UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
EXTENSIÓN EN EL CARMEN
CARRERA DE INGENIERÍA EN SISTEMAS

Creada Ley No. 10 – Registro Oficial 313 de Noviembre 13 de 1985

TRABAJO DE INVESTIGACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

AUDITORÍA INFORMÁTICA DE SEGURIDAD LÓGICA PARA INFORMACIÓN DE DOCENTES "UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ" INGENIERÍA EN SISTEMAS

AVILA CEVALLOS ANTHONY ALDAIR

AUTOR

ING. POZO HERNÁNDEZ CLARA GUADALUPE MG.

TUTORA

EL CARMEN, AGOSTO DEL 2019

Uleam

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
EXTENSIÓN EN EL CARMEN

DECLARACIÓN DE AUTORÍA

Yo, Anthony Aldair Ávila Cevallos, con número de cédula 131470821-3, estudiante de la carrera de Ingeniería en Sistemas de la Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen, en relación al Trabajo de Titulación presentado para su defensa y evaluación en el período 2019-2020(1), declaro ser el único titular del este trabajo de investigación cuyo tema es: **"Auditoría Informática de Seguridad Lógica para Información de Docentes "Universidad Laica Eloy Alfaro de Manabí" Ingeniería en Sistemas",** el mismo que autorizo a la Universidad Laica Eloy Alfaro de Manabí Extensión en El Carmen hacer uso completo o parcial del contenido solo con fines académicos.

_____
Anthony Aldair Ávila Cevallos
CI. 131470821-3

CERTIFICACIÓN DE APROBACIÓN

Uleam UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ	**NOMBRE DEL DOCUMENTO:** **CERTIFICADO DE TUTOR(A).**	**CÓDIGO: PAT-01-F-010**
	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO.	**REVISIÓN: 1**
		Página 1 de 1

CERTIFICACIÓN

En calidad de docente tutor(a) de la Extensión el Carmen, de la Universidad Laica "Eloy Alfaro" de Manabí, certifico:

Haber dirigido y revisado el trabajo de titulación, cumpliendo el total de 400 horas, bajo la modalidad de proyecto de titulación, cuyo tema del proyecto es "**AUDITORÍA INFORMATICA DE SEGURIDAD LOGICA PARA LA INFORMACION DE DOCENTES "UNIVERSIDAD LAICA ELOY ALFARO DE MANABI" INGENIERÍA EN SISTEMAS**", el mismo que ha sido desarrollado de acuerdo a los lineamientos internos de la modalidad en mención y en apego al cumplimiento de los requisitos exigidos por el Reglamento de Régimen Académico, por tal motivo CERTIFICO, que el mencionado proyecto reúne los méritos académicos, científicos y formales, suficientes para ser sometido a la evaluación del tribunal de titulación que designe la autoridad competente.

La autoría del tema desarrollado, corresponde al señor **AVILA CEVALLOS ANTHONY ALDAIR**, estudiante de la carrera de Ingeniería en Sistemas, período académico 2019-2020, quien se encuentra apto para la sustentación de su trabajo de titulación.

Particular que certifico para los fines consiguientes, salvo disposición de Ley en contrario.

El Carmen, 08 de agosto de 2019

Lo certifico,

Ing. Clara Guadalupe Pozo Hernández, Mg.
Docente Tutor(a)

DEDICATORIA

El presente trabajo está dedicado en primer lugar a Dios por ser el creador y fuente de vida, por brindarme cada día salud y permitir seguir compartiendo grandes momentos con mi familia y amigos.

A mis padres por brindarme su apoyo y comprensión en todo momento en el transcurso de mi carrera universitaria.

A mis compañeros de estudios por formar parte de mi educación en el trayecto de la carrera y ser fuentes de apoyo, a los docentes que fueron parte de mi formación profesional y personal.

Anthony Ávila

AGRADECIMIENTO

Quiero agradecer en primer lugar a Dios por cada bendición en mi vida y permitirme seguir adelante con mis estudios y brindarme la oportunidad de tener una familia maravillosa.

A mis padres por su apoyo moral e incondicional por ser los principales promotores de mi educación, gracias por confiar y creer en mí y brindarme todo su amor, dedicación y esmero, por siempre querer lo mejor para mi vida.

A mis compañeros y amigos por ser las mejores personas, por estar y compartir con ellos grandes momentos, por brindarme su amistad y apoyo.

A los docentes por cada conocimiento otorgado y a la ULEAM Extensión El Carmen por ser parte de mi educación.

Anthony Ávila

ÍNDICE

ÍNDICE DE CUADROS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE ANEXOS

RESUMEN

La presente investigación tiene como objetivo evaluar el cumplimiento de las políticas de seguridad al compartir información por los docentes de la Universidad Laica Eloy Alfaro de Manabí El Carmen, con el fin de identificar el nivel de cumplimiento con las mismas. Para realizar el trabajo se inició fundamentando bibliográficamente aspectos que intervienen en el desarrollo del tema relacionado con la auditoría informática y la seguridad lógica, consecutivamente se aplicó un diagnóstico a los docentes del área de Ingeniería en Sistemas para verificar el nivel de conocimiento sobre las políticas de seguridad, donde se evidencio que la mayoría no tenía conocimiento sobre la existencia de la política de seguridad por lo que se consideró pertinente el desarrollo del trabajo de investigación. En la propuesta se aplicó etapas de una auditoría informática iniciando por la planificación cuyo objetivo fue verificar el cumplimiento de las políticas de seguridad de la información a los profesores del área de Ingeniería en Sistemas, para su aplicación se elaboró un instrumento en base a la norma ISO/27002 que constó de 94 preguntas cerradas y de selección, las cuales dirigidas a los docentes del área de Ingeniería en Sistemas una vez tabuladas se pudo comprobar que el nivel de cumplimiento de políticas fue del 58% pudiéndose notar que los aspectos que menos se cumplió fue en acceso al aula virtual, finalmente se propone una guía para acceder de forma segura a los datos

SUMMARY

The objective of this research was to evaluate the compliance of the security policies in the teachers of the Eloy Alfaro Laica University of Manabí El Carmen, in order to identify if they comply with them. In order to carry out the work, bibliography was based on aspects that are involved in the development of the topic related to computer auditing and logical security. A diagnosis was applied to teachers in the Systems Engineering area to verify the level of knowledge about security policies. Therefore, it is possible to identify that there was an ignorance of the policies. In the proposal, stages of a computer audit were applied starting with the planning whose objective was to verify compliance with the information security policies to the professors of the Systems engineering area, for its application an instrument was developed based on the standard ISO / 27002 consisting of 94 closed and selection questions, which addressed to teachers in the area of Systems Engineering once tabulated, it was found that the level of policy compliance was 58% and it can be noted that the aspects that least complied was in access to the virtual classroom, finally a guide is proposed to securely access the data.

INTRODUCCIÓN

La auditoría informática se basa en analizar los sistemas informáticos para descubrir las vulnerabilidades que se pueden mostrar, los cuales sirven de ayuda por que detectan, y al mismo tiempo se puede estudiar y corregir dichos errores que se presentan, (Tejada, 2015)

En años anteriores la seguridad lógica era considerada, seguridad de los equipos informáticos, centrados en proteger los dispositivos de los usuarios que tenían acceso a ellas, otorgándole seguridad a sus ordenadores y al sistema operativo para evitar que dejen de funcionar y además como protección contra virus informáticos. Luego con la llegada del internet y su uso globalizado en las empresas, la seguridad informática se enfoca en la conectividad de las redes, protegiendo los equipos de aplicaciones informáticas accesibles a través del internet. (López, Mendoza, Reyes, Rivas, Ramos, & Pedraza, 2015)

La seguridad de la información abarca las técnicas de la información frente a accesos, uso, revelación, complicación, alteración o desgracia no autorizados. Este proceso interactivo comporta un continuo proceso de formación, evaluación, protección, monitorización y detección, respuesta y resolución de incidentes, documentación y revisión. (Barman, 2001)

El presente proyecto tuvo como objetivo general evaluar el cumplimiento de las políticas de seguridad en el proceso de la información dirigida a los docentes de la carrera Ingeniería en Sistemas de la Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen con el fin de identificar si cumplen con las mismas.

Para el desarrollo del trabajo se inició fundamentando bibliográficamente aspectos que se involucran en el desarrollo del tema, relacionados con la auditoría informática y seguridad lógica, posteriormente se aplicó un diagnóstico a los docentes del área ingeniería en sistemas para identificar el nivel de conocimiento sobre políticas de seguridad, pudiéndose identificar que existía un desconocimiento de las normas. Con el fin de verificar si los docentes cumplen con las mismas.

La presente investigación se encuentra estructurada de la siguiente manera:

En el primer capítulo se encuentra la investigación de cada una de las variables tales como, auditoría informática y seguridad lógica; en el segundo capítulo se encuentra: los tipos de investigación y los métodos que se utilizan, la población que se tomó para llevar acabo la presente investigación, técnicas e instrumentos de investigación el resultado de la encuesta aplicada y el análisis de los resultados de la presente investigación; en el tercer capítulo concierne a la propuesta, el cual se empleó con la planificación de la auditoría, también encontramos el informe de auditoría la nómina del personal relacionado, se encuentra el alcance y los hallazgos, donde se refleja si los miembros de la carrera de Ingeniería en Sistemas cumplen o no con las normas de seguridad requeridas.

Se propone una guía de buenas prácticas para la seguridad de la información como es el uso de contraseñas, uso de correo electrónico, acceso al sistema operativo y el alojamiento en la nube.

CAPÍTULO I

1 MARCO TEÓRICO

1.1 Auditoría

Es el proceso que se lleva a cabo por profesionales especialmente capacitados para el efecto, este proceso solo lo pueden realizar profesionales formados para ello de manera específica, ya que a través de él se van determinando si e sistema implantado en un negocio realiza sus funciones correctamente, el objetivo de la auditoria es mejorar las posibles incidencias que pueda presentar un sistema informático, así como establecer diferentes criterios relacionados con el buen uso (Razo, 2002)

1.1.1 Auditoría Informática

El cambio y la complejidad de los sistemas informáticos hicieron necesario la aparición de personas especializadas que evalúen el correcto funcionamiento de los mismos una considerada actividad y descubrir aquellos puntos frágiles que soliciten un acogimiento de medida correctiva o de prevenciones para disminuir problemas de perdida en la información, integridad y disponibilidad de la información que hoy en día es el bien más preciado de toda empresa o institución. La imagen de un auditor hace cada vez más necesaria en las organizaciones ya que solicita un experto que ajusté la validez de los sistemas informáticos con la capacidad de manifestar recomendaciones y propuestas (Diego A. Arcentales Fernández, 2017)

1.1.2 Código deontológico de la función de auditoría

La auditoría informática es el sistema de análisis íntegro para detectar distintas fuentes de vulnerabilidades que se pueden presentar en los diferentes sistemas informáticos, los cuales sirven de ayuda por que detectan, y al mismo tiempo se puede analizar y solucionar dichos errores presentados, el código deontológico consiste en una serie de preceptos en los que se determinan los derechos exigibles a ciertos expertos con el fin de ajustar los principios ético y moral. La auditoría interna es una actividad independiente y objetiva de

aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una programación a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno, es necesario con código de ética llegando a incluir dos componentes esenciales. (Tejada, 2015)

Para la auditoria informática existe una organización internacional que es la encargada de diseñar los estándares de auditoría y control de los sistemas de información aceptados por la comunidad general de auditoria. Esta organización llamada ISACA por sus siglas en ingles de (Information Systems Audit and Control Association) que en español significa Asociación de Control y Auditoría de Sistemas de Información es la que expide el certificado CISA que es el certificado de auditor de sistemas de información el cual es entregado a las personas que cumplen con los requisitos estipulado en cuanto a normas, código ético, procedimiento de control, entre otros. Las personas que pertenezcan a ISACA o poseen su certificación CISA deben comprometerse a comprender y cumplir diez normas de auditoria de sistema de información que mantienen la independencia entre el auditor y la empresa que se audita el objetivo de la auditoria y sobretodo los códigos de ética profesional (Lieberman, 2015).

1.1.3 Antecedentes de la auditoría

A medida que se expandía el comercio pasando por el trueque las operaciones comerciales y las personas que la realizaban sintieron la necesidad de establecer mecanismos de registros que le permitieran el dominio de las actividades comerciales, al pasar el tiempo los comerciantes se agremiaron y crearon mercados locales lo que produjo la necesidad de mejorar el registro de las actividades tanto individuales como grupales, al aumentar el número de los integrantes de las agrupaciones fue imprescindible crear normas de control que detallaran las actividades financieras. (Tejada, 2015)

Gracias a esta evolución de los procedimientos mercantiles nacieron las escribas que después se convertirían en partida doble y en la actualidad son

conocidos como teneduría de libros, la evolución de esta técnica permitió impulsar la contabilidad y los registros de operaciones en libros y pólizas, hoy en día todos estos procedimientos contables son realizados en sistemas computacionales, por ello fue necesario que alguien evaluara estos registros y resultados fueran correctos, veraces se puedan verificar y sean confiables; fue en ese instante donde nació el acto de auditar (Razo, 2002).

La necesidad de toda organización garantiza sus inversiones, los servicios de auditoría de sistemas, hoy todavía no se encuentran excesivamente difundidos, principalmente por el desconocimiento de sus existencias. El éxito demostrado en las experiencias obtenidas, va repercutiendo en una mayor proliferación de estos servicios en las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier (Portera, 2009)

1.1.4 Objeto de la auditoría

En relación con el objeto de la auditoria se establece que la auditoría tiene con finalidad verificar el cumplimiento de las medidas de seguridad, de acuerdo a la lógica con la que se dispone para así llegar al problema que genera el poco conocimiento en este ámbito con todo este paso logramos establecer lógicamente la vulnerabilidad. (Portera, 2009)

Aquellas organizaciones que deciden implementar y certificar sus procesos de acuerdo a las diferentes normas internacionales ISO y trabajan con Sistemas de Gestión Normalizados bien para conseguir la excelencia de la calidad de sus productos y servicios, bien para garantizar su compromiso con el medio ambiente, bien para asegurar modelos eficientes de seguridad y salud en el trabajo y otro largo etcétera de normas que ayudan a esas organizaciones a alcanzar la excelencia en sus procesos, están ampliamente familiarizadas con el concepto de auditoría. Si bien, como muchos auditores comentaban en ese debate, no siempre se entiende el trabajo de los auditores, internos y externos, más allá de que sea un requisito en las normas internacionales, por esto, nos gustaría recoger qué objetivo debe tener una auditoría (Razo, 2002)

Auditar radica principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos. Los mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia (Borda, 2013)

1.1.5 Funciones de la auditoria informática

En el proceso de la auditoria es importante asegurarse que se cumplan por lo menos los principios primordiales de un proceso formal. Los elementos indispensables para cumplir este requisito, la principal función que debe cumplir una auditoría es la evaluación de actividades y observar los resultados de lo que se determina si son los adecuados y si cumplen los objetivos y estrategias que plantea la organización o institución. (Portera, 2009)

1.1.6 Auditoría informática en diversos sectores

La auditoría consiste de información, dada a su relación con la tecnología de la información con entidades y organización los usuarios en general mantienen relaciones interprofesionales. (Navarro, 2001)

El auditor antes que todo deberé empezar con una elaboración planificando en lo que se detalle de los objetivos y procedimiento que se llevaran a cabo en la auditoria informática con los lugares en los que realizaran también deberá de tallar la duración de la auditoria la organización de un equipo auditor requiere de un orden jerárquico que garantice el flujo de la información de conformidad con la autoridad y responsabilidad asignados a todos y cada uno de sus integrantes. (Lieberman, 2015)

1.1.7 Auditoría de sistemas computacionales (Auditoría Informática)

Originados por la clase de continuar con la exposición de las definiciones de cada uno de los tipos de auditorías, debido a que los atributo de este libro es enfatizar la trascendencia, utilidad y especialidad de la auditoría de sistemas

computacionales (ASC), con el cual demostramos cada una de las definiciones de auditorías especializadas de los sistemas computacionales, en las cuales se aplican para las diferentes áreas y disciplinas de este contexto informático. (Razo, 2002)

Es la revisión técnica, especializada y absoluta que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes. Dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumo necesarios para el trabajo del centro de cómputo. (Borda, 2013)

El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de sus resultados en la institución, incluyendo la evaluación en el desempeño de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa. (Razo, 2002)

En la redacción del informe, el auditor señala los resultados de su investigación, sus evaluaciones, hallazgos, aportaciones y conclusiones sobre el trabajo realizado; también señala las técnicas, herramientas, métodos y procedimientos que utilizó en la obtención de datos, las observaciones, interpretaciones de los fenómenos y hechos evaluados que le sirvieron de sustento en la elaboración del documento de situaciones encontradas o relevantes que informa, así como todas las demás aportaciones con las cuales da su sello personal al informe presentado. (Navarro, 2001)

1.1.8 Explicación de los requerimientos que deben cumplir los hallazgos de auditoría

Dentro del ámbito de la auditoria, un hallazgo se refiere a un conjunto de información que recopila específicamente sobre la actividad, tarea y proceso analiza y evalúa, en general, los hallazgos obtenidos se emplean a modo de

crítica y muestran información sobre deficiencias o debilidades con esto se analiza la explicación que cada docente deberá saber al momento de evaluar sus datos porque gracias al sistema auditado y presentadas en el informe de auditoría detectamos las debilidades. (Tejada, 2015)

1.1.9 Funciones de la auditoria informática

(Navarro, 2001), nos dice que la importancia del proceso de auditoria es el de asegurar que los principios básicos de un proceso formal sean cumplidos. Para lo cual se han establecido elementos indispensables para el cumplimiento de este requisito, los cuales son: seguimiento del desempeño, planeación y el control, de esta forma se garantiza lo siguiente:

- Que los todos los equipos y demás recursos informáticos se encuentren orientados a cumplir los objetivos y las estrategias de la institución.
- Elaborar, difundir y cumplir políticas, procedimientos y controles propios de la auditoria informática
- Que se puedan obtener los resultados ambicionados por la institución por medio de la coordinación y apoyo mutuo con: la alta dirección, asesores externos y asesores internos.

1.1.10 Importancia del control y la Auditoria Informática

Dentro de la auditoria informática se hace referencia a algunos factores críticos que vulneran el bien más importante y atesorado de las instituciones, la información. Estos factores se clasifican en: privacidad de los datos, abuso informático, coste de perdida datos, toma de decisiones incorrectas. (Navarro, 2001)

1.1.11 Normas, técnicas, estándares y procedimientos de auditoria

En la actualidad la ejecución de una auditoria informática se encuentra basada en la aplicación de estándares, normas, técnicas y procedimientos que garanticen el éxito del proceso. Gran parte de la documenta existente coincide

en que las normas de auditoria son requisitos mínimos de calidad, concernientes a las cualidades de la persona que aplica la auditoria, los procedimientos y métodos aplicados en la auditoria y los resultados que nazcan de la misma. Mientras que las técnicas se definen como todos aquellos métodos que hacen evidenciar y fundamentar las opiniones y conclusiones del auditor, permitiendo emitir de forma cuantitativa y cualitativa el análisis de los procesos que lleva la institución. (Tejada, 2015)

1.1.12 Organizaciones y Normas al más relevante

(Razo, 2002), da a conocer qué en la actualidad se dispone de un marco regulatorio y normativo de la auditoria informática, sin embargo dicho margo es muy reducido, por tal motivo es indispensable estudiar las normativas y organizaciones internacionales más relevantes en AI, Las organizaciones de prestigio mundial y con renombre en Auditoria Informática son las siguientes: Institute of InternalAuditors(IIA), e Information System Audit and Control Association (ISACA)

Dichas organizaciones han creado normas y estándares con la finalidad de fijar políticas y lineamientos que garanticen el proceso de Auditoria. Los estándares más utilizados y recomendados por los expertos son:

- COBIT: Control Objectives for Information and related Technology. Realizado por ISACA. Se enfoca principalmente en la gobernabilidad, aseguramiento, control y auditoria para las TIC´s (Tecnología de la Información y la Comunicación).
- ITIL: Information Technology Infrastructure Library. Agrupa las mejores prácticas para la administración de los servicios de Tecnología de la Información (TI).
- COSO: Committee of Sponsoring Organizations. Recomienda las personas encargadas de TI sobre la manera de informar, evaluar, informar e implementar sistemas de control, manteniendo como principal objetivo la efectividad y la eficiencia de las operaciones, la información y

la ejecución adecuada de las regulaciones, vlorando los riesgos, las actividades de control, información y comunicación y su verificación.

- ISO Serie 27000: Integra un conjunto de normas sobre Sistemas de Gestión de Seguridad de la Información (SGSI), que a través de su aplicación, permi-te administrar la información mediante el modelo Plan – Do – Check – Act(PDCA).
- SAC:SystemsAuditability and Control, ofrece una guía de estándares y con-troles a auditores internos sobre la forma de controlar y auditar los sistemas de información y tecnología

1.1.13 Políticas de seguridad y seguridad de información

La seguridad en una Institución acoge mucho más allá de usar un antivirus o de la configuración que tenga la empresa para la prevención de intrusos. Las políticas son los instrumentos que explica sobre como la institución realiza sus actividades para alcanzar los objetivos. Muchas organizaciones no han definido de manera adecuada las políticas de seguridad que estas políticas se las realiza de acuerdo a las necesidades de la empresa, existen situaciones que provocan vulnerabilidades que así pueden ser aprovechadas por atacantes. (Quintero, 2017)

La política de contraseñas poco robustas, este tipo de contraseñas pueden ser descubiertas de manera fácil esto ocurre porque no se cambia la contraseña con frecuencia, cuando se comparten las contraseñas los usuarios suelen anotar sus contraseñas o en ciertas ocasiones comunican a otra persona no se preocupan por la seguridad de la misma, por el deficiente control de accesos al sistema es cuando existen fallos de autenticación y no se toman las medidas adecuadas para resolver los riesgos que se presentan. El escaso control de acceso a los recursos los usuarios que tienen permisos más de lo que necesitan, procesos inadecuados en los soportes informáticos, el escaso control de información sensible trata de que no se tiene vigilancia cuando se tiene información en papel. (Vieites, 2014)

Políticas de contraseña el objetivo es proteger la información y recursos de tecnologías de información de la Universidad Laica Eloy Alfaro de Manabí a los riesgos asociados a la pérdida de confidencialidad integridad y disponibilidad de la información las contraseñas establecidas serán administradas y gestionadas bajo única responsabilidad. Política de seguridad de la información el objetivo es controlar la gestión de la seguridad de la información institucional, en todo su ciclo de vida y formatos, con el propósito de proteger la información mediante la implementación de medidas de seguridad preventivas y de la recuperación, que contribuyan a garantizar la confiabilidad, integridad y disponibilidad de la información física y digital (Uleam)

1.1.14 ISO 27001: el método MAGERIT

Es un documento el cual su uso es facultativo y es el resultado que se da por ciertas partes beneficiadas y éstas deben afirmar por parte de una corporación que sea reconocido. ISO (Organización Internacional de Normalización) es un organismo que se dedica a desarrollar reglas de normalización en varios ámbitos, especialmente en el área de informática. IEC este organismo publica normas de estandarización referentes a electrónica. El método MAGERIT, son las siglas de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones, dicho método cubre la fase AGR (Análisis y Gestión de Riesgos). Si hablamos de Gestión global de la Seguridad de un Sistema de Seguridad de la Información basado en ISO 27001, MAGERIT, es el núcleo de toda actuación organizada en dicha materia, ya que influye en todas las fases que sean de tipo estratégico y se condiciona la profundidad de las fases de tipo logístico. (Ramos & García Cervigón Hurtado, 2011)

1.2 Seguridad lógica

1.2.1 Principios de seguridad lógica

La seguridad de la información automática se encuentra distribuida en varios temas actualmente, al encontrarse involucrada en varia ramas de la computación, es necesario cumplir con un diverso grupo de estándares para poder establecer un adecuado grado de madurez y disminuir el riesgo en una

organización que debe mantener disponible permanentemente el funcionamiento de su red, las aplicaciones informáticas y de más servicios que brindan a sus clientes y usuarios. (Escrivá, Romero, & Ramada, 2013) (Chicano, 2015)

Una seguridad adecuada debe cumplir con un sin números de procedimientos que permitan resguardar el acceso a los datos y sus aplicaciones informáticas, por aquello se emplean software de seguridad y principios para la prevención de riesgos, recordando que los principios básicos que establece un sistema de seguridad informático son: integridad disponibilidad y confidencialidad. (Escrivá, Romero, & Ramada, 2013) (Chicano, 2015)

1.2.2 La seguridad de la información

Barman (2001), da a conocer que la seguridad de la información implica técnicas de la información frente a accesos, uso, revelación, complicación, alteración o desgracia no autorizadas. Este proceso interactivo comporta un continuo proceso de formación, evaluación, protección, monitorización y detección, respuesta y resolución de incidentes, documentación y revisión, también que la seguridad de datos y servicios se basan en:

- **Confidencialidad**

La confidencialidad se obtiene cuando se previene la resolución o exposición de la misma a usuarios o sistemas no autorizados. Una información se considera confidencial cuando solo debe ser accedida, usada, copiada o revelada a personas autorizadas para ello, y solo cuando existe una necesidad razonable para ello. Cuando la información que se considera de naturaleza confidencial ha sido o puede haber sido accedida, usada, copiada o relevada por destinarios no autorizados no se produce brecha en la confidencialidad

- **Integridad**

En el campo de la seguridad de la información, la integridad significa que los datos no pueden ser creados o eliminados sin autorización. También significa que los datos almacenados en una parte del sistema son conscientes con otros datos asociados y almacenado en otra parte del sistema. Por ejemplo, se

produce una pérdida de la integridad cuando un sistema de base de datos no se apaga de forma adecuada antes de una tarea de mantenimiento o por una perdida repentina de energía eléctrica así mismo se produce una pérdida de integridad cuando un empleado elimina un fichero de datos accidentalmente.

- **Disponibilidad**

Se hace referencia a que la información, los sistemas de computación utilizados para procesar esa información y los controles de seguridad empleados para protegerla están disponibles y funcionando todo correctamente cuando se necesitaba

1.2.3 La seguridad de la información atreves del tiempo

Desde los primeros tiempos de la escritura, los jefes de estado y mandados militares entendieron la necesidad de proporcionar algún mecanismo para proteger la confidencialidad de la correspondencia escrita y de disponer de medios para intentos de trasmisión, como su momento los fueron los sellos lacrados. (Peltier, 2001)

El rápido crecimiento y la gran expansión del procesado electrónico da datos y el comercio electrónico a través de internet, junto con las numerosas ocurrencias de terrorismo internacional han impulsado el desarrollo de nuevos métodos de protección de las redes de computadoras y los datos que almacenan, procesan y transmiten. De esta manera, el campo de la seguridad de la información ha crecido y evolucionado de forma satisfactoria en los últimos años apareciendo especialidad como auditoria de sistemas de información, planificación de continuidad de negocio y ciencia forense digitales (Barman, 2001)

Se le atribuye a julio cesar la invención de cifrado cesar en el año 50 para prevenir que sus mensajes secretos cayeran en manos equivocadas. En la segunda guerra mundial se provocaron grandes avances en la seguridad de la información y marca el comienzo de esta disciplina como un campo profesional. En esta guerra se produjeron progreso en la protección física de la información mediante la protección de los centros de información barricadas y

guardias armadas controlando la entrada también se produjo la información de la clasificación formal de los datos basada en la sensibilidad de la información y quien podía tener acceso a dicha información. (Peltier, 2001)

1.2.4 Clasificación de la seguridad de la información

Un paso de particular importancia para la seguridad de la información y la gestión de riesgos es el reconocimiento del valor de la información y la definición de los procedimientos apropiados y los requerimientos de protección para la información. No toda la información es igual y, por tanto, no toda la información exige el mismo grado de protección. En consecuencia, es evidente la necesidad de clasificación de la información. (Whitman & Mattord, 2011)

Algunos de los factores que influyen en que información de clasificación se debería asignar son el valor cuantitativo de esa información para la organización, la antigüedad de la información y la posible obsolescencia de la misma. Otra consideración importante a la hora de clasificar los datos es la existencia de leyes o normas a seguir con determinado tipo de datos. (Barman, 2001)

La primera fase de la clasificación de seguridad de la información es la identificación de un miembro de la dirección de la compañía como propietario de la información a ser clasificada para desarrollar una política de clasificación. Esta política debe describir las diferentes etiquetas de clasificación, los criterios por los cuales a unos datos se les aplica una determinada etiqueta y lista de los controles de seguridad necesarios para cada categoría. (Whitman & Mattord, 2011)

Todos los empleados de la organización, así como socios de negocios, deben ser entrenados en los esquemas de clasificación y comprender a los controles de seguridad y procedimiento de manipulación requeridos por cada categoría. La categoría asignada a un determinado conjunto de datos debería ser revisada de forma periódica para garantizar que la clasificación sigue siendo la adecuada y que los controles requeridos se mantienen. (Baca, 2016)

1.2.5 Control de acceso

Los controles de acceso lógico sirven para evitar eventos inesperados y proceder técnicamente sobre un recurso informático, asegurando que solo los sujetos identificados y autenticados accedan a los recursos autorizados, comprobando de manera estricta la identidad del sujeto que solicita acceso a un sistema tras realizarse la autenticidad del solicitante; controles que pueden ser implementados en aplicaciones móvil o en sistemas operativos, los cuales en su mayoría están asociados con dos operaciones ya mencionados; la identificación y autenticación aquellos trabajan de manera conjunta para comprobar la identidad del sujeto. (Castro, Díaz, Alzorríz, & Sancristóbal, 2014)

Consiste en verificar como un usuario se registra o inicia sesión en sus aplicaciones. El control de acceso hace uso de la autentificación, filtrando los accesos en función de usuario, el método de autentificación utilizado, el tipo de estación y localización, e incluso, una auditoria de acceso centralizado. El acceso de la información protegida debe estar restringido a los individuos, computadores o programas autorizados para ello. Esto requiere la implementación de mecanismos de control de acceso a los datos protegidos. La sofisticación de esto mecanismos de control de acceso debe ser coherentes con valor de la información que se está protegiendo, es decir, cuando más sensible valiosa sea la información, más robustos deberán ser los mecanismos de control. Existen tres tipos existen administrativo, físico y lógico (Galindo & Gamboa, 2016)

La seguridad en todos los ámbitos es de vital importancia, en informática la seguridad hace referencia a la protección de sistemas de información aplicando controles que restrinjan el acceso no autorizado, como divulgación, supresión, ejecución de programas, modificación, lectura y creación de archivos. Para evitar estas prácticas indebidas se debe aunar una serie de controles de accesos lógicos que denieguen el acceso de sujetos no autorizados a los recursos lógicos, mediante controles de autorización, identificación, autenticación y políticas de seguridad establecidas; empleando para aquello dos metodologías los controles de acceso discrecional que son configurados

por el sujeto y los obligatorios que son definidos por el sistema. (Baca, 2016) (Gómez Vieites, 2014)

Existen algunos métodos de autenticación de usuarios entre ellos el identificador y contraseña que son los más comunes y aplicados en diferentes medios de autentificación, asimismo está el encriptado o cifrado en donde la información trasmitida solo puede ser decodificada por los sujetos que poseen permiso y las claves para hacerlo, las listas de control de acceso o ACL también son utilizados para otorgar permisos y detallar de manera más especifica que usuarios tienen permiso y acceso para realizar alguna acción, para ello se relaciona cada objeto a una lista con todos los dominios a los que pueden acceder y la forma en la que se deben realizar, en fin los controles de accesos deben realizar bien dos parámetros básicos; permitir el acceso solo a sujetos autentificados e impedir el acceso a otros. (Gómez Vieites, 2014) (Carpentier, 2016)

1.2.5.1 Control administrativo

Los controles administrativos denominados controles de procedimiento consiste en políticas, estándares y guías explícitamente aprobadas en una compañía de control administrativo componen el marco para la práctica del negocio y la gestión personal. Informan a los empleados como debe llevarse a cabo el negocio y como deben conducir las operaciones en el día a día. Las leyes y regularizaciones impuestas por el gobierno también son un tipo de control administrativo. Algunos sectores de la industria disponen de políticas, procedimiento, estándares y guías propios como estándares de seguridad de datos. (Barman, 2001)

Los controles administrativos forman la base para la selección e implementación de controles lógicos y físicos, ya que estos son la manifestación de los controles administrativos. (Baca, 2016)

1.2.5.2 Control lógico

Los controles lógicos también denominado controles técnicos utilizan software especializados y propios para monitorizar y controlar el acceso al sistema de información. Dentro de esta categoría se sitúan las contraseñas, el cortafuego de red y personales, sistemas de detección de intrusión, lista de control de acceso y la encriptación de datos. Un control lógico de gran importancia que es frecuente obviado es el principio menor privilegiado, que establece que no se debe conceder al individuo, programa o sistema más privilegiado de los estrictamente necesarios para realizar su trabajo. Un flagrante ejemplo de fallo en la aplicación de este principio menor es el acceso a Windows como el usuario administrador simplemente para leer el correo y navegar por internet. También ocurren violaciones de este principio cuando un individuo ha ganado privilegios con el tiempo. Esto ocurre cuando las tareas de un empleado cambian y se añaden los nuevos privilegios a los ya existentes, los cuales podrían no ser ya necesarios o incluso apropiados. (Barman, 2001)

1.2.5.3 Control físico

Los controles físicos monitorizan y controlan el entorno de trabajo y os recursos de computación. También monitorizan y controlan el acceso a y desde esos recursos, como por ejemplo, puertas cerraduras, calefacción y aire acondicionado, alarmas contra incendios, cámaras, barreras, guardas de seguridad, etc. Dividir la red y la zona de trabajo en áreas funcionales también es un tipo de control físico. (Carpentier, La seguridad informática en la PYME: Situación actual y mejores prácticas, 2016)

Un importante tipo de control físico no siempre ha tenido en cuenta es la separación de obligaciones, que asegura que un individuo no puede completar una tara critica por sí mismo. Un ejemplo seria que el empleado que envía una solicitud de reembolso no debería ser el mismo que aprueba el pago. Por otro lado, un programador de aplicaciones no debería ser también el administrador de servidores o de base de datos. (Costas, 2014)

1.2.6 Mecanismo del control de acceso

Fundamento con el que se construyen os mecanismos de control de acceso comienza con la identificación y la autentificación. La identificación es la certificación de quien es algo o alguien. Si una persona hace declaración, está haciendo una afirmación de quien es. Sin embargo, esa afirmación puede sr o no cierta. Antes de que obtenga el acceso a información protegida será necesario verificar que esa persona que afirma sea efectivamente. (Ferraiolo, Kuhn, & Chandramouli, 2003)

Los sistemas de información utilizados en la actualidad en la actualidad, el nombre de usuario es la forma más habitual de identificación y la contraseña de la forma más habitual de autentificación. Las parejas de nombre de usuarios más contraseña han cumplido su propósito, pero poco a poco se van sustituyendo por mecanismos de autentificación más sofisticados (Galindo & Gamboa, 2016)

La autentificación es la acción de verificar la afirmación de la identidad. Cuando, le indican su nombre a la persona que le atiende o realiza una afirmación de su identidad. Ese empleado del banco solicita ver una identificación con foto, por lo que ella o el entrega su permiso de conducir. El empleado chequea el permiso para verificar el nombre y comparar la foto con la persona que se la ha entregado. (Ferraiolo, Kuhn, & Chandramouli, 2003)

1.2.7 Creación de políticas viables

La clave para asegurar que las políticas de la compañía es útil y utilizable es desarrollar una suite de documentos que recojan la política, enfocados al público objetivo y que casen con las políticas de operación existentes. (Carpentier, 2016)

Las políticas deben ser utilizables, viables y realistas. Para lograr es imprescindible involucrar y conseguir el apoyo por parte de los principales integrantes del equipo que desarrolla la política así como de aquellos que tendrán que utilizar las políticas como parte de su trabajo diario. De cara a

conseguir esto, un factor fundamental consiste en transmitir la importancia y la utilidad de las políticas a aquellas que tienen que convivir con ellas. A menudo, el usuario tiende a pensar que la política de seguridad es un estorbo para su trabajo diario. Un elemento muy importante para el desarrollo de la política para asegurar que será puesta en práctica y no rechazada es comunicar el mensaje de que las políticas resultan de gran utilidad para los usuarios a largo plazo, ya que proporcionan un marco seguro de buenas prácticas que aseguran el cumplimiento de los requerimientos. (Carpentier, 2016)

Una vez que los usuarios entienden que las políticas de seguridad es algo que les puede ayudar a realizar su trabajo de forma más eficaz y eficiente, serán muchos más receptivos tanto a colaborar en su desarrollo como a garantizar su cumplimiento. De forma similar, una vez que la alta dirección se hace cargo de que la política de seguridad es una herramienta que pueden emplear para garantizar la adherencia los requerimientos legales y para impulsar nuevas iniciativas empresariales, también se vuelven más partidarios de dar su apoyo términos de inversiones financieras. (Carpentier, La seguridad informática en la PYME: Situación actual y mejores prácticas, 2016)

1.2.8 Tipos de políticas de seguridad

En las grandes compañías existen distintos tipos de público para las políticas de seguridad, y se cubren distintos aspectos a distintos niveles. Por esta razón, en un entorno empresarial grande es necesario un conjunto de documentos que recojan las políticas de seguridad, y se constituye utilizando dos tipos de política, apoyados en documentos procedimentales, para cubrir todos los aspectos a todos los niveles de público. (Carpentier, La seguridad informática en la PYME: Situación actual y mejores prácticas, 2016)

Para compañías u organizaciones más pequeñas o para aquellas que están iniciando el desarrollo de una política de seguridad, es posible utilizar este marco de trabajo, pero únicamente con pequeños números de políticas de seguridad, e incluso, sin guía de usuario en las primeras fases del proceso. Antes que intentar desarrollar una gran jerarquía desde el primer momento, es más realista comenzar con el desarrollar una política de gobierno y un pequeño

número de políticas técnicas, para después ir incrementando su número y los documentos que lo apoyan. (Baca, 2016)

1.2.8.1 Políticas de gobierno

Políticas de gobierno debe cubrir un concertó de seguridad de la información a alto nivel, definir esos conceptos y describir la razón de su importancia. La política de gobierno está dirigida a directivos y usuarios finales, por tanto, también es leída por personal técnico, ya que también son usuarios finales. Todos grupos utilizan la política para hacerse una idea de cuál es la filosofía sobre seguridad de la información de la compañía. (Chicano, 2015)

La políticas de gobierno debe estar fuertemente alineada con las políticas de recursos humanos y otras políticas existentes futuras de la compañía, especialmente las relacionadas con aspectos e seguridad, como el uso del correo electrónico o el acceso a salas ordenadores. El documento que recoge la política de gobierno debe estar al mismo nivel que estas otras políticas de la compañía. (Carpentier, La seguridad informática en la PYME: Situación actual y mejores prácticas, 2016)

Esta política de gobierno se apoya en una serie de políticas técnicas que cubren los mismos aspectos pero de forma más detallada y técnica. En términos de nivel de detalle, la política de gobierno debe definir el que de las políticas de seguridad. (Gómez Vieites, 2014)

1.2.8.2 Políticas técnicas

Son utilizadas por el personal del departamento de sistemas y comunicación para llevar a cabo sus responsabilidades. Son políticas más detalladas que las políticas de gobierno y son específicas para un sistema o aspecto concreto, por ejemplo, política para AS-300 o política de seguridad técnica de nivel físico. (Barman, 2001)

Las políticas cubren muchos de los aspectos de las políticas de gobierno, así como otros conceptos adicionales específicos para una tecnología concreta. Son el manual de como un sistema operativo o un dispositivo de red deben ser

securizados. Describen que debe ser realizado, pero no como debe ser realizado. En términos de nivel de detalle, una política técnica debe expresar el "que" en mayor detalle y también el "cuando" y "donde" de las políticas de seguridad. (Baca, 2016)

1.2.8.3 Documentos procedimentales o guías de usuario

La documentación procedimental o Guías de Usuarios proporcionan directivas paso a paso sobre cómo llevar a cabo los enunciados de la política de seguridad. Por ejemplo una guía para reforzar un servidor Windows puede ser uno de los documentos en los que se apoya la política técnica de sistemas Windows. Los procedimientos y guías son adjuntos a las políticas y por eso constituyen el siguiente grado de granularidad, describiendo "como" algo debe ser ejecutado proporcionado información práctica y sistemática de la política de seguridad, para facilitar a los lectores su comprensión con explicaciones (Carpentier, La seguridad informática en la PYME: Situación actual y mejores prácticas, 2016)

CAPÍTULO II

2 DIAGNÓSTICO

2.1 Tipos de investigación

2.1.1 Descriptiva

La investigación descriptiva es fundamentar teóricamente información; donde se explica gradualmente el fenómeno del estudio, detallando características y que induzcan a un mejor entendimiento del objeto de estudio, representándolo de manera figurada por partes mediante clase o categoría destacando los aspectos más distintivos y a su vez identificando hechos y situaciones del fenómeno, para luego diseñar modelos o prototipos que den solución al problema. Las técnicas utilizadas para describir la situación del estudio son por lo general la entrevista, encuestas, la observación entre otras. (Bernal, 2006) (Naghi, 2000)

El presente estudio es de tipo descriptivo, en el que se narra información de los hechos y situaciones que presentan las variables independiente y dependiente, donde la independiente manifestará en gran parte los resultados de la auditoría informática y la dependiente representará las políticas, controles y procedimientos que se necesitan para probar un resultado; información que servirá para fundamentar científicamente las particularidades presentadas en el caso de estudio, apoyándose en técnicas indagatorias para figurar de forma numérica los resultados obtenidos de cada concepto de estudio.

2.1.2 Exploratoria

Para Naghi (2000), la investigación exploratoria es captar una perspectiva general del problema. Mediante herramientas que ayuden a fragmentar el objeto de estudio en varias partes para entender de manera más concisa el problema y poder formular buenos criterios y a su vez desarrollar varias hipótesis acordes a la investigación. Este tipo de investigación se utiliza para fundamentar el proceso de estudio de manera observacional, basada en herramientas que permitan detallar información para dar a conocer la situación del objeto de estudio y a su vez para el desarrollo de hipótesis.

En la presente investigación se aplicó la metodología exploratoria la cual se empleó en el sondeo previo sobre las políticas de seguridad que tiene como finalidad sentar las bases y lineamientos generales sobre la seguridad.

2.1.3 Bibliográfica

La investigación bibliográfica es la que permite fundamentar teóricamente información mediante la búsqueda de un tema en libros o artículos obtenidos de fuentes o investigaciones originales, de la cual se pueden o no derivar nuevas inquietudes que serán indagadas en nuevas fuentes de información. (Borda, 2013). Se utilizó la presente investigación para guiarnos de fuentes confiables y libros sobre la auditoría informática y la seguridad lógica, temas a investigar mediante fuentes bibliográficas, los cuales permiten buscar información relevante y confiable.

2.2 Métodos

2.2.1 Analítico – Sintético

“Estudia los hechos, partiendo de la descomposición del objeto de estudio en cada una de sus partes para estudiarlas en forma individual (análisis), y luego se integran dichas partes para estudiarlas de manera holística e integral (síntesis).” (Bernal Torres, 2006). Método de ayuda para realizar la descomposición la auditoría informática y seguridad lógica, objetos de estudio del capítulo 1 para analizarla y sintetizarla en base a la información investigada en los diferentes libros, destacando información relevante de cada variable del objeto de estudio.

2.2.2 Inductivo – Deductivo

Método de inferencia basado en la lógica y relacionado con el estudio de hechos particulares, obteniendo conclusiones de lo más específico a lo general de hechos observados(inductivo) y de lo general hacia lo más específico, basándose en hechos observados en leyes o reglas generales(deductivo). (Ibáñez, 2015). Este método es implementado en el capítulo 2 para llevar a cabo las inferencias relacionadas al estudio de la auditoría informática.

2.3 Técnicas e instrumentos

2.3.1 Cuestionario

Es el principal instrumento de recogida de datos dentro de las técnicas de encuesta, impresas o virtuales que el consultado llena por sí mismo. (Mendoza, 2014). Un instrumento que permite recoger información de manera más amplia, mediante ciertas preguntas que ayuden a solventar dudas mediante varias opiniones referentes al tema de estudio Auditoría informática de seguridad lógica para información de docentes “Universidad Laica Eloy Alfaro de Manabí” Ingeniería en Sistemas.

2.3.2 Encuesta

Es una metodología que utiliza un conjunto de procedimiento estandarizados de investigación mediante las cuales se recogen y analizan una serie de datos de una muestra de casos representativos de una población, considerando las respuestas de los sujetos de estudio. (Aquiahuatl, 2015). Técnica que permite encuestar a un grupo de persona en este caso se aplicó a los docentes de la carrera de Ingeniería en Sistemas base al tema de estudio, con el cual se fundamentará de manera inductiva los resultados.

2.3.3 Entrevista

Es una conversación que se sostiene con un propósito definido y no por sentir satisfacción de conversar, se realiza con el propósito definido y se dirige en un área determinada. (Figueroa, 2002)

2.4 Población y Muestra

Es un conjunto de individuos, objetos o medidas que poseen características comunes observables en un lugar o un momento determinado. La población que servirá como base en este proyecto está conformada por 20 docentes de la ULEAM carrera Ingeniería en Sistemas. Para el control de acceso.

Es un subconjunto fielmente representativo de la población, hay diferentes tipos de muestreo y según del tipo que se seleccione dependerá la calidad, en la presente documentación no se aplicará el muestreo ya que nuestra población es mínima y se utilizará toda la población

Este instrumento se aplicó al encargado de informática de la Universidad para tener un mejor conocimiento sobre las políticas de seguridad de la información.

2.5 Entrevista

1. **¿La Universidad tiene políticas de seguridad de la información?**

   En la institución si existen políticas de seguridad pero a nivel de Universidad

2. **¿Por qué medios a socializado las políticas de seguridad de la información?**

   Cualquier tipo de información se lo realiza por medio del correo electrónico en este caso las políticas de seguridad de la información se las comunica por el mismo medio desde la matriz.

3. **¿Cuáles son los mecanismos que se utilizan en la institución para evaluar el cumplimiento de las políticas de seguridad de la información?**

   Hasta el momento no tiene conocimiento de que exista algún tipo de mecanismo para verificar si se cumple las políticas de seguridad de la información.

4. **¿En la institución se ha socializado las políticas de seguridad de la información con los docentes?**

   No se ha realizado ningún tipo de socialización de políticas en la institución.

5. **¿Cuáles son los problemas más frecuentes que los docentes saben tener y porque se producen?**

   Los problemas más frecuentes son la perdida de contraseñas debido a varios sistemas.

6. **¿Cuándo los docentes tienen dificultad del envío de información acuden a Ud.?**

   Cuando no es un problema complicado lo realizan por sí mismo y cuando ya es más complejo o los docentes no tienen conocimiento del tema acuden al encargado de informática.

7. **¿Cuáles son las recomendaciones que Ud. da a los docentes que al compartir información ésta sea segura?**

   Que los docentes realicen por medio de la plataforma office365 que es una plataforma oficial y tiene bastante espacio de almacenamiento y es la que utiliza la universidad.

8. **Dentro de la Universidad se utiliza el correo institucional, personal y grupos de trabajo a su criterio cual sería el más recomendable para compartir información sea segura y no exista fugas y no sea utilizada por terceros.**

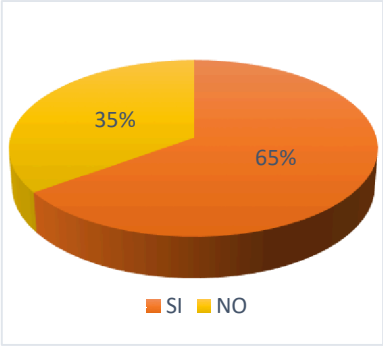
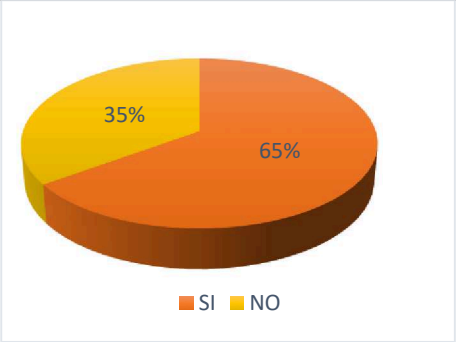
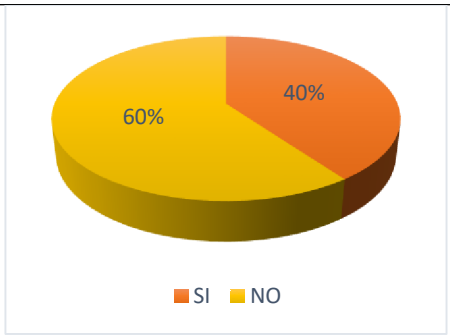
   El medio más recomendable para compartir información recomienda que es el correo institucional siempre y cuando tenga las debidas precauciones al compartir información.

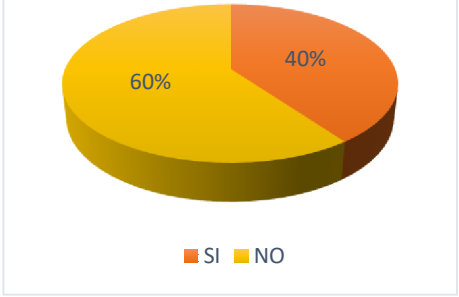
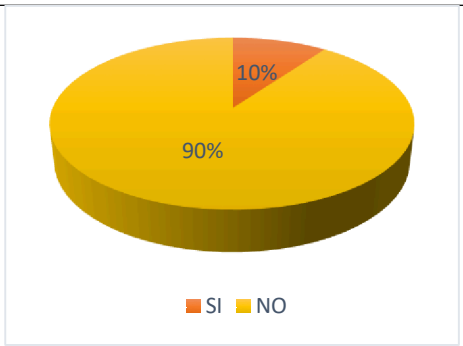
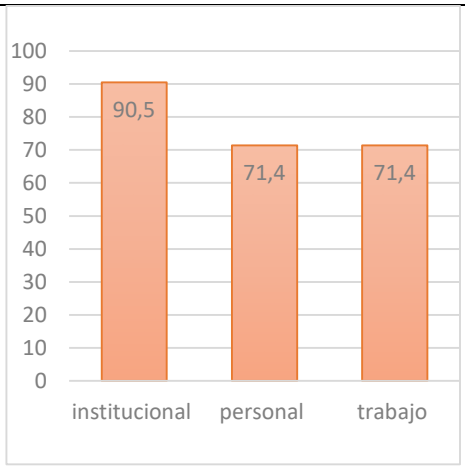
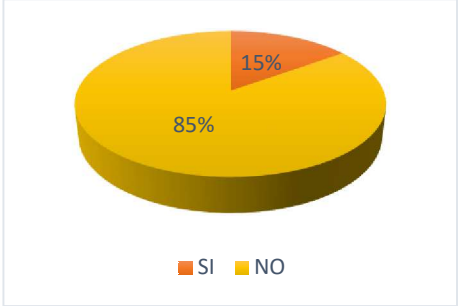
Interpretación de la entrevista.

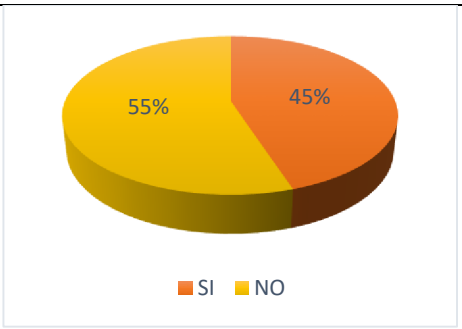
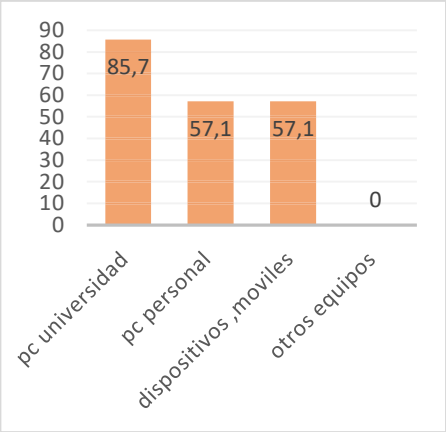
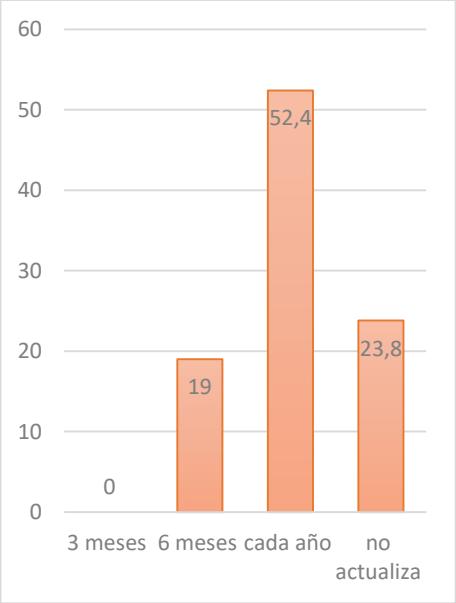
Al analizar las respuestas obtenidas mediante la entrevista al Ing. Wladimir Mora sobre el acceso remoto a datos, se puede argumentar que; de acuerdo a los resultados obtenidos en la pregunta 3 no se tiene conocimiento de que exista algún tipo de mecanismo para verificar si se cumplen las políticas de seguridad de la información, además en la pregunta 4 se manifiesta que no se han socializado las políticas de la universidad a los docentes lo que conlleva a que en la pregunta 5 se describa que existen pérdidas de contraseñas sobre todo causados por el mal uso de los sistema, para evitar inconvenientes en la pérdida de información en la pregunta 7 se recomienda utilizar office365 debido a que es una plataforma oficial y tiene suficiente espacio de almacenamiento; mediante el correo institucional de acuerdo a la recomendación establecida en la pregunta 8.

2.5.1 Encuesta a docentes

Esta encuesta fue dirigida a los docentes de la carrera de ingeniería en sistemas de la Universidad Laica “Eloy Alfaro” de Manabí Extensión El Carmen, con el objetivo de recaudar información sobre los cumplimientos de las normativas en el almacenamiento de documentos en línea.

Preguntas	Gráficas	Análisis
1. ¿Conoce ud sobre políticas de seguridad de la información digital?		Más de la mitad de los docentes manifiestan tener conocimientos de las políticas de seguridad digital sin embargo no en su totalidad
2. ¿Tiene conocimiento de las políticas de seguridad de la información?		Más de la mitad de los docentes que se aplicó la encuesta manifiestan conocer sobre las políticas de seguridad de la información.
3. ¿Conoce ud si la Universidad tiene establecidas políticas de seguridad para el manejo de información digital?		La mayoría de docentes de la institución desconocen que se establece políticas de seguridad para el manejo de la información.

Preguntas	Gráficas	Análisis
4. ¿La institución le ha dado a conocer las políticas de seguridad de la información?		En su totalidad (60%) los docentes mencionan que no conocen las políticas de la institución sin embargo con un mínimo (40%) de docentes dicen conocer.
5. ¿Ha recibido capacitaciones sobre cómo mantener segura la información?		Todos los docentes encuestados mencionan no haber recibido capacitaciones de como tener segura la información.
6. ¿Por qué medio ud comparte la información laboral?		La mayor parte de los docentes de la universidad mencionan que comparten la información por medio de correo institucional y correo personal casi la mitad utilizan grupos de trabajo medios tradicionales.
7. Existe en la institución controles para verificar si se cumplen las políticas de seguridad de la información?		La mayor parte de los docentes desconocen que re realice un monitoreo de políticas, con un mínimo que si conocen que exista este control

Preguntas	Gráficas	Análisis
8. ¿Ud toma precauciones de seguridad al momento de compartir información institucional?		La mayoría de los docentes encuestados mencionan tomar precauciones cuando comparten información con otras personas.
9. Para realizar su trabajo utiliza:		La mayoría de profesores realizan sus trabajos en la pc de la universidad así como en sus pc personal, mientras que otra parte utilizan los dispositivos móviles, una menor parte realizan en otros equipos.
10. ¿Con que frecuencia cambia su contraseña de acceso a plataforma de la institución?		La mayoría de profesores realizan sus cambios en un tiempo de 6 meses a 1 año y casi la mitad no actualiza. .

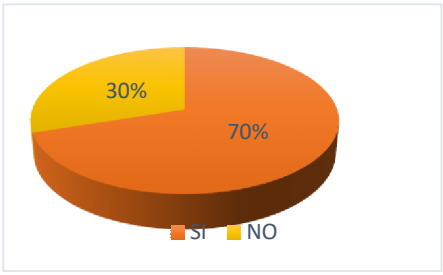
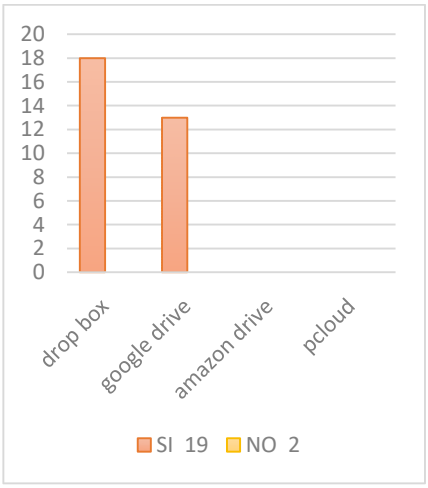
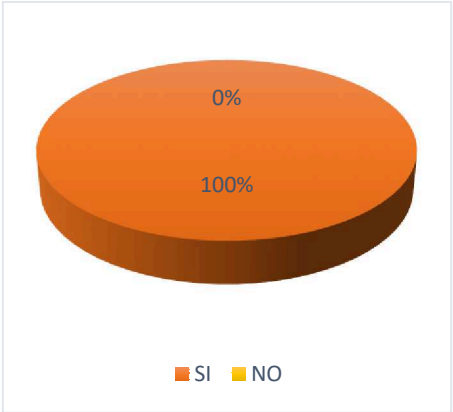
Preguntas	Gráficas	Análisis
11. ¿Utiliza algún antivirus en su ordenador?		La mayoría de docentes dicen tener un antivirus en su ordenador (70%) y con un mínimo mencionan no utilizarlo (30%)
12. ¿Utiliza algún servicio de alojamiento de archivos con acceso compartido?		La mayor parte de docentes si utilizan contraseñas y usuarios exclusivos en su correo y Dropbox, casi la mitad utilizan exclusivo en google drive excluyendo a amazon drive y iCloud
13. ¿Considera usted que es importante conocer las políticas de seguridad de la información?		En su totalidad los docentes consideran que es importante conocer las políticas de seguridad de la información.

Tabla 1 Resultados de las encuestas

Interpretación de la encuesta.

Se puede observar de acuerdo a la encuesta realizada a los docentes de la ULEAM, que según lo que se describe en la pregunta 3 en su mayoría desconocen que existan políticas para la seguridad de la información, esto se debe a que tampoco conocen que existan políticas que se deben cumplir

dentro de la institución según lo que se detalla en la pregunta 4, todo esto se da porque los docentes no han sido capacitados sobre el uso y existencia de las políticas institucionales según se menciona en la pregunta 5, se menciona además en la pregunta 7 que no existe un control en el cumplimiento de dichas políticas.

2.6 Análisis de Resultados

Considerando los resultados de los instrumentos utilizados podemos dar a conocer que los docentes desconocen que en la Universidad haya políticas de seguridad de la información, en su totalidad los docentes mencionan que la institución no les ha dado a conocer las políticas y tampoco se les ha realizado capacitaciones para mantener segura la información.

Por su parte el encargado de informática menciona que la institución si tiene políticas de seguridad pero a nivel de universidad y que las políticas se a compartido por medio de correo electrónico, por ellos se considera importantes realizar una mayor difusión para que todos conozcan de las políticas de seguridad de la información que existen en la universidad y éstas sean aplicadas y así tener mayor seguridad al compartir información.

En la pregunta 1 de la entrevista el encargado del área de informática afirma que en la Universidad si existen políticas de seguridad, pero en la pregunta 3 de la encuesta a los docentes, gran parte de ellos mencionan que son desconocidas, de la misma manera se menciona tanto en la pregunta 4 de la entrevista como en la pregunta 4 de la encuesta que en la institución no se realizado ninguna clase de socialización de las políticas de seguridad, aunque algunos docentes la han conocido por sus propios medios, demostrando estos resultados, se tiene el riesgo de pérdida de información por falta de conocimiento de las políticas y de cómo mantener seguro los datos, por último en la pregunta 8 de la entrevista, el encargado del área de informática recomienda que la mejor manera de compartir la información es mediante el correo institucional, una respuesta positiva que dan los docentes en la pregunta 6 de la encuesta, ya que mencionan que la mayor parte de los trabajos la comparten por el medio mencionado.

CAPÍTULO III

3 PROPUESTA

3.1 Antecedentes

El 10 de junio de 1986, el Comité de Gestión para la creación de esta Unidad Académica, el cual estuvo conformado por el Sr. Gilberto Farfán Espinoza, Dr. Jorge Garzón Delgado, Sr. Ever Barberán Vera, Prof. Ariolfo Cuadros, Sr. Benigno Andrade Falcones, Sr. Ernesto García Espinoza y Sr. Walter López Candela, viajó a la ciudad de Manta para sostener un diálogo con el Señor Dr. Medardo Mora Solórzano, Rector de la Universidad Laica “Eloy Alfaro” de Manabí, a fin de solicitarle la creación de un centro de estudios superiores en El Carmen. El Dr. Mora manifestó que realizaría un estudio de la Ley de Universidades y en base a aquello determinaría la posibilidad de atender el pedido. En marzo de 1987, el Sr. Rector acompañado entre otras personas por el Ing. José Emilio Muñoz Galarraga, Director del Departamento de Planeamiento de la Universidad, visitó este cantón. Sostuvo una reunión con las fuerzas vivas de El Carmen.

El Dr. Mora se comprometió realizar el mejor de los esfuerzos para darle a este cantón un Centro Universitario; así, le encargó en ese mismo momento al Director de Planeamiento que iniciara el estudio necesario para el efecto.

El 12 de marzo de 1988, el Ing. José Emilio Muñoz Galarraga, comunicó al Comité de Gestión que la creación del Centro Universitario de Estudios a Distancia de El Carmen es un hecho, y que se abrirá con tres carreras: Tecnología Agropecuaria, Tecnología en Administración Rural y Licenciatura en Educación Primaria.

En ese mismo mes y año, el Señor Rector invitó al Comité para dar lectura al Proyecto de Creación del Centro de Estudios a Distancia de El Carmen. Posteriormente, se lo puso a consideración del Honorable Consejo Universitario; este organismo resolvió su aprobación. El Ing. Emilio Muñoz Galarraga fue designado como Director, el Sr. Kléver Soledispa Toala,

Coordinador en Manta y el Lic. Guido Vásconez González, Coordinador en El Carmen.

El 4 de julio del 1988 el Sr. Rector inauguró oficialmente el Centro Universitario de Estudios a Distancia. El 9 de julio del mismo año iniciaron formalmente las actividades académicas. El personal docente estuvo integrado por: Ing. José Robles García, Ing. Víctor Román Posligua, Dr. Auter Cuenca Ramón, Dr. Miguel Santana Chávez, Dr. Oliver Vera Paz, Lic. Iván Medranda Saltos, Lic. Milton Utreras y el Lic. Stalín Morejón. Fue designada como Secretaria-Tesorera la Lic. Patricia Salvatierra y, posteriormente, el Sr. Nery Ramón Figueroa, como Auxiliar de servicios.

El lugar donde se laboró inicialmente fue en el Colegio Nacional Mixto El Carmen.

EL 13 enero 1994, por gestión del Dr. Medardo Mora Solórzano, Rector, el CONESUP entregó a esta Institución de Estudios Superiores de El Carmen, la calidad de Extensión Universitaria, facultando expresamente la modalidad presencial. (http://carreras.uleam.edu.ec/elcarmen/resena-historica-2/)

3.1.1 Misión

La Universidad Laica “Eloy Alfaro” de Manabí Extensión en El Carmen es una institución de educación superior cuyo compromiso es formar ciudadanos y ciudadanas profesionales responsables, éticos y solidarios con la sociedad; capaces de generar y aplicar sus conocimientos y estrategias que contribuyan al desarrollo sustentable y al mejoramiento de las condiciones de vida de los y las habitantes de El Carmen y Manabí.

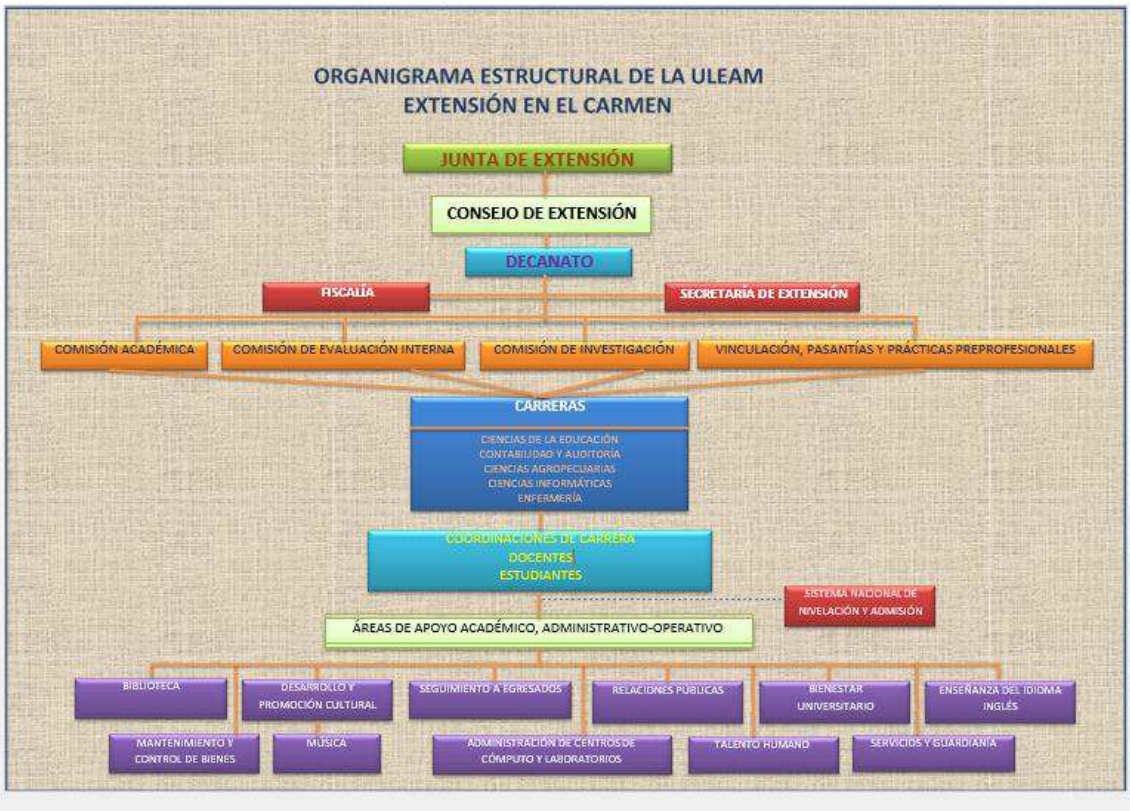
3.1.2 Visión

La Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen es una institución de educación superior moderna y líder en el ámbito de su actividad académica-científica y formativa de ciudadanos profesionales, quienes participan, colaboran, promueven y se comprometen con el desarrollo sustentable y el mejoramiento de las condiciones de vida de los y las habitantes de El Carmen y Manabí.

(http://carreras.uleam.edu.ec/elcarmen/mision-y-vision/)

3.1.3 Organigrama

(http://carreras.uleam.edu.ec/elcarmen/wp-content/uploads/sites/47/2016/06/ORGANIGRAMA-ESTRUCTURAL-DE-LA-ULEAM-EXT.-EN-EL-CARMEN.pdf)



3.2 Programa de auditoría

Programa de Auditoría al cumplimiento de políticas de seguridad de la información en las comisiones de la Universidad Laica Eloy Alfaro de Manabí Extensión en El Carmen		
OBJETIVO: Verificar el cumplimiento de políticas de seguridad de la información a los profesores del área de Ingeniería en Sistemas.		
TÉCNICAS Y PROCEDIMIENTOS	**REFERENCIA**	**FECHA**
1. Seleccionar normas de seguridad de la información	PT1	28-05-2019
2. Obtener el manual de políticas de seguridad	PT2	04-06-2019
3. Elaborar un instrumento para recolección de información	PT3	05 al 11-06 2019
4. Entrevista a docentes de la carrera de Ingeniería en Sistemas	PT4	12 al 18-06- 2019
5. Tabulación y acceso a datos	PT5	19 al 25-06- 2019
6. Análisis de resultados	PT6	09 al 16 -07- 2019
7. Elaboración de informe	PT7	24 al 30-07- 2019

Tabla 2 Programa de auditoría

AUDITORÍA INFORMÁTICA DE SEGURIDAD LÓGICA PARA INFORMACIÓN DE DOCENTES "UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ" INGENIERÍA EN SISTEMAS

Realizado por: Anthony Aldair Ávila Cevallos

Instituciones Particulares: 1

Instituciones evaluadas: 1

Docentes relacionados: 20

El Carmen, agosto 2019

3.3 Informe de auditoría

En el presente informe nos da a conocer los resultados de la auditoría informática en el cumplimiento de las políticas de seguridad de la información la cual fue aplicada a los docentes de la carrera de Ingeniería en Sistemas Universidad Laica “Eloy Alfaro” de Manabí Extensión el Carmen especificando el cumplimiento de las normas y medidas que tienen cada docente para prevenir los riesgos que podrían afectar a la información.

3.3.1 Objetivo

Verificar el cumplimiento de las políticas de seguridad de la información a los profesores del área de ingeniería en Sistemas

3.3.2 Personal relacionado

En la presente auditoria se contó con la disponibilidad de los docentes de la carrera ingeniería en sistemas de la Universidad Laica Eloy Alfaro de Manabí

3.4 Alcance

El presente trabajo es el resultado de una evaluación realizada a los docentes de la carrera de la ingeniería en sistemas con la finalidad de evaluar el cumplimiento de las políticas de seguridad en el control de acceso a la información de cada docente.

Para ello se analizaron las normas ISO estas normas son conjuntos orientadas a ordenar la gestión en sus distintos ámbitos. Las normas ISO son establecidas por el Organismo Internacional de Estandarización (ISO) que se componen con estándares de guías relacionados con sistemas y herramientas específicas de gestión para aplicarla en cualquier tipo de investigación además se revisó las guías de las políticas de la universidad que las encontramos en la página oficial de la universidad Laica “Eloy Alfaro” de Manabí que de distribuye en políticas institucionales de 7 secciones en bases a esas normas y políticas se elaboró el instrumento en el cual se reflejan en el cual fue desglosado en 5 bloques en el cual se distribuye en 46 preguntas sobre el uso de contraseña en preguntas de respaldo de la información distribuidas en 28 preguntas sobre el acceso del sistema operativo que se distribuye en 8 preguntas y por el uso del correo electrónico 10 preguntas

Una vez realizado el cuestionario se procedió a realizar una entrevista personalizada con cada uno de los docentes de ingeniería en sistemas para obtener sus respuestas en función del cumplimiento de las políticas de seguridad de acceso a la información.

Una vez realizado el cuestionario se procedió a realizar una entrevista personalizada a cada uno de los miembros docentes de la carrera de ingeniería en sistemas para obtener sus respuestas en función al cumplimiento de las políticas

Se procedió a una codificación de los instrumentos para un fácil registro esto nos permitirá a realizar una auditoría al proceso de tabulación de los datos la codificación fue de la siguiente manera se le asignó un código de letra P1 a P20 a cada uno de los docentes sin tomar en cuenta sus respectivos nombres.

CÓDIGOS	
P1	Profesor sistemas 1
P2	Profesor sistemas 2
P3	Profesor sistemas 3
P4	Profesor sistemas 4
P5	Profesor sistemas 5
P6	Profesor sistemas 6
P7	Profesor sistemas 7
P8	Profesor sistemas 8
P9	Profesor sistemas 9
P10	Profesor sistemas 10
P11	Profesor sistemas 11
P12	Profesor sistemas 12
P13	Profesor sistemas 13
P14	Profesor sistemas 14
P15	Profesor sistemas 15
P16	Profesor sistemas 16
P17	Profesor sistemas 17
P18	Profesor sistemas 18
P19	Profesor sistemas 19
P20	Profesor sistemas 20

Tabla 3 Código de asignación de docentes

Nº	PREGUNTA	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	lica cor	lica co
	ACCESO AL AULA VIRTUAL																						
1	¿Usted recibió su usuario y contraseña vía correo para el ingreso del aula virtual?	0	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1	0	1	1	1	16	4
2	¿Ha cambiado su contraseña de acceso del aula virtual?	1	1	1	1	0	1	1	1	1	1	1	1	0	1	0	1	1	1	1	0	16	4
3	¿Su contraseña tiene más de 8 caracteres?*	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	1	1	1	1	0	17	3
4	¿Su contraseña contiene letras, números y caracteres?	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	20	0
5	¿Usted ha compartido su contraseña con otros usuarios?*	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	20
6	¿En su computadora Ud. mantiene abierta la sesión de la cuenta del aula virtual?	1	0	0	0	1	0	0	0	0	0	0	0	1	1	1	0	1	0	1	1	8	12
7	¿Usted actualiza su contraseña con frecuencia?	0	1	0	0	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	4	16
8	¿Conoce Ud. el límite de intentos para ingresar el usuario y contraseña?*	1	0	0	0	1	0	0	0	0	0	1	0	1	0	0	0	1	0	0	0	5	15
9	¿Usted acostumbra a guardar su usuario y contraseña en su computadora?	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	1	1	1	0	6	14
10	¿Realiza usted registros de sus contraseñas (papel, archivos)? *	1	0	1	1	1	0	1	1	0	0	0	1	1	1	0	1	0	0	1	0	11	9
11	¿Usted ingresa al aula virtual a través de su celular?	0	1	0	1	0	1	0	1	1	1	0	0	0	0	1	0	1	1	0	1	10	10
12	¿Usted ingresa al aula virtual desde su computadora personal?	1	1	1	1	0	1	1	1	1	1	1	1	0	1	1	1	0	1	1	1	17	3
13	¿Usted ingresa al aula virtual en computadoras fuera de la institución?	0	1	1	0	1	1	1	0	1	1	1	0	0	1	1	0	0	1	1	1	13	7
14	¿Usted ha olvidado su contraseña para acceder a la plataforma?	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	2	18
15	¿Recuperó con facilidad su contraseña de acceso al aula virtual?	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	20
	ACCESO DE CORREO IINSTITUCIONAL																						
16	¿Usted tiene una cuenta de correo institucional?	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	20	0
17	¿Ha cambiado su contraseña de acceso del correo?	1	1	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	18	2
18	¿Su contraseña tiene más de 8 caracteres?	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	19	1
19	¿Su contraseña contiene letras, números y caracteres?	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	20	0
22	¿Cuándo recibió su usuario y contraseña realizó el respectivo cambio?	1	1	1	1	1	1	1	1	1	0	1	1	0	1	1	1	1	1	1	1	18	2
23	¿Usted ha compartido su contraseña con otros usuarios?	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	20
24	¿En su computadora Ud. Mantiene abierta la sesión del correo institucional?	1	0	0	1	1	0	0	1	1	0	0	0	1	0	1	0	1	1	0	1	10	10
25	¿Usted Actualiza con frecuencia su contraseña?	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	2	18

Tabla 4 Tabulación de cumplimiento de políticas

Para la tabulación de los datos se realizó una matriz en Excel para lo cual se procedió a realizar una codificación de los instrumentos aplicados con un código y un nombre, y también se llenó asignando 1 y 0 tomando en cuenta que 1 significa que si existe un control y se cumple con las políticas y 0 para aquellas respuestas que no existe un control que no cumplen con las políticas y son perjudiciales para la seguridad de la información

No existe control o no se cumple las políticas	0		
Si se aplica la política contiene un control	1		

Tabla 5 Código de cumplimiento de políticas

Si se cumplen del 81% al 100% de las políticas de seguridad el porcentaje de riesgo de una usurpación de identidad o el uso no permitido de la información es bajo, en cambio si este rango se encuentra entre el 61% al 80% el riesgo es medio, por lo contrario si disminuye del 41% al 60% el riesgo que presenta es moderado, si se presenta del 21% al 40% el riesgo es alto y entre el 0% al 20% el riesgo es extremo. Se encontró que existen una relación inversamente proporcional entre el cumplimiento de las políticas y el riesgo que presentan.

Cumplimiento de políticas	**Porcentaje de riesgo**
81% a 100%	bajo
61% a 80%	medio
41% a 60%	moderado
21% a 40%	alto
0% a 20%	extremo

Tabla 6 Niveles de riesgo

Cumplimiento de políticas	**Porcentaje de Seguridad**
81% a 100%	Alto
61% a 80%	Medio Alto
41% a 60%	Medio Bajo
21% a 40%	Bajo
0% a 20%	Muy bajo

Tabla 7 Nivel de seguridad

3.5 Hallazgos

Al realizar la evaluación del cumplimiento de políticas de seguridad de la información a los docentes de la carrera de ingeniería en sistemas de la Extensión se pudo encontrar lo siguiente:

3.5.1 Cumplimiento general de políticas de seguridad

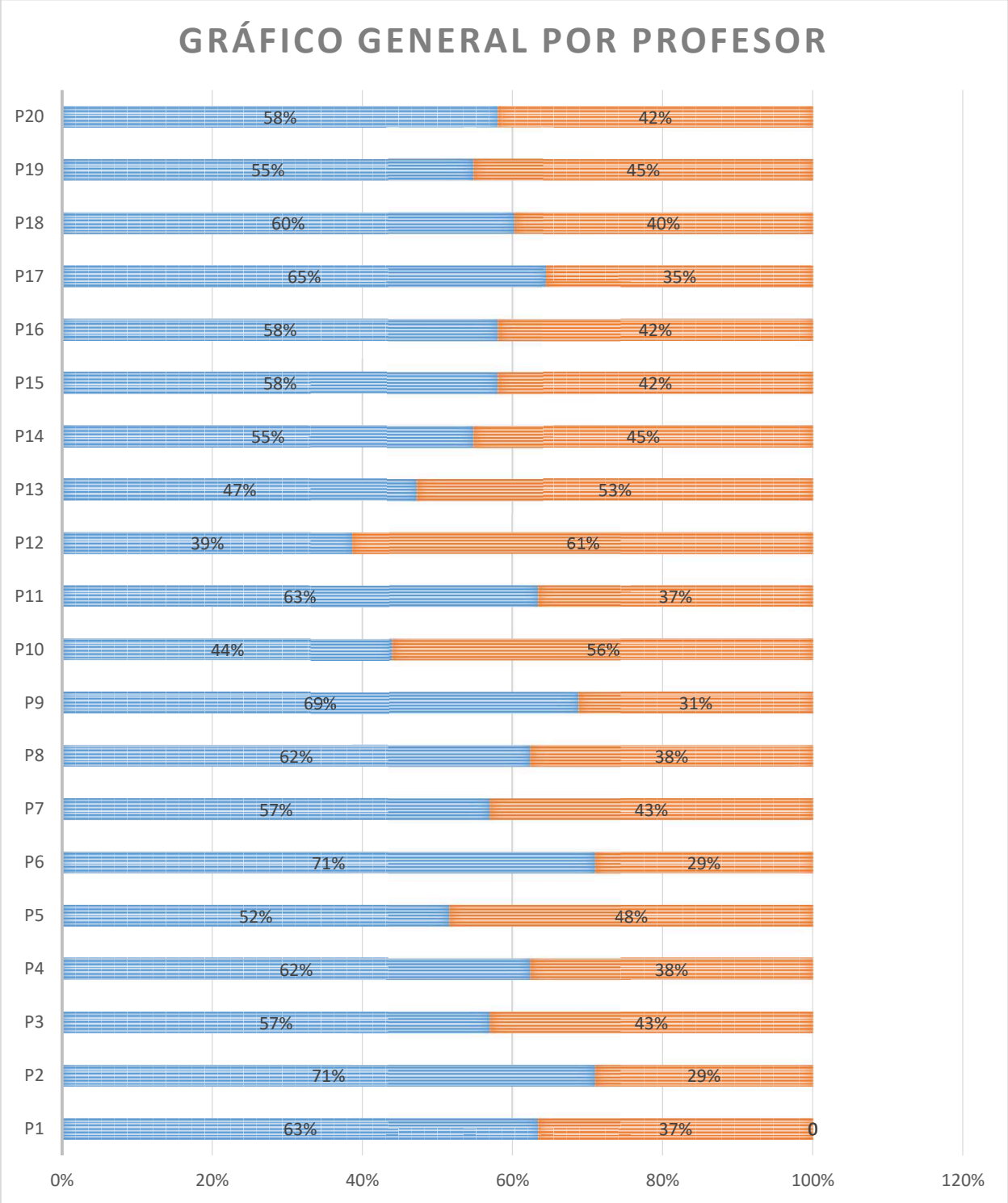


Ilustración 2 Resultado general por cada docente

Ilustración 3 Grafico general de los docentes

El promedio del cumplimiento de políticas de seguridades de los docentes de la carrera de ingeniería en sistemas es del 58% la mayoría de docentes cumple las políticas de seguridad en un rango cercano al promedio entre 41 y 60 %, siendo esto un nivel de seguridad medio bajo, lo que significa que existe riesgo de seguridad de la información moderado cabe destacar que un cuarenta y dos por ciento de las políticas no se cumplen.

3.5.2 Políticas de aula virtual

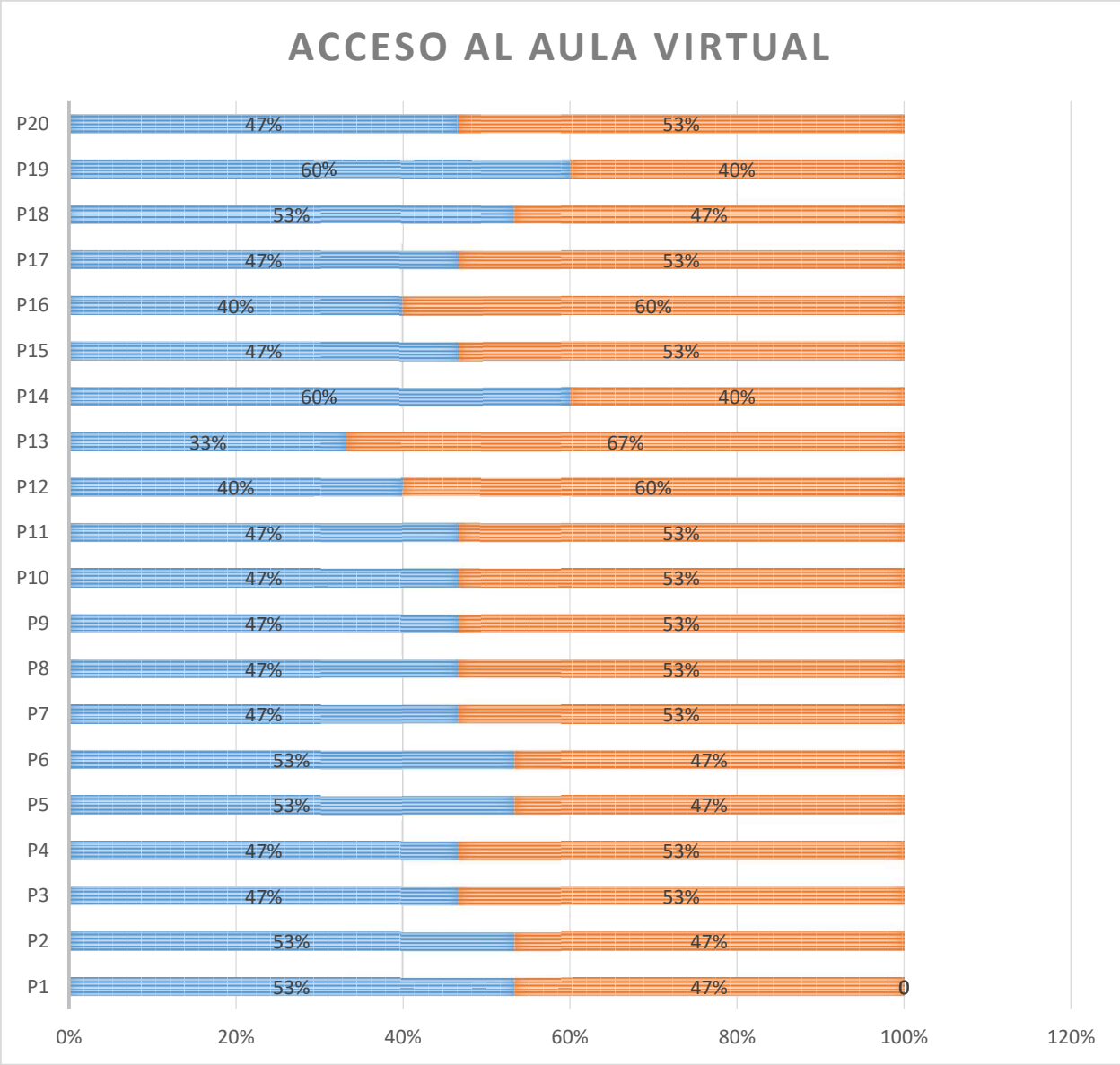


Ilustración 4 Resultado de acceso al aula virtual

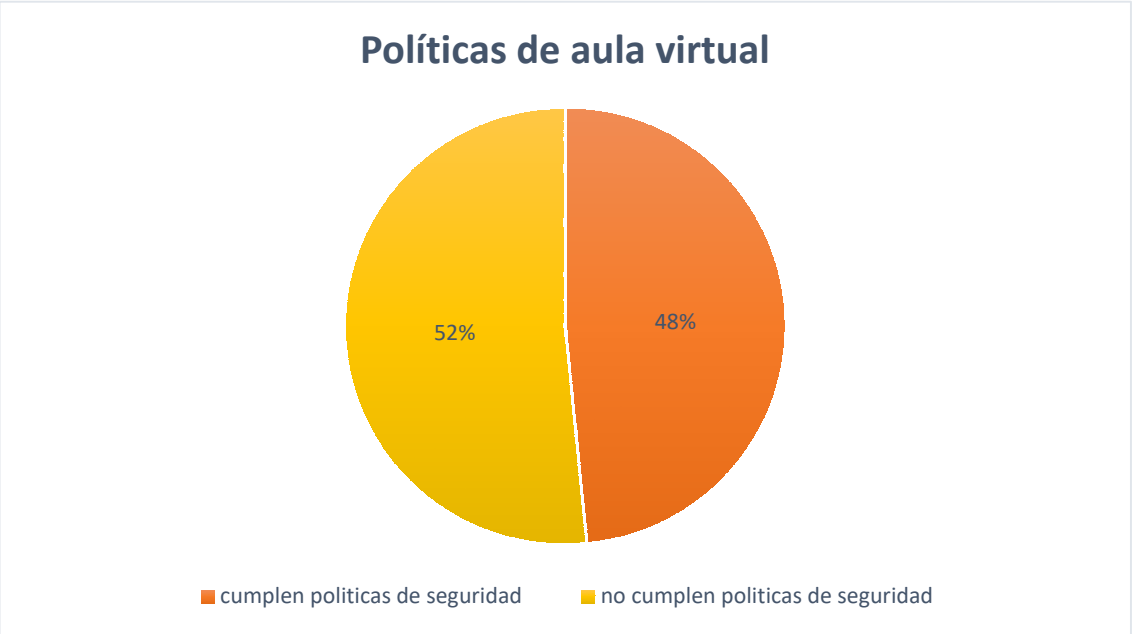


Ilustración 5 Políticas del aula virtual

En el promedio de todos los encuestados en lo que es de políticas del aula virtual

El promedio general no supera más que el rango moderado de acuerdo al cuadro superando más de la mitad de los docentes excluye las políticas de seguridad del aula virtual cabe resaltar que una moderada parte de los docentes si cumplen con las políticas de seguridad. Las principales causas de riesgo son:

- No cambiar su contraseña de acceso
- Mantienen abierta su sección en su computadora laboral
- Sus contraseñas no contienen más de 8 caracteres
- En su computadora mantienen abierta la sesión de la cuenta del aula virtual
- Ingresan al aula virtual desde su teléfono celular manteniendo aplicaciones de origen desconocido o poco confiable

3.5.3 Políticas del correo institucional

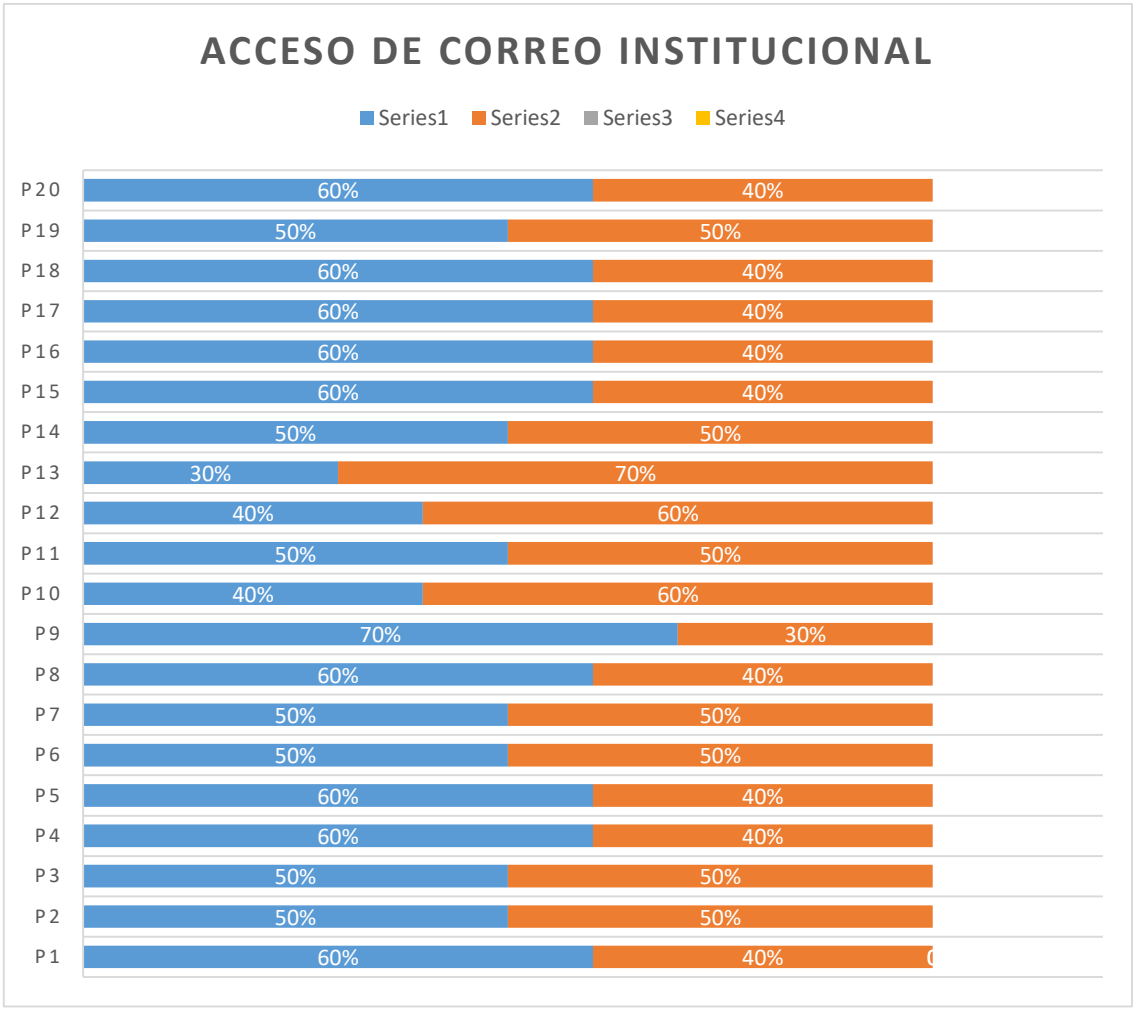


Ilustración 6 Acceso de correo institucional

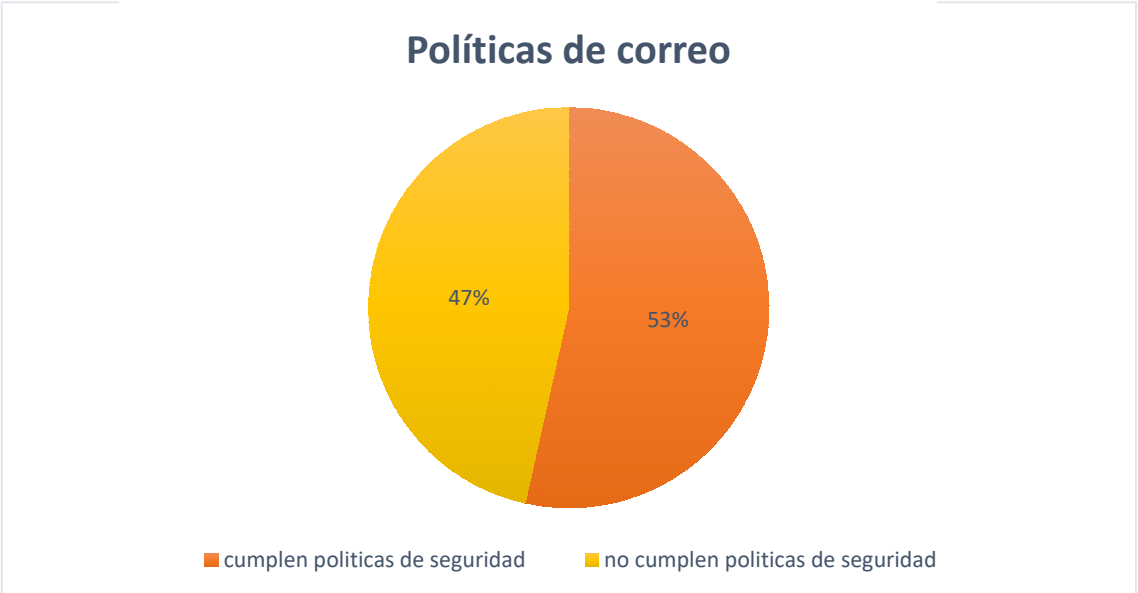


Ilustración 7 Políticas de correo intitucional

En las políticas del correo institucional se obtiene resultados que si defienden conocimiento estando en un rango general moderado sobre la seguridad de su correo institucional de parte de los docentes del área encuestada el déficit que no mantiene conocimiento estando el docente con mayor probabilidad de riesgo estando en un rango Alto de riesgo al no cumplir con las normas y es evidente que la mayoría está cerca de la media, al destacar que las preguntas que menos cumplen son:

- Mantienen abierta su sección de correo institucional en computadoras laborales
- No actualizan su contraseña en un tiempo aceptable

3.5.4 Políticas del uso de contraseña

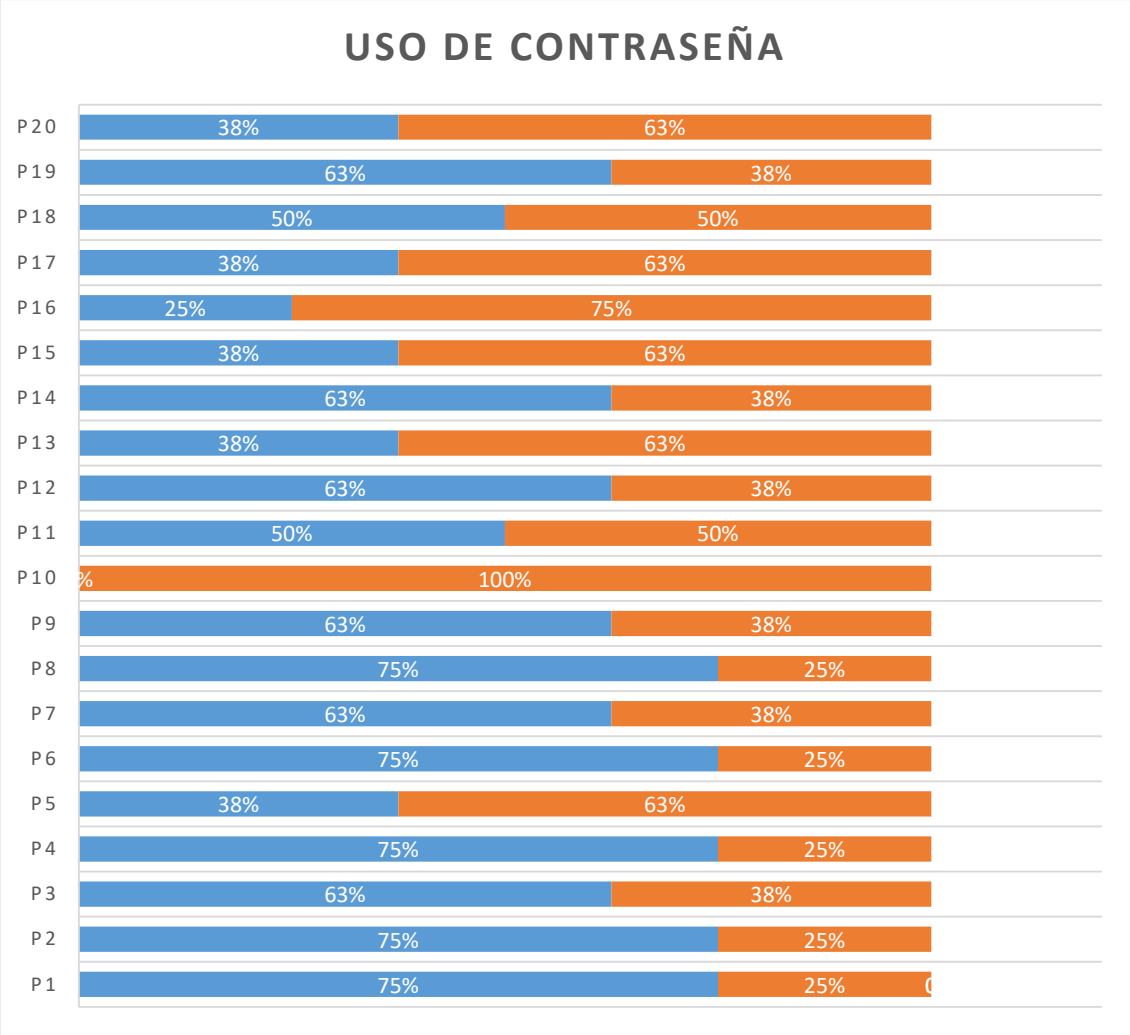


Ilustración 8 Políticas de uso de contraseña

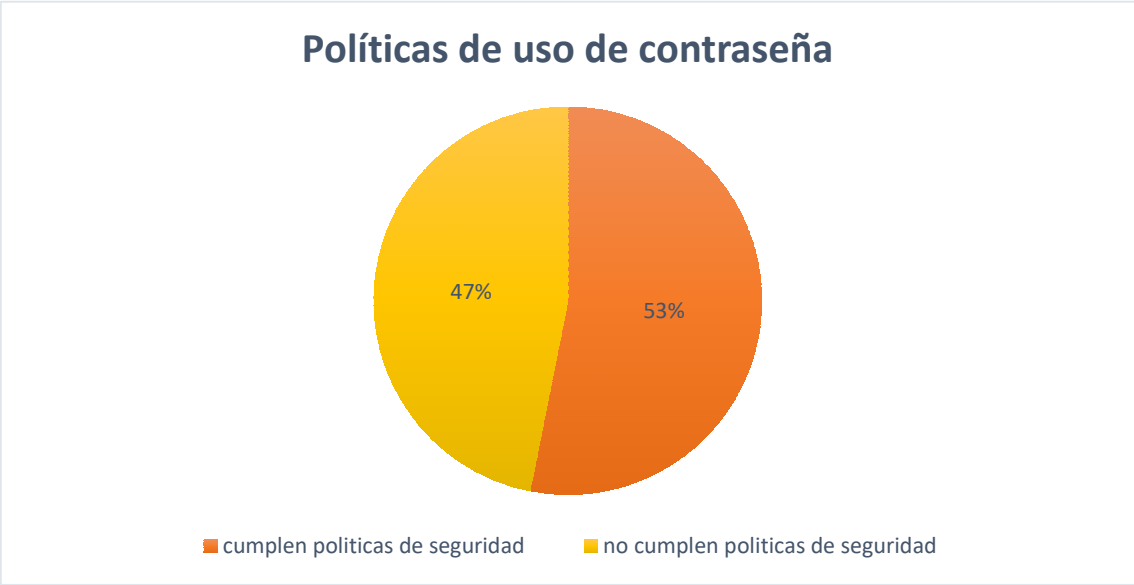


Ilustración 9 Políticas de uso de contraseña

Al notar el porcentaje general en lo que es de las políticas del uso de contraseña sobrepasa la media moderada de todos los encuestados que si cumplen recalcando que un significante 47% no cumple con todas las normas de seguridad destacando que el mayor porcentaje de los encuestado llega a la media aceptable en cuanto a protección de riesgos, recalcando que las preguntas que menos se cumplen son:

- No conocer los límites de intentos al ingresar su usuario y contraseña
- Acostumbran a guardar su usuario y contraseña en su computadora
- Realizan registros de sus usuarios y contraseñas en papeles o archivos físicos

3.5.5 Políticas acceso al correo personal

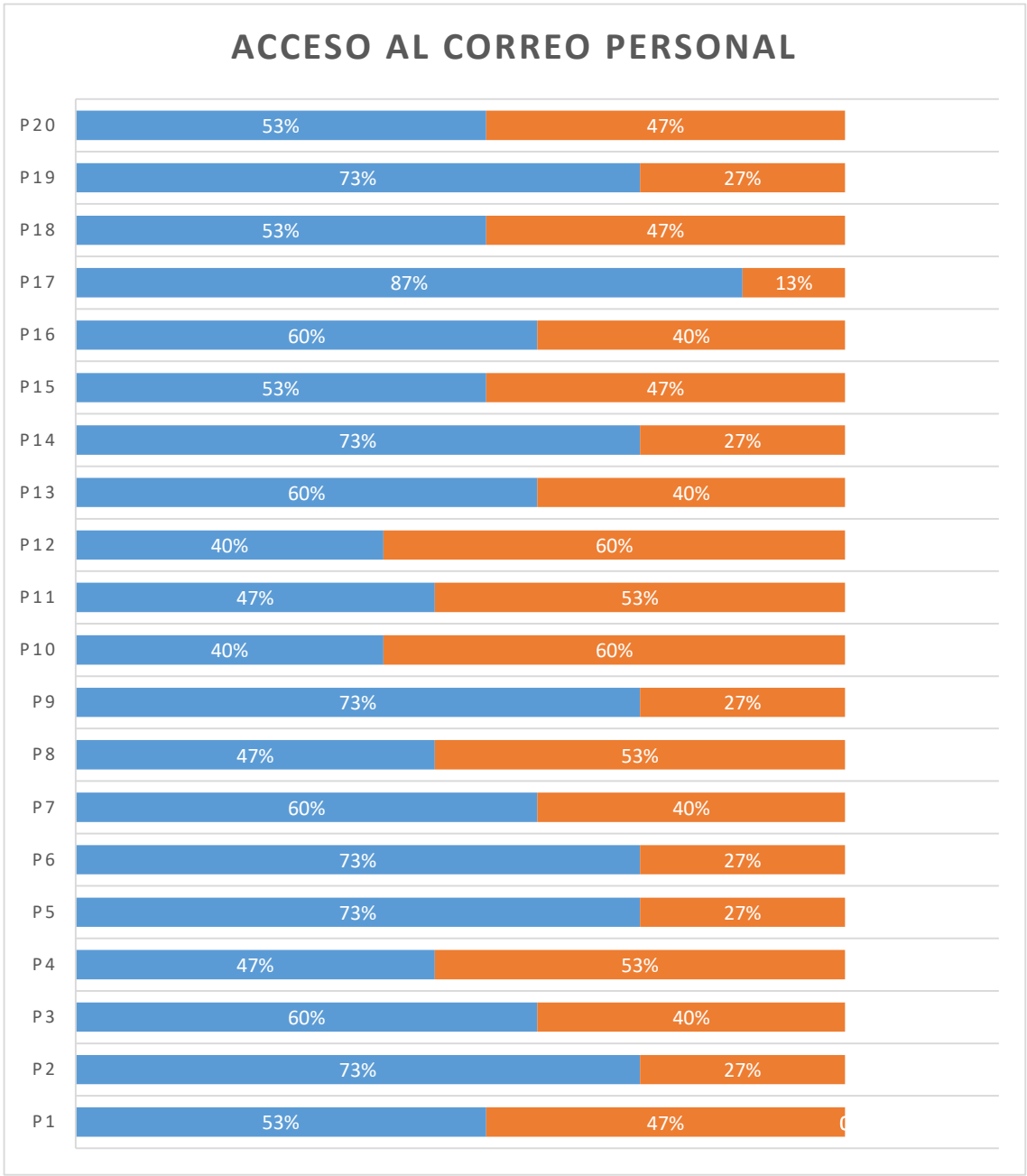


Ilustración 10 Políticas de acceso al correo personal

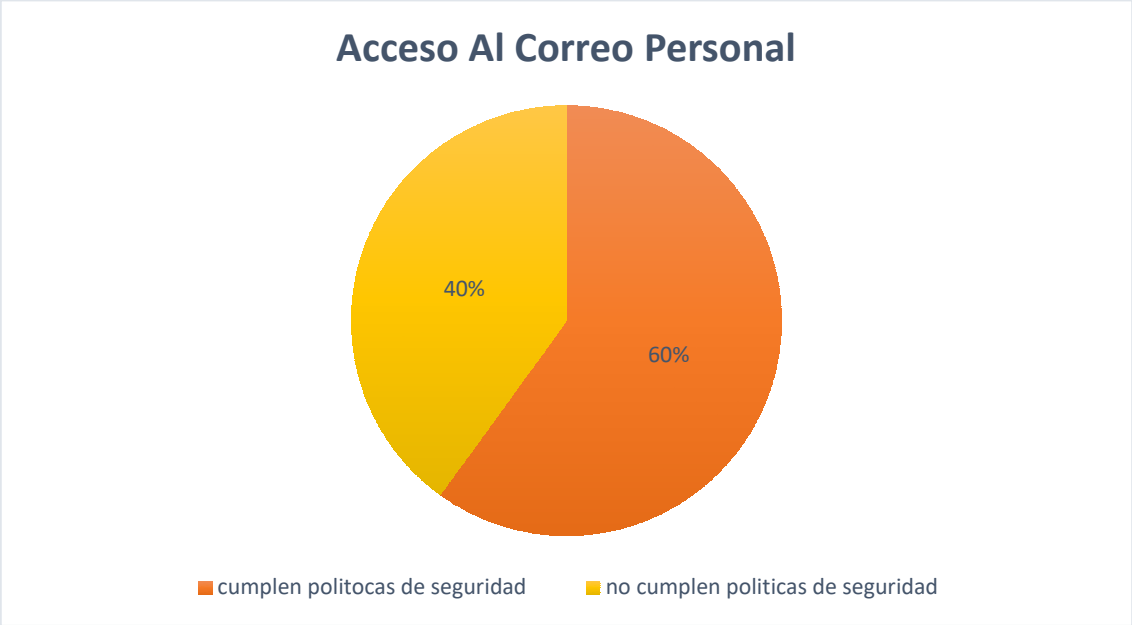


Ilustración 11 Acceso al correo personal

Las políticas de seguridad en el acceso del correo personal se notó con experiencia de parte de los docentes al hablar de que tanto conocen sobre el acceso a su correo personal estando lo aceptable en tanto a su seguridad, destacando que más de la mitad de los docentes sobrepasando el porcentaje medio a su seguridad sin menos preciar y destacar a el docente que sobrepasa con el 80% de las normas estando así en un promedio bajo a sufrir algún riesgo y destacando las siguientes preguntas que por parte de los docentes que menos se cumplen:

- No cambian su contraseña de correo personal en un periodo aceptable
- Su contraseña no contiene 8 caracteres
- Su contraseña no contienen mezclas de numero letras y caracteres
- Comparten su contraseña con otros usuarios
- Acostumbran a guardar su contraseña en papeles o archivos

3.5.6 Políticas de respaldo de la información

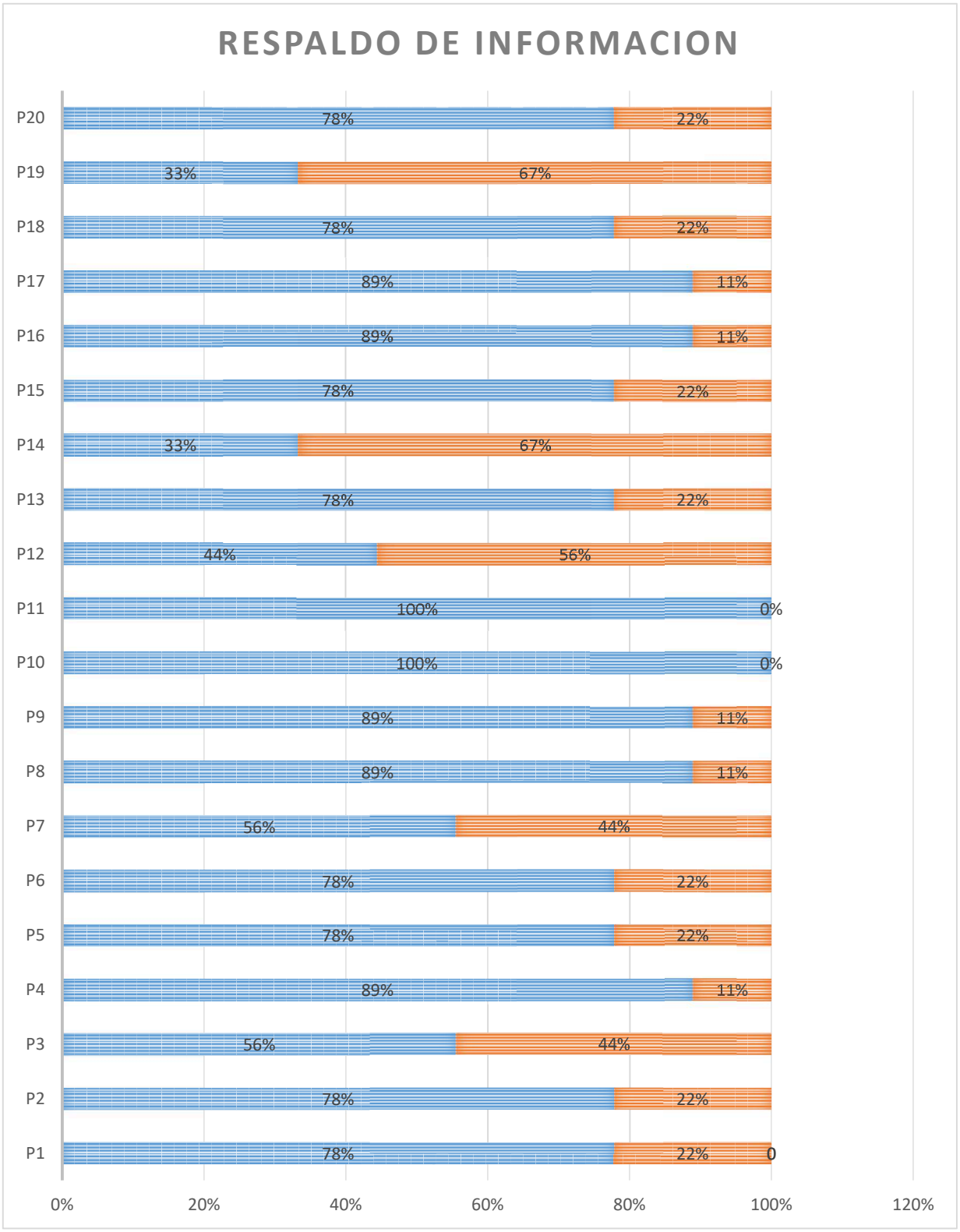


Ilustración 12 Políticas de respaldo de la información

Ilustración 13 Políticas de respaldo de laiinformación

La seguridad del respaldo de la información se encuentra en un riesgo medio, pues los 74% de las normativas analizadas se cumplen mientras que una cuarta parte de las mismas no son consideradas, más de la mitad de los docentes entrevistados encajan en el rango moderado del análisis del riesgo, sin embargo dos de los veinte entrevistados se encuentran en un alto grado de riesgo por no cumplir con la mayoría de las políticas. Las políticas que menos se cumplen son:

- Al no realizar respaldo de su información
- No medir el nivel de importancia al momento de realizar un respaldo
- No contar con productos antimalware o de detección de intruso
- No modificar las opciones de uso de su información
- No dar mantenimiento de su información al finalizar cada periodo académico

3.5.7 Políticas de alojamiento en la nube

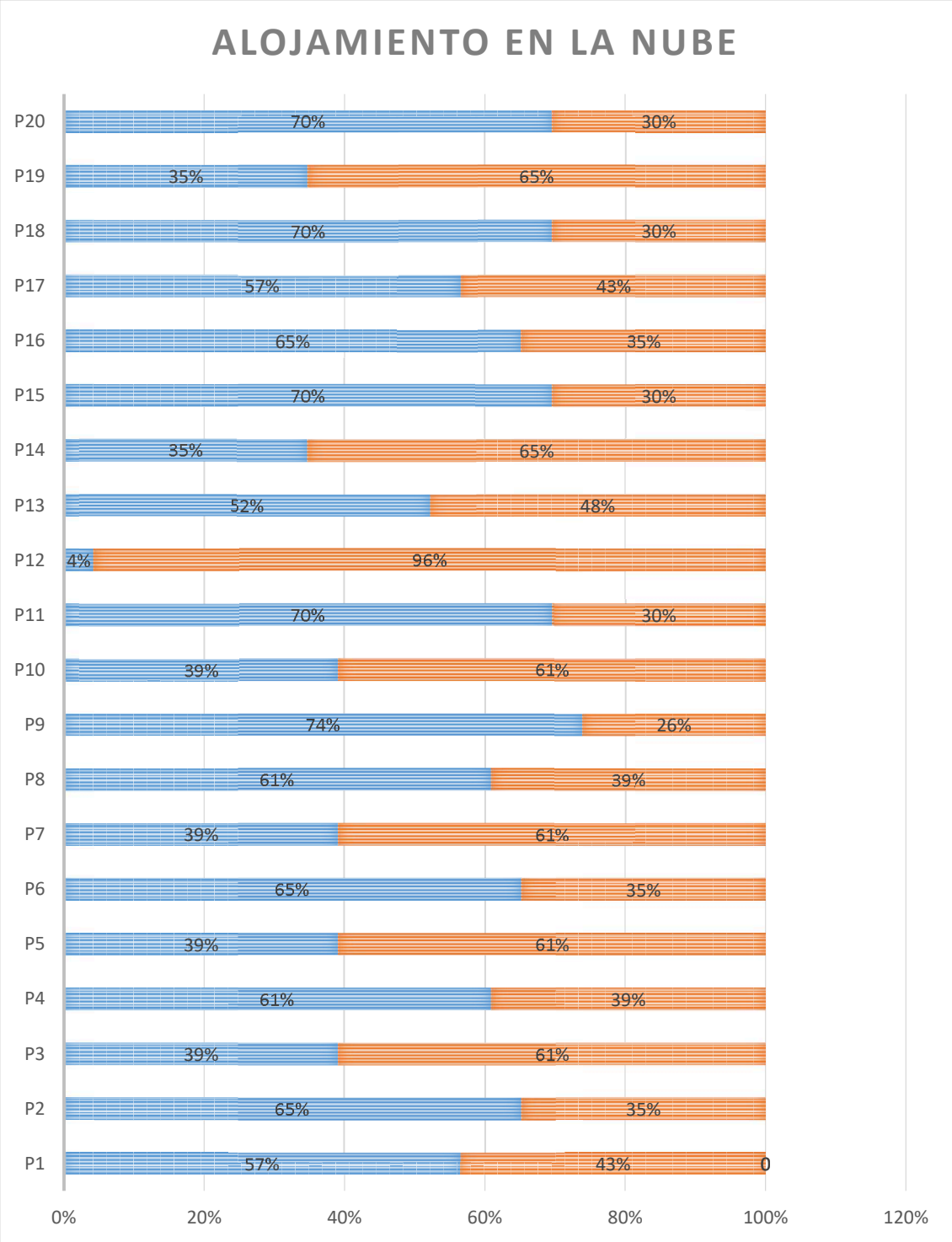


Ilustración 14 Políticas de alojamiento en la nube

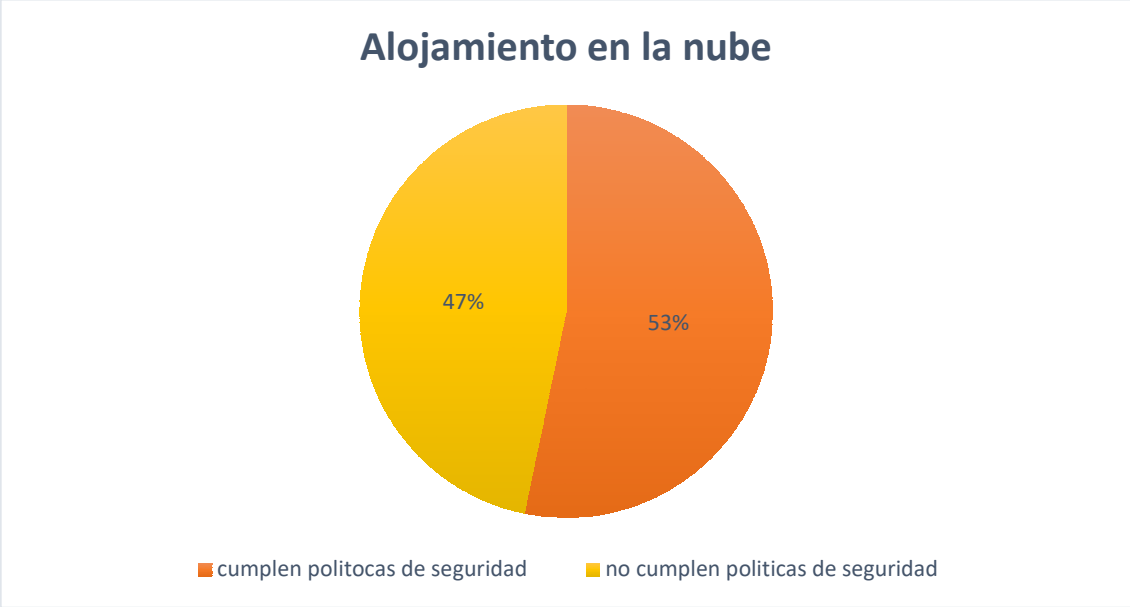


Ilustración 15 Políticas de alojamiento en la nube

La seguridad de alojamiento en la nube se encuentra en un rango moderado en las normativas analizadas se cumplen mientras que al notar que casi la mitad de las normas no se cumplen en su compleción, al considerar que más de la mitad de los docentes están en el rango moderado destacando que el mayor cumple con la categoría media en cuanto a su seguridad consecuentemente uno de los veinte entrevistado se descubre en el calidad extrema al sufrir riesgo. Las políticas que menos cumplen son:

- Desconocen los servicios de respaldo de información
- Desconocen cómo se protege los datos en la plataforma que usan
- Desconocen la seguridad que les ofrece la plataforma que utilizan
- No leen los términos de condición y contrato de la plataforma del alojamiento en la nube
- No se mantiene al tanto de la información relacionada con las aplicaciones y los riesgos que enfrenta la información
- No cuentan con una solicitud de acceso en sus cuentas
- No restringen los privilegios de información que comparten en la nube

3.5.8 Políticas acceso al sistema operativo

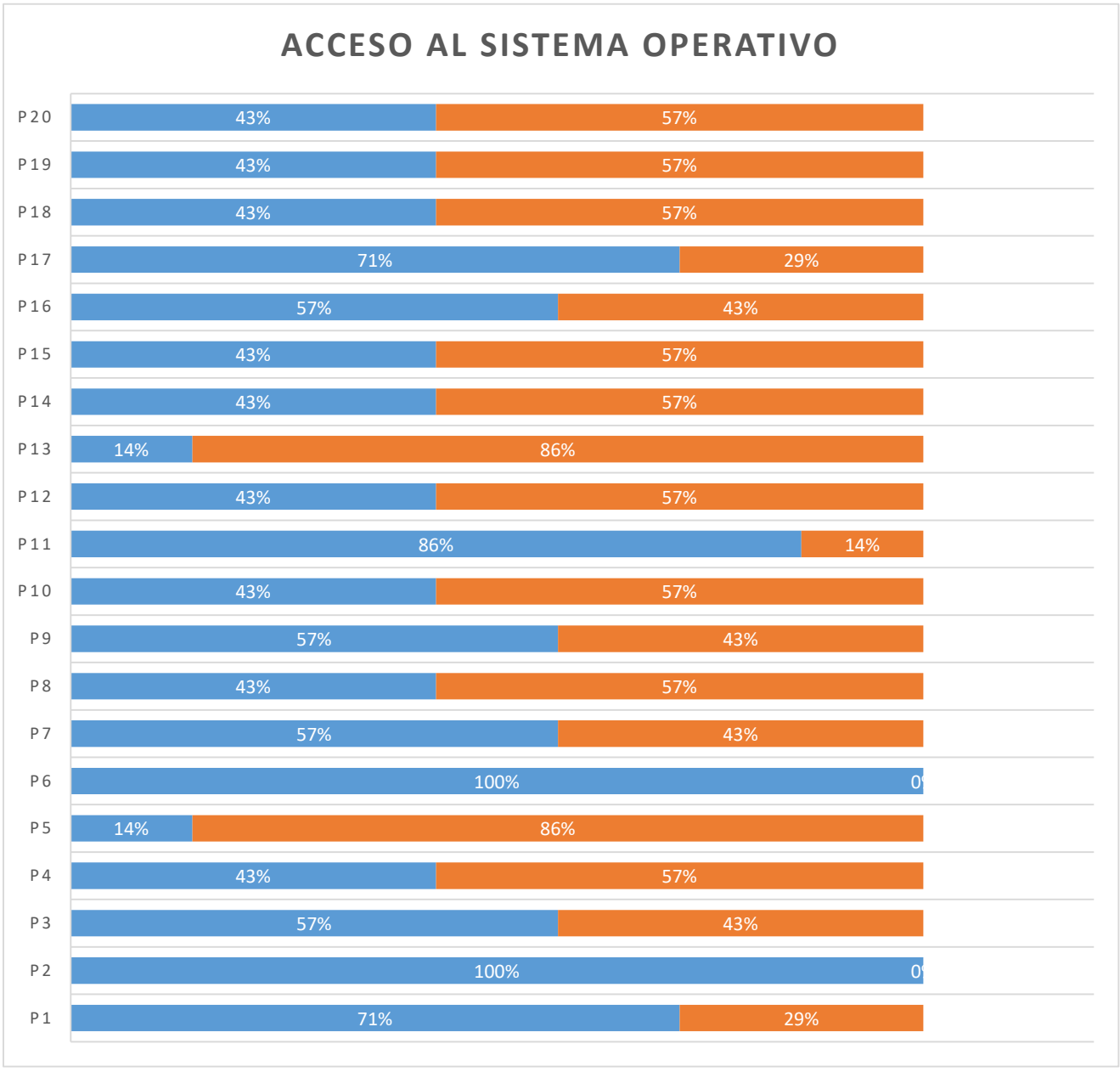


Ilustración 16 Acceso al sistema operativo

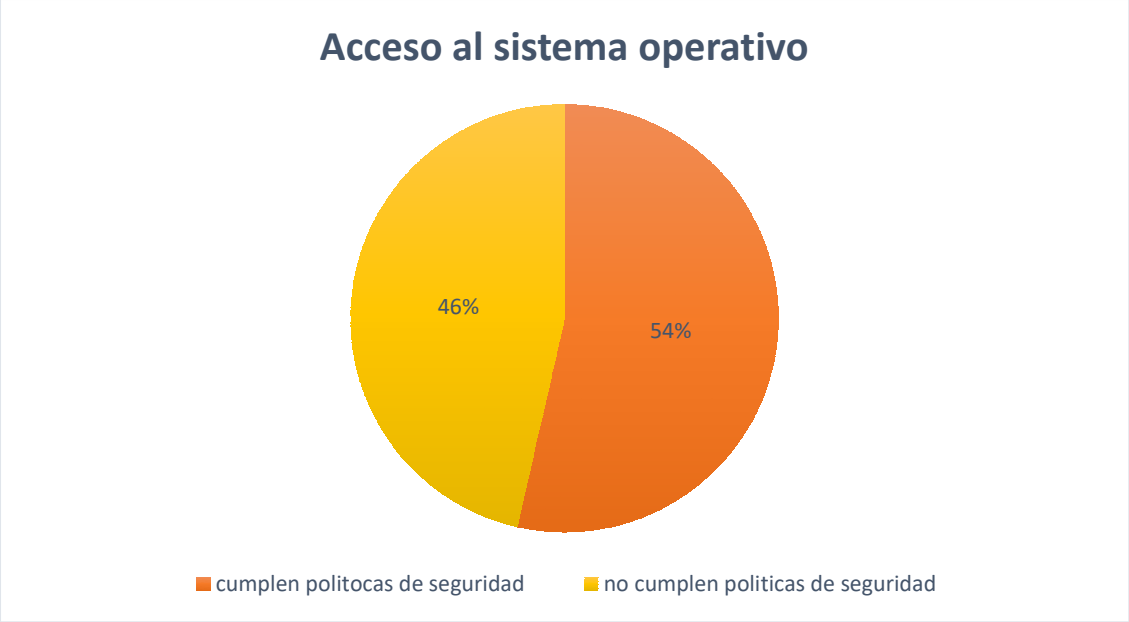


Ilustración 17 Políticas al sistema operativo

En el acceso al sistema operativo se encuentra en una condición moderada en cuanto a las normativas analizadas que al notar que casi la mitad de las normas si las cumplen en su generalidad, considerando que más la mitad de los docentes se mantienen en el rango moderado destacando que dos de los veinte entrevistado cumplen en la categoría baja en sufrir algún riesgo al cumplir el 100% de las políticas en lo que es a sistema operativo sin excluir que dos de veinte docentes se mantienen en el rango extremo en sufrir alguna inseguridad las normas que menos se cumplen son:

- No mostrar una advertencia en su computadora para personas autorizadas
- No conocer el límite de intentos para ingresar al sistema
- No contar con la sección de invitado para ser utilizadas por otros usuarios

3.5.9 Políticas del uso de correo electrónico

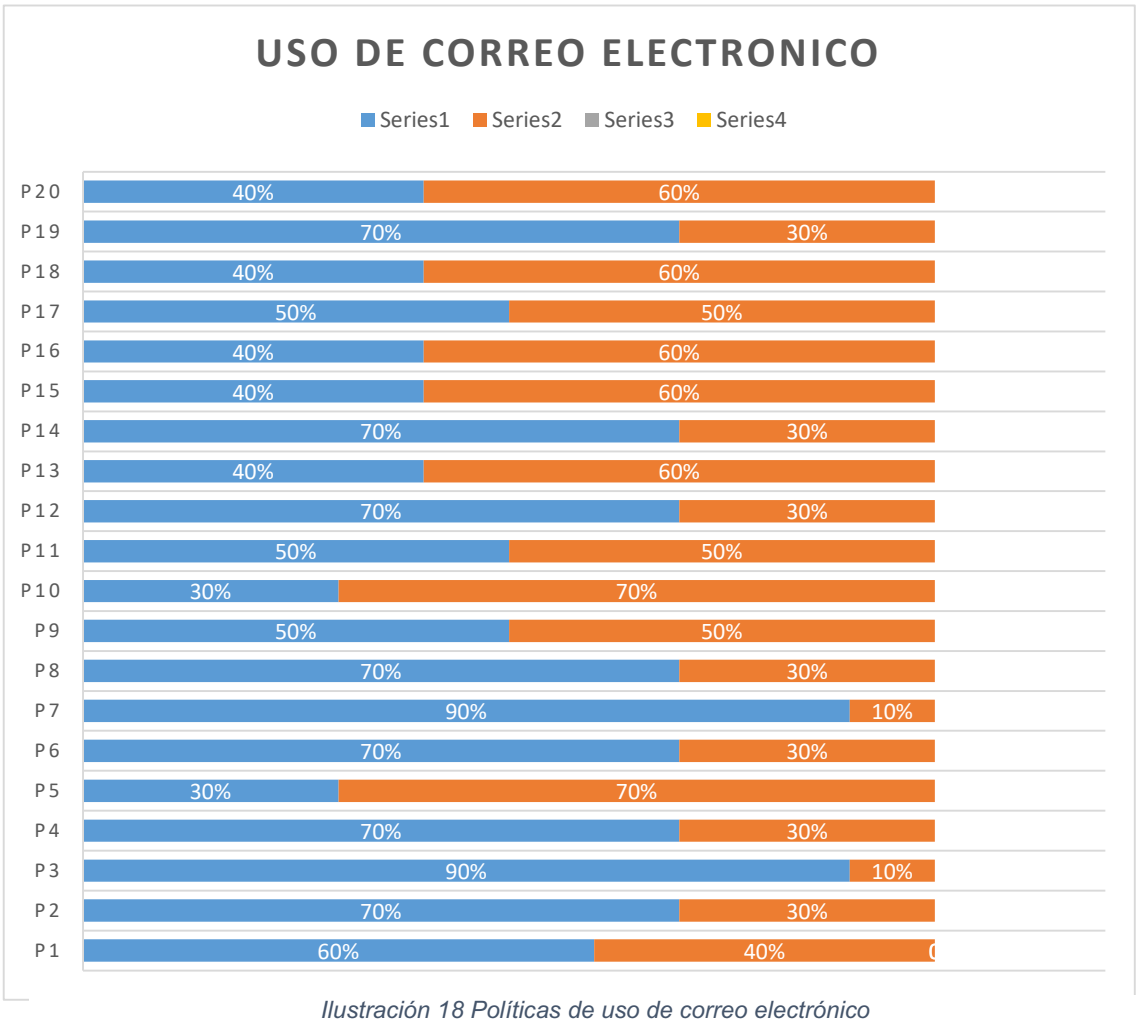


Ilustración 18 Políticas de uso de correo electrónico

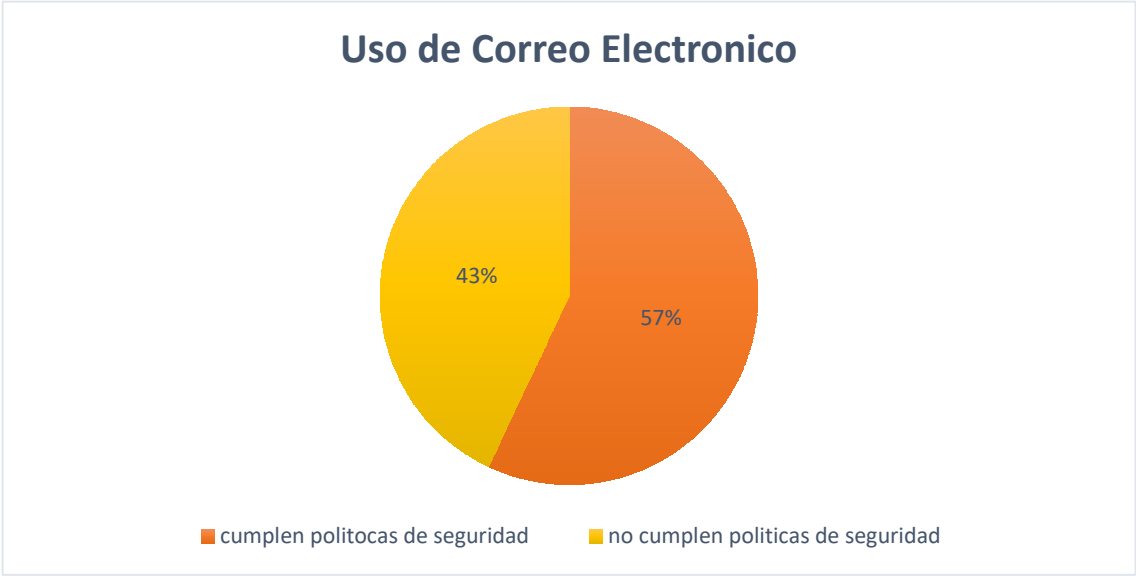


Ilustración 19 Políticas del uso de correo electrónico

Observamos que en la presente encuesta del uso de correo electrónico notamos que más de la mitad de los profesores cumplen con las políticas de seguridad con un insignificante 43% que no cumplen con lo requerido por las políticas

3.5.10 Sistema de alojamiento en la nube

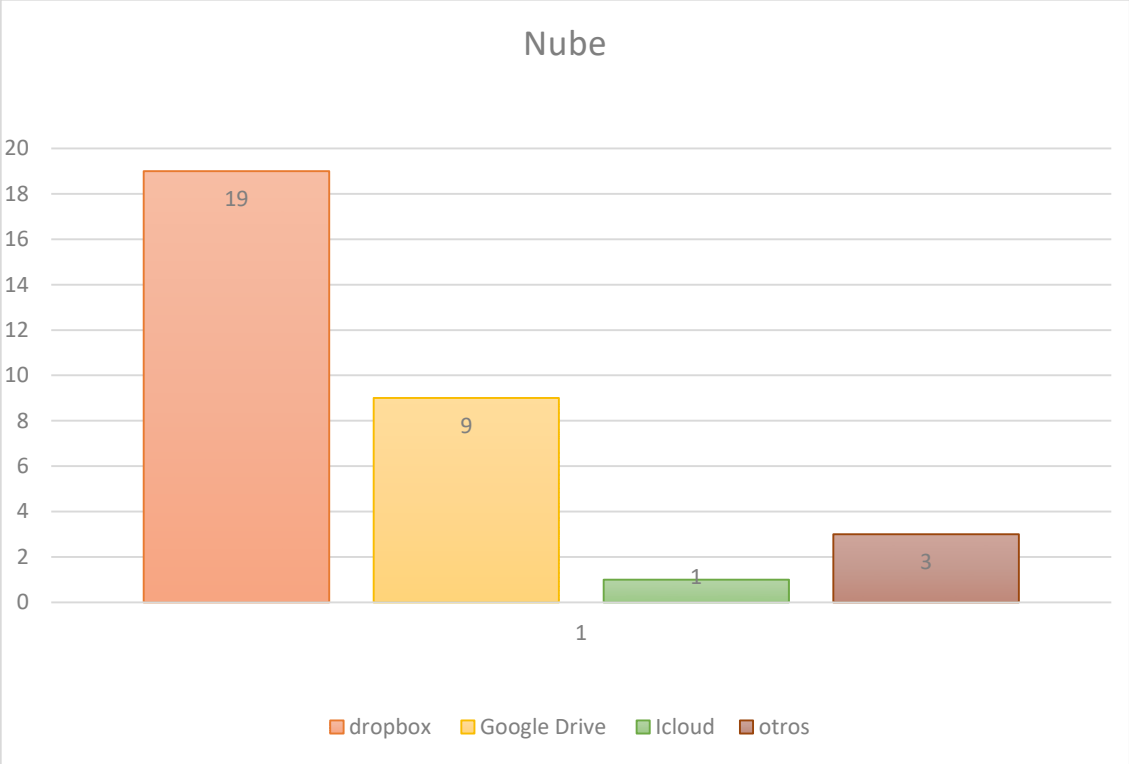


Ilustración 20 Alojamiento de nube

El servicio de almacenamiento en línea más utilizado según la entrevista es dropbox, seguido de google drive, Icloud y otros; esto nos permite comprender que la mayoría de los docentes de la carrera de ingeniería en sistemas utilizan las herramientas tecnológicas para el almacenamiento de los documentos que realizan en sus labores diarias.

3.6 Opinión

Al finalizar la evaluación sobre cumplimiento de políticas de acceso a la información por parte de los docentes de la carrera de ingeniería en sistemas mi opinión es:

Criterio	Cumplimiento	Nivel de seguridad
Cumplimiento general de políticas de seguridad Políticas de aula virtual	48%	Medio bajo
Cumplimiento general de políticas de seguridad del correo institucional	53%	Medio bajo
Cumplimiento general Políticas de seguridad del Uso de contraseñas	53%	Medio bajo
Cumplimiento general Políticas de seguridad del Acceso del correo personal	60%	Medio bajo
Cumplimiento general Políticas de seguridad del Respaldo de información	74%	Medio alto
Cumplimiento general Políticas de seguridad del Alojamiento en la nube	53%	Medio bajo
Cumplimiento general Políticas de seguridad del Acceso al sistema operativo	54%	Medio bajo
Cumplimiento general Políticas de seguridad del correo electrónico	57%	Medio bajo

Tabla 8 Nivel de cumplimiento de políticas

3.7 Conclusiones

- ✓ Como resultado de la evaluación realizada se concluye que no se toman en consideración la importancia de la seguridad, es evidente que el promedio general de las políticas de seguridad está en un rango medio hacia abajo al realizar esta auditoria informática se obtuvieron datos de información y documentación, teniendo en cuenta que existen varias amenazas por lo que se debe tener cuidado y saber sobre las políticas de seguridad que se les ofrece para tener cuidado con lo que se abre en internet o en correos electrónicos que llega de contenidos desconocidos ya que pueda ser víctima de alguna amenaza mal intencionada, pero el número de amenazas se puede reducir si se toma las medidas necesarias que les ofrecemos en este estudio.
- ✓ Al realizar este trabajo, he podido comprobar que cada vez es más evidente la necesidad de centralizar las políticas de seguridad de la información, afortunadamente se realizó un estudio sobre la seguridad de los docentes de la carrera ingeniería en sistemas donde llegamos al punto de qué medidas tomar entorno a lo referido que es la protección de su información
- ✓ Con esta auditoria se llega a una conclusión de que la mayoría de los docentes no aplica todas las políticas de seguridad que se necesita para tener su información completamente segura Para ello se analizaron las normas ISO estas normas son conjuntos orientadas a ordenar la gestión en sus distintos ámbitos. Las normas ISO son establecidas por el Organismo Internacional de Estandarización (ISO) que se componen con estándares de guías relacionados con sistemas y herramientas

3.8 Recomendación

- ✓ Para prevenir riesgos que podrían dañar o perder información importante de las actividades que realizan los docentes de la carrera de ingeniería en sistemas es necesario que se tome como política para el intercambio de información utilizar los servicios de alojamiento en la nube para tener acceso a la información de manera oportuna y de forma segura, por lo

que a continuación se propone una guía de configuración de un espacio compartido…

a) Políticas a cumplir en el acceso remoto a datos

i. Confidencialidad

- Cada docente es completamente consiente de que el uso no adecuado, la emulación copia o difusión de la información sin la correspondiente autorización puede conducir a la Institución a una situación de riesgo. Por lo consiguiente, la firma del presente documento, el docente comprende y acepta el cumplimiento en todo momento de las normativas que se especifican que son indicadas en cada momento por los responsables de la Institución.
- La totalidad de la información que se encuentra almacenada en la red corporativa de la institución, sea esta de forma estática o se encuentre circulando en mensajería electrónica, tiene carácter confidencial.

ii. Acceso al aula virtual

- La recesión del usuario y contraseña para el ingreso a las plataformas de la Institución se solicitara y realizara única y exclusivamente mediante el correo institucional.
- El tiempo de duración de una contraseña será de cada 6 meses, transcurrido dicho tiempo el usuario deberá cambiar su contraseña de ingreso la misma que debe contener más de 8 caracteres, letra mayúsculas y minúsculas, por lo menos un número y un símbolo
- Los equipos de cómputo de acceso personal deben contener su debido usuario y contraseña para su acceso, sin tener habilitado el usuario de invitado; no almacenar usuarios o contraseñas en navegadores, archivos o papeles físicos.

b) Acceso de correo institucional

- Cada ingreso al correo institucional mediante las contraseñas enviadas por el administrador del sistema como primer paso para el uso de las herramientas informáticas es la modificación de contraseña.
- El tiempo de duración de una contraseña será de cada 6 meses, transcurrido dicho tiempo el usuario deberá cambiar su contraseña de ingreso la misma que debe contener más de 8 caracteres, letra mayúsculas y minúsculas, por lo menos un número y un símbolo
- El tiempo máximo de sección abierta sin actividad será de 5 minutos pasado este tiempo deberá volver a ingresar

c) Uso de contraseña

- El máximo del ingreso de contraseña errónea será de 3 intentos pasado ese número deberá solicitar mediante correo institucional al administrador del sistema su reseteo de contraseña
- El ingreso a la plataforma de la institución mediante dispositivos móviles se realizara previo a cotejamiento mediante MAC y número celular.

d) Acceso al correo personal

- Para que su cuenta de correo personal se encuentre matriculada como una vía de recuperación de credenciales de las plataformas de la institución se debe enviar mediante correo institucional la debida solicitud adjunta firmada y escaneada.
- Su correo personal funcionara solo como correo alterno para la recuperación de credenciales mas no para recibir información o para reemplazar al correo institucional
- Los equipos de cómputo de acceso personal deben contener su debido usuario y contraseña para su acceso, sin tener habilitado el usuario de invitado; no almacenar usuarios o contraseñas en navegadores, archivos o papeles físicos.

e) Respaldo de información y alojamiento en la nube

- La información que almacene en servidores de alojamiento de documentos que correspondan a información de la institución debe realizarse mediante correo previamente matriculados
- Por ningún motivo se almacenara algún tipo de aplicación o herramienta informática de la institución en servidores ajenos a las mismas.
- No alojar documentación correspondiente a la institución en servidores de alojamiento que vayan en contra de las políticas establecidas o que coloquen el riesgo la información que los documentos contengan.

f) Guía de configuración de espacio compartido información en el sistema de alojamiento en la nube de los docentes

Introducción

La importancia de la nube ha ido adquiriendo fuerza y relevancia a medida que las personas han tomado conciencia de la necesidad de guardar datos personales a buen recaudo, compartir contenido digital de forma rápida e instantánea, y al tiempo que los soportes "físicos" han sido menos accesible o limitados en sus capacidades de manejo de archivos.
Si bien las memoria USB siguen siendo un medio físico muy factible para trasladar grandes cantidades de datos de forma puntual y para un propósito determinado, el uso de la nube se ha convertido en un medio más factible para compartir archivos sin necesidad de contacto físico entre las personas: aunque parezca una contradicción, la nube es una solución de almacenamiento en Red muy social, tanto que incluso proveedores como Dropbox se han integrado totalmente en Facebook, la red social por excelencia.

La nube ha despegado socialmente gracias a las cualidades técnicas de las redes móviles (3G HSPA+) y a la banda ancha de soluciones ADSL y Fibra Óptica: la velocidad de carga en estas redes ha contribuido a un rápido almacenamiento de cientos de Megabytes de datos en unos pocos minutos. Dropbox es uno de los servicios en la nube de uso habitual entre los usuarios de dispositivos móviles y PCs, con acceso a más de 5GB de almacenamiento gratuito para compartir fotografías y vídeos a distancia, ya sea a través de

correo electrónico o Facebook. La nube da confianza a aquellas personas preocupadas por tener un sitio seguro donde poder almacenar información más susceptible de ser perdida o deteriorada: los discos duros de ordenadores, los Cds o DVDs con datos y las memorias USB pueden terminar fallando con el tiempo o incluso perderse.

Tener los datos en la Nube es muy ventajoso por que el usuario puede acceder a ellos desde cualquier dispositivo con acceso a Internet, bien sea una computadora, un Tablet o un Smartphone. Gracias a la nube se puede comenzar a editar un documento desde un teléfono móvil y terminar de prepararlo desde un PC unas horas después, guardándose los datos en la cuenta online personal. La nube es una solución no solo destinada a almacenar, sino a compartir. Gracias a ella, una persona puede compartir un extenso álbum de fotografías con varios amigos, enviándoles un enlace de descarga, y sin la necesidad de intercambiar con cada uno de ellos el contenido con un CD/DVD o memoria USB. La nube también cuenta con el gran atractivo de poder realizar copias de seguridad de los datos almacenados en un Tablet o Smartphone, de forma remota, conectado a una red 3G/4G o a banda ancha por Wi-Fi. Es habitual que servicios de almacenamiento online se integren en el software de un Smartphone para que las fotografías tomadas con el dispositivo se almacenen automáticamente en la nube una vez el usuario se conecte a una red Wi-Fi o incluso al utilizar una red móvil.

Para la realización de cuenta de alojamiento en la nube en Dropbox ver anexo 6

Cuadro comparativo de sistemas de alojamiento en la nube

	Box	Google Drive	Dropbox	iCloud	Microsoft OneDrive
Almacenamiento gratuito	5 GB	5 GB	2GB	5GB	7GB
Cuenta Premium	25 GB por $10/anual	25 GB por $30/anual	50 GB por $100/anual	20 GB por $40/anual	27 GB por $10/anual
Máximo de carga por archivo	25 MB/1GB para clientes pagos	10 GB	300MB/Sin límite desde escritorio	25 MB/250 MB para clientes pagos	2 GB
Gestor de archivos en línea	Si	si	si	Limitado (Work y fotos)	si
Soporte nativo de archivo	Docs colaborativos	Docs colaborativos	Fotos y videos	fotos	Fotos y Docs colaborativos
Aplicación para escritorio	PC y Mac	PC y Mac	PC y Mac, Linux	PC y Mac	PC y Mac
Aplicaciones móviles	Android, iOS y Blackberry, WebOS	Android, iOS	Android, iOS y Blackberry	iOS	Windows pone, iOS
API para desarrolladores	si	si	si	si	si
Funciones especiales	no	Integracion con Gmail y Google Docs	Oportunidad para upgrades gratuitos	Copia de seguridad contactos, notas, calendario, mail	no
Seguridad de Cifrado	AES 256 bits	HTTPS / TLS	AES 256 bits	AES 128 bit	PFS
Seguridad en 2 pasos	si	si	si	si	si

Conclusiones

En base a lo desarrollado en este trabajo de investigación podemos concluir lo siguiente:

- Como resultado de la evaluación realizada se concluye que no se toman en consideración la importancia de la seguridad, es evidente que el promedio general de las políticas de seguridad está en un rango medio hacia abajo al realizar esta auditoria informática se obtuvieron datos de información y documentación, teniendo en cuenta que existen varias amenazas por lo que se debe tener cuidado y saber sobre las políticas de seguridad que se les ofrece para tener cuidado con lo que se abre en internet o en correos electrónicos que llega de contenidos desconocidos ya que pueda ser víctima de alguna amenaza mal intencionada, pero el número de amenazas se puede reducir si se toma las medidas necesarias que les ofrecemos en este estudio.

- Las metodologías aplicadas fueron de gran ayuda para realizar un trabajo sistemático y sintetizado, de los puntos más importantes de la investigación como también sirvieron de apoyo para realizar pruebas reales del uso y, otorgando de esta manera un trabajo estructurado y exploratorio. los cuales en gran parte están implementados en docentes de la Universidad laica “Eloy Alfaro” de Manabí Extensión El Carmen

Recomendaciones

- Para prevenir riesgos que podrían dañar o perder información importante de las actividades que realizan los docentes de la carrera de Ingeniería en Sistemas es necesario que se tome como política para el intercambio de información utilizar los servicios de alojamiento en la nube para tener acceso a la información de manera oportuna y de forma segura, por lo que a continuación se propone una guía de configuración de un espacio compartido
- Para mantener la integridad de los datos es recomendable que los docentes implementen medidas más rigurosas que cumplan varios parámetros de identificación y autenticación de usuarios y así poder mantener y controlar la seguridad de acceso lógico.
- Emplear medidas metodologías teóricas y empíricas que permitan recolectar información de fuentes confiable o a su vez información verídica de proyectos reales para que sean fuentes de apoyo, como también emplear técnicas que permitan explorar y observar las características del objeto de seguridad lógica en estudio.
- Utilizar la guía propuesta por parte de los docentes de la carrera de Ingeniería en Sistemas de la Universidad Laica Eloy Alfaro de Manabí Extensión en El Carmen, para un mejor cumplimiento en las políticas de la seguridad en el acceso remoto

Bibliografías

Aquiahuatl, E. C. (2015). *Serie: Metodología de la investigación interdisciplinaria: Tomo I Investigación monodisciplinaria.* Self published Ink.

Baca, G. (2016). *Introducción a la seguridad informática.* México: Grupo Editorial Patria.

Bañuelos , J. (2013). Claves de la Fotografía Digital Contemporánea: prácticas, competencias, socialización y tendencias. *Tecnológico de Monterrey-Campus Ciudad de México*, 11-21.

Barman, S. (2001). *Writing Information Security Policies.* New Riders Publishing Thousand Oaks, CA.

Benito, J. (2013). *Un año de fotografia.* España.

Bernal Torres, C. A. (2006). *Metodología de la investigación: para administración, economía, humanidades y ciencias sociales.* México: Pearson Educación.

Bernal, C. A. (2006). *Metodología de la investigación: para administración, economía, humanidades y ciencias sociales.* México: Pearson Educación.

Bilissi, E., & Langford, M. (2013). *Langford's Advanced Photography.* Italia: Taylor & Francis.

Borda, M. (2013). *El Proceso de Investigacion: Visión general de desarrollo.* Colombia: Universidad del Norte.

Borges, M., Hirt, T., & Wulf, A. (2000). *Gran libro Adobe In Design 1.5.* España: Marcombo.

Carpentier, J.-F. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas.* Barcelona: Ediciones ENI.

Carpentier, J.-F. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas.* Ediciones ENI.

Castro, M. A., Díaz, G., Alzorríz, I., & Sancristóbal, E. (2014). *PROCESOS Y HERRAMIENTAS PARA LA SEGURIDAD DE REDES.* Madrid: Editorial UNED.

Chicano, E. (2015). *Gestión de incidentes de seguridad informática. IFCT0109.* Málaga: IC Editorial.

Colobran, M., Arqués, J., & Galindo, E. (2008). *Administración de sistemas operativos en red.* Barcelona: Editorial UOC.

Costas, J. (2014). *Seguridad y alta disponibilidad.* Madrid, España: RA-MA.

Cuevas, A. (2010). *Tecnologia sensores de imagen.* Escazú.

Deng, R., Weng, J., Ren, K., & Yegneswaran, V. (2017). *Security and Privacy in Communication Networks: 12th International Conference, SecureComm 2016, Guangzhou, China, October 10-12, 2016, Proceedings.* USA: Springer.

Diego A. Arcentales Fernández, X. C. (2017). *Dialnet.* Obtenido de Auditoría informática: https://dialnet.unirioja.es/servlet/articulo?codigo=6102836

Escrivá, G., Romero, R. M., & Ramada, D. J. (2013). *Seguridad informática.* Madrid: Macmillan Iberia.

Ferraiolo, D. D., Kuhn, R., & Chandramouli, R. (2003). *Role-based Access Control.* Artech House.

Figueroa, C. M. (2002). *Persona y profesion; profesion y tecnicas de seleccion y orientación.* Madrid .

Galindo, J. P., & Gamboa, S. A. (2016). Control de Acceso a Archivos y Carpetas A Través del Reconocimiento Facial. *Revista Electrónica del programa de Ingenieria en Sistemas*.

Giménez, J. F. (2015). *Seguridad en equipos informáticos. IFCT0109.* Málaga: IC Editorial.

Gómez Vieites, Á. (2014). *Seguridad en equipos informáticos.* Madrid, España: RA-MA.

Gómez, Á. (2014). *Enciclopedia de la Seguridad Informática.* España: Grupo Editorial RA-MA.

http://carreras.uleam.edu.ec/elcarmen/mision-y-vision/. (s.f.). Obtenido de http://carreras.uleam.edu.ec/elcarmen/mision-y-vision/

http://carreras.uleam.edu.ec/elcarmen/resena-historica-2/. (s.f.). Obtenido de http://carreras.uleam.edu.ec/elcarmen/resena-historica-2/

http://carreras.uleam.edu.ec/elcarmen/wp-content/uploads/sites/47/2016/06/ORGANIGRAMA-ESTRUCTURAL-DE-LA-ULEAM-EXT.-EN-EL-CARMEN.pdf. (s.f.). Obtenido de http://carreras.uleam.edu.ec/elcarmen/wp-content/uploads/sites/47/2016/06/ORGANIGRAMA-ESTRUCTURAL-DE-LA-ULEAM-EXT.-EN-EL-CARMEN.pdf

Ibáñez, P. J. (2015). *Métodos, técnicas e instrumentos de la investigación criminológica.* Madrid: Editorial Dikynson.

Lieberman, G. (2015). *Researchgate.* Obtenido de Preparing for a Cyberattack by Aextending BCM into the C-suite: https://www.researchgate.net/profile/Gary_Lieberman/publication/282443424_Preparing_for_a_Cyberattack_by_Extending_BCM_Into_the_C-suite/links/5610492a08aec422d11517b5/Preparing-for-a-Cyberattack-by-Extending-BCM-Into-the-C-suite.pdf

Martinez, C. (2016). *Video Digital 2007.* Paradimage Soluciones SL.

Mendoza, J. (8 de Octubre de 2014). *12. Instrumentos de recolección de datos*. Obtenido de SlideShare: https://es.slideshare.net/JoseMendozaCastillo/12-instrumentos-de-recoleccin-de-datos

Naghi, M. (2000). *Metodología de la investigación.* México: Editorial Limusa.

Navarro, E. d. (2001). *Audítoria Iinformaticá Un Enfoque Prático.* RA-MA Editorial.

Nguyen, N. (2018). *Essential Cyber Security Handbook In Spanish: Manual esencial de seguridad cibernética en español.* Nam H Nguyen.

Pallás, R. (2004). *Sensores y acondicionadores de señal.* Barcelona: Marcombo.

Peltier, T. R. (2001). *Information Security Policies, Procedures, and Standards.* New York: Auerbach Publications.

Pequeño, M. V. (2015). *MF0490_3 - Gestión de servicios en el sistema informático.* España: Elearning, S.L.

Pérez , J., & Badía, E. (2012). *El debate sobre la privacidad y seguridad en la red: regulación y mercados.* España: Fundación Telefónica.

Pertusa, J. (2003). *Tecnicas de análisis de imagen: aplicaciones en biología .* Valencia : Universitat de València.

Portera, A. M. (2009). *La Auditoria De Seguridad En La Protección De Datos De Caracter Personal.* EDICIONES EXPERIENCIA.

Quintero, E. B. (2017). *MF0221_2 Instalación y configuración de aplicaciones .* España : Editorial elearing .

Ramos, M. d., & García Cervigón Hurtado, A. (2011). *Seguridad informática.* Madrid : Parainfo.

Razo, C. M. (2002). *Auditoria En Sistemas Computacionales.* Mexico: PEARSON EDUCACION.

Ruiz, E. (2017). *Nuevas tendencias en los sistemas de información.* España: Centro de Estudios Ramon Areces SA.

Shao, Z., Rastogi, V., Guo, G., Qu, Z., Chen, Y., Chen, H., y otros. (2016). AppShield: Enabling Multi-entity Access Control Cross Platforms for Mobile App Management. *Security and Privacy in Communication Network*, 3-23.

Tejada, E. C. (2015). *Auditoría De Seguridad Informatica .* IC EDITORIAL.

Terán, D. M. (2014). *Administración Estratégica de la función informática.* México: Alfaomega Grupo Editor.

Trabadela, J., Durante, J. L., & Calleja, J. A. (2015). *Fotografía digital.* España: Ministerio de Educación, Cultura y Deporte.

Uleam. (s.f.). *http://www.uleam.edu.ec/politicas-institucionales/*. Obtenido de http://www.uleam.edu.ec/politicas-institucionales/

Vieites, Á. G. (2014). *Gestion de incidentes de seguridad informática .* España : RA-MA .

Whitman, M. E., & Mattord, H. J. (2011). *Principles of Information Security.* Fourth.

Zarzar, C. A. (2015). *Métodos y Pensamiento Crítico 1.* México: Grupo Editorial Patria.

Anexos

UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ EXTENSIÓN EN EL CARMEN

Proyecto de Titulación

Auditoria informática de seguridad lógica para información de docentes “Universidad Laica Eloy Alfaro de Manabí” Ingeniería en Sistemas.

Objetivo: realizar el diagnóstico sobre políticas de seguridad de la información a los docentes miembros de comisiones de la Universidad Laica Eloy Alfaro de Manabí “Extensión en El Carmen

1. ¿Conoce ud sobre políticas de seguridad de la información?

   Si ☐ **No** ☐

2. ¿Tiene conocimiento de las políticas de seguridad de la información?

   Si ☐ **No** ☐

3. ¿La institución le ha dado a conocer las políticas de seguridad de la información?

   Si ☐ **No** ☐

4. ¿Ha recibido capacitaciones sobre cómo mantener segura la información?

   Si ☐ **No** ☐

5. ¿Porque medio ud comparte la información laboral?

   Correo institucional ☐
   Correo personal ☐
   Grupo de trabajo ☐

6. ¿Cree ud que por los medios que comparte información están dentro de las políticas de seguridad?

   Si ☐ **No** ☐

7. ¿Existe en la institución controles para verificar si se cumplen las políticas de seguridad de la información?

   Si ☐ **No** ☐

8. ¿Ud toma precauciones de seguridad al momento de compartir información institucional?

   Si ☐ **No** ☐

9. Para realizar su trabajo utiliza:

Pc de la universidad ☐
Pc personal ☐
Dispositivos móviles ☐
Otros equipos ☐

10. ¿Con que frecuencia cambia su contraseña de acceso a plataforma de la institución?
    Cada 3 meses ☐
    Cada 6 meses ☐
    Cada año ☐
    No actualiza ☐

11. ¿Utiliza algún antivirus en su ordenador?
    Si ☐ **No** ☐

12. ¿Para acceder a las plataformas institucionales utiliza usuario y contraseña?

			Exclusiva	
Correo institucional	**Si**	☐	**No**	☐
Aula virtual	**Si**	☐	**No**	☐
Sistema de gestión	**Si**	☐	**No**	☐
Académico	**Si**	☐	**No**	☐

    Otro: ……..

13. ¿Utiliza algún servicio de alojamiento de archivos con acceso compartido?
    Si ☐ **No** ☐
    Drop box ……
    Google Drive ……..
    Amazon Drive …….
    pCloud …….
14. ¿Considera ud que es importante conocer las políticas de seguridad de la información?
    Si ☐ **No** ☐

Anexo 1. Encuesta de diagnostico

Fuente: Anthony Ávila.

Anexo 2. Encuesta de auditoria Ing. Alexandra Mendoza.

Fuente: Anthony Ávila.

Anexo 3. Encuesta auditoria Ing. Andrea Coello

Fuente: Anthony Ávila.

Anexo 4.Encuesta auditoria Ing. Orlen Araujo

Fuente: Anthony Ávila.

Anexo 5 Encuesta auditoria Ing. Danilo Arévalo

Fuente: Anthony Ávila.

UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

Proyecto de Investigación "Auditoría y Seguridad Informática"

CERTIFICACIÓN

Quien suscribe Ing. Clara Guadalupe Pozo Hernández, Directora del proyecto de investigación "AUDITORÍA Y SEGURIDAD INFORMÁTICA" tengo a bien CERTIFICAR:

Que el Señor **ÁVILA CEVALLOS ANTHONY ALDAIR** N° 131470821-3, ha realizado el trabajo de investigación: **"AUDITORÍA INFORMÁTICA DE SEGURIDAD LÓGICA PARA LA INFORMACIÓN DE DOCENTES "UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ "INGENIERÍA EN SISTEMAS"**, como una actividad del proyecto de investigación, "Auditoría y Seguridad Informática" durante el período 2018(2) y 2019(1) según la planificación y documentación que reposa en los archivos del proyecto.

El Señor **ÁVILA CEVALLOS ANTHONY ALDAIR**, puede hacer uso del presente documento en lo que estime conveniente, dentro del marco legal académico establecido.

El Carmen, 08 de agosto del 2019

Ing. Clara Guadalupe Pozo Hernández, Mg.

DIRECTORA DEL PROYECTO

Anexo 6 Certificación de proyecto

Uleam	NOMBRE DEL DOCUMENTO: NOTIFICACIÓN DE DESIGNACIÓN DE TUTORES	CÓDIGO: PAT-01.F-007
	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO	REVISIÓN: 1
		Página 8 de 13

COMISIÓN ACADÉMICA
EXTENSIÓN EL CARMEN

MEMORANDUM No. 008-2019-PCA-TCL-CIS

PARA: **Ing. Clara Pozo, Mg. tutor(a) designado(a)**
DE: **Eco. Tito Cedeño Loor, Mg., Presidente Comisión Académica**
ASUNTO: **Designación para desarrollar tutorías de titulación**
FECHA: **El Carmen, 8 de febrero del 2019.**

En cumplimiento a la distribución de la carga horaria dispuesta dentro de la planificación académica de esta unidad y considerando los artículos 76 y 77 del proceso de titulación del Reglamento de Régimen Académico, la Comisión Académica de la Extensión El Carmen, ha considerado que, de acuerdo con su experticia en el área de conocimiento asignado, usted deberá dirigir y verificar el desarrollo de los trabajos de titulación de los siguientes estudiantes:

Estudiante/s	Nivel	Modalidad de Titulación	Tema de investigación
Ávila Cevallos Anthony Aldair	Noveno	Proyecto de Investigación	Auditoría informática de seguridad lógica para información de docentes "Universidad Laica Eloy Alfaro de Manabí " Ingeniería en Sistemas
Moreira Apuntes Liliana Magali	Noveno	Proyecto de Investigación	Auditoría informática a la gestión de seguridad de información en las comisiones "Universidad Laica Eloy Alfaro de Manabí" Extensión en "El Carmen"

Además, es de vital importancia su aporte profesional en los trabajos de tutorías desarrollados por los demás compañeros tutores, debiendo realizar equipos de trabajo en conjunto, para lo cual le adjunto el informe de designación de tutorías, el mismo que ha sido conocido por el Consejo de Facultad.

Particular que se informa para los fines consiguientes.

Atentamente,

Eco. Tito Cedeño Loor, Mg.
PRESIDENTE COMISIÓN ACADÉMICA
tcll_cedeo01@hotmail.com

Recibido
08-02-19

Anexo 7 Oficio de asignación de tutor

Dropbox

Servicio de alojamiento Dropbox es un lugar único para todos sus archivos. Cuando agrega un archivo a su cuenta de Dropbox, está disponible esté donde esté (siempre y cuando tenga acceso a Dropbox). Si descarga las aplicaciones de Dropbox en su computadora, teléfono o tablet, sus archivos se sincronizaran automáticamente en todos sus dispositivos.

Condiciones del servicio de Dropbox

Dónde se almacenan los datos

En todo el mundo. Los Servicios de Dropbox, podremos almacenar, procesar y transmitir información en todo el mundo. La información también podrá almacenarse de forma local en los dispositivos que usted utiliza para acceder a los Servicios.

Archivos y Permisos

Al usar los Servicios, porciones sus archivos, contenido, mensajes, contactos, etc. ("Tus archivos"). Sus archivos son Suyos. Estas Condiciones no conceden derechos sobre Sus archivos, excepto los derechos limitados que permiten prestar los Servicios.

Necesitan de su autorización para llevar a cabo ciertas acciones, como alojar Sus archivos, crear copias de seguridad y compartirlos cuando solicite hacerlo. Dropbox ofrece servicios de características como miniaturas de fotos, vistas previas de documentos, y capacidad de comentar, ordenar fácilmente, editar, compartir y buscar. Estas y otras funciones podrán requerir que nuestros sistemas accedan a sus archivos, los almacenen y los examinen.

Objetivo

- ✓ Aprender a crear una cuenta de Dropbox y el manejo de la misma
- ✓ Las características de Dropbox
- ✓ Como compartir archivos mediante Dropbox
- ✓ Aprender el manejo de Dropbox en nuestros dispositivos móviles

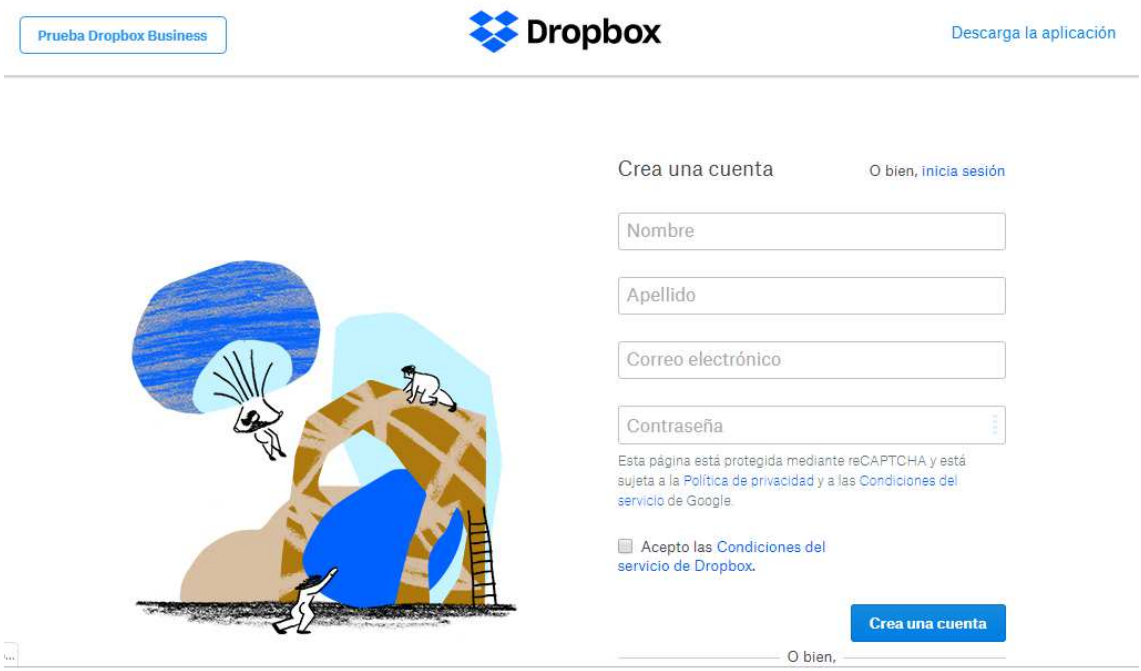
Pasos a seguir

Crear una cuenta en Dropbox

Para registrarte y obtener una cuenta de Dropbox, sigue estos pasos:

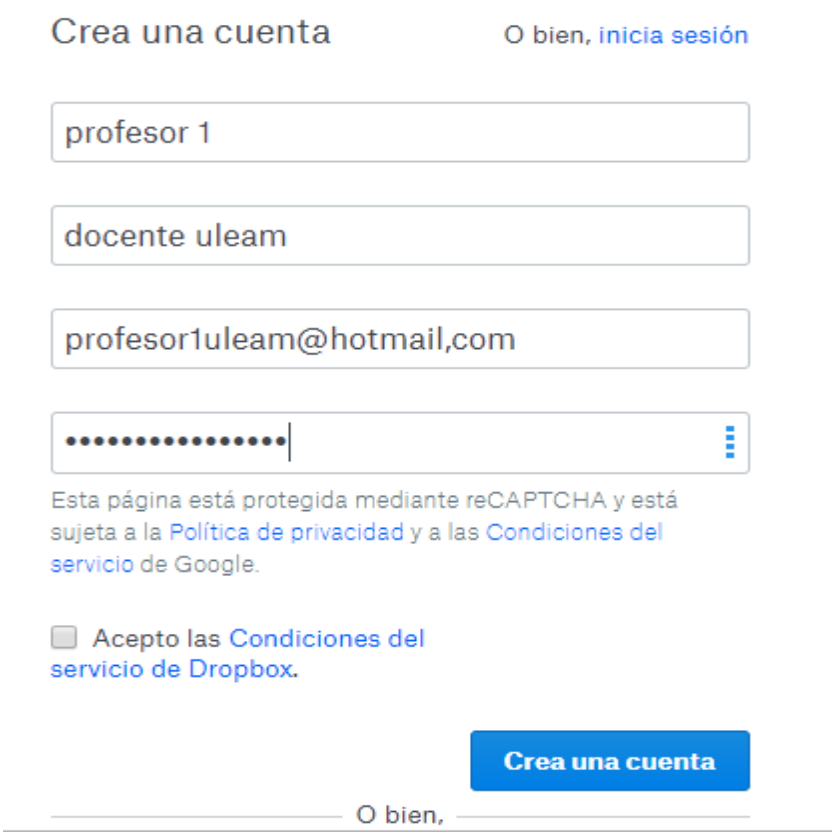
Primer paso

Ingresamos al navegador de nuestra preferencia en el cual escribimos www.dropbox.com



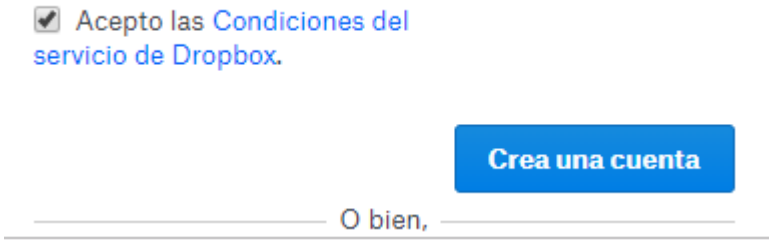
Segundo paso

Escriba su nombre y direcicion de correo electronico Su direccion de correo electronico es el nombre de usuario

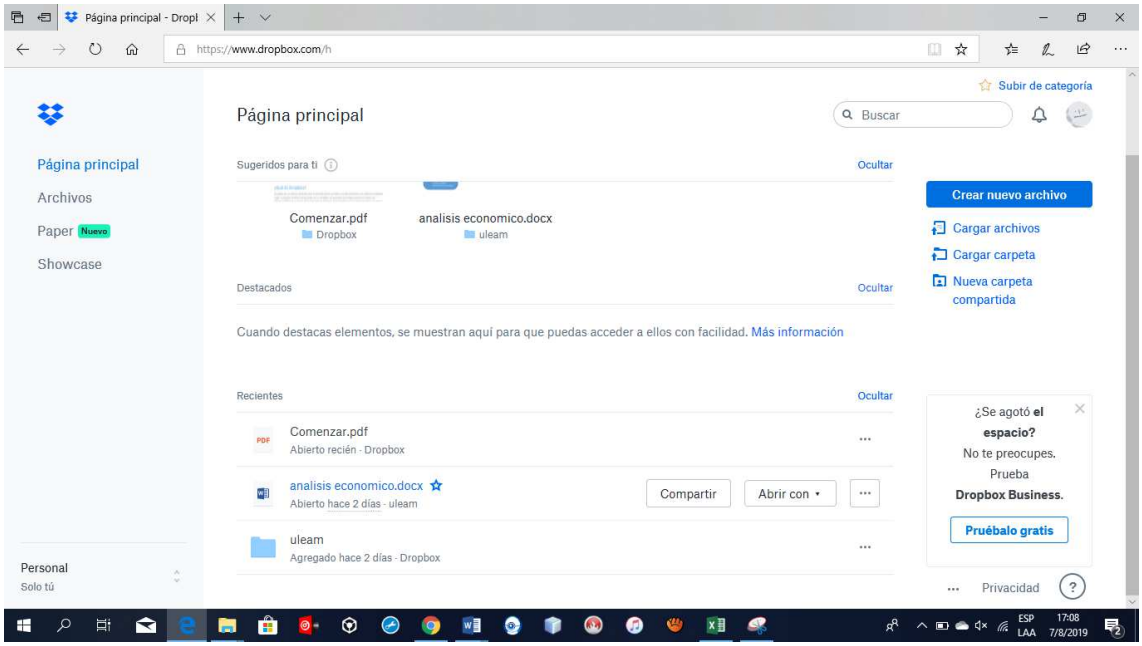


Su contraseña debe tener como mínimo 8 caracteres y combinación de letras, números, y símbolos en cumplimiento de las políticas de la Institución

Después de llenar todo los datos aceptamos los términos de condiciones del servicio de Dropbox



Finalizamos el proceso dando clic en **crear una cuenta**



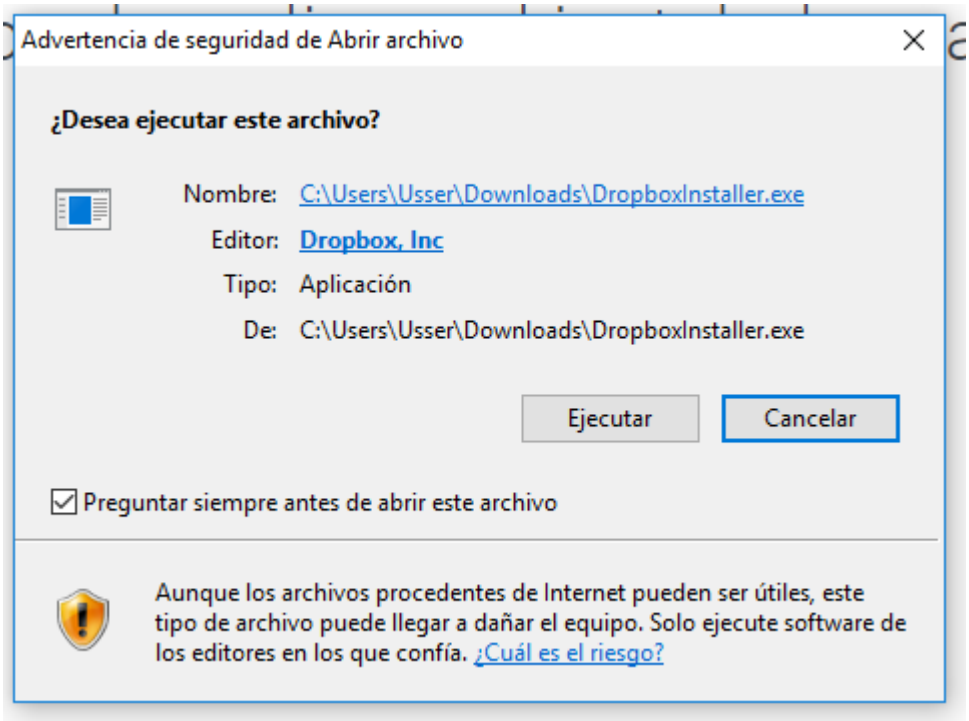
Ya estando dentro de la plataforma podemos navegar o ver nuestros documentos ya recibidos y enviados

Al momento de recibir un documento no da las opciones de **descargar** o **guardar en nuestro dropbox**

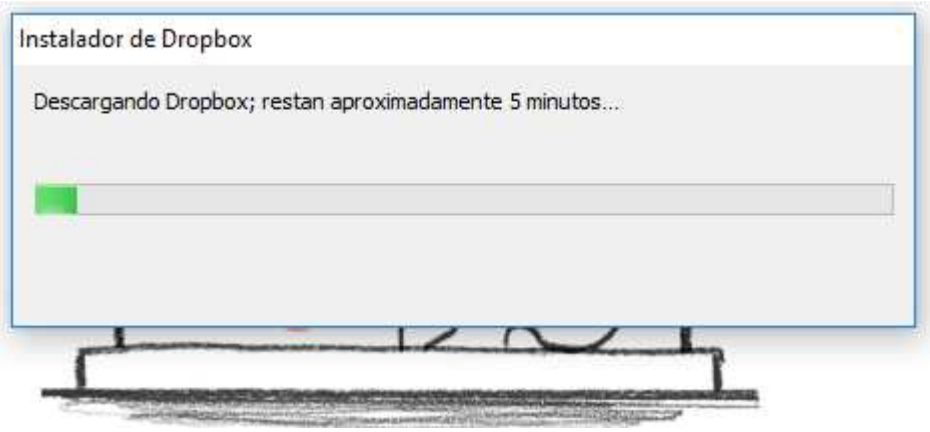
Tercer paso

Estando dentro de la plataforma de dropbox nos llega un mensaje de si deseamos descargar la aplicación

Si desea descargar la aplicación damos clic en **descargar la aplicación** y automáticamente se descargara en su computadora el **ejecutable** el cual damos clic en **ejecutar**



Esperamos un tiempo determinado hasta que se termine de instalar la aplicación en nuestra PC



Una vez culminado el proceso de instalacion procedemos a ingresar nuestro usuario y coontraseña

Cuarto paso

Una vez ya obtenida la aplicación descargada en su PC procedemos a ingresar desde la aplicación ya descargada. Luego que ya finalizó la instalación, se crea una carpeta de Dropbox. Cualquier archivo que guardes en tu carpeta de Dropbox también se guarda en todos tus otros equipos por ejemplo teléfono, sitio web donde tengas activa tu sección

En la parte superior te aparece un icono de color verde que te permite saber tu estado

Círculo verde y marca de verificación:

Todos los archivos en tu Dropbox están actualizados.

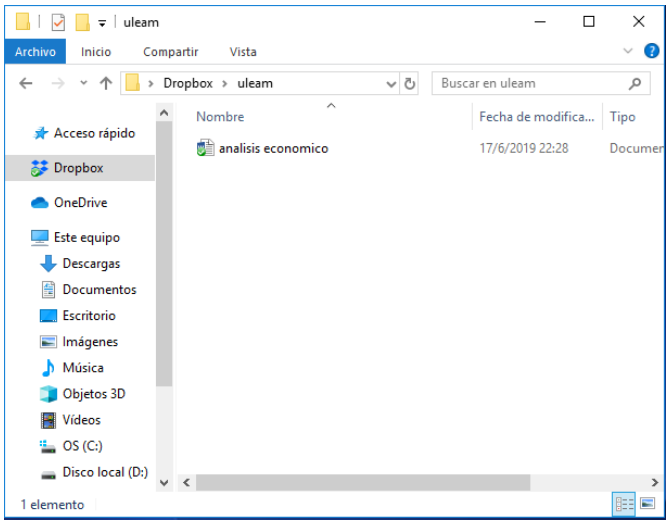
Círculo azul y flechas:

Los archivos en tu Dropbox se están actualizando.

Como añadir un archivo

Paso 1

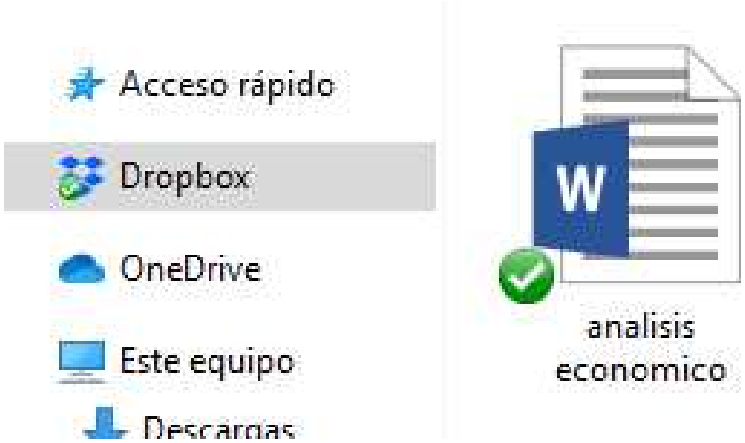
Arrastra el archivo y suelta en tu carpeta de Dropbox.



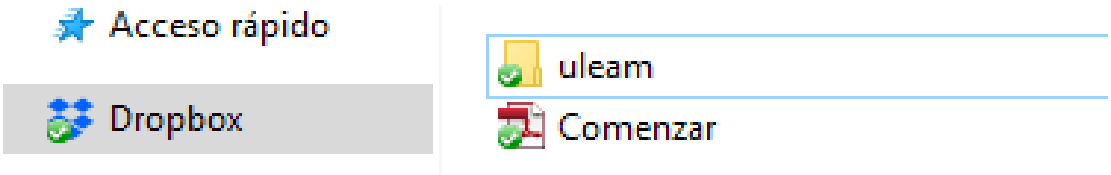
Paso 2

El icono azul significa que tu archivo se está sincronizando con dropbox

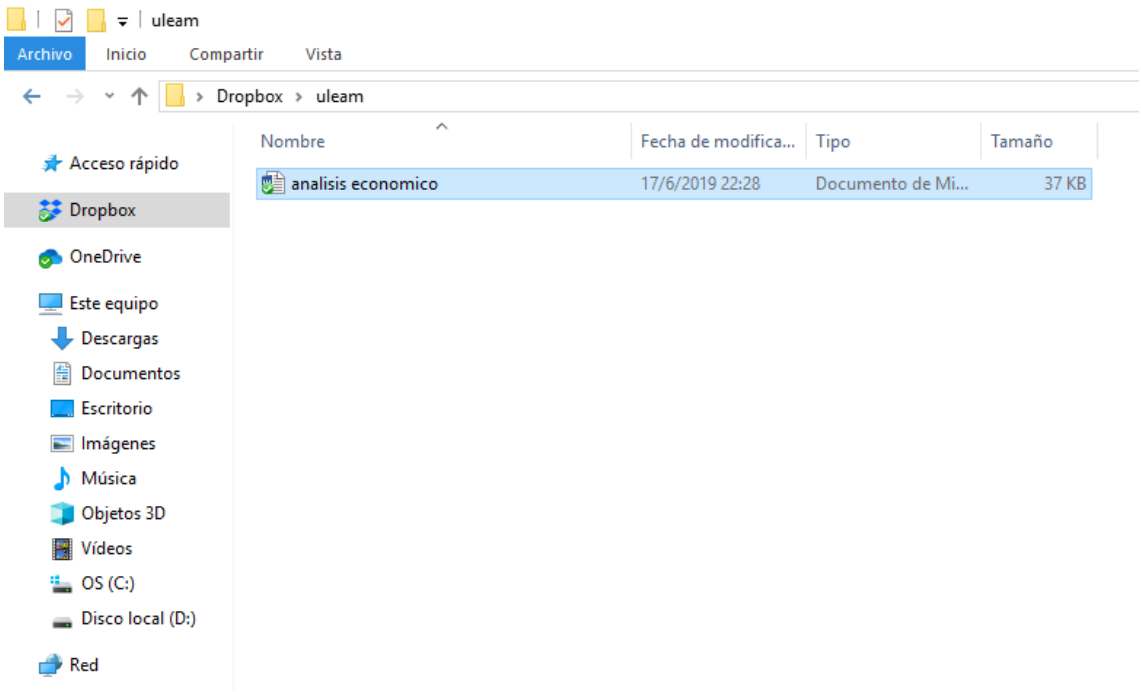
Cuando tu archivo refleje un icono de color verde significa que u archivo se terminó de guardar en los otros equipos y en el sitio web de dropbox. Estando ya tu archivo en dropbox cualquier notificación se destacara y actualizara de forma automática en los otros archivos



Crea la carpeta que desee adjuntar archivo para compartir arrastre los archivos dentro de la carpeta ya creada

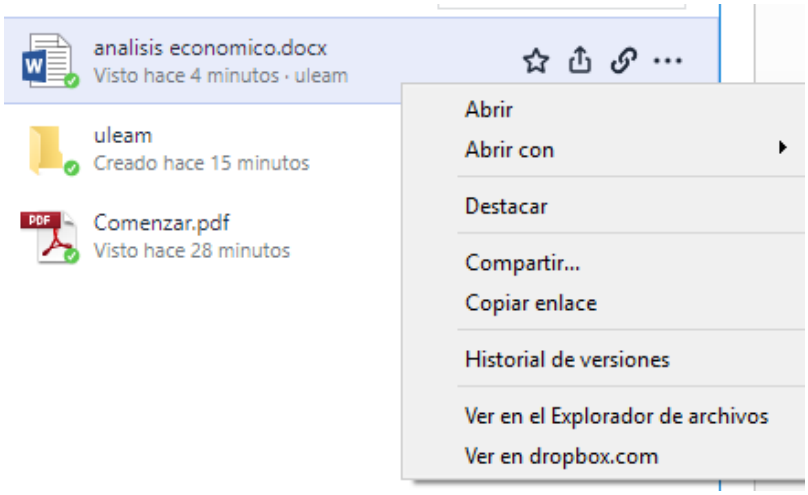


Al finalizar el proceso de la carpeta que compartimos nos aparecerá un icono de color verde el cual nos indicara que finalizo el proceso estando ya tu archivo en dropbox cualquier notificación que realice se destacara y actualizara de forma automática en los otros archivos.

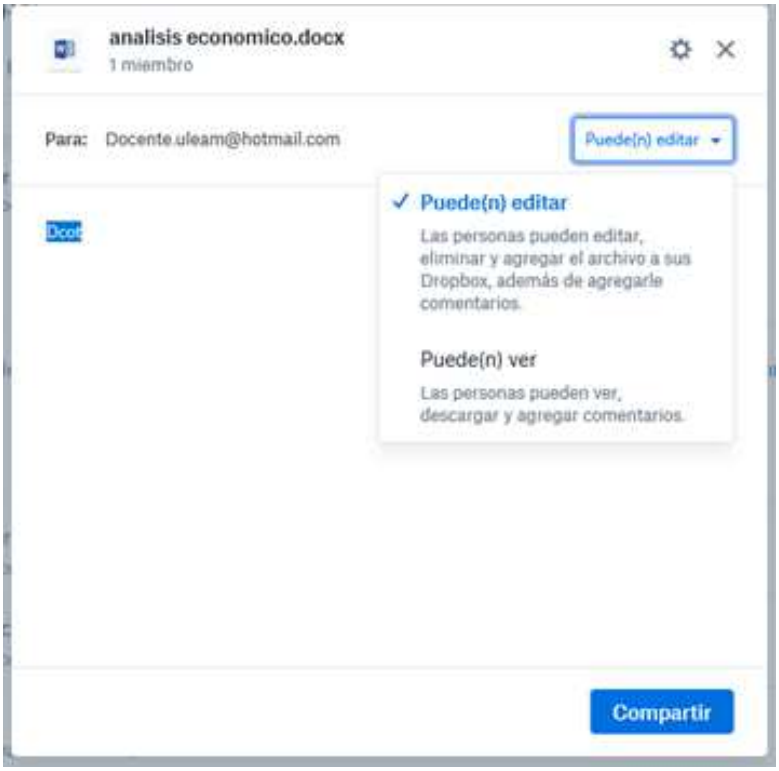


Al hacer clic derecho sobre un archivo o una carpeta en tu dropbox, veras un menú que te permite hacer:

- ✓ **Compartir una carpeta**
- ✓ **Ver versiones anteriores**
- ✓ **Navegar en el sitio web**
- ✓ **Obtener enlace**



Al querer compartir un archivo en Dropbox damos clic en **compartir** donde nos reflejara las opciones de que el documento puede ser editado o el documento solo lo pueden ver.



Dropbox en dispositivos móviles

Paso 1

Ingresa a la Play Story del dispositivo móvil para obtener la aplicación de dropbox si ya tiene instalada la aplicación salte al paso 3

Pasó 2

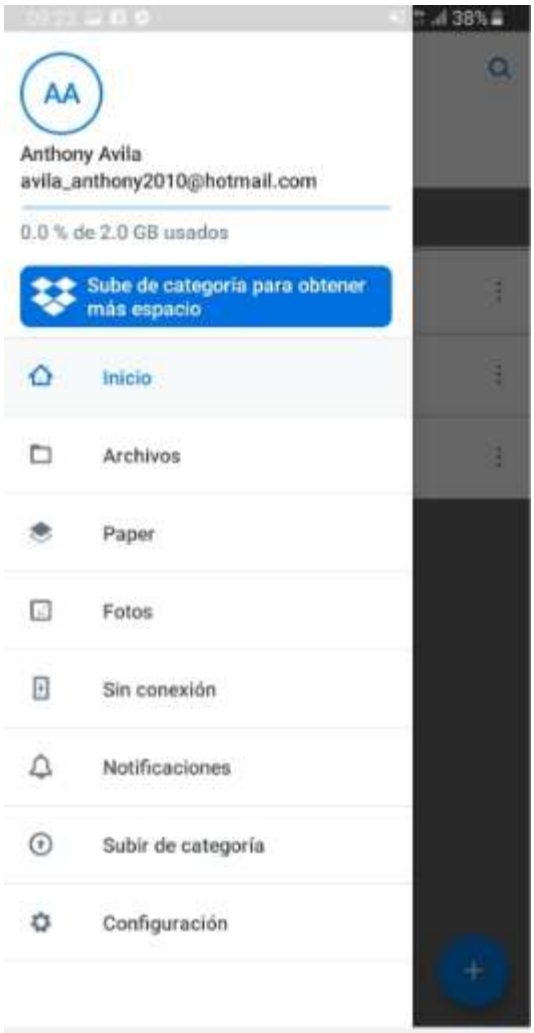
Busca **Dropbox** en la tienda in procedemos a la respectiva instalación

Paso 3

Una vez finalizada la instalación procedemos a entrar y nos aparece la pantalla principal donde nos da las opciones de iniciar con **Google**, **Registrarte** y si ya tienes una cuenta **Iniciar sesión**

Finalizando los pasos ya podrá usar su cuenta de dropbox en su dispositivo móvil para compartir un archivo desde su dispositivo móvil, arrastra el archivo y

suelta en tu carpeta de Dropbox. Te aparecerá en icono color verde cuando finalice la sincronización de todos tus dispositivos



Anexo 8 Guía de buenas practicas