un enfoque mixto aplicando encuestas y entrevistas, las cuales fueron necesarias para poder analizar la documentación que posee el departamento de TIC y evaluar cada uno de los riesgos que este presentaba, después de haber realizado la investigación correspondiente y el análisis se pudo observar los siguientes resultados: a) El departamento solo cuenta con dos de los documentos necesarios para el análisis de riesgos y contingencias informáticas, b) el personal no poseen las certificaciones para administrar el data center, c) no disponen de los siguientes documentos: plan de recuperación ante desastres, análisis de riesgos, plan de contingencia, evaluación y tratamiento de riesgos y el plan de ejecución. Por esta razón se presentó el Plan de Contingencia que contiene el estado actual del departamento, un análisis de riesgos, y las acciones para controlar los riesgos encontrados en el Data Center. Este trabajo puede servir como referencia y modelo para el desarrollo de planes de contingencia en los demás departamentos de entidades pública o privada.

Palabras Claves: Riesgo, Amenaza, plan de contingencias, Auditoría, Activos.

ABSTRACT

This research project was carried out to demonstrate the problems that the data center has, which must have the necessary documentation to keep it working optimally and uninterrupted. However, the increasing development of the University has caused this type of documentation to become completely obsolete, since it was designed and structured for the year 2017. To carry out this project, a mixed approach was applied, applying surveys and interviews, which were necessary to analyze the documentation that the ICT department has and evaluate each of the risks that it presented, after having carried out the corresponding investigation and analysis, the following results could be observed: a) The department only has two of the documents necessary for risk analysis and computer contingencies, b) the staff do not have the certifications to manage the data center, c) they do not have the following documents: disaster recovery plan, risk analysis, contingency plan, risk evaluation and treatment, and the execution plan. For this reason, the Contingency Plan was presented, which contains the current state of the department, a risk analysis, and the actions to control the risks found in the Data Center. This work can serve as a reference and model for the development of contingency plans in other departments of public or private entities.

KEYWORDS: Risk, Threat, contingency plan, Auditing, Assets.

INTRODUCCIÓN

En la era digital, los data centers se han convertido en pilares fundamentales para el almacenamiento, procesamiento y gestión de datos empresariales. Sin embargo, la operatividad de estos centros de datos puede verse amenazada por una amplia gama de riesgos, como interrupciones en el suministro eléctrico, fallas en el equipamiento, desastres naturales o ataques cibernéticos. Ante la posibilidad de enfrentar situaciones de crisis, resulta indispensable contar con un plan de contingencia efectivo que permita mantener la continuidad operativa del data center y salvaguardar la integridad del activo más importante que es información. El presente trabajo de investigación curricular se enfoca en el diseño y desarrollo de un plan de contingencia específicamente diseñado para un data center, con el objetivo de identificar los principales riesgos a los que está expuesto, evaluar su impacto potencial y establecer estrategias de respuesta y recuperación adecuadas. A través de un enfoque multidisciplinario y la revisión exhaustiva de literatura especializada, se busca proporcionar a las organizaciones una guía práctica y sólida para la implementación de un plan de contingencia eficiente, que minimice los tiempos de inactividad y garantice la continuidad operativa del data center en situaciones de crisis.

I.PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

En la actualidad, las instituciones educativas de nivel superior a nivel mundial se encuentran en una constante evolución y dependencia tecnológica de las tecnologías de la información y comunicaciones (TIC). Por esto, los Data Centers desempeñan un papel más que esencial en estas instituciones, dado que son el corazón de la infraestructura tecnológica, además de ser responsables del almacenamiento, procesamiento y distribución de la información crítica utilizada en la gestión académica y administrativa.

Sin embargo, las operaciones y servicios brindados por los Data Centers pueden verse afectados por diversos factores como: fallas de hardware o equipos, desastres naturales, ataques cibernéticos y errores humanos. Ante estos acontecimientos, es fundamental que las instituciones estén preparadas para tratar cada eventualidad que se presenta de forma óptima.

La UPEC al ser un organismo del sector público, se ve obligada al cumplimiento de las Normas de Control Interno de la Contraloría General del Estado, en donde se establece que: "Las Normas de Control Interno se aplicarán en todas las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, a las que se refiere la Constitución de la República del Ecuador y la Ley Orgánica de la Contraloría General del Estado (Contraloría General del Estado, 2023, p2)".

Cabe recalcar que esta norma también posee una sección dedicada a los requerimientos con los que debe contar un Plan de Contingencia. Esta sección es la 410-12, titulada "Plan de Contingencias", en donde se especifica cada aspecto que debe poseer un plan de contingencia para ser considerado como tal.

Es por esta razón que el Data Center de la Universidad Politécnica Estatal del Carchi, al ser parte fundamental para el almacenamiento y procesamiento de datos críticos, además de ayudar con la gestión académica y administrativa de la institución, debe

contar con la documentación necesaria para mantenerse funcionando de manera óptima e ininterrumpida. Sin embargo, el creciente desarrollo de la Universidad ha generado que este tipo de documentación quede completamente obsoleta, dado que fue diseñada y estructurada para el año 2017, lo cual en la actualidad no cumple

con la suficiente robustez necesaria para mantener el Data Center en óptimas condiciones y preparado para eventualidades catastróficas que afecte sus activos e información. Es por este motivo que el departamento de Tecnologías de la Información y Comunicación de la UPEC no logra implementar de forma adecuada las normas para el análisis y gestión de riesgos asociados con la seguridad de la información y los activos del Data Center.

1.2. FORMULACIÓN DEL PROBLEMA

La obsolescencia del plan de contingencia genera un riesgo a la seguridad de la información en el Data Center en la Universidad Politécnica Estatal del Carchi en el periodo académico 2022 B.

1.3. JUSTIFICACIÓN

La mayoría de las organizaciones no conocen de la magnitud del problema que están enfrentando al no darle la debida importancia a la seguridad de la información, dejándola en segundo plano, es decir, no intervienen ni capital humano ni tecnológico para prevenir el daño, control y la pérdida de información.

INDECI (citado en Palacios y Quiroz, 2013) nos señala que: El uso de las tecnologías de la información es más creciente por parte de las diversas instituciones y organizaciones. También se refleja en el medio, donde cada vez son más las oficinas, instituciones y entidades sistematizadas, lo que ha dado lugar en la mayoría de los casos a la dependencia de frágiles sistemas informáticos y redes de datos para soportar las funciones más críticas de la actividad institucional; pero lamentablemente no existe una amplia conciencia sobre la importancia de garantizar en la misma medida, la seguridad de los recursos involucrados al trato de la información.

A causa de lo antes mencionado, es importante que toda institución de educación superior que ofrece servicios en sus oficinas públicas o servicios en la web intervenga en la seguridad de la información mediante un plan de contingencia, el cual va a

identificar las debilidades de los servicios tecnológicos ante eventualidades de carácter natural o humana.

En la investigación se desarrollará una propuesta de un plan de contingencia que ayudará a la Universidad Politécnica Estatal del Carchi a reconocer todos los activos informáticos tanto software como hardware que son vulnerables a desgaste, pérdida y que estos pueden generar grandes problemas para el correcto funcionamiento de los servicios que ofrece la institución.

Además, Llerena, 2018 menciona que:

Un plan de contingencia informático está enfocado en el correcto mantenimiento y control de lo sucedido en cuanto a materia de información, que, aunque la información es la parte fundamental en cualquier organización, dentro de un plan informático de contingencias se controlan varios otros aspectos como la infraestructura, los activos empresariales y ambiente de desenvolvimiento de la información, es decir el entorno el cual la rodea y los usuarios que acceden a todos estos elementos.

Su propósito es de estructurar y ejecutar los procedimientos que admitan una pronta recuperación, asignación de responsables de salvaguardar componentes físicos, lógicos y sobre todo la información que permita su recuperación, garantizando la confidencialidad, integridad y disponibilidad de esta en el menor tiempo posible, brindando un ambiente de tranquilidad y seguridad en cuanto a los activos de Tecnologías de Información de la institución minimizando los costos en el levantamiento de la información y de los recursos informáticos. (Palacios y Quiroz, 2013, p.17)

Mediante el desarrollo del plan de contingencias se entregará una documentación como respuesta en caso de emergencia, catalogándolo como un instrumento para la gestión administrativa de las TI y que servirá como requerimiento para futuras certificaciones a las se someterá el departamento de TIC de la UPEC.

1.4. OBJETIVOS Y PREGUNTAS DE INVESTIGACIÓN

1.4.1. Objetivo General

Proponer un plan de contingencia para el data center de la Universidad Politécnica estatal del Carchi.

1.4.2. Objetivos Específicos

- Identificar riesgos que generen daños sobre los activos de la información del data center del departamento de TIC mediante el uso de normativas internacionales.
- Evaluar de forma críticamente el impacto que tienen los riesgos encontrados en los activos de la información del Data Center del departamento de TIC.
- Establecer acciones a ejecutar en caso de fallas a los activos del data center para minimizar el impacto del riesgo y apoyar la continuidad de las operaciones.
- Elaborar un plan de contingencia dirigido al departamento de Tecnologías de la información para actuar ante situaciones de emergencia del data center.

1.4.3. Preguntas de Investigación

- ¿Cuáles son los riesgos que generan daños sobre los activos de la información del Data Center?
- ¿Cómo se evalúan los riesgos que afectan los activos del Data Center?
- ¿Qué acciones se pueden tomar para minimizar el impacto del riesgo y apoyar la continuidad de las operaciones del Data Center?
- ¿Qué propuesta se dará para realizar de forma correcta el tratamiento de los riesgos en el Data Center?

II.FUNDAMENTACIÓN TEÓRICA

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

Se realizó la revisión y análisis bibliográfico en diferentes repositorios de diferentes universidades, además de realizar la correspondiente revisión de las diferentes normas existentes para el análisis de riesgos y planes de contingencia.

En el trabajo de (Buitrón, 2021) con tema: "GESTIÓN DE RIESGOS INFORMÁTICOS APLICANDO UNA METODOLOGÍA DE ANÁLISIS PARA VERIFICAR LA SEGURIDAD DE LA INFORMACIÓN EN UNA EMPRESA DE AUDITORÍA, CONSULTORÍA Y CAPACITACIÓN" en donde se destaca el cómo gestionar los riesgos informáticos aplicando metodologías para el análisis de la seguridad de la información, esto se genera desde la recolección de información que se obtuvo como punto de inicio para con ello generar políticas y acciones que permitan asegurar la información ante las amenazas y que estas se puedan mitigar.

De la misma manera se encontró información en la tesis de (Aranda, 2022) con tema: "EVALUACIÓN DE RIESGOS INFORMÁTICOS Y DISEÑO DE UN PLAN DE CONTINGENCIA PARA EL ÁREA DE TECNOLOGÍA DE LA EMPRESA IMPORTADORA ALVARADO VÁSCONEZ CIA. LTDA., UBICADA EN LA CIUDAD DE AMBATO", en la cual se puede evidencias que sin importar el tipo de empresa o entidad ninguna está libre de sufrir ataques además de poseer amenazas las cuales afectan a la confidencialidad, integridad y la disponibilidad de la información

Por otra parte, en el trabajo de (Burgos, 2020) con el tema: "PLAN DE CONTINGENCIA INFORMÁTICO PARA EL ÁREA DE TI CON BASE EN LA NORMA DE CALIDAD ISO 27001:2013 PARA LA FUNDACIÓN CULTURAL Y EDUCATIVA AMBATO - UNIDAD EDUCATIVA ATENAS". en este trabajo de titulación se llevó a cabo un plan de contingencia el cual tomo como base principal la norma ISO 27001, además en la cual se aclara cada una de las fases que debe de poseer un plan de esta índole, también se puede evidenciar la existencia del análisis de los riesgos valorando cada uno de ellos.

También se encontró una tesis en la cual se desarrolló un plan de contingencia informático, fue desarrollada por Gonzabay en el año 2021, esta tesis se denomina "Desarrollo de un plan de contingencia informática para el centro de datos y comunicaciones de la empresa AGUAPEN-EP medial el uso de normas internacionales", este plan de contingencia serviría como una guía para el desarrollo del plan de contingencia que se desea plantear en este trabajo de titulación.

Una vez dado los conocimientos de los antecedentes investigativos, se puede afirmar que para todo entidad pública o privada que genere o acumule información en gran cantidad, haciendo referencia a miles de datos, es más que necesario que dicha entidad necesite de un plan de contingencia para estar preparado ante todo tipo de amenaza o riesgo.

2.2. MARCO TEÓRICO

2.2.1. Seguridad Integral de la Información

La seguridad integral de la información es la garantía que posee una empresa o entidad, esta garantía es un acuerdo o documentación que estipula la seguridad de la información o que la información que resguarda la institución no será removida, modificada o alterada en ninguna circunstancia. Por otra parte, la norma ISO/IEC 27000 lo define como "el hecho de preservar la confidencialidad, integridad y disponibilidad de la información de la empresa u organización, denominados a su vez como los tres pilares fundamentales de la seguridad de la información."

2.2.2. Plan de Continuidad de Negocio

El plan de continuidad de negocio es una guía práctica y teórica que determina los pasos a seguir para corregir, prevenir o estar preparado en caso de ocurrir una catástrofe, otra descripción es la que le da Granizo Cesar (2019) quien afirma: "El plan de continuidad de negocios, tiene como principal objetivo proteger los servicios críticos del negocio, contra desastres, naturales, humanos o tecnológicos y evaluar las posibles secuelas que pueden generarse como pérdida de continuidad de los servicios" (p. 1).

Es por esta razón por la que toda institución que posea información de los clientes o usuarios de los servicios ofrecidos por esta misma debe de contar con un sistema que provenga todo tipo de catástrofes o problemas, además de que es un requisito fundamental para toda institución que posea un data center, así garantiza los servicios ofrecidos por dicha organización.

2.2.3. ¿Qué es un Data Center?

Un data center se podría describir como un conjunto de equipos tecnológicos capaces de ofrecer diferentes servicios, además de alojar información en grandes cantidades, pero una descripción más acertada es la que le da Kionetworks (2022) en donde afirma que "Un Data Center es un área o una sección donde se alojan y mantienen diversos sistemas de tecnología de la información (TI) y almacenes de datos, los cuales pueden contener mainframes, servidores y bases de datos.".

2.2.4. Equipos de un Data Center

Un data center está compuesto por múltiples componentes físicos como, por ejemplo: Racks, una arquitectura o un cuarto con una buena distribución, además de contar con un buen sistema de enfriamiento, un sistema eléctrico que provea de energía a todos los componentes que lo necesiten o también conocido como un sistema de alimentación ininterrumpida, algo que no debería de faltar en un data center es un control de alimentación o en otras palabras un control que controle el voltaje que alimenta todo el data center, un sistema de defensa contra el fuego, un sistema de cableado, una infraestructura de red y un sistema de seguridad física.

2.2.5. ¿Qué es la Auditoría?

Una auditoría informática se puede interpretar como una serie de pasos o leyes que se deben seguir para analizar, evaluar y mitigar o eliminar un riesgo potencial en una empresa o entidad financiera o educativa, para con ello garantizar la seguridad de la información que esta almacena, otra definición técnica de lo que es una autoría es el que refiere Sánchez Javier (2020) en su artículo Auditoría Informática donde afirma que: "La auditoría informática es una modalidad de auditoría que concierne a la evaluación en profundidad de los recursos informáticos y tecnológicos de una organización".

2.2.6. Tipos de Auditoría que se Aplican en un Data Center

Existen muchos tipos de auditorías que se pueden aplicar en un data center, esto siempre dependerá de la zona que se desee evaluar, un ejemplo de esto podemos decir que en caso de que deseemos auditar la infraestructura del data center puede ser que debamos aplicar una auditoría física, la cual consisten en analizar, evaluar y medir los riesgos que se pueden tener o generar en cuanto a la estructura perimetral del data center.

Otra de las auditorías que se podría realizar es hacking ético que consiste en realizar test de intrusión en los servidores o más específicamente en el data center,

2.2.7. Etapas de la Auditoría Informática

Es bien sabido que para poder realizar una auditoría informática se deben seguir una serie de fases, las cuales son:

- Etapa de exploración, esta etapa es caracterizada por inspeccionar todo el entorno a ser auditado, es decir, esta etapa se encarga de visitar la entidad, revisar que componentes pertenecen a cada sección y detallar como se distribuye la entidad para con ello facilitar la siguiente fase de la auditoría informática.
- La segunda etapa de una auditoría es el planteamiento, este se caracteriza por planificar cada aspecto que se realizará en cada departamento de la entidad, en otras palabras, esta etapa se encarga de realizar una planificación específica de ¿cómo se llevará a cabo la auditoría?, una vez terminada esta etapa de se procede a realizar la supervisión de que en efecto con lo planteado anteriormente se lleven a cabo los propósitos que se tienen para realizar la auditoría informática.
- La siguiente etapa a ser desarrollada es la ejecución del plan, esta etapa consiste en llevar a cabo todo lo planteado de tal manera en que se cumplan los objetivos de la auditoría, una vez se termine con la ejecución llega la etapa de la realización del informe, en esta etapa se realiza el informe final que contempla todos los resultados obtenidos por la auditoría realizada, para finalizar con la auditoría se lleva a cabo la etapa de seguimiento, la cual consiste en dar seguimiento a todos los resultados de la auditoría y verificar si los resultados no fueron alterados.

2.2.8. Evaluación de Data Center

La forma de evaluar un data center es un tanto sencilla de explicar dado que este proceso conlleva en la medición de carga y descarga de información, además de revisar todo lo que involucra hardware, es decir, problemas de calefacción o ventilación, además de temas de cableados.

2.2.9. Análisis de Procesos

El análisis de procesos es básicamente la comprensión de todos los pasos que se llevan en un proceso que se realiza en una entidad, esto quiere decir, que el análisis de procesos es detallar minuciosamente todos los pasos que se deben realizar al momento de realizar una tarea específica.

2.2.10. Análisis de Riesgos en un Data Center

El análisis de riesgos en un data center es un proceso clave para la realización de un plan de contingencia, dado que sin este proceso no se podrían medir los riesgos por escalas ni mucho menos poder diseñar una forma de mitigar o eliminar los efectos maliciosos de estos riesgos.

2.2.11. Respaldo

2.2.11.1. Respaldo Interno

Palacios y Quiroz (2013) mencionan que un respaldo de tipo interno tiene el objetivo principal dar solución a contingencias leves que no fuerce el desplazamiento de equipos informáticos fuera de los locales donde se encuentran ubicados, sus soluciones se enfocan en disponer de más de un elemento con el fin de reemplazar el que dejó de funcionar, evitar los puntos únicos de fallo y también la alta disponibilidad.

Las ventajas que nos brinda el respaldo interno son el costo moderado en la solución, aumenta la seguridad de los sistemas de información y además el que no es necesario acudir a alguien externo para el normal funcionamiento (p. 23).

Uno de los inconvenientes que tiene un respaldo interno es que no soporta contingencias graves, es decir, que afectan la seguridad física de los equipos o de las instalaciones, además en ciertos casos el respaldo va a generar un funcionamiento (Dirección de Prevención y Atención de Emergencias, 2009).

2.2.11.2. Respaldo Externo

El objetivo primordial es el resolver contingencias graves como son la desaparición del edificio, daño de plataformas virtuales, catástrofes ambientales que afectan y producen el desplazamiento de los equipos a ubicaciones diferentes de lo normal.

Estas soluciones se van a aplicar cuando la amenaza es más grave que las soluciones de respaldo interno no se puedan aplicar, debido a que no cubren la contingencia o las instalaciones quedan inoperables para el uso.

Las soluciones de respaldo externo se aplican después de un proceso de toma de decisiones y además se activa el Plan de Contingencias Informáticas (Palacios y Quiroz, 2013).

Las ventajas que presenta son: soporta contingencias graves que van a afectar la seguridad física de la informática a demás este tipo de respaldo genera un funcionamiento similar al ordinario.

DPAE, 2009 nos menciona que unos inconvenientes que presenta el respaldo externo es su coste elevado, además su complejidad es elevada, ya que hay que mantener y actualizar más equipos.

2.2.12. La Matriz de Evaluación de Riesgos

Su fin es reconocer eficazmente todos los riegos a los que se expone la institución y a través de esta información planificar acciones para disminuir los niveles de riesgos que existan y estar mejor preparados ante una emergencia (Palacios y Quiroz, 2013).

Para la elaboración de una matriz de evaluación de riesgo, se sigue 3 pasos:

- Descripción del área interna y externa de la institución.
- Evaluación de amenaza
- Evaluación de vulnerabilidades. (SNR, 2010)

Para manejar los riesgos es necesario: establecer políticas para el riesgo, inclusión del sistema de control y el establecimiento de planes de contingencia. (Marulanda, López y Cuesta, 2009).

2.2.13. Elementos para la Evaluación de la Amenaza

La evaluación se la realiza al responder algunas preguntas:

- ¿Qué tipo de eventos pueden afectarnos o ponernos en riesgo?
- ¿Cuál es el origen de dichos eventos?
- Anteriormente, ¿qué eventos han ocurrido en este sector?, ¿en esta institución?, reseña histórica sobre eventos pasados.
- ¿Cómo están relacionados con otras amenazas?
- ¿Cuál es la frecuencia con que se han presentado en el pasado?
- ¿Cuál ha sido su intensidad?
- ¿Cuáles son los lugares o zonas más expuestos al evento?

Cuando se respondan todas estas preguntas con la ayuda de fuentes verídicas se tomará en cuenta la frecuencia de la amenaza, la intensidad y la cobertura, de esta manera determinaremos el grado de la amenaza.

2.2.14. Características de la Amenaza

- **Frecuencia:** Hace referencia al número de veces en el año que ocurre la amenaza.
- **Magnitud:** Se refiere a la afectación o suspensión de actividades o funciones de la institución en relación con la amenaza, pudiendo considerarse como: baja, media, alta y muy alta.
- **Intensidad:** Permite estimar la fuerza con la que se manifiesta la amenaza, además determina el porcentaje de área física afectada por la amenaza.
- **Vulnerabilidad:** Una vulnerabilidad es una situación que puede significar un riesgo para una empresa, la cual puede generar todo tipo de pérdidas, ya sean económicas o de fiabilidad.

2.2.15. Evaluación de la Vulnerabilidad

Para determinar los factores se debe responder a las siguientes preguntas:

- Frente a una determinada amenaza, ¿Qué elementos (físicos, económicos, ambientales, sociales) representan fortalezas o debilidades?
- ¿Cuál es la causa (o causas) de que esto sea así?
- ¿De estos factores, cuáles son más importantes?

El análisis de Vulnerabilidad corresponde a la descripción de cada una de las condiciones relacionadas con los factores de vulnerabilidad según el tipo de amenaza (SNR, 2010).

2.2.16. Riesgos

(Peltier, 2001, como se citó en Palacios y Quiroz, 2013) nos indican que el riesgo se define como la probabilidad que una amenaza pueda explotar una vulnerabilidad en particular. En tecnología, el riesgo se considera una amenaza, considerando las pérdidas de la ocurrencia como grado de exposición, un claro ejemplo es la pérdida de datos debido a ruptura del disco duro o virus informático.

Por otro lado, la organización internacional por la normalización define al riesgo como: "la probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o de un grupo de activos, generando pérdidas o daños".

2.2.17. Evaluación del Riesgo

El conocer el riesgo a los que se encuentran sometidos los activos de una empresa es de vital importancia para poderlos gestionar, y por ello existen variadas guías que buscan saber que tan seguro o inseguro están los activos.

Hoy día la norma ISO 27001:2007, proporciona una base para la elaboración de reglas, métodos eficaces de seguridad y además permiten establecer un informe de confianza en las transacciones y las relaciones entre instituciones.

Si la Universidad no conoce sobre el riesgo que ocurren en sus activos de información, con dificultad está preparada para mitigar una posible ocurrencia de contingencias (leves o graves), es por ello la importancia de conocer y establecer controles para disminuir o en lo posible eliminar la ocurrencia de contingencias que afecten a los activos.

2.2.18. Análisis de Riesgo

(Brenes, 2007, como se citó en Palacios y Quiroz, 2013) indican que generalmente el análisis o evaluación de riesgos se define como el proceso de valorar la probabilidad con la que ocurra un suceso que no se desea, con un rango severidad y consecuencias en la seguridad. También, se debe elaborar un Plan de Emergencias y Contingencias que permitirá prevenir y mitigar riesgos, minimizar daños y recuperarse en el menor tiempo posible.

2.2.19. Evaluación de Riesgo

Este proceso permite a la organización alcanzar requerimientos estándar. En este proceso se compara los riesgos estimados contra los criterios de riesgo establecidos o dados, esto para determinar el grado de importancia del riesgo.

Su objetivo principal es identificar y evaluar los riesgos. Los riesgos son calculados por la combinación de:

- Estimación del valor de los activos de riesgo.
- Probabilidad de ocurrencia de riesgo.
- Valoración del riesgo.

2.2.20. Tratamiento de Riesgo

El tratamiento de riesgos se define como el conjunto de decisiones, todas con cada activo de información. También la ISO/IEC guide 73:202, índica la conceptualiza como "proceso de selección e implementación de medidas para modificar el Riesgo".

Las medidas de tratamiento del riesgo pueden contemplar acciones como: evitar, optimizar, transferir o retener el riesgo (Fritalina, 2009, como se citó en Palacios y Quiroz, 2013).

2.2.21. Plan de contingencia

Un plan de contingencia es una serie de reglas, lineamientos y acciones documentadas y especificadas que permiten a una empresa a estar preparada para toda eventualidad catastrófica, riesgo o amenaza que pueda sufrir, sin importar su tamaño o índole, este debe de contener información de la empresa o entidad actual y la situación en la que se encuentra, debe de seguir una normalización internacional además de que este debe poseer una gran cantidad de acciones puntuales que

deben de seguir para poder trabajar en caso de alguna situación de riesgo presentado.

2.2.22. Norma ISO/IEC 27000.

La norma ISO/IEC 27000 es un conjunto de normas o estándares internacionales que proveen de salvaguardias para los activos de la información de las organizaciones, además ayudan a facilitar una serie de procesos para la seguridad de la información.

2.2.23. Descripción de la Norma ISO/IEC 27002

Es un estándar para la seguridad de la información, su publicación la realizó la organización internacional de normalización y la comisión electrónica internacional. El objetivo principal de la norma es el establecer directrices y prácticas de la gestión de la seguridad de la información, incluye la selección, implementación y gestión de controles, basándose en el entorno de riesgo de la seguridad de la información de la institución.

El uso de la norma ISO 27002 en el departamento de TIC permitirá aplicar controles, lineamientos y directrices para el manejo de los activos físicos y lógicos e integridad de datos, de esta manera aportará buenas prácticas que gestionen y reduzcan los niveles de ocurrencia de incidentes que pueden afectar la continuidad de las operaciones de la institución.

2.3. MARCO LEGAL

Las normas de control interno están dirigida a empresas del sector público y privado para el establecimiento de guías generales que son emitidas por la Contraloría General del Estado. Las normas que son consideradas para el desarrollo de planes de contingencias informáticos están manifestadas mediante:

2.3.1. Norma de Control Interno 410-01

La Contraloría General del Estado establece que "Las entidades y organismos del sector público deben estar acopladas en un marco de trabajo para procesos de tecnología de la información y comunicaciones que aseguren la transparencia y el control, así como el involucramiento de la alta dirección, por lo que las actividades y procesos relacionados con las tecnologías de información y comunicaciones de la entidad deben estar bajo la responsabilidad de una unidad que se encargue de regular, estandarizar y dar seguimiento a los temas tecnológicos a nivel institucional."(p.82)

2.3.2. Norma de Control Interno 410-12

Es responsabilidad de la unidad de tecnología de información de cualquier empresa, el desarrollar e implementar un plan de contingencias que describa acciones a poner en marcha ante una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado (Contraloría General del Estado, 2023).

2.3.3. Norma ISO/IEC 27002

Esta Norma Internacional está diseñada para que las organizaciones la utilicen como referencia para seleccionar controles dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001 o como documento de orientación para las organizaciones que implementan controles de seguridad de la información comúnmente aceptados. Este estándar también está diseñado para usarse en el desarrollo de pautas de gestión de seguridad de la información específicas de la industria y la organización, teniendo en cuenta sus entornos de riesgo de seguridad de la información específicos (ISO/IEC 27002, 2013).

III.METODOLOGÍA

3.1. ENFOQUE METODOLÓGICO

3.1.1. Enfoque

Dado que se busca realizar un plan de contingencia diseñado específicamente para el data center de la UPEC, además de que se busca cumplir con todos los objetivos que se plantearon en la investigación, se decidió utilizar un enfoque metodológico mixto que involucre encontrar valores numéricos para evaluar los riesgos que existen en el data center y también comprender los funcionamientos y características que posee el personal que se encarga del data center.

3.1.2. Tipo de Investigación

En el presente trabajo de investigación se decidió de tomar como base principal los siguientes tipos de investigaciones:

- Investigación documental, este tipo de investigación se basa en la búsqueda de información a través de documentos científicos, con el fin de comparar y utilizar dicha información en una investigación relacionada, con esta investigación se llevó a cabo la recolección de información a través de: tesis con temas relacionados en: Normas Internacionales ISO/IEC, Acuerdos legales y leyes nacionales, con las cuales se logró justificar por medios legales la realización del plan de contingencia.
- También se llevó a cabo una investigación de campo, debido a que se recolectó información por medio de encuestas, con el fin de recoger datos que sean capaces de definir que normas cumple el departamento de TIC de la UPEC.

3.2. IDEA A DEFENDER

El plan de contingencia facilitará el tratamiento de los riesgos del Data Center de la Universidad Politécnica Estatal del Carchi de forma más efectiva y eficiente.

3.3. DEFINICIÓN Y OPERACIONALIZACIÓN DE LAS VARIABLES

En la tabla 1 se muestra la operación de las variables dependientes: infraestructura tecnológica del Data Center, por otra parte, la tabla 2 es la operación de la variable independiente: plan de contingencia, en las dos tablas se muestra la conceptualización, dimensión, indicadores, técnicas e ítems y preguntas para realizar la operacionalización.

Tabla 1. Operacionalización de la variable dependiente

Conceptualización	Dimensión	Indicador	Técnica	Ítem=preguntas
La infraestructura del data center hace referencia al equipo informático que posee, estos equipos incluyen: cableado, servidores, equipos de comunicación, etc.	• Hardware • Software	• Equipos tecnológicos. • Cantidad de mantenimientos al año. • Cantidad de chequeos al mes. • Frecuencia con la que se realizan Backups.	Encuestas.	• ¿Cuántas veces se da mantenimiento a todo el data center? • ¿Cuántas veces al mes se realizan los chequeos al data center?

Tabla 2. Operacionalización de la variable independiente.

Conceptualización	Dimensión	Indicador	Técnica	Ítem= preguntas
Es un documento sobre las estrategias necesarias para determinar todos los procesos que afectan a los equipos informáti**cos** del data center y de esta manera preparar a la organización para actuar y recuperar los principales servicios.	• Estrategias para recuperación de servicios información. • Monitoreo de sistema de información y comunicación. • Gestión de riesgos. • Gestión de simulacros.	• Caídas de los sistemas cada año. • Tipos de estrategias. • Identificar el tiempo de recuperación. • Identificar el punto de recuperación. • Control de simulacros en la entidad.	Encuesta.	• ¿Existe políticas de para el análisis de riesgos y plan de contingencia? • ¿Se realizan simulacros de caídas de los sistemas de información? • ¿Existen estrategias de actuación y recuperación de servicios? • ¿Existe un control de los procesos críticos?

3.4. MÉTODOS UTILIZADOS

3.4.1. Observación Participativa

En la investigación se utilizó el método de observación participativa debido a que existió un acercamiento con el Departamento de tecnologías de información y comunicación, se dialogó sobre la problemática que presenta el data center y que afecta el normal funcionamiento, además, de que en el desarrollo de la investigación nos involucraremos con los trabajadores del departamento de TIC.

3.4.2. Auditoría

Se aplicó una auditoría Informática a la necesidad de levantar información del cumplimiento de controles que tiene el departamento de TIC basados en la Norma ISO/IEC 27002.

3.4.3. Entrevista

Se recurrió a la utilización de una entrevista al personal del departamento de TIC, dado que, al estar involucrados con la administración del Data Center, este personal está más que informado de todos los acontecimientos que pasan y pasaron en el Data Center.

3.4.4. Encuesta

Se aplicó una encuesta de selección simple con el objetivo de recolectar información que indique la posibilidad de que un estudiante sea capaz de realizar un ataque a los servidores del Data Center y con esta información dar una valoración más precisa en ciertos riesgos que involucren a personas externas del departamento de TIC.

3.5. ANÁLISIS ESTADÍSTICO

3.5.1. Población y Muestra

La investigación se desarrollará utilizando la totalidad de la población que se beneficiará con el plan de contingencia del Data Center de la Universidad Politécnica Estatal del Carchi.

A demás, se decidió tomar una muestra de la población total de estudiantes de la carrera de computación, por la razón que estos estudiantes son propensos a tener los conocimientos suficientes para provocar un ataque directamente a los servidores de la del Data Center, la muestra fue tomada considerando la formula específica para medir una población finita, tenemos un nivel de confianza del 98%, con una

probabilidad de ocurrencia de un ataque a los servidores del 25% y por consecuencia un porcentaje de no ocurrencia del 75%, además se debe considerar que la población es de 244 estudiantes matriculados en la carrera, con estos datos se procede a calcular el tamaño de la muestra de estudiantes que debe ser encuestada mediante las siguiente formula.

$$n = \frac{N * {Z_\propto}^2 * p * q}{d^2 * (N-1) + {Z_\propto}^2 * p * q}$$

Donde:

n= muestra.

N= tamaño de la población

$\boldsymbol{{Z_\propto}^2}$**=** 3.84 si el nivel de confianza es del 95%

p= probabilidad de éxito por lo tanto es del 5% =0.05

q= 1-p de tal manera que (1-0,05 = 0,95)

d= precisión (se usó el 5%)

Por consiguiente:

$$n = \frac{244 * 5.42 * 0.25 * 0{,}75}{0.0498^2 * (244-1) + 5.42 * 0{,}25 * 0{,}75} = \frac{247.965}{1.61}$$

$$n = 153.16 \rightarrow \ n = 154$$

Con base a esta información y calculando mediante la formula podemos afirmar que la muestra es de 150 encuestas.

La tabla 3 informa la población total del Departamento de TIC de la Institución quienes están involucrados en la administración del data center.

Tabla 3. Población del DTIC-UPEC.

Población	Número	Porcentaje
Director Departamento de TIC	1	11.1%
Unidad de desarrollo de software.	4	44.4%
Unidad de Redes y Telecomunicaciones.	1	11.1%
Unidad de Soporte Técnico Informático	3	33.3%
Total	**9**	**100%**

3.6. RECURSOS

3.6.1. Recursos Humanos

En la tabla 4 se muestra información de los recursos humanos que se utilizaron para la realización del trabajo de integración curricular.

Tabla 4. Recursos Humanos de la Investigación.

Nombres	Cargo	Función
Sr. Fuel Piarpuezán Alexis Fernando	Estudiante de noveno nivel de la Carrera de Computación.	Investigador
Sr. López Mosquera Willian Alejandro	Estudiante de noveno nivel de la Carrera de Computación.	Investigador
Msc. Marco Yandún	Docente de la Carrera de Computación.	Tutor
Msc. Andrea Guevara	Director del Departamento de Tecnologías de Información y Comunicación.	Directora de TIC
Msc. Andrés Zabala	Coordinador de la Unidad de Desarrollo de Software	Coordinador
Msc. Javier Torres	Coordinador de proyecto de la Unidad de TIC.	Coordinador

3.6.2. Recursos Financieros

En la tabla 5 se muestran los recursos financieros que se utilizaron para la realización del trabajo de integración curricular.

Tabla 5. Recursos Financieros de la Investigación.

RECURSOS	PRECIO
NORMA ISO 27001	20 $
NORMA ISO 27005	20 $
INTERNET	40 $
PAPEL	5 $
IMPRESIONES	8 $
Movilización	30 $
Materiales Bibliográfico	5 $
Total	128 $

3.6.3. Recursos Tecnológicos

- Internet.
- Impresora.
- Computador Portátil.
- USB.

3.6.4. Recursos Institucionales

- Biblioteca Institucional.
- Acceso a Internet.
- Acceso al departamento de TIC.

IV. RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

4.1.1. Resultados Obtenidos de las Encuestas a los miembros de TIC

En el presente capítulo se presentarán los resultados de las diferentes preguntas que se realizaron en la encuesta que se aplicó a los miembros involucrados en el manejo y administración del data center de la universidad, los cuales reflejarán la valoración que posee dichos miembros con respecto a algunos riesgos existentes. También se enfatiza que si se desea observar las respuestas dadas por los encuestados se dirija al ANEXO 5.

Pregunta 1.

De acuerdo con las explicaciones anteriores, llene la información solicitada a continuación con respecto a su criterio.

Riesgos /Vulnerabilidades / Amenazas	Probabilidad					Impacto					Tratamiento					Nivel de Madurez			Responsable
	1	2	3	4	5	1	2	3	4	5	A	M	E	T	I	D	A	O	
Pérdida de las fuentes energéticas																			
Errores Humanos																			
Indisponibilidad de la red																			
Deterioro de los componentes, equipos e insumos																			
Fallas de los componentes, equipos e insumos																			
Daño o deterioro de la estructura física del cuarto seguro																			
Desorganización del cableado (energético, datos																			
Incendio																			
Inundación																			
Temblores, terremoto o movimientos telúricos.																			

Intento de acceso no autorizado al cuarto seguro																		
Fallas de climatización																		
Errores de software																		
Tráfico inusual de la red																		
Fallas de acceso																		
Intentos de acceso no autorizado																		
Intento de infección con software malicioso																		
Ingreso de infección con software malicioso																		
Cambios no autorizados																		
Ataques de DDoS (denegación de servicios)																		
Caducidad de licencias																		
Pérdida o falla en el almacenamiento de información en la base de datos.																		
Se dispone de una persona Back-up para la administración del data center																		

Figura 1. Ejemplo de valoración de riesgos.

RESULTADO OBTENIDO.

N.º	Riesgos /Vulnerabilidades / Amenazas	Probabilidad					Impacto					Valoración
		1	2	3	4	5	1	2	3	4	5	
R1	Pérdida de las fuentes energéticas					x				x		20
R2	Errores Humanos			x				x				6
R3	Indisponibilidad de la red		x						x			6
R4	Deterioro de los componentes, equipos e insumos	x								x		4
R5	Fallas de los componentes, equipos e insumos	x								x		4
R6	Daño o deterioro de la estructura física del cuarto seguro	x						x				2
R7	Desorganización del cableado (energético, datos)		x							x		8
R8	incendio	x								x		4
R9	inundación	x					x					1
R10	Temblores, terremoto o movimientos telúricos.	x					x					1
R11	Intento de acceso no autorizado al cuarto seguro		x							x		8
R12	Falla en la climatización					x				x		20
R13	Errores de software		x					x				4
R14	Tráfico inusual de la red		x					x				4
R15	Fallas de acceso	x					x					1
R16	Intentos de acceso no autorizado		x					x				4
R17	Intento de infección con software malicioso	x							x			2
R18	Ingreso de infección con software malicioso	x							x			3
R19	Cambios no autorizados	x								x		4
R20	Ataques de DDoS (denegación de servicios)		x							x		4
R21	Caducidad de licencias				x				x			12
R22	Pérdida o falla en el almacenamiento de información en la base de datos.		x								x	10

Figura 2. Valoración de riesgos de acuerdo con los responsables.

Una vez presentadas las valoraciones de los riesgos presentados, aparentemente se observa que los riesgos mencionados no poseen suma importancia, pero es todo lo contrario debido a que los riesgos mencionados se deben valorar de acuerdo con su nivel de impacto y probabilidad de ocurrencia, por esta razón se pudieron clasificar por porcentajes la cantidad de riesgos graves, medio y leves que los responsables del data center consideraron.

Figura 3. Cantidad de riesgos según su nivel de gravedad.

Descripción: en el gráfico se muestra los porcentajes de los riesgos con gravedad alta, media y baja, auditados a lo largo del desarrollo del plan de contingencia.

Pregunta 2.

Indique otros factores internos o externos que no fueron considerados en la pregunta anterior

RESULTADO OBTENIDO.

Con base a las respuestas brindadas por los encuestados se pudo deducir que los factores internos y externos son fallas tanto como el mismo personal o de empresas que prestan servicios a la institución.

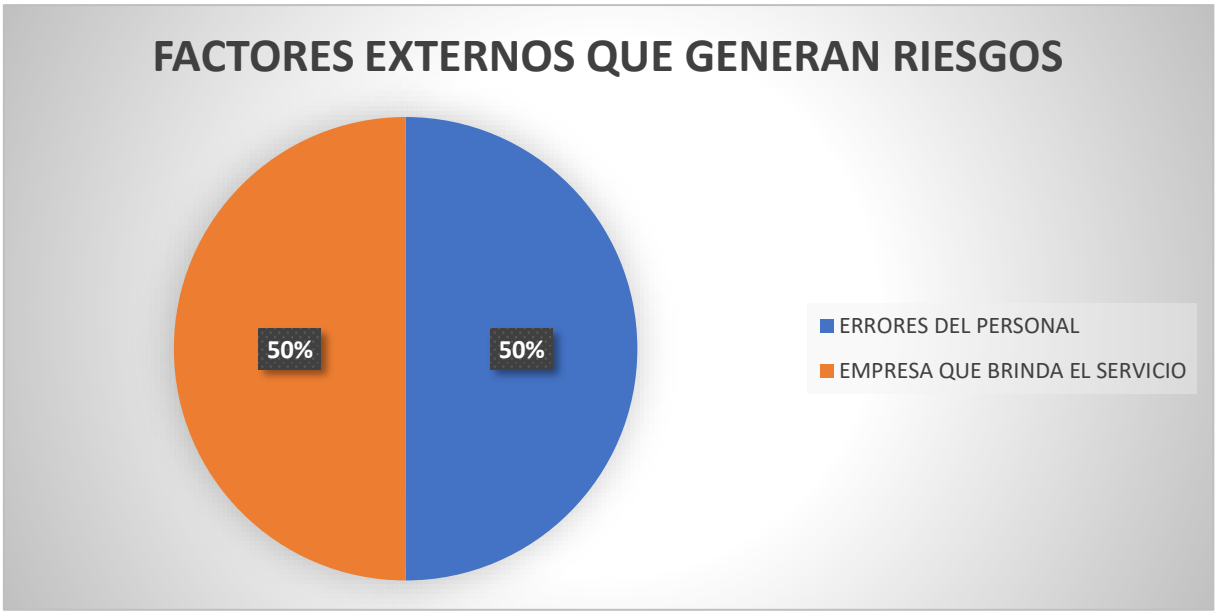


Figura 4. Factores externos que generan riesgos.

Descripción: En la figura se muestra el porcentaje de los factores más comunes que generan riesgos de forma externa al data center.

Pregunta 3.

Indique como se encuentran los siguientes documentos, manuales que ayudan a gestionar los riesgos:

PUBLICADO (P)	SOCIALIZADO (S)	EN DESARROLLO (D)	Versionado (V)	NO DISPONE (ND)	NO APLICA (NA)

Figura 5. Explicación de siglas, estado de documentos.

Descripción: En la tabla que indica las siglas que corresponden a los estados que poseen los riesgos analizados.

DOCUMENTOS	P	S	D	V	ND	NA
Análisis de Riesgos						
Análisis de impacto de negocio						
Plan de recuperación ante desastres						
Plan de continuidad de negocio						
Estrategias para la gestión de Crisis						
Plan de Contingencias						
Plan de Evaluación y Tratamiento de riesgos						
Políticas de Seguridad de la Información						
Políticas para el etiquetado de la información						
Políticas para el uso aceptable de la información y de los activos asociados con la información						
Políticas para la gestión de medios extraíbles						
Política de control de acceso						
Políticas para la instalación de software						
Plan de mantenimiento de activos						

Figura 6. Ejemplo de clasificación estado de documentos.

Descripción: En la tabla se observa el formato con el que se recolectó la información correspondiente con el estado de los riesgos revisados.

RESULTADO OBTENIDO.

Con base en las respuestas proporcionadas por los encuestados, se puede concluir con que en el 14.28% de los documentos se encuentran en desarrollo, el 7.14% se encuentra socializado y 78.58% se encuentra no disponibles.

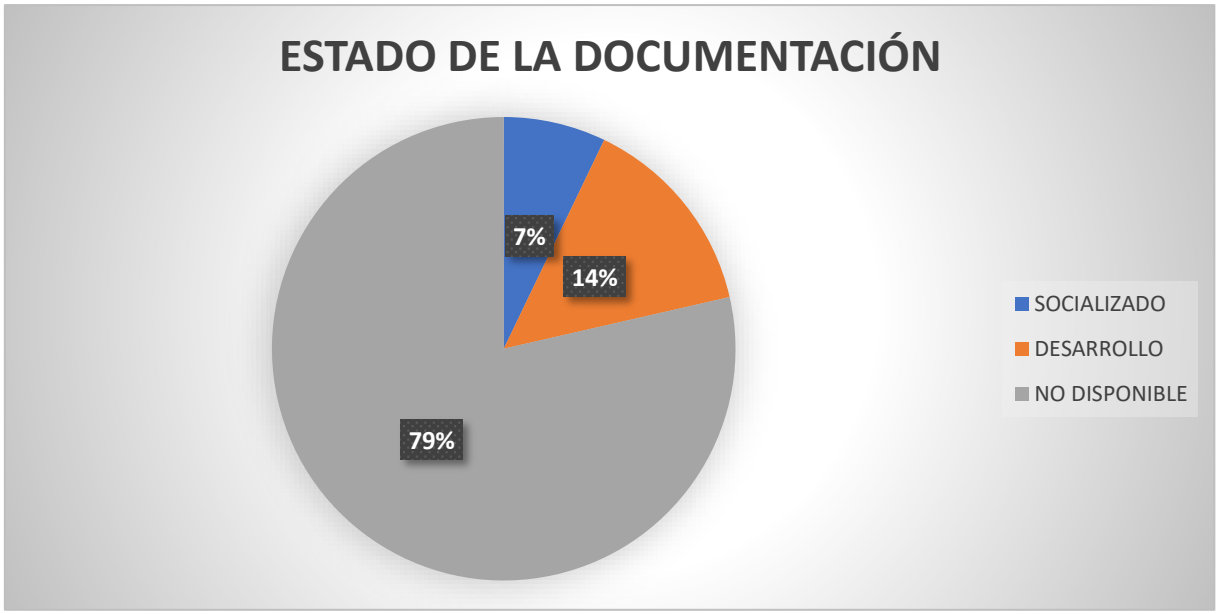


Figura 7. Estado de la documentación.

Descripción: En la figura se observa el porcentaje con el que los riesgos se encuentran socializados, desarrollo y no disponible.

Pregunta 4.

¿Cuáles son los criterios que ustedes siguen para considerar que un riesgo es aceptable?

RESULTADO OBTENIDO.

Con base en las respuestas, los criterios con los que se evalúan los riesgos son los siguientes:

- Tiempo de riesgo limitado
- Restricción de servicios por poco tiempo
- Continuidad de servicios
- Consecuencias mínimas
- Control sobre el riesgo

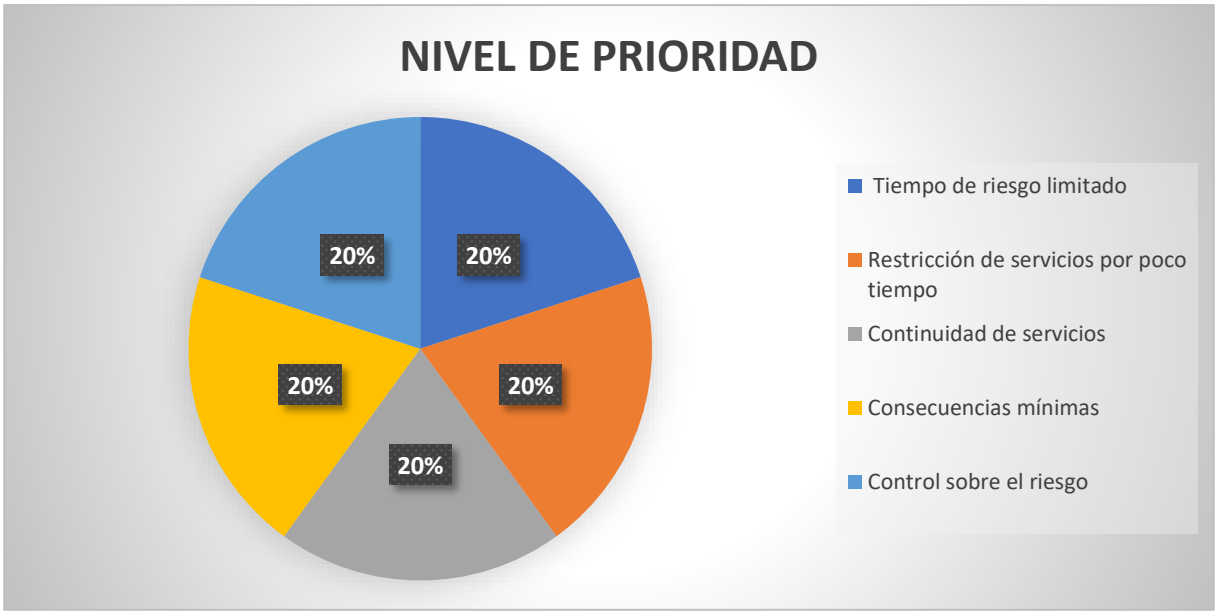


Figura 8. Nivel de prioridad.

Descripción: La figura muestra el porcentaje de prioridad que poseen los criterios con los que se evalúan los riesgos.

Pregunta 5.

De acuerdo con la pregunta anterior, ¿Cómo consigue que el riesgo residual de los riesgos principales sea aceptable?

RESULTADO OBTENIDO.

De acuerdo con las respuestas obtenidas en la pregunta, todos los miembros encuestados están de acuerdo con realizar las acciones correspondientes para mitigar dichos riesgos al punto de que los residuos del riesgo ya no representen un problema para la institución.

Pregunta 6.

¿Cuántas auditorías se han realizado al data center?

RESULTADO OBTENIDO.

De acuerdo con los miembros encuestados, el número de auditorías que se han realizado son nulas, por lo que se puede decir que todas las acciones que se hicieron fueron por experiencia personal, además esto anula las siguientes preguntas.

Pregunta 9.

¿Qué herramientas utiliza para la valoración de riesgos?

- Check-list
- Matriz de riesgos
- Matriz de calor
- Árbol de fallas
- Diagrama causa-efecto
- Otras
- Ninguna

RESULTADO OBTENIDO.

Con respecto a los resultados obtenidos en las encuestas se puede observar que con el 66,66% la herramienta más utilizada es el check-list y con el 33,33% la segunda herramienta de valoración más utilizada es la matriz de calor.

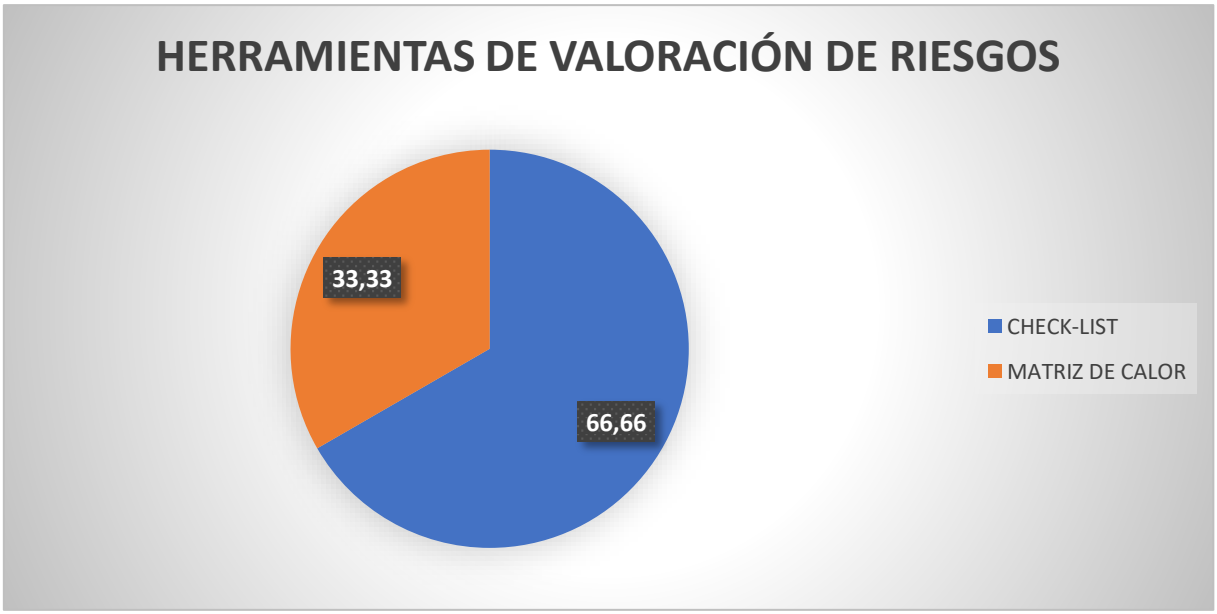


Figura 9. Herramientas de valoración de riesgos.

Pregunta 10.

¿Cómo identifica los cambios o configuraciones en equipos que usted administra?

- Monitoreo por consola del equipo
- Monitoreo manual
- Alertas o alarmas del equipo
- Desconexión o reinicio automático
- No se realizan
- Otros

RESULTADO OBTENIDO.

Con respecto a los resultados obtenidos con las encuestas, se puede observar que las herramientas con las que se detectan los cambios en el data center tienen los siguientes porcentajes: el monitoreo por consola del equipo se realiza en un 43%, el monitoreo manual posee un 14%, las alertas o alarmas del equipo contiene un 29% y al final la desconexión o reinicio automático con el 14%.

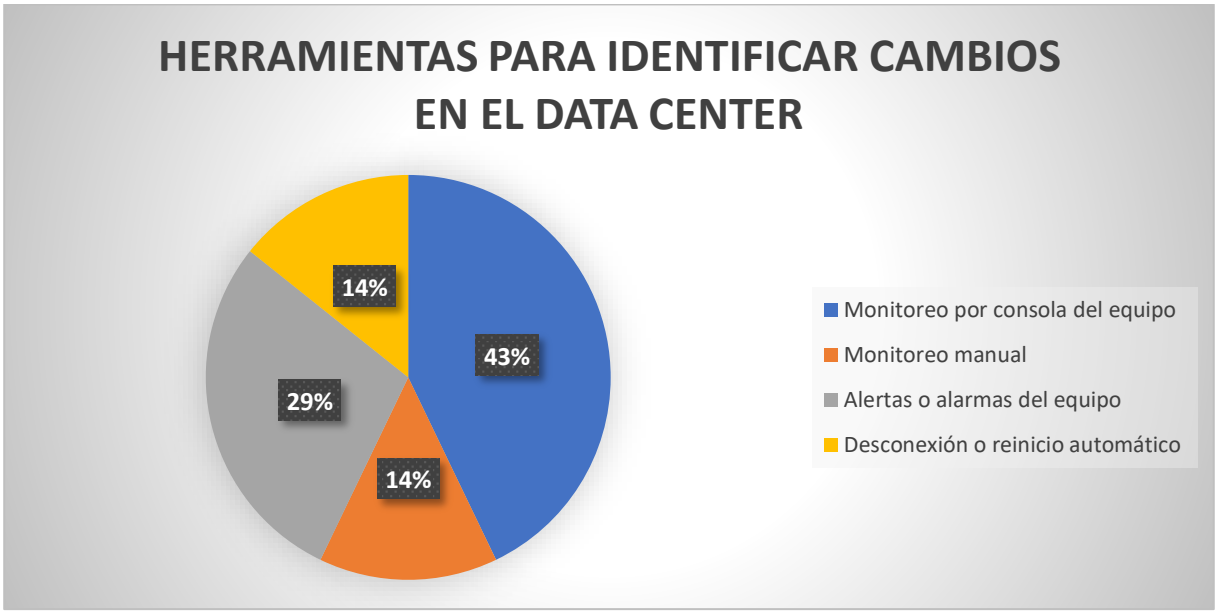


Figura 10. Herramientas para identificar cambios en el data center.

Pregunta 11.

¿El área de trabajo de los responsables de la operación del data center se encuentra aislado de las instalaciones del data center?

- Si
- No

RESULTADO OBTENIDO.

Con base en las respuestas obtenidas por medio de la encuesta realizada a los miembros responsables, se obtuvo con un porcentaje del 100% que las instalaciones del data center y el área de trabajo de los miembros del departamento de TIC si se encuentran aisladas de este.

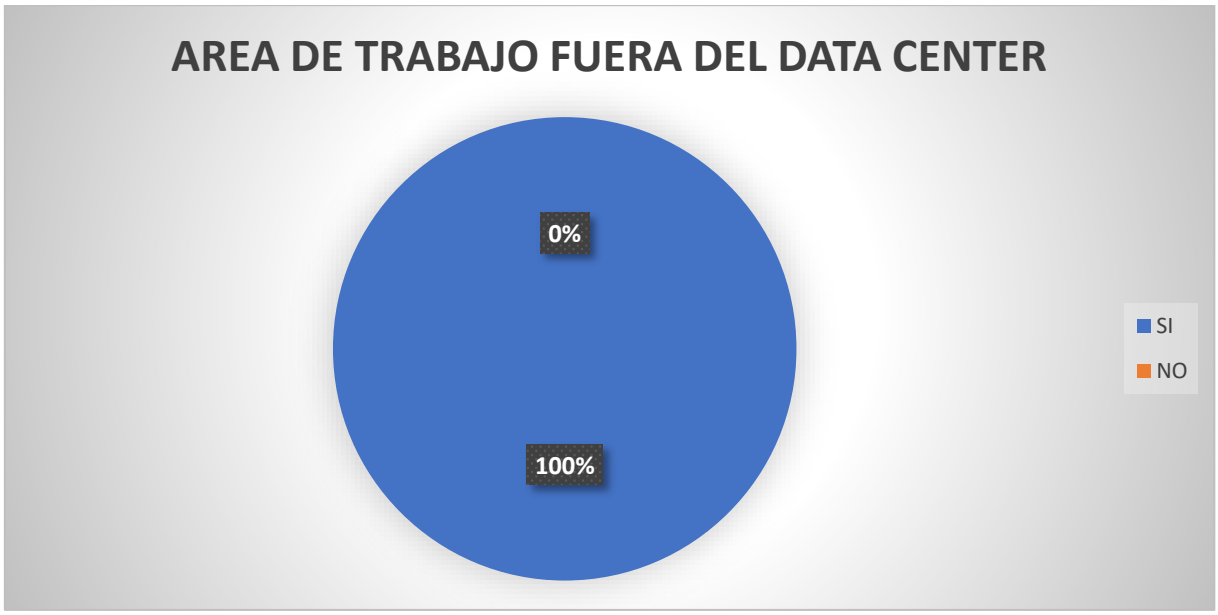


Figura 11. Área de trabajo fuera del data center.

Pregunta 12.

¿Se encuentran segregadas las funciones de los funcionarios del data center?

- Si
- No
- No estoy seguro

RESULTADO OBTENIDO.

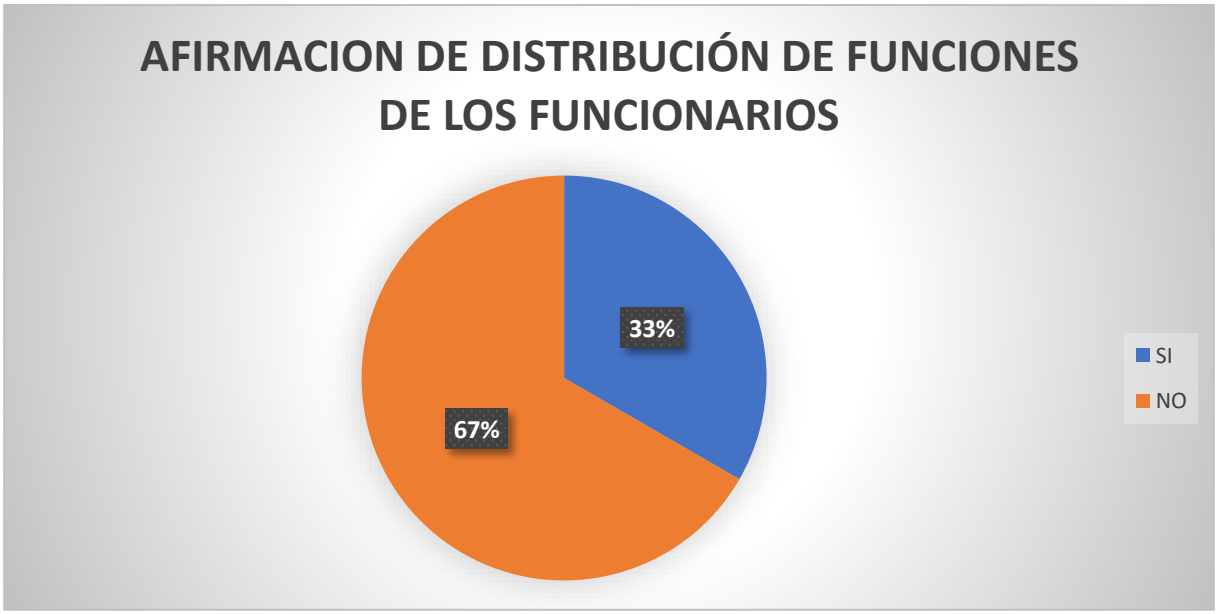


Figura 12. Afirmación de distribución de funciones de los funcionarios.

Con base en la figura 12 se puede observar que la opción "No" tiene un 66,6 % y que la opción "Sí" tiene un 33,3 %, esto indica que las funciones que deben cumplir cada funcionario dentro del data center no se encuentran segregadas en su totalidad.

Pregunta 13.

¿Cuál es el criterio para la segregación de actividades?

RESULTADO OBTENIDO.

Por motivos de que la pregunta anterior la respuesta fue un no, no se pueden verificar los criterios que se toman para asignar las actividades o tareas en el data center.

Pregunta 14.

Marque lo que corresponda

Dispone de la siguiente información	SI	NO	
Contactos de expertos en data center			
Pertenezco a grupos de expertos en data center			
Asisto a foros de seguimiento			**FRECUENCIA**
Pertenezco a asociaciones administradores o responsables de data center			

Figura 13. Ejemplo de disponibilidad de información

RESULTADO OBTENIDO.

Con los resultados obtenidos se consiguieron los siguientes resultados:

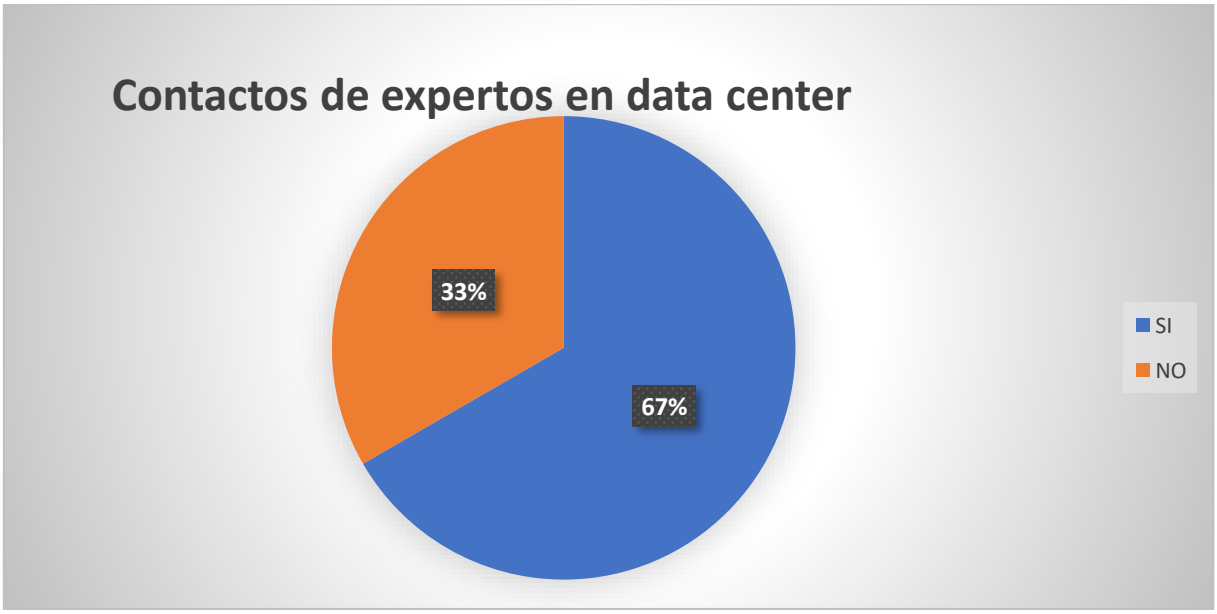


Figura 14. Contactos de expertos.

Figura 15. Pertenezco a grupos de expertos en data center.

Figura 16. Asisto a foros de seguimiento.

Figura 17. Pertenezco a asociaciones de data center.

Con base en las gráficas mostradas anteriormente se puede afirmar que a pesar de tener contactos con personal capacitado en el manejo de data centers, los miembros de TIC no forman parte ni tienen capacitación en este entorno.

Pregunta 15.

¿Qué tipos de controles se realizan a los candidatos para trabajar en el data center?

TIPOS DE CONTROLES	Si	No	Realiza otro Departamento	No Aplica
Pruebas de polígrafo				
Verificación de datos personales				
Verificación de antecedentes penales				
Verificación de certificaciones				
Entrevista al candidato				
Verificación de Autenticidad de documentos				
Pruebas de Personalidad				

Figura 18. Tipos de controles.

RESULTADO OBTENIDO.

Según los resultados obtenidos, se concluye que con un 100% de los resultados no se llevan controles para contratar trabajadores porque de este tipo de controles los realiza el departamento de recursos humanos, El DTIC-UPEC manifiesta el perfil para el puesto de trabajo.

Figura 19. Controles para contratación de personal.

Pregunta 16.

¿De las siguientes certificaciones cuáles posee para administrar el data center?

Conocimientos y certificaciones que debe disponer el personal que labora en el data center	Si	No
Técnico en Computación e informática o carreras afines		
Conocimiento en Sistemas Operativos, Redes y Soporte TI		
Inglés nivel Intermedio		
Scrum Foundation		
AWS cloud Practitioner		
Azure Fundamentals		
ITIL		
Microsoft 365 Fundamentals		
Certificado de base del centro de datos (DCFC®)		
Profesional Certificado en Centros de Datos (CDCP)		
Especialista certificado en centros de datos (CDCS)		
Experto certificado en centros de datos (CDCE)		
Profesional Certificado en Diseño de Cableado de Red (CNCDP)		
Especialista certificado en operaciones de instalaciones de centros de datos (CDFOS®)		
Gerente Certificado de Operaciones de Instalaciones de Centros de Datos (CDFOM)		
Especialista Certificado en Sostenibilidad Ambiental del Centro de Datos (CDESS)		
Profesional certificado en riesgos de centros de datos (CDRP)		
Especialista certificado en migración de centros de datos (CDMS)		
Consultor de diseño certificado TIA-942 (CTDC)		
Auditor Interno Certificado TIA-942 (CTIA)		

Figura 20. Capacitaciones que necesita un miembro a cargo del Data Center.

RESULTADO OBTENIDO.

Según los resultados de la encuesta, se entiende que los miembros del departamento de TIC tienen un promedio del 4,33 % de las capacitaciones y cursos necesarios para mantener un centro de data.

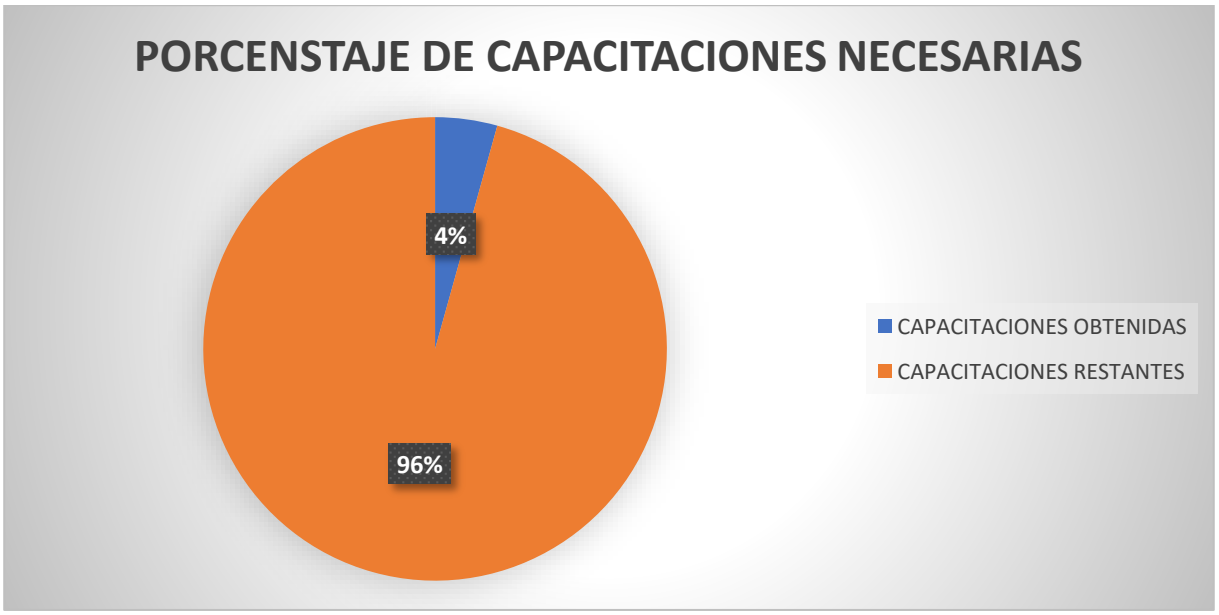


Figura 21. Porcentajes de capacitaciones necesarias.

Descripción: En la figura se muestra la cantidad de capacitaciones y certificaciones recomendadas para estar a cargo de un data center.

Pregunta 17.

¿Qué porcentaje de los equipos del data center pertenecen a la Universidad Politécnica Estatal del Carchi?

- Todos
- 75% de los equipos
- 50% de los equipos
- 25% de los equipos
- 0% de los equipos

RESULTADO OBTENIDO.

De acuerdo con los resultados obtenidos se puede afirmar que el 100% de los equipos que conforman el data center son pertenencia de la UPEC.

Pregunta 18.

¿Indique cómo realizan la clasificación de la información en el Data Center?

Privada (P)	Pública (PU)	Restringida (R)	Confidencial (C)	No Aplica (NA)

Figura 22. Siglas de la clasificación de la información en el data center.

INFORMACIÓN ALMACENADA EN EL DATA CENTER	P	PU	R	C	NA
Contraseñas					
Configuraciones de equipos					
Información de Autoridades					
Información de funcionarios					
Información de Docentes					
Información de Trabajadores					
Información de Estudiantes					
Sistema integrado					
Código fuente					
Información de pág. web					
Eventos					
Información Financiera					
Información académica					
Información Arquitectónica y estructural					
Inventario de Activos					

Figura 23. Tipos de información que posee el data center.

RESULTADO OBTENIDO.

Según la encuesta, el 60 % de la información del centro es privada, el 13 % pública y el 27 % restringida.

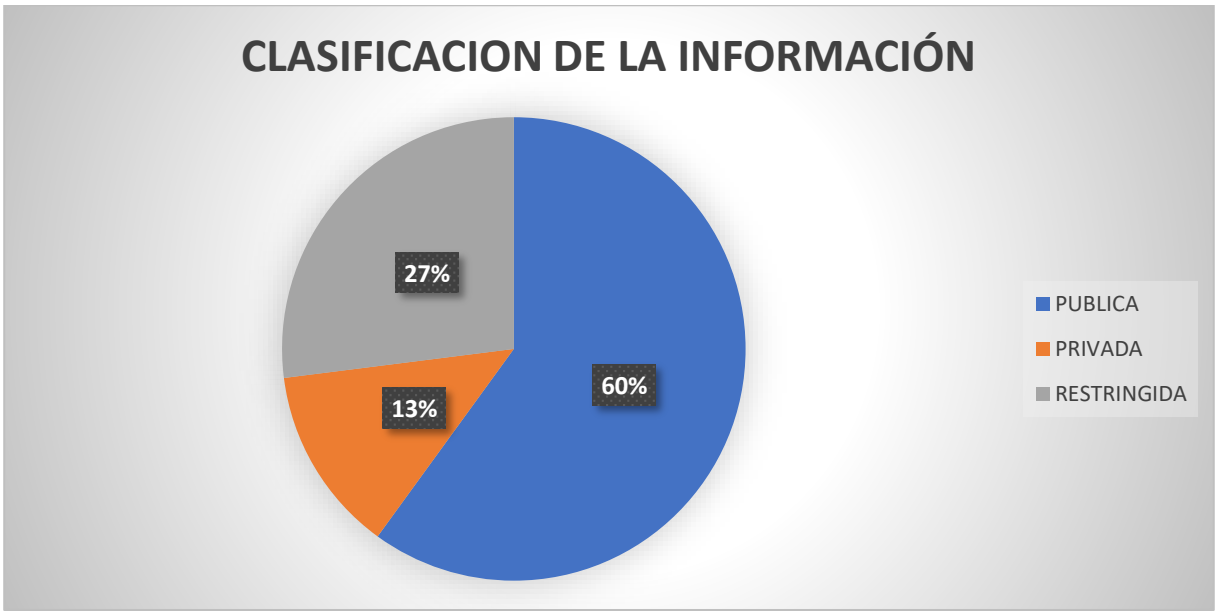


Figura 24. Clasificación de la información.

Descripción: En la figura se puede observar el porcentaje de la información que se encuentra pública, privada y restringida.

Pregunta 19.

¿Qué métodos utilizan para proteger la información ante accesos no autorizados?

Métodos	Si	No
Control de accesos		
Vigilancia 24/7		
Sistemas de videovigilancia y/o alarmas		
Climatización de los servidores		
Protección contra incendios		
Plan de gestión de riesgos		
Segmentación de redes y equipos críticos		
Firewalls físicos y virtuales		
IPS (Sistema de Prevención de Intrusos)		
Adecuación de Permisos		
Controles integrales de seguridad		
DLP (Solución de Prevención de Pérdida de Datos)		
DRP (Plan de Recuperación de Desastres)		
SIEM (Correlacionado de Eventos)		
Plan de Detección y Respuesta a Incidentes.		

Figura 25. Métodos para restringir el acceso no autorizado.

RESULTADO OBTENIDO.

De acuerdo con los resultados se obtuvo un 46.66% de cumplimiento con los métodos para evitar intrusos recomendados para un Data center.

Figura 26. Métodos recomendados para evitar intrusos.

Pregunta 20

¿Con qué frecuencia se cambia el acceso de los usuarios en los activos críticos del data center?

- Cada mes
- Cada 3 meses
- Cada 6 meses
- Cada año
- Más de un año
- Nunca

RESULTADO OBTENIDO.

De acuerdo con la información recolectada por medio de la encuesta realizada a los miembros encargados del manejo del data center, establecen que las copias se realizan en un 66.66% cada 6 meses y con un 33.33% cada mes, lo que indica que están dentro del promedio general aceptado por la normativa ISO 17799 la cual se centra en el uso de claves y periodos de cambio de estas.

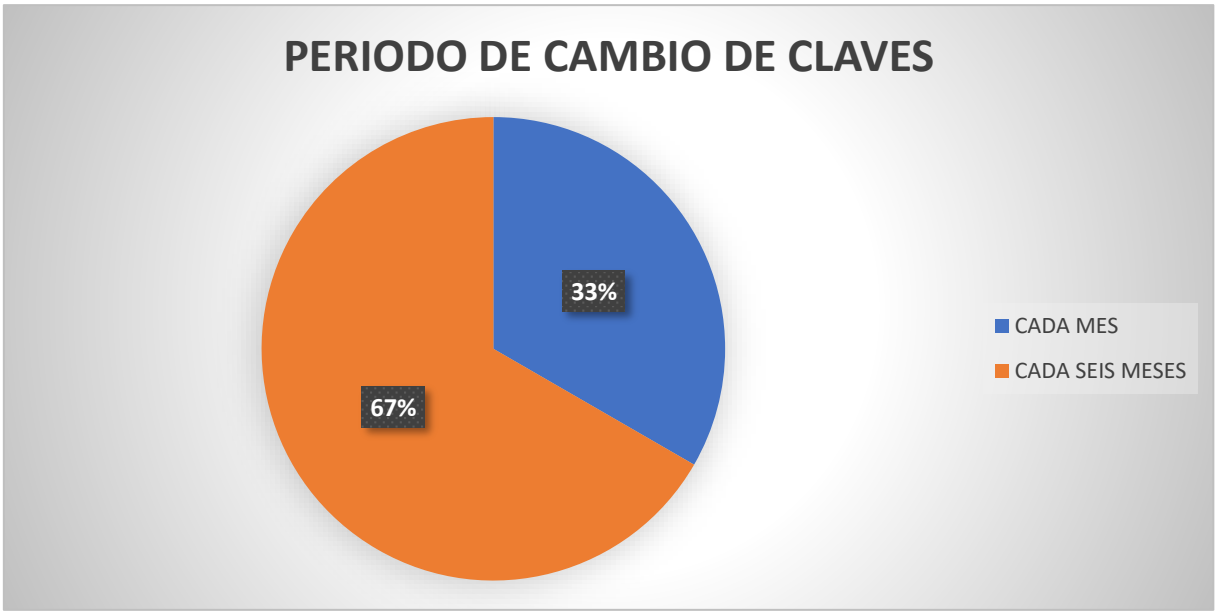


Figura 27. Periodo de cambio de claves.

Pregunta 21

¿Con qué frecuencia se cambia el acceso al firewall del data center?

- Cada mes
- Cada 3 meses
- Cada 6 meses
- Cada año
- Más de un año
- Nunca

RESULTADO OBTENIDO.

Con base en los resultados obtenidos en la encuesta realizada, se puede concluir con que el cambio de acceso al firewall se realiza con un porcentaje del 33,33% cada mes, con un 33,33% cada tres meses y con un 33,33% cada 6 meses, con base en esto se afirma que se sigue la normativa para cambio de contraseñas.

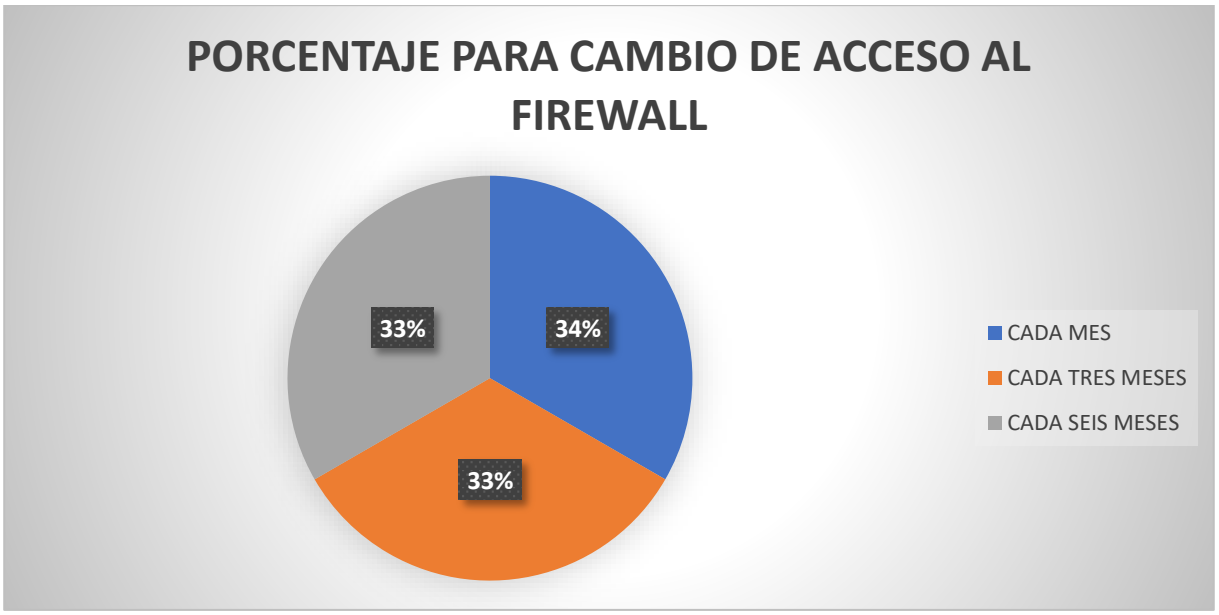


Figura 28. Porcentaje para cambio de acceso al firewall.

Pregunta 22.

¿Cómo controlan el acceso del personal que ya no se encuentra trabajando en la institución?

Control	Aplica	No Aplica
Eliminación de credenciales de acceso		
Reasignación de credenciales		
Cambio de contraseñas		
Suspensión del ingreso		

Figura 29. Controles que se aplican al personal no autorizado.

RESULTADO OBTENIDO.

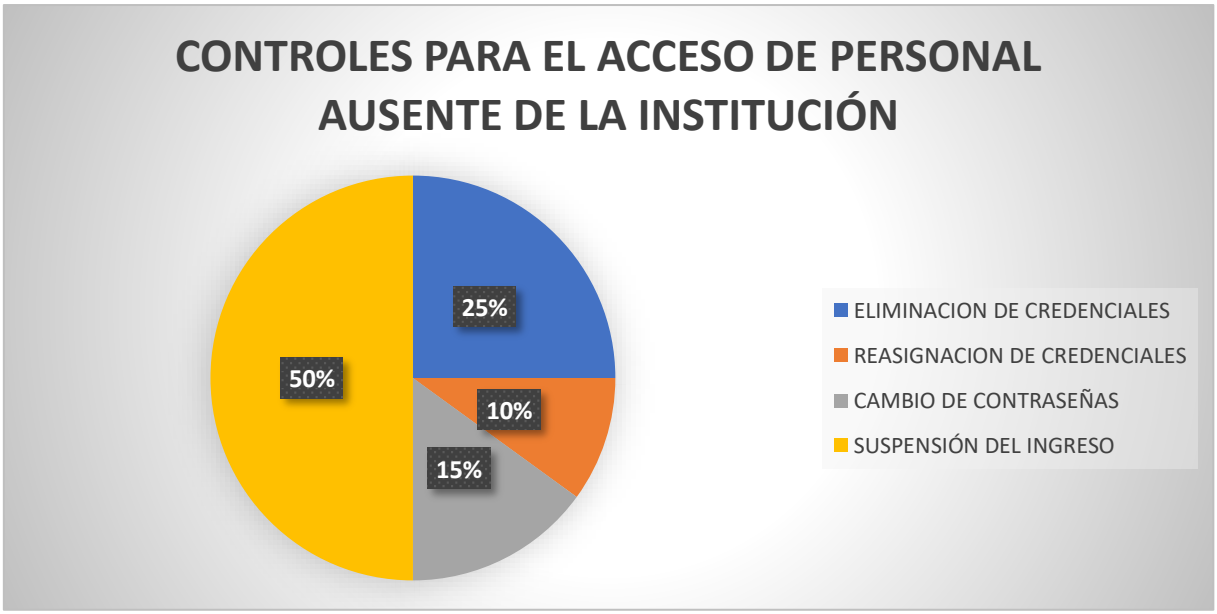


Figura 30. Controles para el acceso del personal ausente de la institución.

Con base en la figura 30 obtenidas mediante la recolección de información con la encuesta, se puede mirar que la suspensión del ingreso es el control más utilizado por los miembros que trabajan en el data center, seguido de la eliminación de credenciales, el cambio de contraseñas y la reasignación de credenciales.

Pregunta 23.

¿Qué controles de acceso utilizan para limitar el acceso a la información y funciones del sistema?

Controles físicos y lógicos	Si	No
Sensor biométrico		
Sensor de proximidad		
Cámaras de seguridad		
Servicio de guardias		
Puerta electrónica		
Acceso por credenciales		
Acceso concedido por administrador		
Firewall		
Cerradura por tarjeta electrónica		
Restricción de acceso por IP y/o MAC		

Figura 31. Controles físicos y lógicos.

RESULTADO OBTENIDO.

De acuerdo con los resultados obtenidos de la encuesta se pudieron extraer los siguientes datos: con un porcentaje del 40% el data center cuenta con los controles físicos recomendados para resguardar el bienestar de este y el 60% restante corresponde a los controles físicos que no disponen.

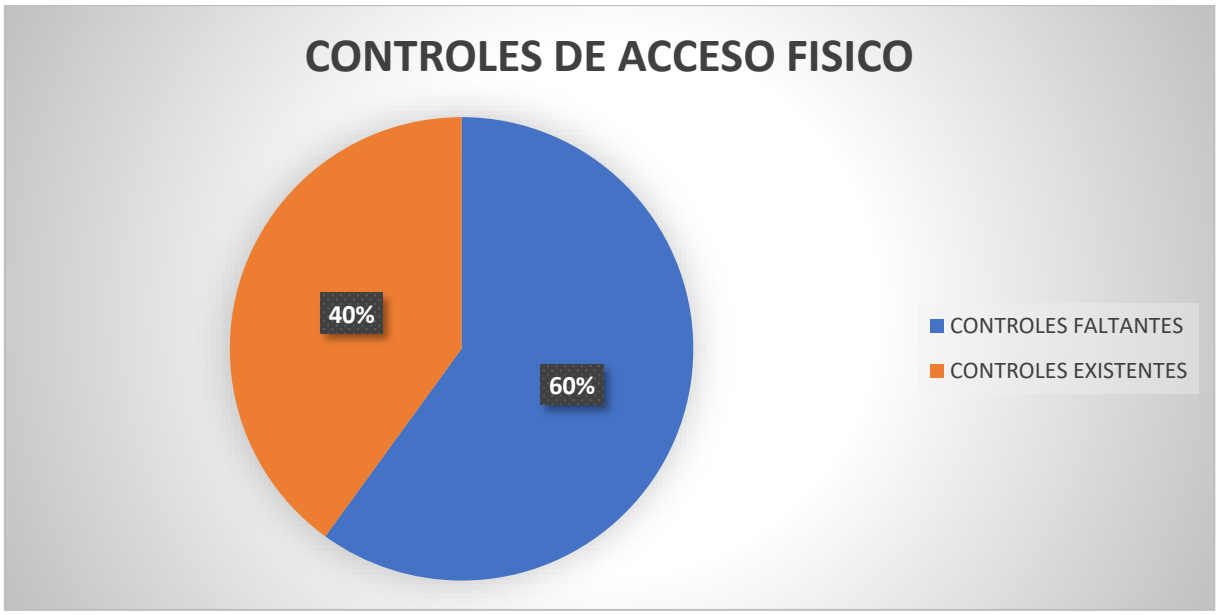


Figura 32. Controles de acceso físico.

Pregunta 24.

Niveles de seguridad de contraseñas

Nivel bajo: La contraseña solamente cuenta con un mínimo de 5 caracteres.

Nivel medio: La contraseña cuenta con un mínimo de 6 caracteres, además de cumplir con los siguientes requisitos:

- Incluir números y letras mayúsculas y minúsculas.
- Incluir al menos un carácter especial (#$%&).

Nivel alto: La contraseña cuenta con un mínimo de 6 caracteres, además de cumplir con los siguientes requisitos:

- Incluir números, letras mayúsculas y minúsculas.
- Incluir al menos un carácter especial (#$%&).
- La contraseña debe de contar con fecha de caducidad por lo menos de 90 días.
- Al cambiar por una nueva contraseña no debe ser igual o parecida a las 5 anteriores contraseñas (Nadeau, 2023).

De acuerdo con lo explicado anteriormente, ¿Cuál es el nivel de seguridad de las contraseñas?

- Nivel Bajo
- Nivel Medio
- Nivel Alto

RESULTADO OBTENIDO.

Se obtuvo un 100% en que las contraseñas que se utilizan en los accesos ya sean físicos o digitales al data center son de nivel medio lo que quiere decir que tienen una buena protección contra intentos de accesos no autorizados, sin embargo, no es excelente.

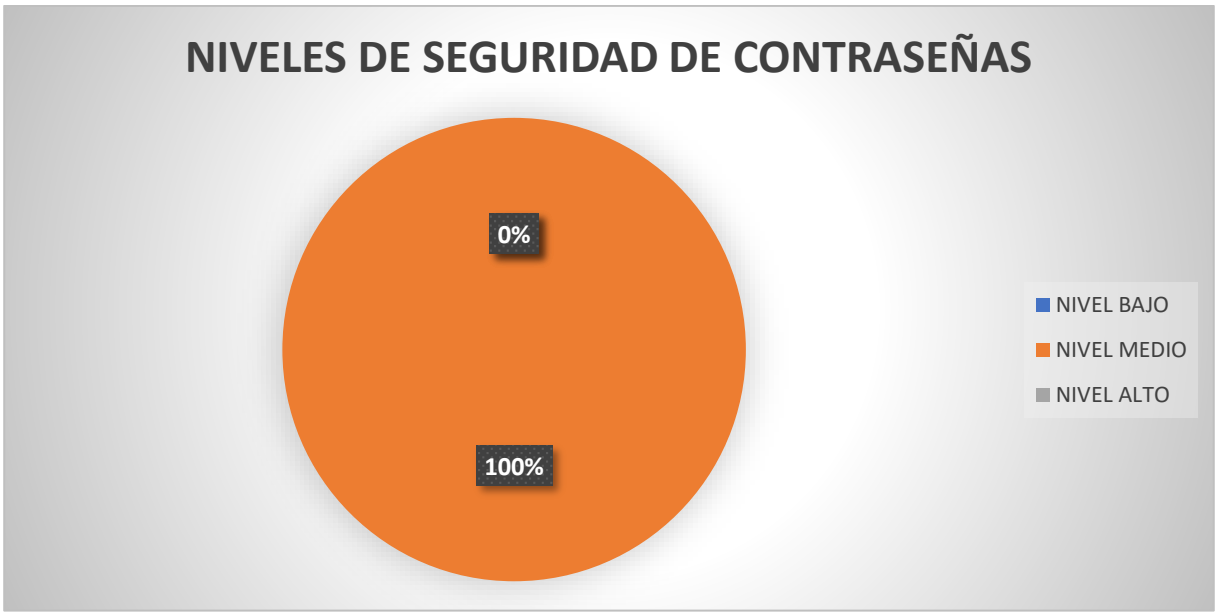


Figura 33. Niveles de seguridad de contraseñas.

Pregunta 25.

¿Existen controles de protección de equipos externos?

- Si
- No

RESULTADO OBTENIDO.

Con base en las encuestas se obtuvo con un 66,66% que los equipos externos no son protegidos por la institución y con un 33,33% que, si se protegen los equipos externos, indicando que algunos de los quipos si son protegidos y el resto no indicando una vulnerabilidad.

Figura 34. Equipos externos protegidos por la institución.

Pregunta 26.

¿Cuáles son los controles y como es la conexión?

RESULTADO OBTENIDO.

De acuerdo con la información recolectada mediante la encuesta y proporcionada por el ingeniero a cargo de telecomunicaciones y redes, se obtuvo que la conexión se lleva a través de convenios institucionales con CEDIA a través de WAP.

Pregunta 27.

¿Con qué frecuencia se realizan copias de respaldo de la información, software y sistema?

- Cada día
- Cada semana
- Cada mes
- Cada 3 meses
- Cada 6 meses
- Cada año
- Más de un año
- Nunca

RESULTADO OBTENIDO.

De acuerdo con la información recolectada por medio de las encuestas realizadas, se pudo observar que las copias de seguridad se realizan con un 60% cada semana, con un 20% cada día y con un 20% cada mes, lo que quiere decir que siguen un estándar o promedio aceptable con respecto con la normativa correspondiente.

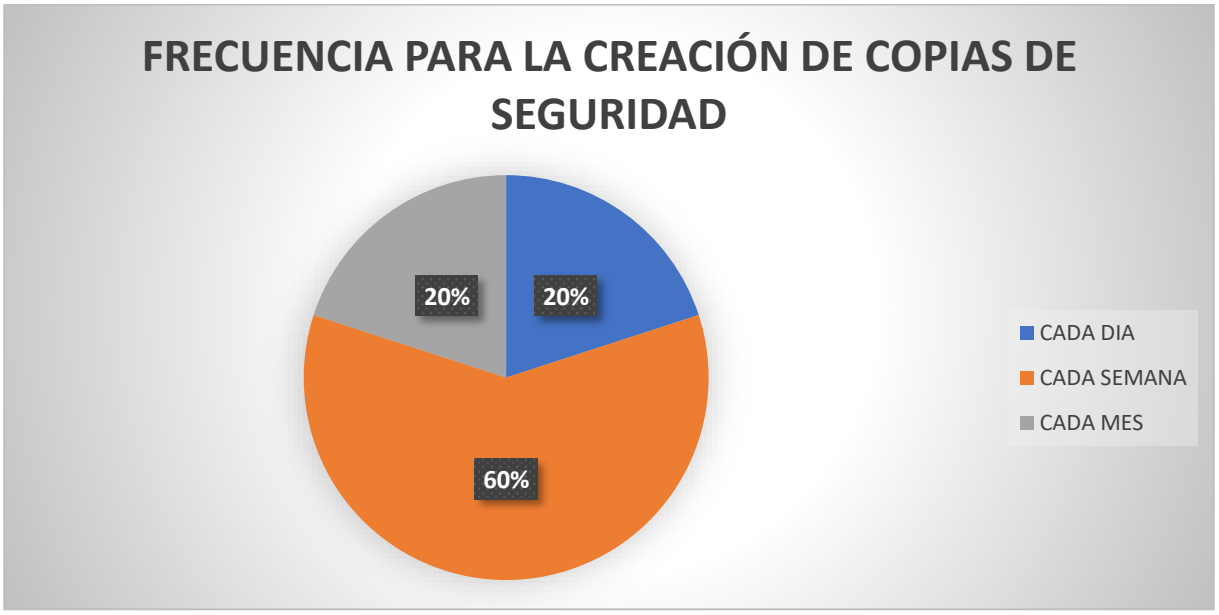


Figura 35. Frecuencia para la creación de copias de seguridad.

Pregunta 28.

¿Con qué frecuencia se realizan las pruebas de las copias de seguridad?

- Cada mes
- Cada 3 meses
- Cada 6 meses
- Cada año
- Más de un año
- Nunca

RESULTADO OBTENIDO.

Con base en las respuestas proporcionadas por los miembros a cargo del data center, se puede afirmar que las pruebas que se realizan a las copias de seguridad tienen un porcentaje del 33,33% cada tres meses, con un porcentaje del 33,33% cada seis meses y con un 33,33% cada año, indicando dos posibilidades que no se realizan pruebas a las copias de seguridad o que se realizan pruebas sin una planificación.

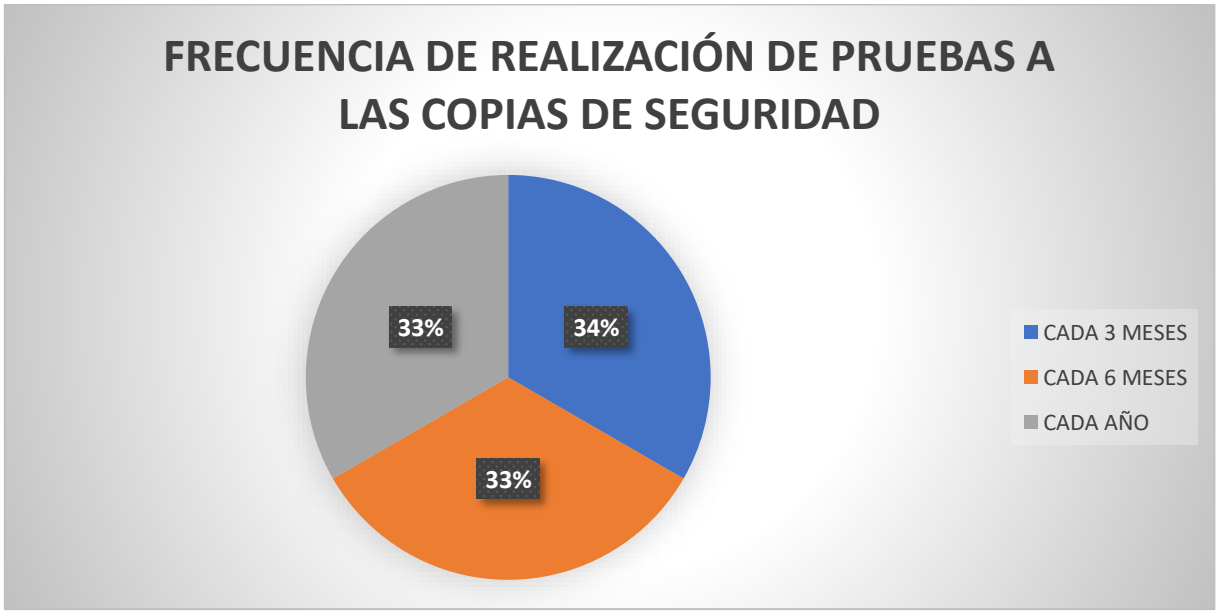


Figura 36. Frecuencia de realización de pruebas a las copias de seguridad.

Pregunta 29.

¿Cuál es el proceso de evaluación a las copias de seguridad?

RESULTADO OBTENIDO.

Con base a las respuestas brindadas por los miembros a cargo del data center, se obtuvieron los siguientes porcentajes en cuanto a los métodos para la evaluación de las copias de seguridad, los cuales corresponden en un 50% a probar la copia en un servidor disponible y el otro 50% en un ambiente de pruebas virtual que pertenece en el data center o al evaluador.

Figura 37. Métodos para evaluar las copias de seguridad.

Pregunta 30.

¿Se almacena las contraseñas en un sobre seguro?

- Si
- No

RESULTADO OBTENIDO.

Con base en la información brindada por la directora a cargo del departamento de TIC y del data center se obtuvo un 100% en que las contraseñas no almacenan las contraseñas de acceso del data center como de los servidores y del firewall en un sobre seguro.

Figura 38. Existencia de un sobre seguro.

Por esta razón se eliminaron las preguntas: 31, 32 y 33 por la razón que están interconectadas con esta pregunta en particular y al no poseer un sobre seguro no se puede tener un custodio ni un reglamento para este apartado.

Resultado Obtenido de la Encuesta aplicada a los miembros del data Center

Tabla 6. Documentos requeridos para la encuesta.

REQUISITOS	EVIDENCIA
Sistema de Gestión de seguridad de la Información	Existe documentación del año 2019 en donde fueron publicadas las políticas de seguridad de la información de la UPEC.
Certificaciones de estudios del jefe del departamento de TIC.	Certifica sus estudios como Ingeniera en ciencias computacionales y Magíster en Ingeniería de Software.
Inventario de activos informáticos	El inventario se encuentra desactualizado desde el 2018.
Matriz de riesgos de seguridad informática	No existe.
Planes de mejoramiento de seguridad informática	No existe.
Plan de contingencia de la seguridad informática	Cuenta con un Plan de contingencias obsoleto y desactualizado desde el 2017.
Procedimientos de asignación de credenciales a los usuarios	No existe, se realiza de forma empírica.
Procedimientos de asignación de contraseñas de red WIFI	No existe, se realiza de forma empírica.
Procedimientos de generación de contraseñas	No existe, se realiza de forma empírica.
Procedimiento de ejecución de Backups	Existen únicamente manuales de respaldo para Sistema Integrado, Aulas Virtuales y página web.
Procedimiento de Manejo de discos extraíbles	No existe, se realiza empíricamente
Procedimientos de control de acceso a internet	No existe, se realiza empíricamente.
Cronograma de mantenimiento de activos informáticos	Se realiza mediante una planificación anual que es aprobada a principios de año.
Hojas de vida de los activos informáticos	No existe
Compromiso de confidencialidad firmado por el personal	Existe el documento de confidencialidad el cual es firmado al realizar el contrato, el documento se anexa en la carpeta de cada trabajador.
Actas de capacitaciones a los usuarios internos en Seguridad Informática	No existe.

4.1.2. Resultados Obtenidos de las Encuestas a los estudiantes y docentes

El propósito fue encontrar probabilidades mínimas de que los estudiantes generen un ataque de ciberseguridad a los servidores del Data Center de la Universidad Politécnica Estatal del Carchi, por lo que todos los resultados obtenidos en todas las preguntas realizadas unirán en un solo resultado en general.

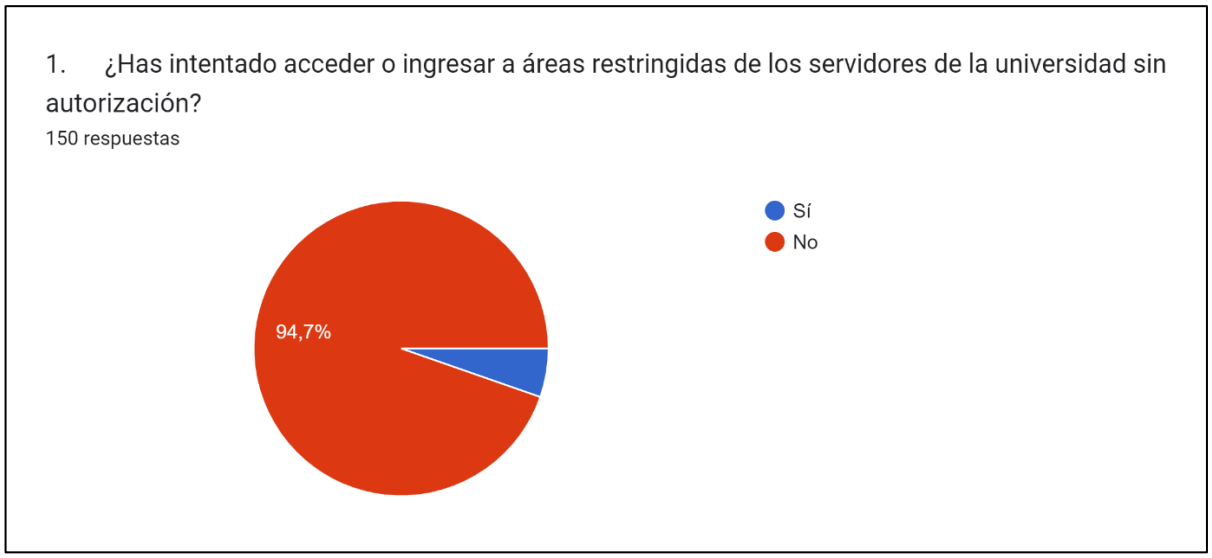


Figura 39. Pregunta para estudiantes y docentes 1.

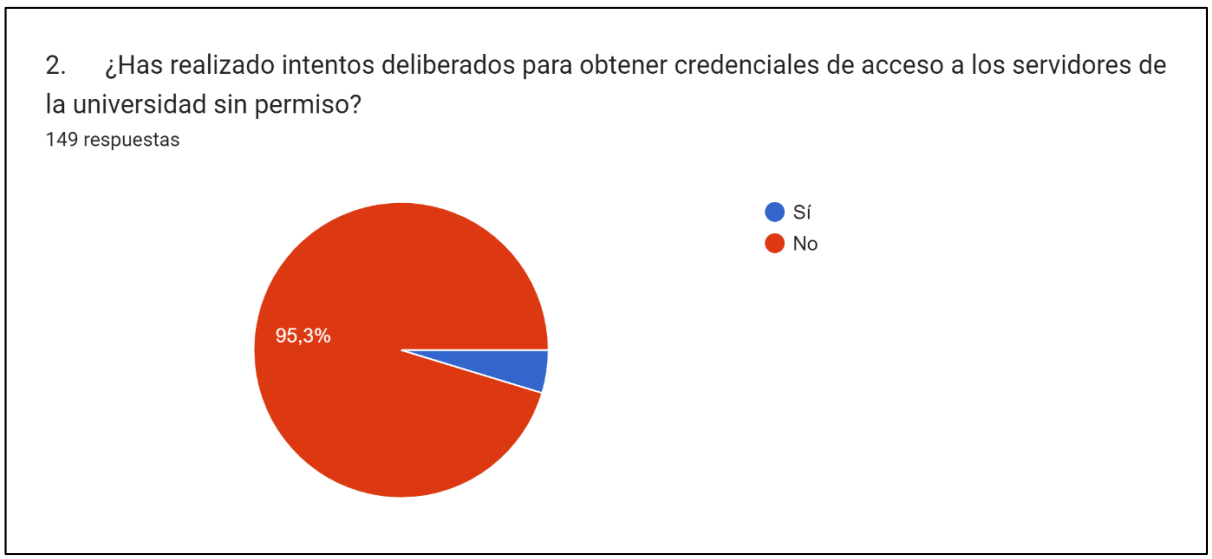


Figura 40. Pregunta para estudiantes y docentes 2.

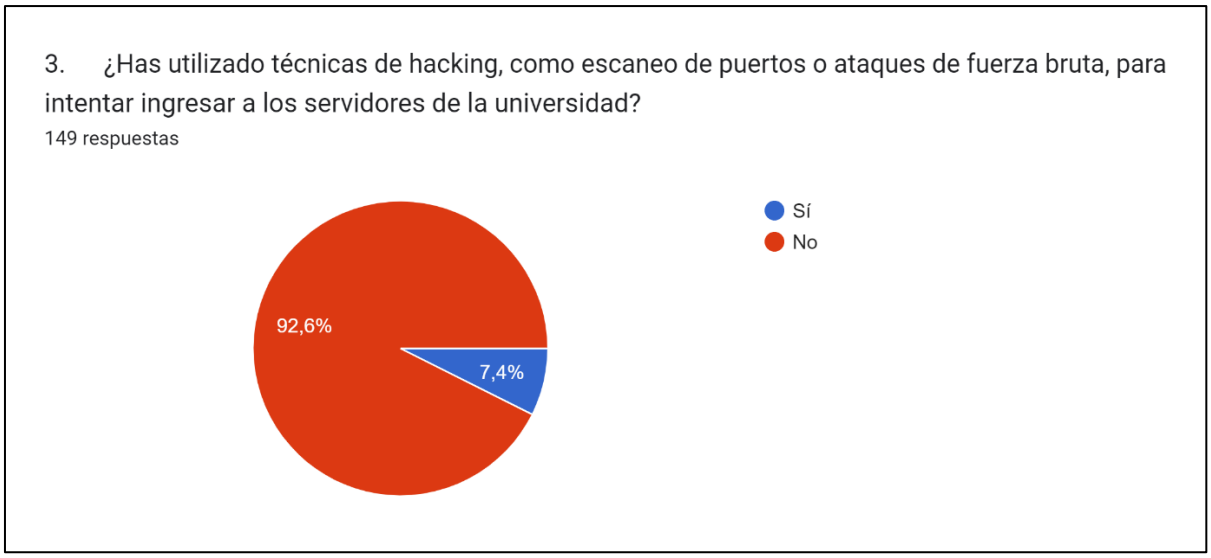


Figura 41. Pregunta para estudiantes y docentes 3.

Figura 42. Pregunta para estudiantes y docentes 4.

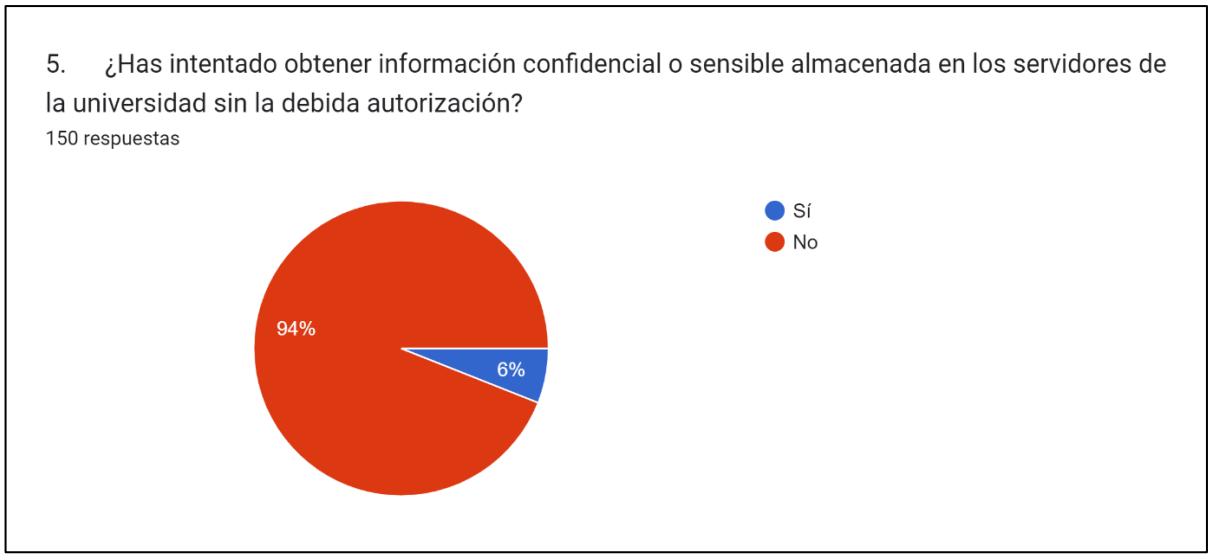


Figura 43. Pregunta para estudiantes y docentes 5.

Figura 44. Pregunta para estudiantes y docentes 6.

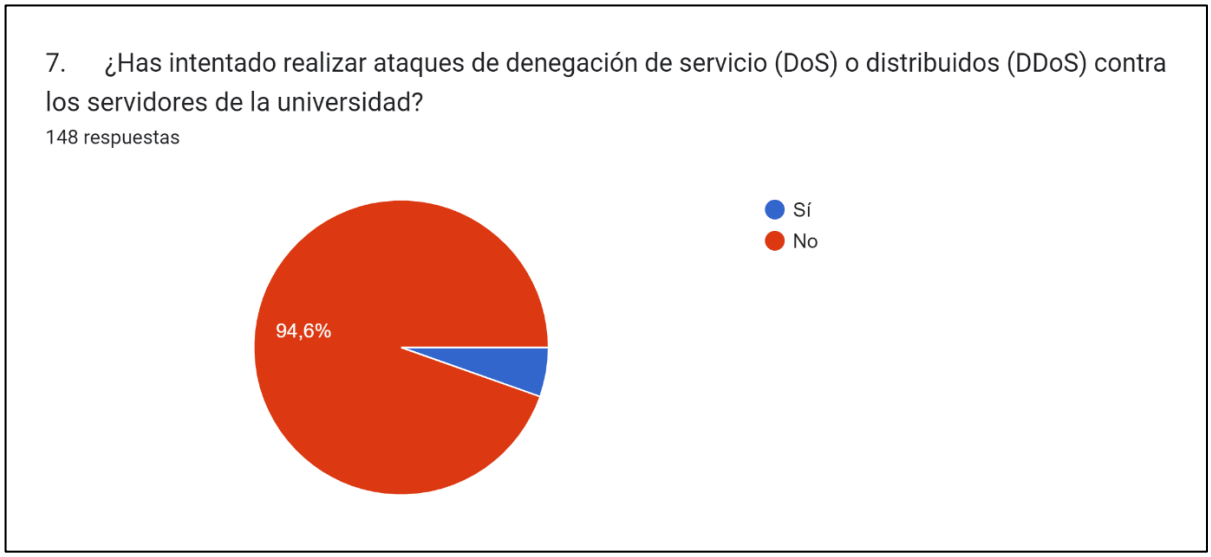


Figura 45. Pregunta para estudiantes y docentes 7.

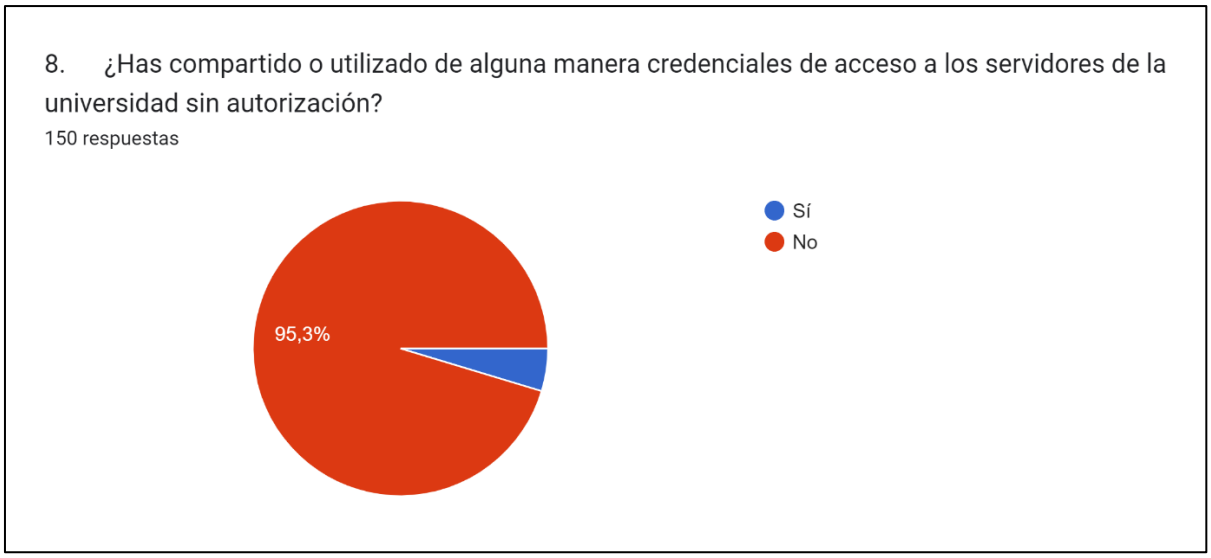


Figura 46. Pregunta para estudiantes y docentes 8.

Resultados obtenidos

Con los resultados de las encuestas realizas fueron: 5.3; 4.7; 7.4; 6.7; 6; 5.4; 5.4 y 4.7 los que generan un promedio general de 5.7% del "sí", lo que significa que la probabilidad de que los estudiantes son los causantes de un ataque de ciberseguridad a los servidores de la UPEC es baja.

4.1.3. Resultados obtenidos de la auditoría informática

Durante una reunión se dio conocer el objetivo y alcance de la auditoría (Anexo 4), la norma ISO/IEC a utilizar y se procedió a la revisión de los controles que van a hacer aplicados al data center, obteniendo que:

- La auditoría de seguridad de la información en el Data Center de la UPEC fue realizada mediante la aplicación de los controles de la normativa: ISO/IEC 27002:2013 "Código de prácticas para los controles de seguridad de la información".
- No se encontró documentación de auditorías previas.
- De un total de 114 controles, 83 no fueron aplicados a la revisión debido a que los controles no se adaptaban al Data Center, es decir, los controles que no fueron aplicados involucraban a otros departamentos que no se iban a ser auditados, además de que el Centro de datos no cuenta con un ambiente de desarrollo.
- 31 controles de la norma ISO 27002:2013 son seleccionados por los responsables del data center (Figura 47).
- Se indica identifica el estado de madures en el que se encuentran los controles seleccionados (Tabla 6).

ISO/IEC 27002:2013				Control Aplicable al Data Center		Estado actual del control
Dominio	**Objetivos de Control**	**Control**	**Acción**	**SI**	**NO**	
POLÍTICAS DE SEGURIDAD	5.1 Directrices de la Dirección en seguridad de la información	5.1.1 Políticas de seguridad de la información	Un conjunto de políticas para la seguridad de la información debe definirse, aprobarse por la gerencia, publicarse y comunicarse a los empleados y partes externas relevantes.	**x**		INICIAL
		5.1.2 Revisión de las políticas de seguridad de la información	Las políticas de seguridad de la información deben revisarse a intervalos planificados o si se producen cambios significativos para garantizar su idoneidad, adecuación y eficacia continuas.	**x**		INICIAL
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	6.1 Organización Interna	6.1.1 Roles y responsabilidades de seguridad de la información	Todas las responsabilidades de seguridad de la información deben definirse y asignarse.	**x**		REPETIBLE
		6.1.2 Segregación de funciones	Los deberes y las áreas de responsabilidad en conflicto deben separarse para reducir las oportunidades de modificación o uso indebido, no autorizado o no intencional de los	**x**		OPTIMIZADO

			activos de la organización.			
		6.1.3 Contacto con las autoridades	Deben mantenerse los contactos apropiados con las autoridades pertinentes.		**x**	
		6.1.4 Contacto con grupos de interés especial	Deben mantenerse los contactos apropiados con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.	**x**		INEXISTENTE
		6.1.5 Seguridad de la información en la gestión de proyectos	La seguridad de la información debe abordarse en la gestión de proyectos, independientemente del tipo de proyecto.		**x**	
	6.2 Dispositivos para movilidad y teletrabajo	6.2.1 Política de dispositivos móviles	Se debe adoptar una política y medidas de seguridad de apoyo para gestionar los riesgos introducidos por el uso de dispositivos móviles.		**x**	
		6.2.2 Teletrabajo	Se debe implementar una política y medidas de seguridad de apoyo para proteger la información a la que se accede, procesa o		**x**	

			almacena en los sitios de teletrabajo.			
SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	7.1 Antes de la Contratación	7.1.1 Investigación de Antecedentes	Los controles de verificación de antecedentes de todos los candidatos para el empleo deben llevarse a cabo de conformidad con las leyes, los reglamentos y la ética pertinentes y deben ser proporcionales a los requisitos comerciales, la clasificación de la información a la que se accede y los riesgos percibidos.	**x**		INEXISTENTE
		7.1.2 Términos y Condiciones de Contratación	Los acuerdos contractuales con los empleados y contratistas deben establecer sus responsabilidades y las de la organización en materia de seguridad de la información.		**x**	
	7.2 Durante la Contratación	7.2.1 Responsabilidades de Gestión	La gerencia debe exigir a todos los empleados y contratistas que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.	**x**		REPETIBLE

		7.2.2 Concienciación, Educación y Capacitación en Seguridad de la Información	Todos los empleados de la organización y, cuando corresponda, los contratistas deben recibir educación y capacitación de concientización adecuadas y actualizaciones periódicas en las políticas y procedimientos de la organización, según corresponda para su función laboral.		**x**	
		7.2.3 Proceso Disciplinario	Debe existir un proceso disciplinario formal y comunicado para tomar medidas contra los empleados que hayan cometido una violación de la seguridad de la información.		**x**	
	7.3 Cese o Cambio de puesto de trabajo	7.3.1 Cese o cambio de puesto de trabajo	Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos después de la terminación o él		**x**	
GESTIÓN DE ACTIVOS	8.1 Responsabilidad sobre los activos	8.1.1 Inventario de Activos	Deben identificarse los activos asociados con la información y las instalaciones de procesamiento de información y	**x**		ADMINISTRADO

			debe elaborarse y mantenerse un inventario de estos activos.			
		8.1.2 Propiedad de los Activos	Los activos mantenidos en el inventario deben ser propiedad.	**x**		INEXISTENTE
		8.1.3 Uso aceptable de los activos	Deben identificarse, documentarse e implementarse reglas para el uso aceptable de la información y de los activos asociados con la información y las instalaciones de procesamiento de la información.		**x**	
		8.1.4 Devolución de Activos	Todos los empleados y usuarios externos deben devolver todos los activos de la organización que posean al terminar su empleo, contrato o acuerdo.		**x**	
	8.2 Clasificación de la Información	8.2.1 Directrices de clasificación	La información debe clasificarse en términos de requisitos legales, valor, criticidad y sensibilidad a la divulgación o modificación no autorizada.	**x**		REPETIBLE
		8.2.2 Etiquetado y manipulación de la Información	Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información de		**x**	

			acuerdo con el esquema de clasificación de la información adoptado por la organización.			
		8.2.3 Manipulación de Activos	Los procedimientos para el manejo de activos deben desarrollarse e implementarse de acuerdo con el esquema de clasificación de la información adoptado por la organización.	**x**		REPETIBLE
	8.3 Manejo de los Soportes de Almacenamiento	8.3.1 Gestión de soportes extraíbles	Deben implementarse procedimientos para la gestión de medios extraíbles de acuerdo con el esquema de clasificación adoptado por la organización.		**x**	
		8.3.2 Eliminación de soportes	Los medios deben eliminarse de forma segura cuando ya no se necesiten, utilizando procedimientos formales.	**x**		INEXISTENTE
		8.3.3 Soportes Físicos en tránsito	Los medios que contienen información deben protegerse contra el acceso no autorizado, el uso indebido o la corrupción durante el transporte.	**x**		INICIAL
CONTROL DE ACCESO	9.1 Requisitos de negocio para control de acceso	9.1.1 Políticas de Control de Acceso.	Se debe establecer, documentar y revisar una		**x**	

			política de control de acceso en función de los requisitos de seguridad de la información y del negocio.			
		9.1.2 Control de acceso a las redes y servicios asociados	A los usuarios solo se les debe proporcionar acceso a la red y a los servicios de red para los que han sido específicamente autorizados.		**x**	
	9.2 Gestión de Acceso de usuario	9.2.1 Gestión de Altas/Bajas en el registro de usuarios	Debe implementarse un proceso formal de registro y cancelación de usuarios para permitir la asignación de derechos de acceso.		**x**	
		9.2.2 Gestión de los derechos de acceso asignados a usuarios	Se debe implementar un proceso formal de provisión de acceso de usuarios para asignar o revocar derechos de acceso para todos los tipos de usuarios a todos los sistemas y servicios.		**x**	
		9.2.3 Gestión de los Derechos de acceso con privilegios especiales	La asignación y el uso de derechos de acceso privilegiado deben estar restringidos y controlados.		**x**	

		9.2.4 Gestión de Información Confidencial de autentificación de usuarios	La asignación de información de autenticación secreta debe controlarse a través de un proceso de gestión formal.	**x**		INICIAL
		9.2.5 Revisión de los derechos de acceso de los usuarios	Los propietarios de activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.	**x**		INEXISTENTE
		9.2.6 Retirada o adaptación de los derechos de acceso	Los derechos de acceso de todos los empleados y usuarios externos a la información y las instalaciones de procesamiento de información deben eliminarse al terminar su empleo, contrato o acuerdo, o ajustarse al cambiar.		**x**	
	9.3 Responsabilidades del Usuario	9.3.1 Uso de información confidencial para la autentificación	Se debe exigir a los usuarios que sigan las prácticas de la organización en el uso de información de autenticación secreta.	**x**		INEXISTENTE
	9.4 Control de acceso a sistema y aplicaciones	9.4.1 Restricción de acceso a la Información	El acceso a la información y las funciones del sistema de aplicaciones debe estar restringido de acuerdo con la política de		**x**	

			control de acceso.			
		9.4.2 Procedimientos seguros de inicio de sesión	Cuando lo requiera la política de control de acceso, el acceso a los sistemas y aplicaciones debe controlarse mediante un procedimiento de inicio de sesión seguro.	**x**		INEXISTENTE
		9.4.3 Gestión de Contraseñas de Usuario	Los sistemas de gestión de contraseñas deben ser interactivos y garantizar contraseñas de calidad.		**x**	
		9.4.4 Uso de herramientas de administración de sistemas	El uso de programas de utilidad que puedan anular los controles del sistema y de las aplicaciones debe restringirse y controlarse estrictamente.		**x**	
		9.4.5 Control de acceso al código fuente de los programas	El acceso al código fuente del programa debe estar restringido.		**x**	
CIFRADO	10.1 Controles Criptográficos	10.1.1 Políticas del uso de los controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	**x**		INICIAL
		10.1.2 Gestión de claves	Se debe desarrollar e implementar una política sobre el		**x**	

			uso, la protección y la vida útil de las claves criptográficas durante todo su ciclo de vida.			
SEGURIDAD FÍSICA Y AMBIENTAL	11.1 Áreas de seguridad	11.1.1 Perímetro de Seguridad Física	Los perímetros de seguridad deben definirse y usarse para proteger las áreas que contienen información confidencial o crítica y las instalaciones de procesamiento de información.	**x**		OPTIMIZADO
		11.1.2 Controles Físicos de Entrada	Las áreas seguras deben estar protegidas por controles de entrada apropiados para garantizar que solo el personal autorizado se les permite el acceso.	**x**		INICIAL
		11.1.3 Seguridad de oficinas, despachos y recursos	Se debe diseñar y aplicar seguridad física para oficinas, salas e instalaciones.	**x**		INICIAL
		11.1.4 Protección contra las amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.		**x**	
		11.1.5 El trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajar en áreas seguras.		**x**	

		11.1.6 Áreas de acceso público, carga y descarga	Los puntos de acceso como las áreas de entrega y carga y otros puntos donde personas no autorizadas podrían ingresar a las instalaciones deben controlarse y, si es posible, aislarse de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	**x**		INICIAL
	11.2 Seguridad de los equipos	11.2.1 Emplazamiento y protección de equipos	El equipo debe ubicarse y protegerse para reducir los riesgos de amenazas y peligros ambientales, y las oportunidades de acceso no autorizado.	**x**		REPETIBLE
		11.2.2 Instalación de suministros	El equipo debe estar protegido contra cortes de energía y otras interrupciones causadas por fallas en los servicios de apoyo.	**x**		INEXISTENTE
		11.2.3 Seguridad del cableado	El cableado de energía y telecomunicaciones que transporta datos o servicios de información de apoyo debe protegerse contra intercepciones, interferencias o daños.		**x**	

		11.2.4 Mantenimiento de los equipos	El equipo debe mantenerse correctamente para garantizar su disponibilidad e integridad continuas.		**x**	
		11.2.5 Salida de activos fuera de las dependencias de la empresa	El equipo, la información o el software no deben sacarse del sitio sin autorización previa.	**x**		ADMINISTRADO
		11.2.6 Seguridad de los equipos y activos fuera de las instalaciones	La seguridad debe aplicarse a los activos externos teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.		**x**	
		11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento	Todos los elementos del equipo que contengan medios de almacenamiento deben verificarse para garantizar que todos los datos confidenciales y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.	**x**		DEFINIDO
		11.2.8 Equipo informático de usuarios desatendido	Los usuarios deben asegurarse de que el equipo desatendido tenga la protección adecuada.		**x**	

		11.2.9 Políticas de puesto de trabajo despejado y bloqueo de pantalla	Debe adoptarse una política de escritorio despejado para documentos y medios de almacenamiento extraíbles y una política de pantalla despejada para las instalaciones de procesamiento de información.		**x**	
SEGURIDAD EN LA OPERATIVIDAD	12.1 Responsabilidades y procedimientos de operación	12.1.1 Documentación de procedimientos de operación	Los procedimientos operativos deben documentarse y ponerse a disposición de todos los usuarios que los necesiten.		**x**	
		12.1.2 Gestión de cambios	Deben controlarse los cambios en la organización, los procesos comerciales, las instalaciones y los sistemas de procesamiento de información que afectan la seguridad de la información.		**x**	
		12.1.3 Gestión de capacidades	El uso de los recursos debe monitorearse, ajustarse y hacerse proyecciones de los requisitos de capacidad futuros para garantizar el rendimiento requerido del sistema.		**x**	

		12.1.4 Separación de entornos de desarrollo, prueba y producción	Los entornos de desarrollo, prueba y operación deben estar separados para reducir los riesgos de acceso no autorizado o cambios en el entorno operativo.	**x**		INEXISTENTE
	12.2 Protección contra código malicioso	12.2.1 Controles contra código malicioso	Deben implementarse controles de detección, prevención y recuperación para proteger contra el malware, combinados con la conciencia adecuada del usuario.	**x**		INEXISTENTE
	12.3 Copias de seguridad	12.3.1 Copias de seguridad de la Información	Las copias de respaldo de la información, el software y las imágenes del sistema deben tomarse y probarse periódicamente de acuerdo con una política de respaldo acordada.	**x**		REPETIBLE
	12.4 Registro de actividad y supervisión	12.4.1 Registro y gestión de eventos de actividad	Se deben producir, mantener y revisar regularmente registros de eventos que registren las actividades de los usuarios, las excepciones, las fallas y los eventos de		**x**	

			seguridad de la información.			
		12.4.2 Protección de registros de información	Las instalaciones de registro y la información de registro deben protegerse contra la manipulación y el acceso no autorizado.		**x**	
		12.4.3 Registro de actividades del administrador y operador del sistema	Las actividades del administrador del sistema y del operador del sistema deben registrarse y los registros deben protegerse y revisarse periódicamente.		**x**	
		12.4.4 Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información relevantes dentro de una organización o dominio de seguridad deben sincronizarse con una única fuente de tiempo de referencia.	**x**		OPTIMIZADO
	12.5 Control de software en explotación	12.5.1 Instalación del software en sistemas en producción	Se deben implementar procedimientos para controlar la instalación de software en los sistemas operativos.	**x**		DEFINIDO
	12.6 Gestión de las vulnerabilidades técnicas	12.6.1 Gestión de las vulnerabilidades técnicas	La información sobre las vulnerabilidades técnicas de los sistemas de información que se utilizan se debe obtener de		**x**	

			manera oportuna, se debe evaluar la exposición de la organización a dichas vulnerabilidades y se deben tomar las medidas apropiadas para abordar el riesgo asociado.			
		12.6.2 Restricciones en la instalación de software	Deben establecerse e implementarse reglas que rijan la instalación de software por parte de los usuarios.		**x**	
	12.7 Consideraciones de las auditorías de los sistemas de información	12.7.1 Controles de auditoría de los sistemas de información	Los requisitos de auditoría y las actividades que involucran la verificación de los sistemas operativos deben planificarse y acordarse cuidadosamente para minimizar las interrupciones en los procesos comerciales.		**x**	
SEGURIDAD EN LAS TELECOMUNICACIONES	13.1 Gestión de la seguridad en las redes	13.1.1 Controles de red	Las redes deben administrarse y controlarse para proteger la información en los sistemas y aplicaciones.		**x**	
		13.1.2 Mecanismos de seguridad asociados a servicios en red	Los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red deben identificarse e incluirse en los acuerdos de		**x**	

			servicios de red, ya sea que estos servicios se brinden internamente o se subcontraten.			
		13.1.3 Segregación de redes	Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en las redes.		**x**	
	13.2 Intercambio de Información con partes externas	13.2.1 Políticas y procedimientos de intercambio de información	Deben existir políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.		**x**	
		13.2.2 Acuerdos de intercambio	Los acuerdos deben abordar la transferencia segura de información comercial entre la organización y partes externas.		**x**	
		13.2.3 Mensajería electrónica	La información involucrada en la mensajería electrónica debe protegerse adecuadamente.		**x**	
		13.2.4 Acuerdos de confidencialidad y secreto	Los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la		**x**	

			información deben identificarse, revisarse periódicamente y documentarse.			
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	14.1 Requisitos de seguridad de los sistemas de información	14.1.1 Análisis y especificación de los requisitos de seguridad	Los requisitos relacionados con la seguridad de la información deben incluirse en los requisitos para nuevos sistemas de información o mejoras a los sistemas de información existentes.		**x**	
		14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas	La información involucrada en los servicios de aplicaciones que pasan por redes públicas debe protegerse de actividades fraudulentas, disputas de contratos y divulgación y modificación no autorizadas.		**x**	
		14.1.3 Protección de las transacciones por redes telemáticas	La información involucrada en las transacciones del servicio de aplicaciones debe protegerse para evitar transmisiones incompletas, enrutamiento incorrecto, alteración de mensajes no autorizados, divulgación no autorizada, duplicación o reproducción de		**x**	

			mensajes no autorizados.			
	14.2 Seguridad de los procesos de desarrollo y soporte	14.2.1 Políticas de desarrollo seguro de software	Las reglas para el desarrollo de software y sistemas deben establecerse y aplicarse a los desarrollos dentro de la organización.		**x**	
		14.2.2 Procedimientos de control de cambios en los sistemas	Los cambios en los sistemas dentro del ciclo de vida del desarrollo deben controlarse mediante el uso de procedimientos formales de control de cambios.		**x**	
		14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativa	Cuando se cambian las plataformas operativas, las aplicaciones críticas para el negocio deben revisarse y probarse para garantizar que no haya un impacto adverso en las operaciones o la seguridad de la organización.		**x**	
		14.2.4 Restricciones a los cambios en los paquetes de software	Deben desaconsejarse las modificaciones a los paquetes de software, limitarse a los cambios necesarios y todos los cambios deben		**x**	

			controlarse estrictamente.			
		14.2.5 Uso de principios de ingeniería en protección de sistemas	Los principios para diseñar sistemas seguros deben establecerse, documentarse, mantenerse y aplicarse a cualquier esfuerzo de implementación de sistemas de información.		**x**	
		14.2.6 Seguridad en entornos de desarrollo	Las organizaciones deben establecer y proteger adecuadamente entornos de desarrollo seguros para el desarrollo de sistemas y los esfuerzos de integración que cubran todo el ciclo de vida del desarrollo del sistema.		**x**	
		14.2.7 Externalización del desarrollo de software	La organización debe supervisar y controlar la actividad de desarrollo de sistemas subcontratados.		**x**	
		14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas	La prueba de la funcionalidad de seguridad debe llevarse a cabo durante el desarrollo.		**x**	
		14.2.9 Pruebas de aceptación	Deben establecerse programas de prueba de aceptación y criterios relacionados		**x**	

			para nuevos sistemas de información, actualizaciones y nuevas versiones.			
	14.3 Datos de prueba	14.3.1 Protección de los datos utilizados en pruebas	Los datos de prueba deben seleccionarse cuidadosamente, protegerse y controlarse.		**x**	
RELACIONES CON SUMINISTRADORES	15.1 Seguridad de la información en las relaciones con suministradores	15.1.1 Políticas de seguridad de la información para suministradores	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso del proveedor a los activos de la organización deben acordarse con el proveedor y documentarse.		**x**	
		15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores	Todos los requisitos de seguridad de la información relevantes deben establecerse y acordarse con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información de la organización.		**x**	
		15.1.3 Cadena de suministros en tecnologías de la información y comunicación	Los acuerdos con los proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los		**x**	

			servicios de tecnología de la información y las comunicaciones y la cadena de suministro del producto.			
	15.2 Gestión de la prestación del servicio por suministradores	15.2.1 Supervisión y revisión de los servicios prestados por terceros	Las organizaciones deben monitorear, revisar y auditar regularmente la prestación de servicios de los proveedores.		**x**	
		15.2.2 Gestión de cambios en los servicios prestados por terceros	Los cambios en la prestación de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, los procedimientos y los controles de seguridad de la información existentes, deben gestionarse teniendo en cuenta la criticidad de la información comercial, los sistemas y los procesos involucrados y la reevaluación de los riesgos.		**x**	
GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	16.1 Gestión de incidentes en la seguridad de la información	16.1.1 Responsabilidades y procedimientos	Deben establecerse responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de		**x**	

			seguridad de la información.			
		16.1.2 Notificación de los eventos de seguridad de la información	Los eventos de seguridad de la información deben informarse a través de los canales de gestión apropiados lo más rápido posible.		**x**	
		16.1.3 Notificación de puntos débiles de la seguridad	Se debe exigir a los empleados y contratistas que utilizan los sistemas y servicios de información de la organización que noten y notifiquen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.		**x**	
		16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones	Los eventos de seguridad de la información deben evaluarse y debe decidirse si se clasificarán como incidentes de seguridad de la información.		**x**	
		16.1.5 Respuesta a los incidentes de seguridad	Se debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.		**x**	
		16.1.6 Aprendizaje de	El conocimiento obtenido del análisis y la		**x**	

		los incidentes de seguridad	resolución de incidentes de seguridad de la información debe utilizarse para reducir la probabilidad o el impacto de futuros incidentes.			
		16.1.7 Recopilación de evidencias	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de la información, que pueda servir como evidencia.		**x**	
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	17.1 Continuidad de la seguridad de la información	17.1.1 Planificación de la continuidad de la seguridad de la información	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o un desastre.		**x**	
		17.1.2 Implantación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel requerido de continuidad para la seguridad de la información durante una situación adversa.		**x**	

		17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe verificar los controles de continuidad de seguridad de la información establecidos e implementados a intervalos regulares para garantizar que sean válidos y efectivos durante situaciones adversas.		**x**	
	17.2 Redundancias	17.2.1 Disponibilidad de las instalaciones para el procesamiento de la información	Las instalaciones de procesamiento de información deben implementarse con suficiente redundancia para cumplir con los requisitos de disponibilidad.		**x**	
CUMPLIMIENTO	18.1 cumplimiento de los requisitos legales y contractuales.	18.1.1 Identificación de la legislación aplicable	Todos los requisitos legales, reglamentarios y contractuales relevantes y el enfoque de la organización para cumplir con estos requisitos deben identificarse, documentarse y mantenerse explícitamente actualizados para cada sistema de información y la organización.		**x**	
		18.1.2 Derechos de propiedad intelectual (DPI)	Deben implementarse procedimientos apropiados para garantizar el cumplimiento de los requisitos		**x**	

			legislativos, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.			
		18.1.3 Protección de los registros de la organización	Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legales, reglamentarios, contractuales y comerciales.		**x**	
		18.1.4 Protección de datos y privacidad de la información personal	La privacidad y la protección de la información de identificación personal deben garantizarse según lo exija la legislación y las reglamentaciones pertinentes, cuando corresponda.		**x**	
		18.1.5 Regulación de los controles criptográficos	Los controles criptográficos deben utilizarse de conformidad con todos los acuerdos, leyes y reglamentos pertinentes.		**x**	
	18.2 Revisiones de la seguridad de la información	18.2.1 Revisión Independiente de la seguridad de la información	El enfoque de la organización para gestionar la seguridad de la información y su implementación (es decir,		**x**	

			objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) debe revisarse de forma independiente a intervalos planificados o cuando ocurran cambios significativos.			
		18.2.2 Cumplimiento de las políticas y normas de seguridad.	Los gerentes deben revisar periódicamente el cumplimiento de los procedimientos y el procesamiento de la información dentro de su área de responsabilidad con las políticas de seguridad, los estándares y cualquier otro requisito de seguridad apropiado.		**x**	
		18.2.3 Comprobación del cumplimiento	Los sistemas de información deben revisarse periódicamente para verificar que cumplan con las políticas y estándares de seguridad de la información de la organización.		**x**	

Figura 47. Selección de Controles de la Normativa ISO/IEC 27002.

En la tabla 7 se muestra el estado de los controles considerados en la auditoría realizada durante la realización del trabajo de integración curricular, esta muestra porcentajes y estados de cada control de la normativa ISO/IEC 27002.

Tabla 7. Estado de controles ISO/IEC 27002.

Estado	Significado	Proporción de Controles de Seguridad de la Información.
Desconocido	No ha sido verificado.	0%
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	8.77%
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte de tener personal de la alta calidad.	7.02%
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos, propios, informales). La responsabilidad es individual. No hay formación.	5,26%
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el responsable de Seguridad ni por la Dirección.	1,75%
Administrado	El control se lleva a cabo de acuerdo con un procedimiento documentado, aprobado y formalizado.	1.75%
Optimizado	El control se aplica de acuerdo con un procedimiento documentado, aprobado y formalizado y su eficacia se mide periódicamente indicadores.	2.63%
No Aplicable	Todos los requerimientos principales de ISO/IEC 27002 son de obligatorios. De otro modo, pueden ser ignorados por administración.	73.68%
	Total	100%

Con base en los resultados mostrados por la tabla 7 se puede observar que el Data Center cumple con un porcentaje del 4.38% de todos los controles establecidos por la normativa ISO/IEC 27002, se espera conseguir con la aplicación del plan de contingencia alcanzar el 27.19% de los controles establecidos por la normativa antes mencionada. Cabe recalcar que el 27.19% se restringe a los controles enfocados a Data Centers, debido a que el presente trabajo de investigación se llevó a cabo con ese enfoque.

Figura 48. Porcentaje de Cumplimiento de controles ISO/IEC 27002.

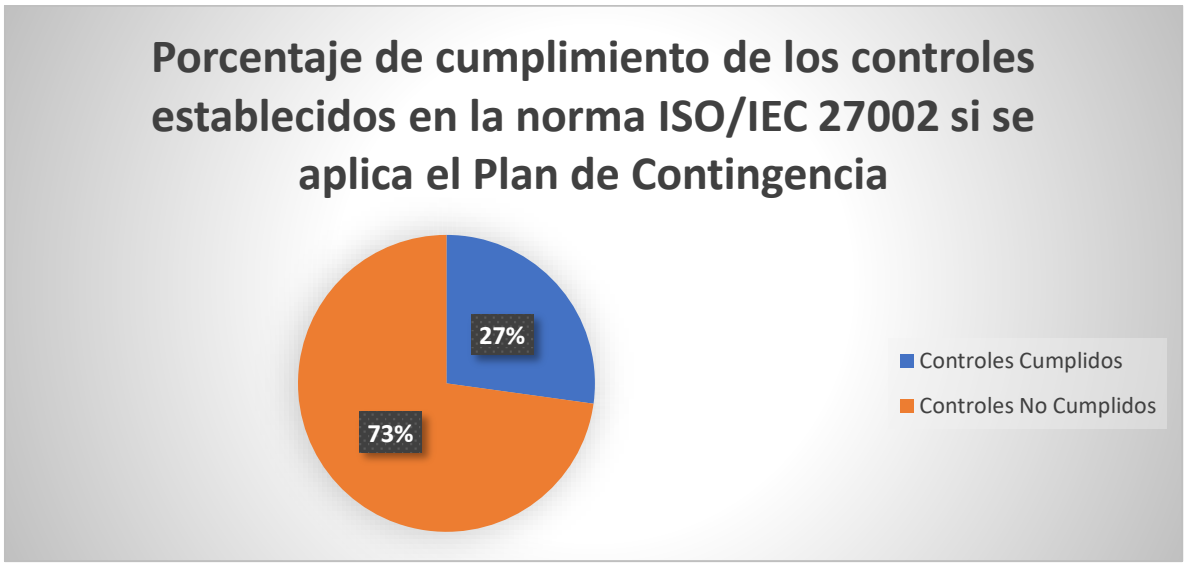


Figura 49. Porcentaje de cumplimiento al aplicar controles ISO/IEC 27002.

Con base a las figuras mostradas anteriormente (Figura 48 y Figura 49) se puede observar la gran mejora en cuanto al cumplimiento de las normativas establecidas si se llega a aplicar la propuesta del plan de contingencia, logrando llevar muchos de

los estados de los controles a uno mayor, es decir, evolucionando de un estado Iniciado o incluso inexistente a un estado Administrado o incluso a un estado Optimizado.

4.2. DISCUSIÓN

Tal como se pudo observar en los resultados del presente trabajo de investigación y la información que se recolectó mediante encuestas a los miembros a cargo del data center, a continuación, se mostraran los resultados obtenidos durante el presente trabajo de investigación:

4.2.1. Identificación de riesgos.

Tal como se mostró en anteriores capítulos se tomó como base las diferentes normas que se relacionan directamente con la creación de planes de contingencia y al tratamiento de riesgos y la seguridad de la información, coincidiendo con los trabajos de Burgos (2020) y Gonzabay (2021-2) en los cuales se realizó diferente formas para la identificación de riesgos que afectan a los Data Centers, tanto en los dos trabajos se realizaron la presentación de riesgos amplios sin especificación, lo cual no se realizó en este trabajo de investigación dado que los riesgos fueron localizados mediante el cumplimiento de controles de la normativa auditada la cual es la norma ISO/IEC 27002, además de que estos riesgos también fueron encontrados mediante la encuesta realizada a miembros del departamento de TIC.

4.2.2. Evaluación de Riesgos

Los resultados obtenidos en la Identificación de riesgos como tal ya se mostraron en la propuesta realizada (Plan de contingencia), cabe recalcar que en el trabajo de Núñez (2022) la Evaluación de los riesgos se llevó a cabo mediante criterio propio del autor, más no fue basado ningún reglamento, por otro lado el trabajo de Gonzabay (2021-2) se destacó que la evaluación de los riesgos se llevó a cabo de acuerdo a la Normativa SGSI el cual utiliza un criterio al nivel de afectación que tiene cada riesgo con respecto a la Disponibilidad, Confidencialidad e Integridad de la Información, pero en el caso de este trabajo de investigación Gonzabay tubo un enfoque de este criterio de acuerdo a los equipos que posee el Data Center estudiado, por lo cual en este trabajo de investigación se utilizó el criterio de evaluación o valoración SGSI pero con un enfoque directo al riesgo y su influencia que este tiene con la Confidencialidad, Disponibilidad e Integridad de la información.

4.2.3. Diseño de Plan de Contingencia

El resultado obtenido del diseño y creación del plan de contingencia en el presente trabajo de investigación coincide con los trabajos de: Gonzabay (2021-2), casa (2020), Burgos (2020), Núñez (2022) y Ponce (2022), en donde todos estos documentos coinciden en el objetivo final el cual es crear un plan de contingencia capas de mitigar y trasladar los riesgos que posee una institución para lo cual se siguen normativas, la diferencia principal que existen entre estas investigaciones con la realizada en el presente trabajo de investigación es la realización de una auditoría informática para conocer el estado en el que se encuentra la institución o el data center con lo cual se consigue localizar las principales falencias que posee el manejo del data center y con ello diseñar un plan que sea capaz de corregir y fortalecer todos los procesos que se llevan a cabo en este, además de asegurar la efectividad del plan desarrollado.

V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Mediante el desarrollo del plan de contingencias se logró favorecer al departamento de Tecnologías de la Información y Comunicación de la Universidad Politécnica estatal del Carchi, debido a que no se había establecido procesos, salvaguardias, roles y responsabilidades que van a facilitar el actuar de manera eficiente ante posibles emergencias que se presenten en el centro de datos, permitiéndoles tomar acciones preventivas y correctivas para precautelar la continuidad de las operaciones beneficiando indirectamente al personal administrativo.
- Se identificó cada una de las amenazas que pueden generar escenarios de contingencias en los activos y servicios informáticos considerados como críticos para la institución, realizando una evaluación de los riesgos, se determinó el nivel de impacto que ocasionarían en caso de que llegara a materializar.
- La incorporación de normas internacionales como las normativas ISO 27002, permitieron el desarrollo del plan de contingencias planteando controles para el tratamiento de riesgos, lo cual destaca a toda la institución como un elemento diferenciador sobre otra por el compromiso en la protección de la seguridad de la información.
- La creación de grupos y asignación de roles en el departamento de TIC en caso de una contingencia permite una mejor organización al momento de dar solución a un incidente, falla o interrupción de los principales servicios de la institución.
- Gracias al desarrollo del presente proyecto se logró establecer controles y salvaguardias tanto sugeridas como establecidas por la normativa ISO 27002, para brindar una correcta gestión de la seguridad de la información y salvaguardar la confidencialidad, integridad y disponibilidad de los datos.

5.2. RECOMENDACIONES

- Ser debe realizar y evaluar las pruebas necesarias del plan de contingencias informáticas realizado para el departamento de TIC, con la finalidad de verificar el nivel de cumplimiento del plan y realizar actualizaciones periódicas a las políticas internas.
- Capacitar al personal del Departamento de TIC-UPEC en el plan de contingencias de los activos, para que se encuentren preparados en caso de presentar algún incidente y puedan reducir el tiempo de respuesta.
- Considerar la certificación en normas para la gobernabilidad, gestión y control del uso de las tecnologías de la información.
- Actualizar de manera constante roles y responsabilidades, controles y procedimientos del plan de contingencia por los posibles cambios del personal, en la infraestructura tecnológica y nuevas amenazas que provoquen riesgos que atenten con la seguridad de la información.

VI. REFERENCIAS BIBLIOGRÁFICAS

Adriana Cristina Núñez Santamaría. (2022). PLAN DE CONTINGENCIA INFORMÁTICO BASADO EN LA NORMA ISO 24762:2008 PARA EL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE LA MUNICIPALIDAD DE AMBATO.

Aranda Moposita, J. P. (2022). EVALUACIÓN DE RIESGOS INFORMÁTICOS Y DISEÑO DE UN PLAN DE CONTINGENCIA PARA EL ÁREA DE TECNOLOGÍA DE LA EMPRESA IMPORTADORA ALVARADO VÁSCONEZ CIA. LTDA., UBICADA EN LA CIUDAD DE AMBATO.

Arias, M. (2009). Percepción general de la virtualización de los recursos informáticos. CR. InterSedes: revista de las Sedes Regionales. Vol.9. pág. 152.

Buitrón, C. (2021). GESTIÓN DE RIESGOS INFORMÁTICOS APLICANDO UNA METODOLOGÍA DE ANÁLISIS PARA VERIFICAR LA SEGURIDAD DE LA INFORMACIÓN EN UNA EMPRESA DE AUDITORÍA, CONSULTORÍA Y CAPACITACIÓN [Tesis de pregrado].

Burgos Gordón Christian Andrés. (2020). PLAN DE CONTINGENCIA INFORMÁTICO PARA EL ÁREA DE TI EN BASE A LA NORMA DE CALIDAD ISO 27001:2013 PARA LA FUNDACIÓN CULTURAL Y EDUCATIVA AMBATO - UNIDAD EDUCATIVA ATENAS.

Carlos Mellado Erices. (n.d.). PLAN DE CONTINGENCIA INFORMÁTICO.

Casa Guayta Carlos Welington. (2020). ELABORACIÓN DE UN PLAN DE CONTINGENCIA PARA LOS SISTEMAS INFORMÁTICOS DE LAS JUNTAS ADMINISTRADORAS DE AGUA POTABLE DE LA PARROQUIA DE GUAYTACAMA - CASO DE ESTUDIO JUNTA ADMINISTRADORA DE AGUA POTABLE PILACOTO.

Contraloría General del Estado. (2023). NORMAS DE CONTROL INTERNO DE LA CONTRALORÍA GENERAL DEL ESTADO. https://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_cge_12_nor_con_int_400_cge.pdf

DPAE (dirección de Prevención y Atención de Emergencias). (2009). Guía para la elaboración plan de emergencias y Contingencias. Recuperado de Guía para elaborar planes de emergencia.pdf (ccb.org.co)

Ferruzola Gómez, E., Duchimaza S, J., Ramos Holguín, J., & L., M. F. A. (2019). Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT. Revista Científica y Tecnológica UPSE, 6(1), 34–41. https://doi.org/10.26423/rctu.v6i1.429

Ferruzola, E., Duchimaza, J., Ramos, J., Alejandro, M. (2019). Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología Magerit. Revista Científica y Tecnológica UPSE, 6 (1), 34-41. DOI: 10.26423/rctu.v6i1.429

Galán, J. S. (2020, March 3). Auditoría informática. Economipedia. https://economipedia. com/definiciones/auditoría-informatica.html

Geraldine Paola VIRGUEZ SOTELO. (2019, 3 diciembre). Seguridad Integral de la información. YouTube. Recuperado de https://www.youtube.com/watch?v= LGZ5s9N-jKU

GONZABAY TOMALÁ RONALD ENRIQUE. (2021). DESARROLLO DE UN PLAN DE CONTINGENCIAS INFORMÁTICO PARA EL CENTRO DE DATOS Y COMUNICACIONES DE LA EMPRESA AGUAPEN-EP MEDIANTE EL USO DE NORMAS INTERNACIONALES.

Granizo, C. (2019). PLAN DE CONTINUIDAD DE NEGOCIOS PARA LA PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR – AMBATO [Archivo PDF] Repositorio Académico Pontificia Universidad Católica del Ecuador. 77022.pdf 77022.pdf.

ISO/IEC 27002. (2018). Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información.

ISO/IEC 27005. (2018). Técnicas de seguridad. *Gestión de riesgos de la seguridad de la información*

ISOtools. (2015). ¿Qué son las normas ISO y cuál es su finalidad? Recuperado de https://www.isotools.org/2015/03/19/que-son-las-normas-iso-y-cual-es-su-finalidad/

Jaramillo, J. (2013). PROPUESTA DE GESTIÓN DEL RIESGO DE INFRAESTRUCTURA TECNOLÓGICA BASADA EN COBIT, PARA LA EMPRESA SOFT WAREHOUSE S.A. [Tesis de Pregrado]. Repositorio Académico Pontificia Universidad Católica del Ecuador. T-PUCE-6426.pdf

Kionetworks (2022) ¿Cómo funciona un Data Center? Recuperado de https://www.kionetworks.com/blog/data-center/cómo-funciona-un-data-center

Llerena, J. (2018). Desarrollo de un plan de contingencias basado en un estándar de seguridad, orientado a un servidor de aplicaciones. (Disertación de grado previo a la obtención del título de Ingeniero de Sistemas y Computación). Pontificia Universidad Católica del Ecuador. Recuperado de https://repositorio.pucesa.edu.ec/bitstream/123456789/2271 /1/76640.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2020). Acuerdo Ministerial N.º. 025-2019. https://www.gobiernoelectronico.gob.ec /wp-content/uploads/2020/01/Registro-Oficial-Acuerdo-Ministerial-No.-025-2019-EGSI-version-2.0.pdf

Palacios, R. y Quiroz, J. (2013). PLAN DE CONTINGENCIA DE LOS EQUIPOS Y SISTEMAS INFORMÁTICOS EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN JUNÍN. [Tesis de pregrado]. Repositorio Académico ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ. Recuperado de TESIS RAÚL ALEJANDRO PALACIOS PACHECO - QUIROZ CARRANZA JUAN DIEGO.pdf (espam.edu.ec)

Pinzón, P. (2014). Gestión del riesgo en Seguridad Informática. Recuperado de (unipiloto.edu.co)

Repositorio Académico Universidad Técnica del Norte. 04 ISC 580 TRABAJO GRADO.pdf (utn.edu.ec)

Shirley Pitta, (2018). DISEÑO DE UN PLAN DE CONTINGENCIA INFORMÁTICO BASADO EN LAS NORMAS ISO/IEC 22301 E ISO/IEC 27031 PARA LA FERRETERÍA CESAR S.A.S. EN LA CIUDAD DE VALLEDUPAR (Propuesta de grado para optar por el título de Especialista en Seguridad Informática). UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD. Recuperado de https://repository.unad.edu.co/bitstream /handle/10596/21434/1065563682.pdf?sequence=1&isAllowed=y

SNR (secretaria nacional de Gestión de Riesgo). (2010). Guía Institucional de Gestión de Riesgo 2010. Recuperado de http:/www.snriesgo.gob.ec

VII. ANEXOS

Anexo 1. Acta de sustentación de Predefensa.

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE COMPUTACIÓN

ACTA

DE LA SUSTENTACIÓN ORAL DE LA PREDEFENSA DEL TRABAJO DE INTEGRACIÓN CURRICULAR

ESTUDIANTE:	ALEXIS FERNANDO FUEL PIARPUEZÁN	**CÉDULA DE IDENTIDAD:**	0401747746
PERIODO ACADÉMICO:	2023A		
PRESIDENTE TRIBUNAL	MSC. CARLITOS ALBERTO GUANO CÁRDENAS	**DOCENTE TUTOR:**	MSC. MARCO ANTONIO YANDÚN VELASTEGUÍ
DOCENTE:	MSC. JAIRO VLADIMIR HIDALGO GUIJARRO		
TEMA DEL TIC:	"Plan de contingencia para el Data Center de la Universidad Politécnica Estatal del Carchi"		

No.	CATEGORÍA	Evaluación cuantitativa	OBSERVACIONES Y RECOMENDACIONES
1	PROBLEMA - OBJETIVOS	7,00	Revisar planteamiento del problema y objetivo de propuesta, de ser necesario reformular con el fin que aporte al objetivo general
2	FUNDAMENTACIÓN TEÓRICA	7,00	Profundizar respecto a normativa legal vigente y que aplica en la UPEC, además de normativas consideradas en el proyecto. Se ha considerado únicamente fundamentación conceptual
3	METODOLOGÍA	7,00	Revisar métodos y metodologías de investigación aplicadas en la investigación, idea a defender. Se recomienda incluir cálculo utilizado para muestra.
4	RESULTADOS	7,00	Analizar que la propuesta de Plan presentada, se encuentre acorde con necesidades institucionales, que brinde acciones de soporte que permitan minimizar los impactos provocados por incidentes reales y no con supuestos. Se recomienda la revisión de formas de cálculo de riesgos, apoyado en estándares, normativas y/o buenas prácticas
5	DISCUSIÓN	7,00	Se recomienda revisar discusión que se encuentre acorde con los resultados obtenidos y en caso de ser necesario modificar
6	CONCLUSIONES Y RECOMENDACIONES	7,00	Revisar conclusiones y recomendaciones, con el fin que se encuentren acorde con los resultados obtenidos y con criterio técnico
7	DEFENSA, ARGUMENTACIÓN Y VOCABULARIO PROFESIONAL	7,00	Contemplar y ampliar aspectos técnicos en la sustentación
8	FORMATO, ORGANIZACIÓN Y CALIDAD DE LA INFORMACIÓN	7,00	Revisar: ortografía y redacción; apliación de normas APA y formato establecido por la UPEC

Obteniendo una nota de: 7,00 Por lo tanto, **APRUEBA** : debiendo el o los investigadores acatar el siguiente artículo:

Art. 36.- De los estudiantes que aprueban el informe final del TIC con observaciones.- Los estudiantes tendrán el plazo de 10 días para proceder a corregir su informe final del TIC de conformidad a las observaciones y recomendaciones realizadas por los miembros del Tribunal de sustentación de la pre-defensa.

Para constancia del presente, firman en la ciudad de Tulcán el jueves, 20 de julio de 2023

MSC. CARLITOS ALBERTO GUANO CÁRDENAS
PRESIDENTE TRIBUNAL

MSC. MARCO ANTONIO YANDÚN VELASTEGUÍ
DOCENTE TUTOR

MSC. JAIRO VLADIMIR HIDALGO GUIJARRO
DOCENTE

Figura 50. Acta de sustentación de Predefensa.

Anexo 2. Informe del Abstract.

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FOREIGN AND NATIVE LANGUAGE CENTER

ABSTRACT- EVALUATION SHEET

NAME: Alexis Fernando Fuel Piarpuezán y Willian Alejandro López Mosquera
DATE: 24 de julio de 2023

TOPIC: " Plan de contingencia para el Data Center de la Universidad Politécnica Estatal del Carchi."

MARKS AWARDED **QUANTITATIVE AND QUALITATIVE**

VOCABULARY AND WORD USE	Use new learnt vocabulary and precise words related to the topic	Use a little new vocabulary and some appropriate words related to the topic	Use basic vocabulary and simplistic words related to the topic	Limited vocabulary and inadequate words related to the topic
	EXCELLENT: 2 ☐	GOOD: 1Vera Játiva Edwin Andrés,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
WRITING COHESION	Clear and logical progression of ideas and supporting paragraphs.	Adequate progression of ideas and supporting paragraphs.	Some progression of ideas and supporting paragraphs.	Inadequate ideas and supporting paragraphs.
	EXCELLENT: 2 ☐	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
ARGUMENT	The message has been communicated very well and identify the type of text	The message has been communicated appropriately and identify the type of text	Some of the message has been communicated and the type of text is little confusing	The message hasn't been communicated and the type of text is inadequate
	EXCELLENT: 2 ☐	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
CREATIVITY	Outstanding flow of ideas and events	Good flow of ideas and events	Average flow of ideas and events	Poor flow of ideas and events
	EXCELLENT: 2 ☐	GOOD: 1,5 ■	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
SCIENTIFIC SUSTAINABILITY	Reasonable, specific and supportable opinion or thesis statement	Minor errors when supporting the thesis statement	Some errors when supporting the thesis statement	Lots of errors when supporting the thesis statement
	EXCELLENT: 2 ☐	GOOD: 1,5 ■	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
TOTAL/AVERAGE	9 - 10: EXCELLENT 7 - 8,9: GOOD 5 - 6,9: AVERAGE 0 - 4,9: LIMITED	TOTAL 9,5		

1

Figura 51. Informe del Abstract.

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI FOREIGN AND NATIVE LANGUAGE CENTER

Informe sobre el Abstract de Artículo Científico o Investigación.

Autor: Alexis Fernando Fuel Piarpuezán y Willian Alejandro López Mosquera
Fecha de recepción del abstract: 24 de julio de 2023

Fecha de entrega del informe: 24 de julio de 2023

El presente informe validará la traducción del idioma español al inglés si alcanza un porcentaje de: 9 – 10 Excelente.

Si la traducción no está dentro de los parámetros de 9 – 10, el autor deberá realizar las observaciones presentadas en el ABSTRACT, para su posterior presentación y aprobación.

Observaciones:

Después de realizar la revisión del presente abstract, éste presenta una apropiada traducción sobre el tema planteado en el idioma Inglés. Según los rubrics de evaluación de la traducción en Inglés, ésta alcanza un valor de 9,5 por lo cual se validad dicho trabajo.

Atentamente

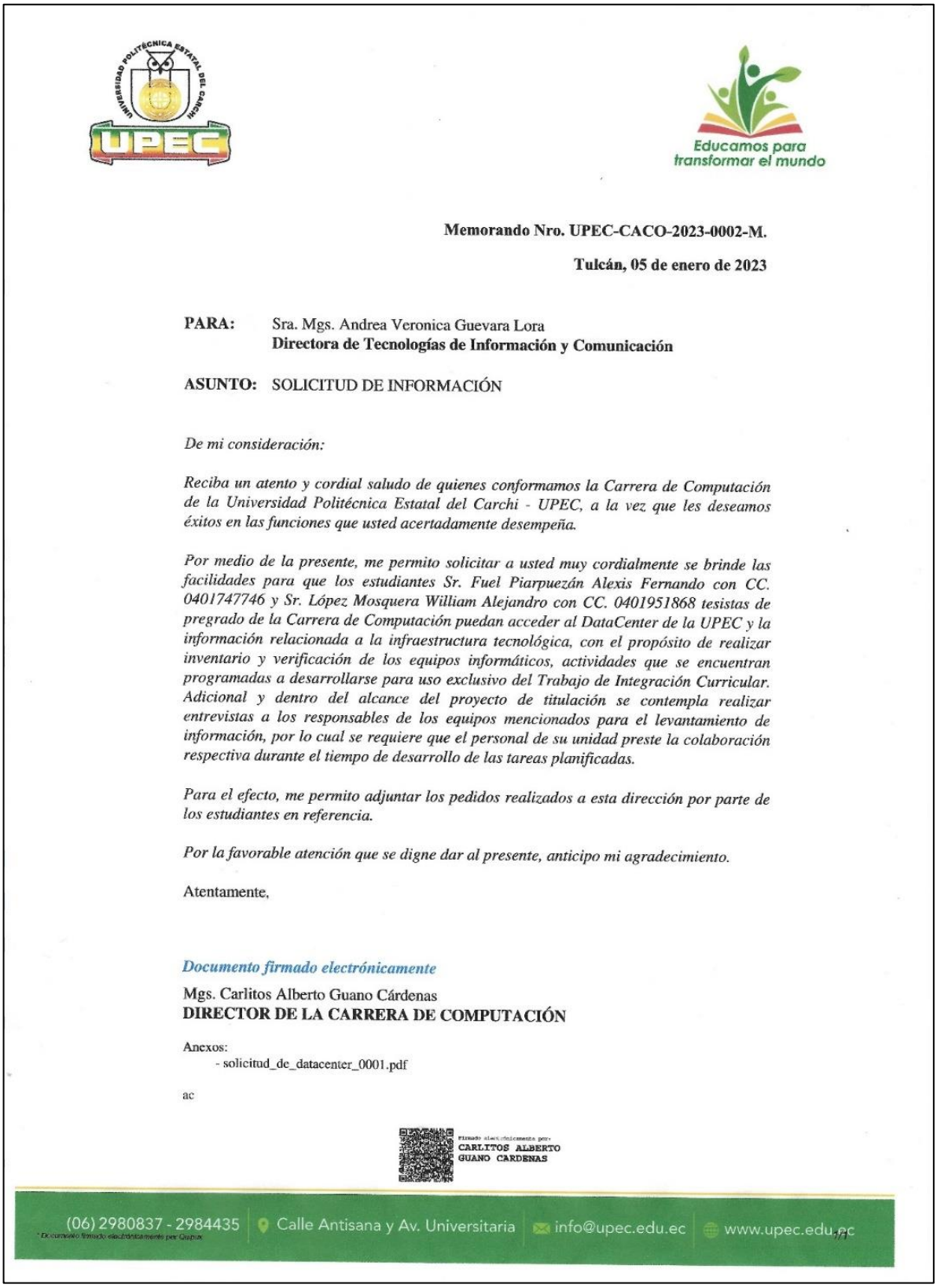
EDISON BOANERGES PEÑAFIEL ARCOS

Ing. Edison Peñafiel Arcos MSc
Coordinador del CIDEN

2

Figura 52. Informe del Abstract 2.

Anexo 3. Solicitud para levantamiento de información.



Educamos para transformar el mundo

Memorando Nro. UPEC-CACO-2023-0002-M.

Tulcán, 05 de enero de 2023

PARA: Sra. Mgs. Andrea Veronica Guevara Lora
Directora de Tecnologías de Información y Comunicación

ASUNTO: SOLICITUD DE INFORMACIÓN

De mi consideración:

Reciba un atento y cordial saludo de quienes conformamos la Carrera de Computación de la Universidad Politécnica Estatal del Carchi - UPEC, a la vez que les deseamos éxitos en las funciones que usted acertadamente desempeña.

Por medio de la presente, me permito solicitar a usted muy cordialmente se brinde las facilidades para que los estudiantes Sr. Fuel Piarpuezán Alexis Fernando con CC. 0401747746 y Sr. López Mosquera William Alejandro con CC. 0401951868 tesistas de pregrado de la Carrera de Computación puedan acceder al DataCenter de la UPEC y la información relacionada a la infraestructura tecnológica, con el propósito de realizar inventario y verificación de los equipos informáticos, actividades que se encuentran programadas a desarrollarse para uso exclusivo del Trabajo de Integración Curricular. Adicional y dentro del alcance del proyecto de titulación se contempla realizar entrevistas a los responsables de los equipos mencionados para el levantamiento de información, por lo cual se requiere que el personal de su unidad preste la colaboración respectiva durante el tiempo de desarrollo de las tareas planificadas.

Para el efecto, me permito adjuntar los pedidos realizados a esta dirección por parte de los estudiantes en referencia.

Por la favorable atención que se digne dar al presente, anticipo mi agradecimiento.

Atentamente,

Documento firmado electrónicamente

Mgs. Carlitos Alberto Guano Cárdenas
DIRECTOR DE LA CARRERA DE COMPUTACIÓN

Anexos:
- solicitud_de_datacenter_0001.pdf

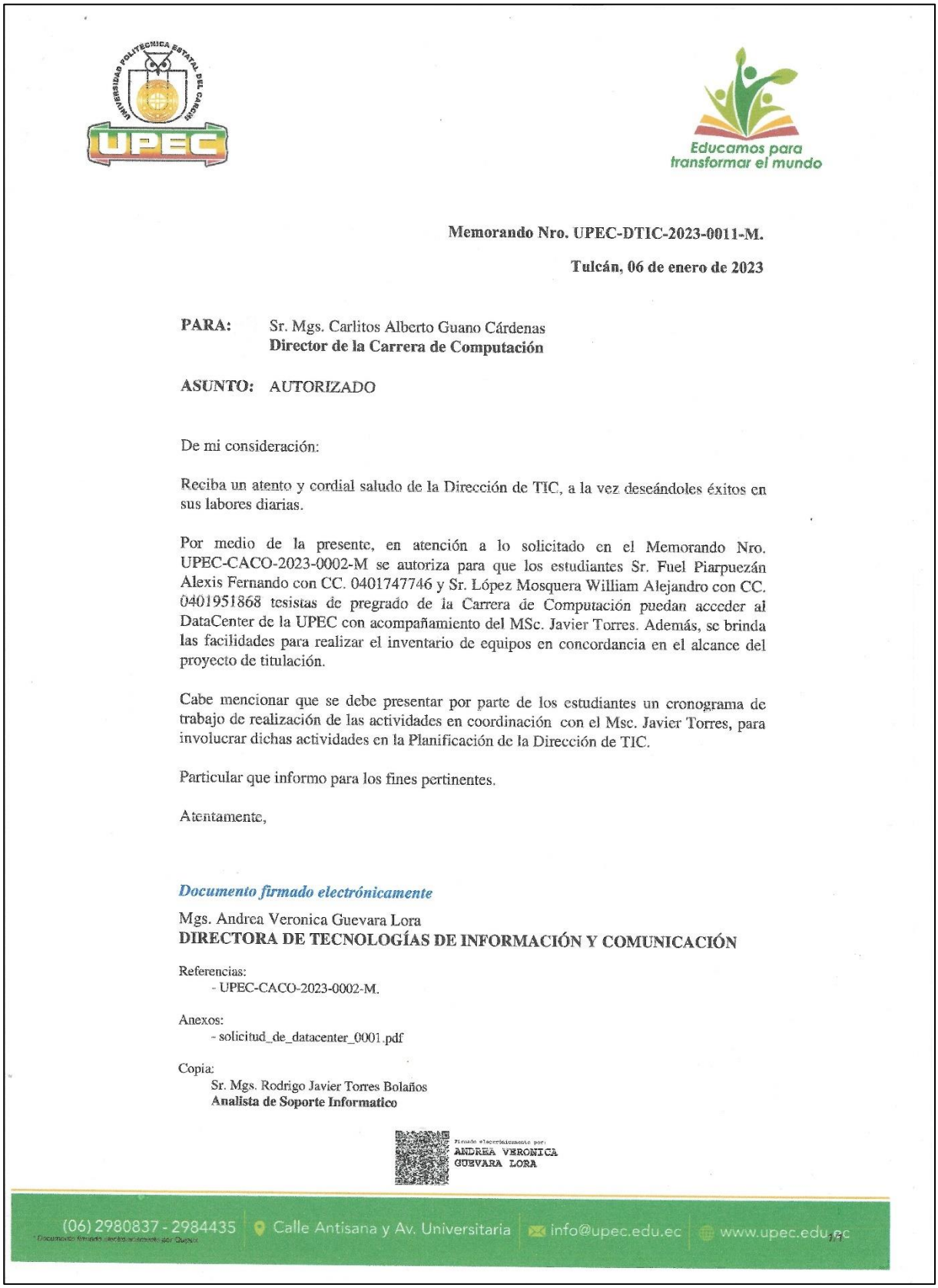
ac

Firmado electrónicamente por:
CARLITOS ALBERTO GUANO CARDENAS

(06) 2980837 - 2984435 | Calle Antisana y Av. Universitaria | info@upec.edu.ec | www.upec.edu.ec

Figura 53. Solicitud para levantamiento de información.

Anexo 4. Autorización para ingreso al data center-UPEC.



Educamos para transformar el mundo

Memorando Nro. UPEC-DTIC-2023-0011-M.

Tulcán, 06 de enero de 2023

PARA: Sr. Mgs. Carlitos Alberto Guano Cárdenas
Director de la Carrera de Computación

ASUNTO: AUTORIZADO

De mi consideración:

Reciba un atento y cordial saludo de la Dirección de TIC, a la vez deseándoles éxitos en sus labores diarias.

Por medio de la presente, en atención a lo solicitado en el Memorando Nro. UPEC-CACO-2023-0002-M se autoriza para que los estudiantes Sr. Fuel Piarpuezán Alexis Fernando con CC. 0401747746 y Sr. López Mosquera William Alejandro con CC. 0401951868 tesistas de pregrado de la Carrera de Computación puedan acceder al DataCenter de la UPEC con acompañamiento del MSc. Javier Torres. Además, se brinda las facilidades para realizar el inventario de equipos en concordancia en el alcance del proyecto de titulación.

Cabe mencionar que se debe presentar por parte de los estudiantes un cronograma de trabajo de realización de las actividades en coordinación con el Msc. Javier Torres, para involucrar dichas actividades en la Planificación de la Dirección de TIC.

Particular que informo para los fines pertinentes.

Atentamente,

Documento firmado electrónicamente

Mgs. Andrea Veronica Guevara Lora
DIRECTORA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Referencias:
- UPEC-CACO-2023-0002-M.

Anexos:
- solicitud_de_datacenter_0001.pdf

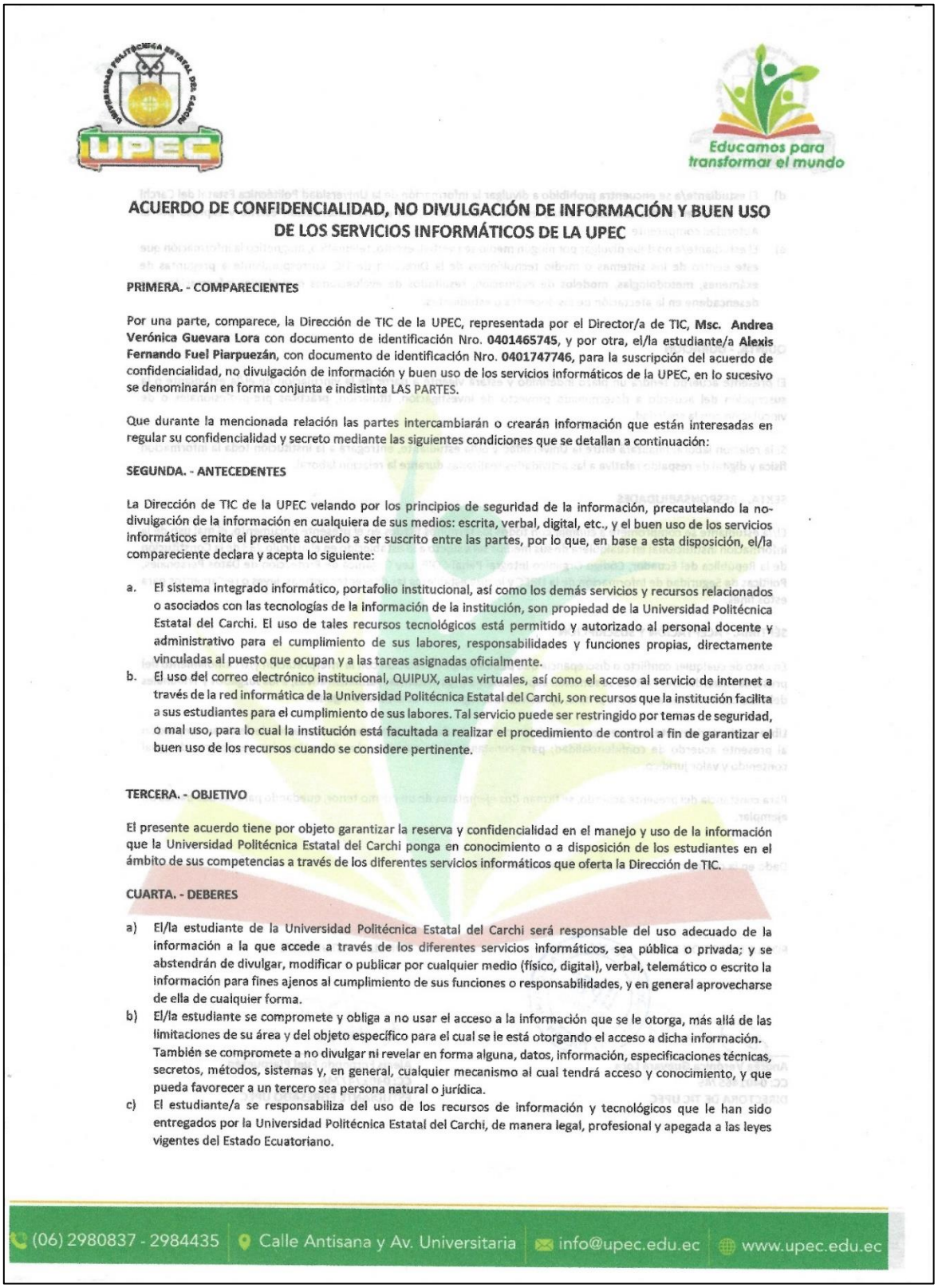
Copia:
Sr. Mgs. Rodrigo Javier Torres Bolaños
Analista de Soporte Informatico

Firmado electrónicamente por:
ANDREA VERONICA GUEVARA LORA

(06) 2980837 - 2984435 | Calle Antisana y Av. Universitaria | info@upec.edu.ec | www.upec.edu.ec

Figura 54. Autorización para ingreso al data center-UPEC.

Anexo 5. Acuerdos de Confidencialidad.



Educamos para transformar el mundo

ACUERDO DE CONFIDENCIALIDAD, NO DIVULGACIÓN DE INFORMACIÓN Y BUEN USO DE LOS SERVICIOS INFORMÁTICOS DE LA UPEC

PRIMERA. - COMPARECIENTES

Por una parte, comparece, la Dirección de TIC de la UPEC, representada por el Director/a de TIC, **Msc. Andrea Verónica Guevara Lora** con documento de identificación Nro. **0401465745**, y por otra, el/la estudiante/a **Alexis Fernando Fuel Piarpuezán**, con documento de identificación Nro. **0401747746**, para la suscripción del acuerdo de confidencialidad, no divulgación de información y buen uso de los servicios informáticos de la UPEC, en lo sucesivo se denominarán en forma conjunta e indistinta LAS PARTES.

Que durante la mencionada relación las partes intercambiarán o crearán información que están interesadas en regular su confidencialidad y secreto mediante las siguientes condiciones que se detallan a continuación:

SEGUNDA. - ANTECEDENTES

La Dirección de TIC de la UPEC velando por los principios de seguridad de la información, precautelando la no-divulgación de la información en cualquiera de sus medios: escrita, verbal, digital, etc., y el buen uso de los servicios informáticos emite el presente acuerdo a ser suscrito entre las partes, por lo que, en base a esta disposición, el/la compareciente declara y acepta lo siguiente:

a. El sistema integrado informático, portafolio institucional, así como los demás servicios y recursos relacionados o asociados con las tecnologías de la información de la institución, son propiedad de la Universidad Politécnica Estatal del Carchi. El uso de tales recursos tecnológicos está permitido y autorizado al personal docente y administrativo para el cumplimiento de sus labores, responsabilidades y funciones propias, directamente vinculadas al puesto que ocupan y a las tareas asignadas oficialmente.
b. El uso del correo electrónico institucional, QUIPUX, aulas virtuales, así como el acceso al servicio de internet a través de la red informática de la Universidad Politécnica Estatal del Carchi, son recursos que la institución facilita a sus estudiantes para el cumplimiento de sus labores. Tal servicio puede ser restringido por temas de seguridad, o mal uso, para lo cual la institución está facultada a realizar el procedimiento de control a fin de garantizar el buen uso de los recursos cuando se considere pertinente.

TERCERA. - OBJETIVO

El presente acuerdo tiene por objeto garantizar la reserva y confidencialidad en el manejo y uso de la información que la Universidad Politécnica Estatal del Carchi ponga en conocimiento o a disposición de los estudiantes en el ámbito de sus competencias a través de los diferentes servicios informáticos que oferta la Dirección de TIC.

CUARTA. - DEBERES

a) El/la estudiante de la Universidad Politécnica Estatal del Carchi será responsable del uso adecuado de la información a la que accede a través de los diferentes servicios informáticos, sea pública o privada; y se abstendrán de divulgar, modificar o publicar por cualquier medio (físico, digital), verbal, telemático o escrito la información para fines ajenos al cumplimiento de sus funciones o responsabilidades, y en general aprovecharse de ella de cualquier forma.
b) El/la estudiante se compromete y obliga a no usar el acceso a la información que se le otorga, más allá de las limitaciones de su área y del objeto específico para el cual se le está otorgando el acceso a dicha información. También se compromete a no divulgar ni revelar en forma alguna, datos, información, especificaciones técnicas, secretos, métodos, sistemas y, en general, cualquier mecanismo al cual tendrá acceso y conocimiento, y que pueda favorecer a un tercero sea persona natural o jurídica.
c) El estudiante/a se responsabiliza del uso de los recursos de información y tecnológicos que le han sido entregados por la Universidad Politécnica Estatal del Carchi, de manera legal, profesional y apegada a las leyes vigentes del Estado Ecuatoriano.

(06) 2980837 - 2984435 | Calle Antisana y Av. Universitaria | info@upec.edu.ec | www.upec.edu.ec

Figura 55. Acuerdos de Confidencialidad 1.

d) El estudiante/a se encuentra prohibido a divulgar la información de la Universidad Politécnica Estatal del Carchi por cualquier medio sea este verbal, escrito o telemático, sin previa autorización escrita y expresa por la Autoridad competente.

e) El estudiante/a no debe divulgar por ningún medio sea verbal, escrito, telemático, magnético la información que este dentro de los sistemas o medio tecnológicos de la Dirección de TIC, correspondiente a preguntas de exámenes, metodologías, modelos de evaluación, resultados de evaluaciones o cualquier información que desencadene en la afectación de los docentes o estudiantes.

QUINTA. - DURACIÓN

El presente acuerdo tendrá un plazo indefinido y estará vigente a partir de la vinculación de el/la estudiante o la suscripción del acuerdo a determinado proyecto de investigación, titulación, prácticas pre-profesionales o de vinculación con la sociedad.

Si la relación laboral finalizará entre la Universidad y el/la estudiante, entregará a la institución toda la información física y digital de respaldo relativa a las actividades realizadas durante la relación laboral.

SEXTA. - RESPONSABILIDADES

El/la estudiante se compromete a cumplir con todos los términos fijados en el presente documento, el mal uso de la información institucional en cualquiera de sus medios será sujeto a lo establecido en el artículo 233 de la Constitución de la República del Ecuador, Código Orgánico Integral Penal COIP, Ley Orgánica de Protección de Datos Personales, Políticas de Seguridad de Información de la UPEC y lo que establezca las diferentes normas, leyes o reglamentos para estos fines.

SÉPTIMA. - ACEPTACIÓN Y SUSCRIPCIÓN

En caso de cualquier conflicto o discrepancia que pueda surgir en relación con la interpretación y/o cumplimiento del presente Acuerdo, LAS PARTES se someten expresamente a las instancias Administrativas, a los Juzgados y Tribunales del País, con renuncia a su fuero propio, aplicándose la legislación ecuatoriana vigente.

Libre y voluntariamente, una vez revisado y leído cada parte del presente acuerdo, las partes declaran su aceptación al presente acuerdo de confidencialidad; para constancia bajo suscriben los firmantes dos ejemplares de igual contenido y valor jurídico.

Para constancia del presente acuerdo, se firman dos ejemplares de un mismo tenor, quedando para las dos partes un ejemplar.

Dado en la ciudad de Tulcán, al día 03 de marzo de 2023.

POR LA DIRECCIÓN DE TIC

Andrea Verónica Guevara Lora
CC: 0401465745
DIRECTORA DE TIC UPEC

POR EL/LA ESTUDIANTE

Alexis Fernando Fuel Piarpuezán
CC: 0401747746
ESTUDIANTE EGRESADO UPEC

Figura 56. Acuerdos de Confidencialidad 2.

ACUERDO DE CONFIDENCIALIDAD, NO DIVULGACIÓN DE INFORMACIÓN Y BUEN USO DE LOS SERVICIOS INFORMÁTICOS DE LA UPEC

PRIMERA. - COMPARECIENTES

Por una parte, comparece, la Dirección de TIC de la UPEC, representada por el Director/a de TIC, **Msc. Andrea Verónica Guevara Lora** con documento de identificación Nro. **0401465745**, y por otra, el/la estudiante/a **William Alejandro López Mosquera**, con documento de identificación Nro. **0401951868**, para la suscripción del acuerdo de confidencialidad, no divulgación de información y buen uso de los servicios informáticos de la UPEC, en lo sucesivo se denominarán en forma conjunta e indistinta LAS PARTES.

Que durante la mencionada relación las partes intercambiarán o crearán información que están interesadas en regular su confidencialidad y secreto mediante las siguientes condiciones que se detallan a continuación:

SEGUNDA. - ANTECEDENTES

La Dirección de TIC de la UPEC velando por los principios de seguridad de la información, precautelando la no-divulgación de la información en cualquiera de sus medios: escrita, verbal, digital, etc., y el buen uso de los servicios informáticos emite el presente acuerdo a ser suscrito entre las partes, por lo que, en base a esta disposición, el/la compareciente declara y acepta lo siguiente:

a. El sistema integrado informático, portafolio institucional, así como los demás servicios y recursos relacionados o asociados con las tecnologías de la información de la institución, son propiedad de la Universidad Politécnica Estatal del Carchi. El uso de tales recursos tecnológicos está permitido y autorizado al personal docente y administrativo para el cumplimiento de sus labores, responsabilidades y funciones propias, directamente vinculadas al puesto que ocupan y a las tareas asignadas oficialmente.
b. El uso del correo electrónico institucional, QUIPUX, aulas virtuales, así como el acceso al servicio de internet a través de la red informática de la Universidad Politécnica Estatal del Carchi, son recursos que la institución facilita a sus estudiantes para el cumplimiento de sus labores. Tal servicio puede ser restringido por temas de seguridad, o mal uso, para lo cual la institución está facultada a realizar el procedimiento de control a fin de garantizar el buen uso de los recursos cuando se considere pertinente.

TERCERA. - OBJETIVO

El presente acuerdo tiene por objeto garantizar la reserva y confidencialidad en el manejo y uso de la información que la Universidad Politécnica Estatal del Carchi ponga en conocimiento o a disposición de los estudiantes en el ámbito de sus competencias a través de los diferentes servicios informáticos que oferta la Dirección de TIC.

CUARTA. - DEBERES

a) El/la estudiante de la Universidad Politécnica Estatal del Carchi será responsable del uso adecuado de la información a la que accede a través de los diferentes servicios informáticos, sea pública o privada; y se abstendrán de divulgar, modificar o publicar por cualquier medio (físico, digital), verbal, telemático o escrito la información para fines ajenos al cumplimiento de sus funciones o responsabilidades, y en general aprovecharse de ella de cualquier forma.
b) El/la estudiante se compromete y obliga a no usar el acceso a la información que se le otorga, más allá de las limitaciones de su área y del objeto específico para el cual se le está otorgando el acceso a dicha información. También se compromete a no divulgar ni revelar en forma alguna, datos, información, especificaciones técnicas, secretos, métodos, sistemas y, en general, cualquier mecanismo al cual tendrá acceso y conocimiento, y que pueda favorecer a un tercero sea persona natural o jurídica.
c) El estudiante/a se responsabiliza del uso de los recursos de información y tecnológicos que le han sido entregados por la Universidad Politécnica Estatal del Carchi, de manera legal, profesional y apegada a las leyes vigentes del Estado Ecuatoriano.

Figura 57. Acuerdos de Confidencialidad 3.

d) El estudiante/a se encuentra prohibido a divulgar la información de la Universidad Politécnica Estatal del Carchi por cualquier medio sea este verbal, escrito o telemático, sin previa autorización escrita y expresa por la Autoridad competente.

e) El estudiante/a no debe divulgar por ningún medio sea verbal, escrito, telemático, magnético la información que este dentro de los sistemas o medio tecnológicos de la Dirección de TIC, correspondiente a preguntas de exámenes, metodologías, modelos de evaluación, resultados de evaluaciones o cualquier información que desencadene en la afectación de los docentes o estudiantes.

QUINTA. - DURACIÓN

El presente acuerdo tendrá un plazo indefinido y estará vigente a partir de la vinculación de el/la estudiante o la suscripción del acuerdo a determinado proyecto de investigación, titulación, prácticas pre-profesionales o de vinculación con la sociedad.

Si la relación laboral finalizará entre la Universidad y el/la estudiante, entregará a la institución toda la información física y digital de respaldo relativa a las actividades realizadas durante la relación laboral.

SEXTA. - RESPONSABILIDADES

El/la estudiante se compromete a cumplir con todos los términos fijados en el presente documento, el mal uso de la información institucional en cualquiera de sus medios será sujeto a lo establecido en el artículo 233 de la Constitución de la República del Ecuador, Código Orgánico Integral Penal COIP, Ley Orgánica de Protección de Datos Personales, Políticas de Seguridad de información de la UPEC y lo que establezca las diferentes normas, leyes o reglamentos para estos fines.

SÉPTIMA. - ACEPTACIÓN Y SUSCRIPCIÓN

En caso de cualquier conflicto o discrepancia que pueda surgir en relación con la interpretación y/o cumplimiento del presente Acuerdo, LAS PARTES se someten expresamente a las instancias Administrativas, a los Juzgados y Tribunales del País, con renuncia a su fuero propio, aplicándose la legislación ecuatoriana vigente.

Libre y voluntariamente, una vez revisado y leído cada parte del presente acuerdo, las partes declaran su aceptación al presente acuerdo de confidencialidad; para constancia bajo suscriben los firmantes dos ejemplares de igual contenido y valor jurídico.

Para constancia del presente acuerdo, se firman dos ejemplares de un mismo tenor, quedando para las dos partes un ejemplar.

Dado en la ciudad de Tulcán, al día 03 de marzo de 2023.

POR LA DIRECCIÓN DE TIC

Andrea Verónica Guevara Lora
CC: 0401465745
DIRECTORA DE TIC UPEC

POR EL/LA ESTUDIANTE

William Alejandro López Mosquera
CC: 0401951868
ESTUDIANTE EGRESADO UPEC

Figura 58. Acuerdos de Confidencialidad 4.

Anexo 6. Planificación de la Auditoría.

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES
"CARRERA COMPUTACIÓN"

Auditoria Data Center-UPEC

Mediante el presente documento damos a conocer el alcance, objetivo y justificación de la auditoria que se llevara a cabo en el Data Center de la Universidad Politécnica del Carchi, además, el cronograma de los auditados para la aplicación de encuestas como estrategia de levantamiento de información del trabajo de titulación "Plan de contingencia para el Data Center de la Universidad Politécnica Estatal del Carchi (UPEC)".

Objetivo de la Auditoria: Desarrollar un análisis de riesgos en el Data Center de la Universidad Politécnica Estatal del Carchi, con el propósito de identificar amenazas y vulnerabilidades que afectan los objetivos del negocio y por consiguiente plantear un plan de contingencias.

Alcance de la Auditoría Informática: La auditoría de seguridad informática en el Data Center de la UPEC abarcará las Unidades de Redes y Telecomunicaciones y Desarrollo de Software, en donde se realizará un diagnóstico a los controles de seguridad que mantienen con la finalidad de identificar vulnerabilidades y amenazas que afectan a los objetivos del negocio.

Justificación: La Auditoría Informática es un proceso de evaluación que detecta las debilidades a nivel tecnológico y de esta manera se plantea mejoras en los servicios que brinda el Departamentos de Sistemas de la UPEC.

Figura 59. Planificación de la Auditoría 1.

Fecha	Hora de inicio	Hora de finalización	Proceso / Control por auditar/Lugar	Auditores	Cargo y nombre
06/03/2023	08:00	09:00	**Identificación de amenazas** Gestión de riesgos y amenazas **Dirección de TIC**	1.- Willian López 2.- Alexis Fuel	Msc. Andrea Guevara **Directora de TIC** Msc. Javier Torres **Analista de Redes y Telecomunicaciones** Msc. Andrés Zabala **Analista de Programador de Sistemas de Software**
	09:00	10:00	**Identificación de controles existentes** Gestión de riesgos y amenazas **Dirección de TIC**	1.- Willian López 2.- Alexis Fuel	Msc. Andrea Guevara **Directora de TIC** Msc. Javier Torres **Analista de Redes y Telecomunicaciones** Msc. Andrés Zabala **Analista de Programador de Sistemas de Software**
	10:00	11:00	**Identificación de vulnerabilidades** Gestión de riesgos y amenazas **Dirección de TIC**	1.- Willian López 2.- Alexis Fuel	Msc. Andrea Guevara **Directora de TIC** Msc. Javier Torres **Analista de Redes y Telecomunicaciones** Msc. Andrés Zabala **Analista de Programador de Sistemas de Software**

Figura 60. Planificación de la Auditoría 2.

	11:00	13:00	**Identificación de consecuencias** Gestión de riesgos y amenazas **Dirección de TIC**	1.- Willian López 2.- Alexis Fuel	Msc. Andrea Guevara **Directora de TIC** Msc. Javier Torres **Analista de Redes y Telecomunicaciones** Msc. Andrés Zabala **Analista de Programador de Sistemas de Software**
07/03/2023	08:00	09:30	**Análisis de riesgos (metodologías y evaluaciones de consecuencias)** Gestión de riesgos y amenazas **Dirección de TIC**	1.- Willian López 2.- Alexis Fuel	Msc. Andrea Guevara **Directora de TIC** Msc. Javier Torres **Analista de Redes y Telecomunicaciones** Msc. Andrés Zabala **Analista de Programador de Sistemas de Software**
08/03/2023	08:00	09:30	**Gestión de activos** Responsabilidad sobre los activos (compra de activos) **Dirección de TIC**	1.- Willian López 2.- Alexis Fuel	Msc. Andrea Guevara **Directora de TIC** Msc. Javier Torres **Analista de Redes y Telecomunicaciones** Msc. Andrés Zabala **Analista de Programador de Sistemas de Software**

Figura 61. Planificación de la Auditoría 3.

09/03/2023	08:00	09:30	**Control de acceso** Requisitos institucionales de control de acceso Gestión de acceso de usuarios Responsabilidades del usuario Control de acceso a sistemas y aplicaciones **Dirección de TIC**	1.- Willian López 2.- Alexis Fuel	Msc. Andrea Guevara **Directora de TIC** Msc. Javier Torres **Analista de Redes y Telecomunicaciones** Msc. Andrés Zabala **Analista de Programador de Sistemas de Software**
	09:30	10:30	**Criptografía** Controles de cifrado de contraseñas de acceso al Data center **Dirección de TIC**	1.- Willian López 2.- Alexis Fuel	Msc. Andrea Guevara **Directora de TIC** Msc. Javier Torres **Analista de Redes y Telecomunicaciones** Msc. Andrés Zabala **Analista de Programador de Sistemas de Software**
10/03/2023	08:00	09:30	**Seguridad física y del entorno** Controles de acceso al Data center Control de acceso al cuarto seguro Seguridad de los equipos **Unidad de Redes y Telecomunicaciones**	1.- Willian López 2.- Alexis Fuel	Msc. Andrea Guevara **Directora de TIC** Msc. Javier Torres **Analista de Redes y Telecomunicaciones** Msc. Andrés Zabala **Analista de Programador de Sistemas de Software**

Figura 62. Planificación de la Auditoría 4.

10/03/2023	09:30	10:30	**Seguridad de las operaciones** Protección contra malware Copias de seguridad Registro y monitoreo **Dirección de TIC**	1.- Willian López 2.- Alexis Fuel	Msc. Andrea Guevara **Directora de TIC** Msc. Javier Torres **Analista de Redes y Telecomunicaciones** Msc. Andrés Zabala **Analista de Programador de Sistemas de Software**
13/03/2023	08:00	09:30	**Gestión de incidentes de la seguridad de la información** Gestión de intentos de acceso y/o ataques **Dirección de TIC**	1.- Willian López 2.- Alexis Fuel	Msc. Andrea Guevara **Directora de TIC** Msc. Javier Torres **Analista de Redes y Telecomunicaciones** Msc. Andrés Zabala **Analista de Programador de Sistemas de Software**
	09:30	10:30	**Cumplimiento** Cumplimiento con las normativas Revisiones de seguridad de la información **Dirección de TIC**	1.- Willian López 2.- Alexis Fuel	Msc. Andrea Guevara **Directora de TIC** Msc. Javier Torres **Analista de Redes y Telecomunicaciones** Msc. Andrés Zabala **Analista de Programador de Sistemas de Software**

Figura 63. Planificación de la Auditoría 5.

Realizado por:

Nombre: Sr. Alexis Fuel

CI: 040174774-6

Auditor

Nombre: Sr. William López

CI: 040195186-8

Auditor

Revisado por:

Nombre: Msc. Marco Yandún

CI: 100276395-9

Asesor del Proyecto de Titulación

Nombre: Msc. Javier Torres

CI: 040167354-6

Coordinador de la Unidad de Redes y Telecomunicaciones

Nombre: Msc. Andrés Zabala

CI: 210027381-8

Coordinador de la Unidad Desarrollo de Software

Figura 64. Planificación de la Auditoría 6.

Aprobado por:

Nombre: Msc. Andrea Guevara

CI: 040146574-5

Directora del Departamento de Tecnologías de la Información y Comunicación-UPEC

Figura 65. Planificación de la Auditoría 7.

Anexo 7. Encuesta.

UNIVERSIDAD POLITECNICA ESTATAL DEL CARCHI

ENCUESTA

Objetivo. Determinar el nivel de cumplimiento que posee el data center de la Universidad Politécnica Estatal del Carchi de acuerdo con las normativas ISO 27005 e ISO 27002 cuya temática principal es la gestión y tratamiento de riesgos informáticos.

Tabla 1

Probabilidad de ocurrencia de amenazas.

Probabilidad de ocurrencia	Calificación cuantitativa	Criterio	Presencia de la Situación
Baja	1	Improbable	Una vez en 3 años
Media baja	2	Raramente	Una vez en 2 años con seis meses
Media	3	Moderada	Una vez en 2 años
Media alta	4	Frecuente	Una vez en 1 año con 6 meses
Alta	5	Siempre	Una vez en años

Nota: Esta tabla muestra la probabilidad de que una amenaza se materialice (Araujo Castro, 2019).

Tabla 2

Calificación del nivel de impacto.

Impacto	Calificación cuantitativa	Criterio
Baja	1	Incomoda
Media baja	2	Controlable
Media	3	Regulable
Media alta	4	Crítico
Alta	5	Irreparable

Nota: Esta tabla muestra el impacto que tiene la amenaza (Araujo Castro, 2019).

NIVELES DE MADUREZ

Iniciado (I): no se ha implementado formalmente un sistema de gestión de riesgo y no hay una adecuada capacitación de cómo actuar frente al suceso.

Definido (D): Cumple con el sistema de gestión de riesgos establecido, existen políticas y procedimientos que involucran a cada miembro de la organización.

Administrado (A): La gestión de riesgo se desarrolla de forma adecuada y hay claridad sobre la tolerancia al riesgo.

Optimizado (O): La gestión de riesgos hace parte de la cultura organizacional, existen indicadores para su medición (Jiménez, 2021).

Figura 66. Encuesta 1.

TRATAMIENTO DE RIESGOS

Aceptado (A): Un riesgo es aceptado cuando las repercusiones o consecuencias de este son mínimas que no influya de gran manera en las actividades de la institución

Mitigado (M): Un riesgo es mitigado cuando las consecuencias de este son grandes y se busca minimizar estas a tal punto de que sea aceptable

Evitado (E): Un riesgo evitado es cuando se logro mitigar el riesgo antes de que llegara a suceder o a influir directamente en la institución

Trasferido (T): Un riesgo es transferido cuando este no pertenece a un área y se lo transfiere a otra para que esta lo trate o gestione.

Pregunta 1

De acuerdo con las explicaciones anteriores, llene la información solicitada a continuación con respecto a su criterio.

Figura 67. Encuesta 2.

Riesgos /Vulnerabilidades / Amenazas	Probabilidad					Impacto					Tratamiento					Nivel de Madurez				Responsable
	1	2	3	4	5	1	2	3	4	5	A	M	E	T	I	D	A	O		
Perdida de las fuentes energéticas					X				X			X			X					Analista de redes.
Errores Humanos			X					X			X				X					DTIC
Indisponibilidad de la red		X						X				X				X				Analista de redes
Deterioro de los componentes, equipos e insumos	X								X				X				X			DTIC
Fallas de los componentes, equipos e insumos	X								X				X				X			DTIC
Daño o deterioro de la estructura física del cuarto seguro	X							X				X			X					Subgestorduc
Desorganización del cableado (energético, datos)		X							X				X				X			Analista de redes
incendio	X								X				X		X					Subgestorduc
inundación	X								X				X		X					"
Temblores, terremoto o movimientos telúricos.	X								X				X		X					"
Intento de acceso no autorizado al cuarto seguro	X								X				X		X					Analista de redes
Falla en la climatización		X							X				X							"
Errores de software		X							X				X				X			Area de software
Trafico inusual de la red		X						X					X				X			Analista de red
Fallas de acceso	X							X					X				X			"
Intentos de acceso no autorizado		X						X					X				X			"
Intento de infección son software malicioso	X							X					X				X			"
Ingreso de infección son software malicioso	X							X					X				X			"
Cambios no autorizados	X							X					X				X			Area de software
Ataques de DoS (denegación de servicios)		X							X				X				X			Analista de red
Caducidad de licencias				X				X					X					X		Area de software
Pérdida o falla en el almacenamiento de información en la base de datos.	X								X			X								"

Figura 68. Encuesta 3.

Pregunta 2

Indique otros factores internos o externos que no fueron considerados en la pregunta anterior

Internos:

Exposes por mantenimientos programados

Externos:

Indisponibilidad de la red del proveedor.

Pregunta 3

Indique como se encuentran los siguientes documentos, manuales que ayudan a gestionar los riesgos:

PUBLICADO (P)	SOCIALIZADO (S)	EN DESARROLLO (D)	Versionado (V)	NO DISPONE (ND)	NO APLICA (NA)

DOCUMENTOS	P	S	D	V	ND	NA
Análisis de Riesgos					X	
Análisis de impacto de negocio					X	
Plan de recuperación ante desastres					X	
Plan de continuidad de negocio					X	
Estrategias para la gestión de Crisis					X	
Plan de Contingencias			X			
Plan de Evaluación y Tratamiento de riesgos					X	
Políticas de Seguridad de la Información			X			
Políticas para el etiquetado de la información					X	
Políticas para el uso aceptable de la información y de los activos asociados con la información					X	
Políticas para la gestión de medios extraíbles					X	
Política de control de acceso					X	
Políticas para la instalación de software					X	
Plan de mantenimiento de activos	X	X				

Figura 69. Encuesta 4.

Pregunta 4

¿Cuáles son los criterios que ustedes siguen para considerar que un riesgo es aceptable?

Los riesgos son aceptables cuando afectan por poco periodo de tiempo la disponibilidad de los servicios

Pregunta 5

De acuerdo con la pregunta anterior, ¿Cómo consigue que el riesgo residual de los riesgos principales sea aceptable?

Realizando las correcciones necesarios para que cuando vuelva a suceder el mismo riesgo saber qué acciones tomar

Pregunta 6

¿Cuántas auditorias se han realizado al data center?

No se han realizado auditorías al Data Center

Pregunta 7

¿Cuáles fueron las principales no conformidades?

No se han realizado auditorías al Data Center.

Pregunta 8

¿Que se hizo al respecto?

No se han realizado auditorías al Data Center.

Figura 70. Encuesta 5.

Pregunta 9

¿Qué herramientas utiliza para la valoración de riesgos?

- 0 Check-list
- 0 Matriz de riesgos
- 0 Matriz de calor
- 0 Árbol de fallas
- 0 Diagrama causa efecto
- 0 Otras
- 0 Ninguna

Pregunta 10

¿Como identifica los cambios o configuraciones en equipos que usted administra?

- 0 Monitoreo por consola del equipo
- 0 Monitoreo manual
- 0 Alertas o alarmas del equipo
- 0 Desconexión o reinicio automático
- 0 No se realizan
- 0 Otros

Pregunta 11

¿El área de trabajo de los responsables de la operación del data center se encuentra aislado de las instalaciones del data center?

- Si
- No

Pregunta 12

¿Se encuentran segregadas las funciones de los funcionarios del data center?

- Si
- No
- No estoy seguro

Pregunta 13

¿Cuál es el criterio para la segregación de actividades?

No se segregan actividades.

Figura 71. Encuesta 6.

Pregunta 14

Marque lo que corresponda

Dispone de la siguiente información	SI	NO	
Contactos de expertos en data center	✓		
Pertenezco a grupos de expertos en data center		X	
Asisto a foros de seguimiento		X	FRECUENCIA
Pertenezco a asociaciones administradores o responsables de data center		X	

Pregunta 15

¿Qué tipos de controles se realizan a los candidatos para trabajar en el data center?

TIPOS DE CONTROLES	Si	No	Realiza otro Departamento	No Aplica
Pruebas de polígrafo		X		
Verificación de datos personales	✓			
Verificación de antecedentes penales	✓		Talento Humano	
Verificación de certificaciones	✓		Talento Humano	
Entrevista al candidato	✓		Talento Hu y TIC	
Verificación de Autenticidad de documentos	✓		Talento Humano	
Pruebas de Personalidad				X

Figura 72. Encuesta 7.

Pregunta 16

¿De las siguientes certificaciones cuales posee para administrar el data center?

Conocimientos y certificaciones que debe disponer el personal que labora en el data center	Si	No
Técnico en Computación e informática o carreras afines	✓	
Conocimiento en Sistemas Operativos, Redes y Soporte TI	✓	
Ingles nivel Intermedio	✓	
Scrum Foundation		X
AWS cloud Practitioner		X
Azure Fundamentals		X
ITIL		X
Microsoft 365 Fundamentals		X
Certificado de base del centro de datos (DCFC®)		X
Profesional Certificado en Centros de Datos (CDCP)		X
Especialista certificado en centros de datos (CDCS)		X
Experto certificado en centros de datos (CDCE)		X
Profesional Certificado en Diseño de Cableado de Red (CNCDP)		X
Especialista certificado en operaciones de instalaciones de centros de datos (CDFOS®)		X
Gerente Certificado de Operaciones de Instalaciones de Centros de Datos (CDFOM)		X
Especialista Certificado en Sostenibilidad Ambiental del Centro de Datos (CDESS)		X
Profesional certificado en riesgos de centros de datos (CDRP)		X
Especialista certificado en migración de centros de datos (CDMS)		X
Consultor de diseño certificado TIA-942 (CTDC)		X
Auditor Interno Certificado TIA-942 (CTIA)		X

Pregunta 17

¿Qué porcentaje de los equipos del data center pertenecen a la Universidad Politécnica Estatal del Carchi?

- Todos
- 75% de los equipos
- 50% de los equipos
- 25% de los equipos
- 0% de los equipos

Figura 73. Encuesta 8.

Pregunta 18

¿Indique cómo realizan la clasificación de la información en el Data Center?

Privada (P)	Pública (PU)	Restringida (R)	Confidencial (C)	No Aplica (NA)

INFORMACIÓN ALMACENADA EN EL DATACENTER	P	PU	R	C	NA
Contraseñas	✓				
Configuraciones de equipos	✓		✓		
Información de Autoridades		✓			
Información de funcionarios		✓			
Información de Docentes		✓			
Información de Trabajadores		✓			
Información de Estudiantes	✓	✓	✓		
Sistema integrado	✓		✓		
Código fuente			✓		
Información de pág. web		✓			
Eventos		✓			
Información Financiera			✓		
Información académica		✓			
Información Arquitectónica y estructural			✓		
Inventario de Activos			✓		

Pregunta 19

¿Qué métodos utilizan para proteger la información ante accesos no autorizados?

Métodos	Si	No
Control de accesos	✓	
Vigilancia 24/7	✓	
Sistemas de video vigilancia y/o alarmas	✓	
Climatización de los servidores	✓	
Protección contra incendios		✗
Plan de gestión de riesgos		✗
Segmentación de redes y equipos críticos	✓	
Firewalls físicos y virtuales	✓	
IPS (Sistema de Prevención de Intrusos)	✓	
Adecuación de Permisos		✗
Controles integrales de seguridad		✗
DLP (Solución de Prevención de Perdida de Datos)		✗
DRP (Plan de Recuperación de Desastres)		✗
SIEM (Correlacionado de Eventos)		✗
Plan de Detección y Respuesta a Incidentes.		✗

Figura 74. Encuesta 9.

Pregunta 20

¿Con que frecuencia se cambia el acceso de los usuarios en los activos críticos del data center?

- 0 Cada mes
- 0 Cada 3 meses
- 0 Cada 6 meses
- 0 Cada año
- 0 Más de un año
- 0 Nunca

Pregunta 21

¿Con que frecuencia se cambia el acceso al firewall del data center?

- 0 Cada mes
- 0 Cada 3 meses
- 0 Cada 6 meses
- 0 Cada año
- 0 Más de un año
- 0 Nunca

Pregunta 22

¿Cómo controlan el acceso del personal que ya no se encuentra trabajando en la institución?

Control	Aplica	No Aplica
Eliminación de credenciales de acceso	✓	
Reasignación de credenciales		✓
Cambio de contraseñas		✓
Suspensión del ingreso	✓	

Pregunta 23

¿Qué controles de acceso utilizan para limitar el acceso a la información y funciones del sistema?

Controles físicos y lógicos	Si	No
Sensor biométrico	✓	
Sensor de proximidad		X
Cámaras de seguridad	✓	
Servicio de guardias	✓	
Puerta electrónica		X
Acceso por credenciales		X
Acceso concedido por administrador		X
Firewall	✓	
Cerradura por tarjeta electrónica	✓	
Restricción de acceso por IP y/o MAC		X

Figura 75. Encuesta 10.

Pregunta 24

Niveles de seguridad de contraseñas

Nivel bajo: La contraseña solamente cuenta con un mínimo de 5 caracteres

Nivel medio: La contraseña cuenta con un mínimo de 6 caracteres, además de cumplir con los siguientes requisitos:

- Incluir números y letras mayúsculas y minúsculas
- Incluir al menos un carácter especial (#$%&)

Nivel alto: La contraseña cuenta con un mínimo de 6 caracteres, además de cumplir con los siguientes requisitos:

- Incluir números y letras mayúsculas y minúsculas
- Incluir al menos un carácter especial (#$%&)
- La contraseña debe de contar con fecha de caducidad por lo menos de 90 días
- Al cambiar por una nueva contraseña no debe ser igual o parecida a las 5 anteriores contraseñas (Nadeau, 2023).

De acuerdo con lo explicado anteriormente ¿Cuál es el nivel de seguridad de las contraseñas?

0 Nivel Bajo
0 Nivel Medio
0 Nivel Alto

Pregunta 25

¿Existen controles de protección de equipos externos?

- Si
- No

Pregunta 26

¿Cuáles son los controles y como es la conexión?

No existen.

Figura 76. Encuesta 11.

Pregunta 27

¿Con que frecuencia se realizan copias de respaldo de la información, software y sistema?

- 0 Cada día
- 0 Cada semana
- 0 Cada mes
- 0 Cada 3 meses
- 0 Cada 6 meses
- 0 Cada año
- 0 Más de un año
- 0 Nunca

Pregunta 28

¿Con que frecuencia se realizan las pruebas de las copias de seguridad?

- 0 Cada mes
- 0 Cada 3 meses
- 0 Cada 6 meses
- 0 Cada año
- 0 Más de un año
- 0 Nunca

Pregunta 29

¿Cuál es el proceso de evaluación a las copias de seguridad?

Montando el backup en un servidor de pruebas.

REFERENCIAS BIBLIOGRÁFICAS

Araujo Castro, G. M. (2019). *Propuesta de un Plan de continuidad del negocio para una entidad pública del Ecuador* (p. 7) [A obtención del Grado Académico de Magister]. https://repositorio.uta.edu.ec/bitstream/123456789/29843/1/Tesis_t1584msi.pdf

Jiménez, M. M. (2021, March 12). *¿Qué es la madurez de gestión de riesgos?* Www.piranirisk.com. https://www.piranirisk.com/es/blog/madurez-gestion-de-riesgos-que-es

Nadeau, C. (2023, January 11). *Configuración del nivel de seguridad de contraseñas*. Ayuda de Zendesk. https://support.zendesk.com/hc/es/articles/4408822149018-Configuraci

Figura 77. Encuesta 12.

Anexo 8. Plan de Contingencia.

Propuesta

Plan de contingencia.

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Plan de contingencia para el Data Center de la Universidad Politécnica Estatal del Carchi

Figura 78. Plan de Contingencia.

Anexo 9. Evidencia de encuestas.

Figura 79. Evidencia de encuestas 1.

Figura 80. Evidencia de encuestas 2.

Anexo 10. Aceptación y Conformidad del plan de contingencia.

UPEC

POLITÉCNICA DEL CARCHI
EDUCAMOS PARA TRANSFORMAR EL MUNDO

Tulcán, 21 de Julio del 2023

ACEPTACIÓN

Por medio del presente, se realiza la aceptación y conformidad del documento: Plan de Contingencia para el Data Center de la Universidad Politécnica Estatal del Carchi elaborado por los estudiantes: Willian Alejandro López Mosquera, portador de la cédula de identidad 0401951868, de nacionalidad ecuatoriana y Alexis Fernando Fuel Piarpuezán, portador de la cédula de identidad 0401747746, de nacionalidad ecuatoriana, como proyecto de Tesis, para la obtención del título de Ingenieros en Computación.

Es cuanto puedo certificar en honor a la verdad, facultando a los interesados hacer uso del presente en la forma que más convenga a sus intereses enmarcado en el campo legal.

Atentamente,

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI UPEC CENTRO TIC TULCÁN

Msc. Andrea Guevara
DIRECTORA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN TIC
UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI UPEC
"EDUCAMOS PARA TRANSFORMAR EL MUNDO"

Calle Antisana y Av. Universitaria
Telf: (06) 2980837 - 2984435
info@upec.edu.ec
www.upec.edu.ec
Tulcán - Ecuador

Figura 81. Aceptación y Conformidad del plan de contingencia.