



**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 PARA PROTECCIÓN DE DATOS
PERSONALES DE LOS DOCENTES DE LA “UNIVERSIDAD
LAICA ELOY ALFARO DE MANABI” EN EL CANTÓN EL
CARMEN, PROVINCIA DE MANABÍ.**

AUTOR


ALFREDO LEONARDO MEDRANDA REYES.

TUTOR

WLADIMIR MINAYA MACIAS, Mg.Sc.

El Carmen, 26 de abril 2023

Uleam

	NOMBRE DEL DOCUMENTO: CERTIFICADO DE TUTOR(A)	CÓDIGO: PAT-01-F-010
	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO	REVISIÓN: 2 Página 1 de 1

CERTIFICACIÓN

En calidad de docente tutor de la Extensión El Carmen, de la Universidad Laica "Eloy Alfaro" de Manabí, certifico:


Haber dirigido y revisado el trabajo integrador, bajo la autoría del estudiante **MEDRANDA REYES ALFREDO LEONARDO**, legalmente matriculado/a en la carrera de Ingeniería en Sistemas, periodo académico 2022-2023, cumpliendo el total de 400 horas, bajo la opción de titulación de trabajo de investigación, cuyo tema del proyecto es "Auditoría Informática para protección de datos personales de los Docentes de la Universidad "Laica Eloy Alfaro de Manabí en el cantón El Carmen", provincia de Manabí.

La presente investigación ha sido desarrollada en apego al cumplimiento de los requisitos académicos exigidos por el Reglamento de Régimen Académico y en concordancia con los lineamientos internos de la opción de titulación en mención, reuniendo y cumpliendo con los méritos académicos, científicos y formales, suficientes para ser sometida a la evaluación del tribunal de titulación que designe la autoridad competente.

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

El Carmen, 22 de Febrero del 2022.

Lo certifico,



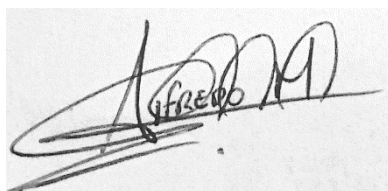
A.S. Wladimir Minaya Macías, Mg.
Docente Tutor
Área: Sistemas

UNIVERSIDAD LAICA “ELOY ALFARO” DE MANABÍ
EXTENSIÓN EN EL CARMEN



DECLARACIÓN DE AUTORÍA

La responsabilidad del contenido de este Trabajo de titulación, cuyo tema es: “Auditoria Informática para Protección de datos personales de los docentes de la “Universidad Laica Eloy Alfaro De Manabí” En El Cantón El Carmen, Provincia De Manabí.”, corresponde exclusivamente a: Alfredo Leonardo Medranda Reyes con cédula de ciudadanía número 131071233-4 y los derechos patrimoniales de la misma corresponden a la Universidad Laica “Eloy Alfaro” de Manabí.



Alfredo Leonardo Medranda Reyes
C.C 131071233-4

DEDICATORIA

A Dios que ha sido pilar principal para poder cumplir una meta más en mi vida.

A mi madre Carmen Reyes quien es la persona más importante, mi inspiración y motivación cada día, mi padre, por estar siempre en cada paso de este camino.

A mis hermanos Yadira e Isaac por brindarme el apoyo, amor y motivarme a no rendirme.

Alfredo Medranda

AGRADECIMIENTO

Al ingeniero Wladimir Minaya Macias, por ser parte de este proyecto y dirigirme de la mejor manera.

A los ingenieros que me impartieron clases durante todos estos años universitarios, por brindarme apoyo y motivarme a seguir adelante. A mis colegas que fueron parte de este proceso durante todo este tiempo de estudio hasta alcanzar esta meta.

Alfredo Medranda

ÍNDICE GENERAL

PORTADA	I
DECLARACIÓN DE AUTORÍA	III
DEDICATORIA	IV
AGRADECIMIENTO	V
ÍNDICE GENERAL.....	VI
ÍNDICE DE TABLAS	XI
Tabla 1 Encuesta a Docentes	XI
Tabla 2 Resultado de la encuesta realizada a Docentes.....	XI
Tabla 3 Programa de auditoría	XI
Tabla 4 Definición de activos	XI
Tabla 5 Datos públicos y privados	XI
Tabla 6 Tipo de amenazas.....	XI
Tabla 7 Matriz Probabilidad-Peligro	XI
Tabla 8 Matriz de riesgos resultados	XI
Tabla 9 Causas de riesgo Phishing.....	XI
Tabla 10 Causas riesgos Virus	XI
Tabla 11 Causas riesgos Rasomware.....	XI
Tabla 12 Guía de buenas prácticas riesgo Phishing	XI
Tabla 13 Guía de buenas prácticas riesgo Virus	XI

Tabla 14 Guía de buenas prácticas riesgo Rasomware	XI
ÍNDICE DE ILUSTRACIONES	XII
RESUMEN.....	XIII
SUMMARY	XIV
INTRODUCCIÓN.....	1
1 CAPÍTULO I.....	3
1.1 MARCO TEÓRICO	3
1.1.1 Introducción a la Auditoria Informática.....	3
1.1.2 Definición a la Auditoria Informática	4
1.1.3 Objetivos de la Auditoria Informática	5
1.1.4 Técnicas de la Auditoria Informática.....	5
1.1.5 Las Etapas de la Auditoria Informática	6
1.1.6 Tipos de Auditoria Informática	7
1.1.7 El auditor de Auditoria Informática.....	7
1.1.8 Herramientas de la Auditoria Informática.....	8
1.1.9 Metodología de Auditoria Informática	9
1.1.10 Aplicación de la Auditoria Informática.....	10
1.1.11 Seguridad Informática	10
1.2 Protección de datos de carácter personal	11
1.2.1 Antecedentes	12
1.2.2 Principios de la calidad de los datos.....	12

1.2.3	Principio de Información	13
1.2.4	Los tipos de datos personales	14
1.2.5	Ley orgánica de protección de datos	14
1.2.6	Derechos a la protección de datos personales	15
1.2.7	Evolución del derecho a la protección de datos	15
1.2.8	Objeto del Reglamento General de Protección de Datos	16
2	CAPÍTULO II.....	16
2.1	ESTUDIO DE CAMPO	16
2.1.1	Metodología de investigación	16
2.1.2	Métodos de Investigación	17
2.1.2.1	Método de análisis histórico y el lógico	17
2.1.2.2	Método deductivo e inductivo	17
2.1.2.3	Método Análisis y Síntesis	18
2.1.3	Técnicas – Instrumentos de investigación	19
2.1.3.1	Observación.....	19
2.1.3.2	La entrevista	19
2.1.3.3	Encuesta.....	20
2.1.3.4	Población	21
2.1.3.5	Muestreo.....	21
2.1.4	Resultados de la investigación de campo.....	22
2.1.4.1	Entrevista.....	22

2.1.4.2	Encuesta a Docentes	25
2.2	Análisis de resultados	31
CAPÍTULO III.....		32
3	DESARROLLO DE LA PROPUESTA	32
3.1	Antecedentes.....	32
3.1.1	Reseña Histórica de la Universidad Laica “Eloy Alfaro de Manabí” Extensión El Carmen	32
3.1.2	Misión.....	33
3.1.3	Visión	33
3.2	Organigrama.....	34
3.3	Programa de Auditoria	34
3.4	Informe de Auditoria.....	35
3.4.1	Dirigido a:	35
3.5	Objetivo	35
3.6	Personal relacionado	36
3.7	Alcance	36
3.8	Definir Activos.....	37
3.9	Definir Riesgos	38
3.9.1	Diseño de instrumentos.....	39
3.9.2	Tabulación.....	40
3.10	Hallazgos.....	42

3.11	Conclusiones de la Auditoría	46
3.12	Recomendaciones de la Auditoría	46
4	CONCLUSIONES	47
5	RECOMENDACIONES.....	47
6	Bibliografía.....	48
	INTRODUCCIÓN.....	64
	Objetivos.....	64
	Anexo B: GUÍA DE ENTREVISTA PARA DOCENTES.....	68
	ENTREVISTA.....	68
	ENCUESTA A DOCENTES.....	70

ÍNDICE DE TABLAS

Tabla 1 Encuesta a Docentes

Tabla 2 Resultado de la encuesta realizada a Docentes

Tabla 3 Programa de auditoría

Tabla 4 Definición de activos

Tabla 5 Datos públicos y privados

Tabla 6 Tipo de amenazas

Tabla 7 Matriz Probabilidad-Peligro

Tabla 8 Matriz de riesgos resultados

Tabla 9 Causas de riesgo Phishing

Tabla 10 Causas riesgos Virus

Tabla 11 Causas riesgos Rasomware

Tabla 12 Guía de buenas prácticas riesgo Phishing

Tabla 13 Guía de buenas prácticas riesgo Virus

Tabla 14 Guía de buenas prácticas riesgo Rasomware

ÍNDICE DE ILUSTRACIONES

Ilustración 1 Origrama de la Uleam

Ilustración 2 Formato cuestionario políticas

Ilustración 3 Formato cuestionario políticas por riesgo

Ilustración 4 Formato de datos para la tabulación de Excel

Ilustración 5 Nivel de riesgo Phishing

Ilustración 6 Nivel de riesgo Virus

Ilustración 7 Nivel de riesgo Rasomware

Ilustración 8 Tabulación evaluación de riesgos fisicos

Ilustración 9 Tabulación evaluación de riesgos general.

RESUMEN

La Auditoría en informática se refiere a la revisión práctica que se realiza sobre los recursos informáticos con que cuenta una entidad con el fin de emitir un informe o dictamen sobre la situación en que se desarrollan y se utilizan esos recursos. (Bautista & Aguirre, 2016)

Hoy por hoy en la Extensión El Carmen existe un control inapropiado de los datos personales que manejan los docentes, la causa más destacada es la falta de información sobre los riesgos, teniendo así vulnerabilidad en sus dispositivos, considerando una población de 68 docentes que se encuentra trabajando en la extensión, tomando una muestra discrecional de 19 docentes, por falta de disponibilidad. La presente investigación fue realizada en el período lectivo 2022(1) teniendo como objetivo realizar un análisis de riesgos para la protección de datos personales en los docentes de la Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen justificando si los docentes tienen control sobre el manejo de información personal en el acceso a la aplicación WhatsApp.

En esta auditoria se aplicaron dos métodos, inductivo y deductivo para poder comprender a que se enfrentan los docentes habitualmente basándose en una secuencia de hechos y así poder llegar a una conclusión general. Se aplicó la metodología ISO 27001 identificando riesgos, vulnerabilidades, amenazas para así poder tener una evaluación de riesgos apropiada dirigida a los docentes.

SUMMARY

The Computer Audit refers to the practical review that is carried out on the computer resources available to an entity in order to issue a report or opinion on the situation in which these resources are developed and used. (Bautista & Aguirre, 2016)

Today in the El Carmen Extension there is an inappropriate control of the personal data handled by teachers, the most prominent cause is the lack of information about the risks, thus having vulnerability in their devices, considering a population of 68 teachers who are working in the extension, taking a discretionary sample of 19 teachers, due to lack of availability. The present investigation was carried out in the 2022(1) school period with the objective of carrying out a risk analysis for the protection of personal data in the teachers of the Laica Eloy Alfaro University of Manabí Extension El Carmen justifying whether the teachers have control over the management of personal information when accessing the WhatsApp application.

In this audit, two methods will be applied, inductive and deductive, in order to understand what teachers will face very broadly in a sequence of events and thus be able to reach a general conclusion. The ISO 27001 methodology was applied, identifying risks, vulnerabilities, threats in order to have a risk assessment appropriately addressed to teachers.

INTRODUCCIÓN

En la actualidad mantener resguardada la información de una persona haciendo caso omiso al derecho a la privacidad y reputación resulta una tarea complicada. La tecnología nos permite llevar el control de nuestros datos mediante dispositivos móviles o de escritorio, por eso se necesita tomar en cuenta diferentes áreas de seguridad que son primordiales para mantener la seguridad en datos personales.

Este impulso tecnológico hace que las personas se responsabilicen íntimamente, aceptando que analizar riesgos es un área importante en la seguridad de datos personales. A través de este análisis tomar decisiones que beneficien la seguridad de los datos. Por otro lado, cada persona controla sus datos como mejor le parezca, pero es necesario considerar evaluar los riesgos.

La ley generalmente va a la defensa de la realidad de que se necesitan normas positivas para regularla, y eso no parece cambiar. Sin embargo, en lo que respecta a los derechos de protección de datos personales, asistimos a una regulación progresiva, rápida y cada vez más sofisticada. Este fenómeno se produce tanto a nivel nacional como europeo y, más concretamente, a nivel internacional. En el contexto de la protección de datos, esto no tiene nada de especial, aunque sí es difícil partir de su pleno desarrollo (todo lo que lo rodea ha sido regulado en detalle y en profundidad solo en las últimas dos décadas), hoy en día sin duda, nuestro derecho (Estado y comunidad) cuenta con una disposición que permite identificar soluciones justas a los problemas que se presentan en beneficio de todos los ciudadanos (Cazurro, 2020).

Es por eso por lo que la seguridad informática es más importante en la vida diaria de las personas que buscan soluciones diarias de problemas que se presentan. Por lo presente, en la Extensión el control inadecuado de datos personales por parte de los docentes es una de las causas más destacadas con la desinformación que existe, tomando en cuenta la cantidad de docentes

laborando en la extensión. Por esa razón esta investigación tiene como intención realizar un análisis de riesgos en la protección de datos personales en docentes de la “Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen” aplicando la metodología ISO 27001 siendo relevante a la seguridad de la información en la preservación de confidencialidad, integridad, y disponibilidad. Evidenciando si los docentes tienen control sobre sus datos personales principalmente en la aplicación WhatsApp.

A continuación, tenemos un documento investigativo estructurado por tres capítulos; el primer capítulo, muestra la investigación soportada de manera teórica con bibliografía actualizada con temas referentes a lo que se usa en este trabajo, el segundo capítulo, nos muestra un diagnóstico de la situación de los docentes en cuanto a la protección de datos y la cual nos da una visión de que se debe hacer una auditoría partiendo de una muestra discrecional de 19 docentes los que contestaron las encuestas digitales. Como ultimo capitulo encontramos la auditoria informática orientada en protección de datos personales basada en la metodología Magerit, estudiando las vulnerabilidades de cada docente y finalmente brindar recomendaciones para mejorar el control, mediante una guía que puede ser aplicada y usada para proteger el uso de los datos de los docentes, por último, se cierra este trabajo con la bibliografía citada en algunos pasajes de la investigación.

1 CAPÍTULO I

1.1 MARCO TEÓRICO

1.1.1 Introducción a la Auditoría Informática

En la actualidad se utilizan dos metodologías para la evaluación de sistemas: Análisis de riesgos y Auditoría informática, lo que implica dos enfoques distintos. Por una parte, la auditoría informática solo identifica el nivel de “exposición” por la falta de controles, mientras que el análisis de riesgos facilita la evaluación de los riesgos para tomar medidas preventivas.

Este libro se dedica al estudio de la auditoría de la seguridad informática. Estudian los virus y otros códigos dañinos, que constituyen una de las principales amenazas para la seguridad de los sistemas informáticos. Aportando los contenidos necesarios para que el lector pueda adquirir las siguientes capacidades profesionales: Analizar y seleccionar las herramientas de auditoría y detección de vulnerabilidades del sistema informático, implantando aquellas que se adecuen a las especificaciones de seguridad informática. (Vieites, 2015)

El trabajo de grupos informáticos está extendido básicamente a la totalidad de organizaciones, negocios, y domicilios. Los conjuntos informáticos intervienen de forma bastante fundamental en la entrega de productos y servicios de una empresa. En varios casos, los grupos informáticos ejecutan aplicaciones que manejan información fundamental, como datos financieros (números de cuentas de banco, saldos, o facturación), o datos de carácter estratégico (planes de negocio e inversión, nuevos productos, entre otros).

En la actualidad es extraña la vida de cualquier proceso, en cualquier entorno de la compañía, que no sea organizado y desarrollado por medio de sistemas informáticos. Las aplicaciones informáticas en el proceso de auditoría ayudan sin ni una duda al estudio de cada una de las zonas, desarrollando labores de comprobación y de síntesis para que ni una quede sin examinar.

1.1.2 Definición a la Auditoría Informática

La auditoría es el análisis exhaustivo de los sistemas informáticos con la finalidad de detectar, identificar y describir las distintas vulnerabilidades que puedan presentarse. En el momento de desempeñar las funciones de auditoría en un sistema de información, los auditores deben cumplir una serie de normas éticas y un código deontológico para cumplir con profesionalidad y rigidez sus objetivos. (Tejada, 2015)

El proceso de auditoría es identificado actualmente como válido para un amplio espectro de entornos. Y para atender a las especificidades de todos dichos entornos se han desarrollado diversos tipos de auditoría: auditoría médica, auditoría medioambiental, auditoría informática, auditoría administrativa, auditoría de calidad. La auditoría se puede clasificar básicamente en 2 tipos: de conformidad y consultiva

- **La auditoría de conformidad** se aplica a puntos sobre los cuales hay reglas y métodos establecidos o pactados y se basa en revisar si estas reglas permanecen siendo seguidas.
- **La auditoría consultiva** tiene interacción con esfuerzos de evaluación de puntos respecto a los cuales no hay reglas externas de obligado cumplimiento. (Carvalho, 2012)

La auditoría no es la investigación fría de las cifras de los estados financieros de una organización o entidad; en ella también se analizan las cualidades de las cifras rubro por rubro de los estados financieros, y se estudia qué tanto influyen en la decisión de las cifras el caso administrativo y la parte operativa de la compañía, si es de producción, o la parte operativa de los servicios, una vez que evaluamos una compañía de servicios. La investigación y análisis de estas ocupaciones tanto administrativas como operativas. (García M. G., 2015)

1.1.3 Objetivos de la Auditoría Informática

Uno de los objetivos es conocer las innovaciones en ataques y vulnerabilidades más actuales en materia informática, haciéndonos más prevenidos y realizar acciones totalmente seguras.

Los criterios que tienen que ser considerados como base para la definición de los objetivos de la auditoría, deberán estar continuamente enfocados a ayudar a los miembros de la organización en el funcionamiento de sus ocupaciones y a asegurar el buen desempeño administrativo y operativo de esta. Éstos tienen la posibilidad de ser: control, productividad, organización, servicio, calidad o hasta para facilitar la toma de decisiones. (Chavarría, 2015)

La finalidad de esta guía es que el auditor documente el razonamiento de la entidad y su ámbito de forma correcta en el proceso de Planificación y que este entendimiento sea conservado y actualizado en cada auditoría, con el objeto de hacer una correcta identificación y evaluación de peligros de error material en los estados financieros.

1.1.4 Técnicas de la Auditoría Informática

Las normas técnicas sobre la ejecución del trabajo, que hacen referencia a la preparación y ejecución del trabajo a realizar por el auditor de cuentas, regularán el conjunto de técnicas de investigación e inspección aplicables a partidas y hechos relativos a los documentos contables sujetos a examen, mediante los cuales el auditor fundamenta su opinión responsable e independiente. (Comamala, 2015)

No continuamente es viable tener plenamente controlados todos los procesos que se desarrollan en un sistema para eludir la aparición de incidentes. Una vez que dichos aparecen, lo primordial es saber qué causa el problema y cómo solucionarlo. Para eso, hay determinadas técnicas que tienen la posibilidad de beneficiar en esta labor. La administración de incidentes se puede enfocar de dos maneras diferentes:

- a) Administración de inconvenientes reactiva. En ella se examina el incidente para saber su causa y plantear una solución.
- b) Administración de inconvenientes proactiva. En ella se monitoriza y examina el sistema con el objetivo de prevenir los incidentes. (Urbano, 2015)

1.1.5 Las Etapas de la Auditoría Informática

Toda auditoría constituye un proceso crítico y sistemático, lo cual significa que todos los auditores siguen ciertos pasos establecidos con anterioridad en su examen, por medio de los cuales tienen la posibilidad de mirar puntos de vista bastante finos de todas las ocupaciones que se hacen en la organización u organización que están auditado los periodos habituales de una auditoría son:

- a) **Planeación de la auditoría.** La primera actividad de un auditor es recabar todos los documentos internos referentes a políticas establecidas y normas que deben acatarse.
- b) **Realización de la auditoría.** En este punto, el auditor observa y verifica la forma en la que se realizan las actividades de manera cotidiana, por lo que requiere de la colaboración de todo el personal del área auditada.
- c) **Análisis de los datos recabados y de las condiciones observadas.** Una vez que el auditor concluyó en forma exhaustiva la etapa 2, analiza a fondo todos los datos recabados y compara los resultados contra estándares generalmente aceptados.
- d) **Elaboración de un informe escrito y emisión de una opinión.** La última etapa, después de que el auditor ha realizado un análisis a fondo de los datos obtenidos, es emitir una opinión, la cual puede estar orientada en cuatro sentidos: Opinión limpia, Opinión Negativa, Opinión adversa y sin opinión. (Baca, 2016)

La legislación vigente sobre la materia (LOPD y RDLOPD) nada establece expresamente relacionadas con las múltiples etapas por las que atraviesa una Auditoría de seguridad de datos. Por esto los autores consideramos eficaz continuar el esquema que dirigiría cualquier Auditoría, describiendo desde luego esas particularidades de la Auditoría de estabilidad de datos particulares que tienen la posibilidad de implantar un criterio diferenciador de otros tipos de Auditorías. (Marzo P. A., 2015)

1.1.6 Tipos de Auditoría Informática

Basado en las definiciones y precedentes observados, observamos que casi todo es auditable; o sea, verificable basado en las diversas posiciones que se le apliquen a lo inspeccionado; es fundamental resaltar lo próximo: varias de estas auditorías necesitan conjuntos multidisciplinarios, es decir, no son 100% preponderantes del quehacer de un contador, sino que se necesitan ingenieros, químicos, físicos, abogados, administradores y otros más. (Tapia, Mendoza, & Castillo, 2019)

“La monitoria del desempeño busca conocer el funcionamiento del sistema de garantía de calidad con el fin de identificar sus desviaciones y poder corregir el rumbo a tiempo. Para esto se requiere de dos grandes procesos:

- *La evaluación persistente del funcionamiento en términos de la calidad esperada por medio de estándares conocidos o predeterminados.*
- *Revisión de la calidad y corrección de las desviaciones encontradas en la evaluación para arrimar los procesos a los estándares anteriormente ubicados.*

Dichos 2 elementos son inseparables en un sistema de garantía de calidad y, por consiguiente, en un modelo de evaluación o auditoría de la calidad. Las auditorías, dependiendo de los objetivos, se pueden dividir en tres tipos.

- a) **Auditoría interna.** Es aquella auditoría de calidad elaborada e implementada por la misma organización para conocer el desarrollo e utilización de sus propios procesos y cambiar o afirmar el sistema según los resultados.
- b) **Auditoría externa.** Es aquella auditoría que ejecuta una organización a otra a sus contratistas o proveedores para comprobar el desarrollo e utilización de sus planes de calidad.
- c) **Auditoría de certificación.** Esta es la auditoría desarrollada por una organización experta y reconocida para el impacto, nacional o internacionalmente, sin vínculos con la organización auditada ni con sus proveedores o consumidores, con el propósito de revisar y calificar el nivel de desarrollo e utilización del sistema de calidad y su ajuste a las reglas legales o de todo el mundo de calidad”. (Álvarez, 2016)

1.1.7 El auditor de Auditoría Informática

Es común que una persona, que tiene el deber de cuidado, sea responsable por los actos de los individuos bajo su supervisión. En muchas situaciones los

contadores públicos cumplen sus deberes gracias a auxiliares. Bajo el supuesto de acuerdo con el cual el contador debería supervisar sus auxiliares y adoptar los correctivos necesarios, frecuenta hacérsele responsable de las secuelas de los actos de sus dependientes. (Bermúdez, 2016)

Una de las preguntas más polémicas que se expone en el momento de hacer la Auditoría de medidas de estabilidad, es la de establecer quién podría ser considerado auditor legítimo acorde a la legislación vigente para desempeñar tal tarea, ya que, así como para los auditores de cuentas existe un censo oficial, no existe ningún registro oficial de los expertos que logren desempeñar labores conocidas como “auditor informático” o “auditor de estabilidad de los sistemas de información”.

El auditor informático es el individuo delegado de hacer una auditoría informática. En la actualidad no existe legislación sobre los requisitos que debería llevar a cabo el auditor para realizar su trabajo, ni sobre los instrumentos y métodos que debería usar para llevarlo a cabo. La figura del auditor no está regulada y no existe legislación al respecto. Se sobrentiende que el auditor debería ser una persona capacitada con los conocimientos necesarios para hacer auditorías de sistemas informáticos en las organizaciones.

El proceso de auditoría con lleva un trabajo en grupo en el cual algunas personas tienen que actuar de manera conjunta y coordinada. Esto continuamente implica cualquier tipo de problema, aun cuando no continuamente tiene porqué significar algo malo. Si se saben manejar bien, la realidad de inconvenientes es un indicador fiable de que el conjunto está funcionando. La clave es enfocar el problema a partir de la perspectiva de la viable solución del mismo. (Chaparro, 2016)

1.1.8 Herramientas de la Auditoria Informática

Los auditores de seguridad informática, para desarrollar sus labores y buscar probables fallos y amenazas del sistema de información, muchas veces se

apoyan en herramientas que analizan todos los diversos puntos de la auditoría. Gracias a la extensa variedad de vulnerabilidades existentes, los instrumentos encargados de su detección y estudio son numerosos y variadas. Para ello, hay dos herramientas fundamentales: ping y traceroute.

- a) **Herramienta Ping:** El nombre de la herramienta ping nace de packet internet groper (rastreador de paquetes de red) y se puede usar en cualquier sistema operativo accediendo por medio de comandos. Se usa básicamente para verificar la calidad y la rapidez de una red definida y para verificar la latencia entre 2 grupos.
- b) **Herramienta traceroute:** La herramienta traceroute se usa para continuar la ruta de los paquetes en una red IP y el retardo que se genera en este tránsito. Se puede usar en diversos sistemas operativos, sin embargo, se debe tener en cuenta que en Microsoft Windows esta herramienta se denomina tracert. En Linux, se realiza el comando traceroute en la consola de comandos y, en Windows, se escribirá el comando tracert en la ventana de MS-DOS que nace al redactar cmd en el signo del sistema. (Tejada, 2015)

1.1.9 Metodología de Auditoría Informática

Según el Anexo A de la Norma UNE-EN-ISO 14001:2015, siempre que sea viable, los auditores deber ser independientes de la actividad auditada y, en todos los casos, deben actuar libre de sesgo y conflicto de intereses

- a) **Planificación de la auditoría interna y externa.** En primer lugar, es primordial entablar un contacto inicial con el auditado. Este contacto puede desarrollarse de forma formal o informal y debería realizarlo continuamente el jefe del equipo auditor.
- b) **Programa de auditoría.** Según la Regla ISO 19011:2011, un programa de auditoría es el grupo de una o más auditorías planificadas para un lapso de tiempo definido y dirigidas hacia un objetivo específico. Puede integrar auditorías de uno o más sistemas de administración, ya sean llevadas a cabo por separado o en conjunción. (Grijalbo, 2017)

La metodología del curso se fundamenta en el trabajo individualizado del temario con el material didáctico postulado, independientemente de la modalidad de impartición escogida. Por otro lado, el propósito importante de este trabajo será poder contribuir a ejercer el razonamiento teórico práctico adquirido al entorno profesional, por lo cual va a ser preciso enfocar el análisis a tal fin. Hablamos de una iniciativa especialmente práctica basada en el autoaprendizaje, de forma

que el estudiante va a poder conseguir las metas didácticas a su propio ritmo. (Chaparro, 2016)

Las únicas metodologías que tenemos la posibilidad de descubrir en la auditoría informática son 2 familias diversas: las auditorías de controles en general como producto estándar de las compañías auditoras expertos, que son una homologación de las mismas a grado universal, y las metodologías de los auditores internos. El propósito de las auditorías de controles en general es “dar una crítica sobre la confiabilidad de los datos del ordenador para la auditoría financiera. (Piattini, 2015)

1.1.10 Aplicación de la Auditoria Informática

La auditoría es aplicable a cualquier tipo de organización debido a que, sin que importe el estilo de gestión, los procesos o lineamientos que se continúen son sujetos a una revisión. Se puede utilizar primordialmente a empresas privadas, públicas o sociales. Son esas que funcionan con capital de particulares y, por consiguiente, sus objetivos son primordialmente lucrativos. En estas organizaciones la auditoría se hace con el fin de hacer más eficientes sus procesos administrativos y operativos para aumentar sus utilidades. (Chavarría, 2014)

1.1.11 Seguridad Informática

Las tecnologías de la información y comunicación (TIC) y precisamente la informática se ha instalado en todos los ámbitos de la sociedad; sanidad, educación, finanzas, prensa, etc. La seguridad informática se apoya en garantizar que los recursos del sistema de información de una organización sean usados de forma que se decidió y que la entrada a la información ahí contenida, así como su modificación, solo sea viable a los individuos que estén acreditadas y en los límites de su autorización. (Santos, 2015)

Uno de los activos más importantes para cualquier compañía es la información que maneja. La información es el grupo de datos que da sentido a una

organización, datos que la definen, datos con los que labora y datos que, en manos inadecuadas, tienen la posibilidad de llevar a la misma a la ruina. La seguridad informática, es una especialidad en el campo de la seguridad de la información que trata de defender la información que usa una infraestructura informática y de telecomunicaciones para ser almacenada o transmitida.

1.2 Protección de datos de carácter personal

Es un derecho importante del individuo que sus datos personales se traten de forma leal y lícita, para finalidades específicas y con su consentimiento o sobre otra base de legitimación del procedimiento, a entrar y rectificar sus datos, así como a ejercer los demás derechos.

Una vez que nos enfrentamos a una rama del Derecho tan especializada y novedosa como la protección de los datos personales", es adecuado determinar y definir los conceptos básicos sobre los que asienta esta disciplina jurídica. Al igual que en el Derecho Penal los conceptos de bien jurídico salvaguardado o conducta tradicional son nucleares para lograr comprender la materia, con la finalidad de una mejor comprensión de la regulación objeto de análisis. (Ayjón, 2020)

Conviene partir de la base de que la normativa europea que, hasta la llegada del Reglamento Europeo, regía en el continente europeo databa de 1995 fecha en la que, realidades como las Redes Sociales, el Big Data o el Cloud Computing, entre otros, no existían o, por lo menos, no con el valor y efecto del que disfrutaban actualmente. Es de esta forma que el Reglamento Europeo pretende abordar el efecto de las novedosas tecnologías, incrementar la transparencia para los interesados y reforzar el control de los individuos sobre sus propios datos. (Davara, Davara, & Davara, 2020)

Ya nos hemos acostumbrado a ver a diario imparables y vertiginosos avances tecnológicos que pueden, y tienen que, servir para mejorar la calidad de vida de las personas, logrando citar, entre otros, ejemplos como las aplicaciones para

todo, y en particular para la salud, las aplicaciones con objetivos educativos, los aún novedosos vestibles, el expediente clínico electrónico o inclusive los dispositivos de papel electrónico que permitan un futuro medioambiental sustentable.

1.2.1 Antecedentes

Es una situación constatada que las reglas emergen como resultado de una necesidad social, lo cual hace del derecho una fórmula de resolver conflictos, ya sean estos personales o colectivos. La necesidad de una regulación jurídica al respecto de la protección de datos no surge hasta que su uso podría ser lesivo de derechos. (Rebollo, 2014)

1.2.2 Principios de la calidad de los datos

Con los avances tecnológicos y la transformación digital, ha crecido la necesidad de utilizar y reutilizar los datos en los entornos más diferentes, aun habiendo sido definidos para un objetivo específico. Esto impone a redefinir la iniciativa de calidad de datos a partir de una “adecuación al uso” a una “adecuación a los usos”. Por consiguiente, está cambiando la manera de notar el valor y utilidad de la calidad de datos; que debería ser adaptada a diferentes entornos de uso y a diferentes sectores industriales. (Gómez, Gualo, & Muñoz, 2018)

En los últimos años se viene enfatizando la importancia de los datos, y se han generalizado expresiones como: “los datos son la nueva moneda”, “los datos son el nuevo petróleo”, “los datos son la mina oculta”, etc. La verdad es que “los datos electrónicos desempeñan un papel importante en la sociedad de las TIC”. De hecho, la transformación digital que está perjudicando a todos los sectores, a partir de la agricultura, la industria, el turismo, la sanidad, etc. Convirtió a los datos en el habilitador más potente de cualquier tipo de organización. (Gualo, Gómez, & Caballero, 2019)

Se han identificado 8 principios de la calidad como un marco de referencia hacia la optimización del funcionamiento de una organización. Sus fines son servir de

ayuda para que las Empresas puedan un triunfo sostenido. Dichos principios los puede usar la dirección de la organización como un marco de referencia para dirigir a sus dependencias en la consecución de la mejora del desempeño y se derivan de la experiencia colectiva y el conocimiento de los expertos internacionales:

- a) **Enfoque al cliente:** Las organizaciones dependen de sus clientes y por lo tanto deberían comprender las necesidades actuales y futuras de los mismos, satisfacer los requisitos por ellos impuestos y esforzarse en exceder también sus expectativas.
- b) **Liderazgo:** Los líderes establecen la unidad de propósito y la orientación de la organización. Ellos deberían crear y mantener un ambiente interno en el cual el personal pueda llegar a involucrarse totalmente en el logro de los objetivos de la organización.
- c) **Participación del personal:** El personal, a todos los niveles, es la esencia de una organización, y su total compromiso posibilita que sus habilidades sean usadas para el beneficio de la organización.
- d) **Enfoque basado en procesos:** Un resultado deseado se alcanza más eficientemente cuando las actividades y los recursos relacionados se gestionan como un proceso.
- e) **Enfoque de sistema para la gestión:** Identificar, entender y gestionar los procesos interrelacionados como un sistema contribuye a la eficacia y eficiencia de una organización en el logro de sus objetivos.
- f) **Mejora continua:** La mejora continua del desempeño global de la organización debería ser un objetivo permanente.
- g) **Enfoque basado en hechos para la toma de decisión:** Las decisiones eficaces se basan en el análisis de los datos y la información.
- h) **Relaciones mutuamente beneficiosas con el proveedor:** Una organización y sus proveedores son interdependientes, y una relación mutuamente beneficiosa aumenta la capacidad de ambos para crear valor. (Hincapie, Salcedo, & Ortíz, 2018)

1.2.3 Principio de Información

El derecho de información en la recogida de datos está regulado en el artículo 5 de la LOPD. Por su lado, el Reglamento UE lleva a cabo la transparencia de la información, la comunicación y posibilidades de ejercicio de los derechos del interesado en su artículo 12. El deber de información anterior al procedimiento de datos de carácter personal pertenece a los derechos básicos y primordiales de los habitantes contenidos en la LOPD y el Reglamento Europeo. Por consiguiente, si se van a registrar e intentar datos de carácter personal, va a ser

primordial informar por medio del medio que se use para la recogida. (Pérez, 2017)

Este principio involucra el deber y el derecho de información. Implica que antes de tratar los datos personales habrá que informar al paciente sobre quién los tratará y para que, además se debería informar sobre la identidad y dirección del responsable del procedimiento. Al respecto, SANCHEZÍCARO y ABELLÁNÍ”, definen al principio de información, diciendo que el afectado ha de estar informado sobre los datos que se recaban sobre él, conociendo esencialmente quién, cómo y para qué se tratan sus datos. (Cristea, 2018)

1.2.4 Los tipos de datos personales

Generalmente, la mayoría de las regulaciones sobre defensa de datos, incluida la de España, han desarrollado un sistema parecido de garantías con propiedades y técnicas concretas que surgieron al inicio como contestación a las amenazas derivadas del uso de la tecnología. Entre ellos tenemos datos públicos y privados, además personalización y anonimato. (Oró, 2015)

1.2.5 Ley orgánica de protección de datos

La protección de las personas físicas relacionadas con el procedimiento de datos personales es un derecho importante. Nuestra Constitución ha sido pionera en el reconocimiento del derecho importante a la custodia de datos particulares una vez que dispuso que “la ley limitará la utilización de la informática para asegurar el honor y la intimidad personal y familiar de los habitantes y el pleno ejercicio de sus derechos”. Internet, por otro lado, se convirtió en una realidad omnipresente tanto en nuestra vida personal como colectiva. Una parte importante de nuestra actividad profesional, económica y privada se lleva a cabo en la Red y consigue una trascendencia importante como para la comunicación humana como para el desarrollo de nuestra vida en sociedad. (Piñar, 2019)

1.2.6 Derechos a la protección de datos personales

Generalmente, la mayoría de las regulaciones sobre protección de datos, incluida la de España, han desarrollado un sistema parecido de garantías con propiedades y técnicas concretas que surgieron al inicio como contestación a las amenazas derivadas del uso de la tecnología. No obstante, mientras en las comunidades modernas aparecían maneras cada vez más sofisticadas de coacción, derivadas del abuso de poder que otorga la acumulación indiscriminada de información personal, el derecho a la custodia de datos ha evolucionado hasta transformarse en una garantía democrática. (Oró, 2015)

La inquietud, por la recolección de datos personales y sobre la pérdida de su control surge paralelamente en que el desarrollo tecnológico permitió la automatización del procedimiento de los datos personales. James Martin describía como, en la sociedad de las telecomunicaciones, los humanos tenemos la posibilidad de sentirnos como osos polares a los que se les haya conectado un radiotransmisor en miniatura con capacidad para mandar sucesivas señales a un satélite, que podrán ser registradas y seguidas a partir de un ordenador. Puesto que, la informática puede hacer nuestras propias vidas tan visibles para quienes controlan los gigantes bancos de información personal como los son para nosotros mismos los peces de colores que poseemos en una pecera. (Domínguez, 2016)

Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. En especial, cabe resaltar la referencia a los derechos de ingreso y rectificación, que son los fundamentales. En ventaja del derecho de ingreso cualquiera puede dirigirse a un responsable del procedimiento, público o privado, para confirmar si trata o no sus datos personales.

1.2.7 Evolución del derecho a la protección de datos

Si queremos saber cómo y cuándo se gestó lo que hoy sabemos por "privacidad" hemos de remontarnos a finales del siglo XIX y situarnos en USA. Es ahí donde

empezó a tenerse una idea legal de derecho a la intimidad, por medio del tiempo, acabaría tomando la manera del derecho a la intimidad tal y como lo conocemos hoy. (Cazurro, 2020)

1.2.8 Objeto del Reglamento General de Protección de Datos

Instituye las normas relativas a la protección de las personas físicas en lo cual respecta al procedimiento de los datos particulares las reglas relativas a la independiente circulación de tales datos. Salvaguarda los derechos y libertades primordiales de los individuos físicas y, en especial, su derecho a la custodia de los datos personales. (Burzaco, 2020)

El objeto de la LOPD es asegurar y defender, en lo cual concierne al tratamiento de los datos particulares, las libertades públicas y los derechos primordiales de los individuos físicas, y en especial de su honor e intimidad personal y familiar.

2 CAPÍTULO II

2.1 ESTUDIO DE CAMPO

2.1.1 Metodología de investigación

La metodología de investigación se denomina el conjunto de procedimientos y métodos de manera organizada para procesar la información, que el investigador busca, decidir y analizar los datos obtenidos, que sirven para alcanzar, otorgar y dar validez, para poder luego dar solución los fines de la investigación (Vera, 2015)

La metodología lleva a cabo el papel de ordenar, se fundamenta en los métodos, como sus caminos y estos en las técnicas como los pasos para transitar por aquellos caminos del pensamiento a la verdad y a la inversa. El método constituye a la vez un orden y un proceso cuya culminación es la obra de leyes, teorías y modelo. (Paz G. M., 2014)

Se aplicó la metodología ISO 27001 puesto que el mismo estándar, se considera más relevante la seguridad de la información en la preservación de confidencialidad, integridad, y disponibilidad, así como los sistemas implicados en su tratamiento, dentro de la institución.

2.1.2 Métodos de Investigación

2.1.2.1 Método de análisis histórico y el lógico

El método histórico estudia la trayectoria real de los fenómenos y acontecimientos en el transcurrir de su historia. El método lógico investiga las leyes en general de manejo y desarrollo de los fenómenos. Lo lógico no repite lo histórico en todos sus detalles, sino que reproduce en el plano teórico lo más relevante del fenómeno, lo cual constituye su esencia. (García D. J., 2016)

El análisis de la trayectoria histórica del objeto crea, premisas importantes para una comprensión más intensa de su esencia; por esto, una vez exitosa la historia del objeto es necesario volver a conceptualizar nuevamente su esencia, arreglar, terminar y desarrollar los conceptos que la manifiestan. (Santiesteban, 2014)

En el marco teórico se hizo una separación entre variable dependiente e independiente declaradas en el análisis. Por consiguiente, se analizó el proceso del desarrollo de la auditoría informática, con la respectiva revisión de cada una de sus fases por separado. Asimismo, se estudió el resultado de la auditoría para reconocer los distintos peligros pueden encontrarse y como evitar dichos peligros.

2.1.2.2 Método deductivo e inductivo

La inducción es un tipo de argumento en el cual está establecido un criterio general desde el estudio de hechos o fenómenos particulares. Es preciso hallar la interacción de propiedades habituales entre cada caso especial, o sea, parte de lo general a lo especial. La deducción es el método racional que posibilita describir hechos particulares desde su incorporación o categorización en un

entendimiento general, llámese teoría, ley, postulado o hipótesis, la cual ya fue comprobada. (Monroy & Nava, 2018)

El método Deductivo se realiza tomando como motivo ciertos principios o conocimientos en general que son aplicables para deducir conclusiones particulares en el área. El método Inductivo estima una secuencia de fenómenos o conocimientos particulares para llegar a conclusiones generales. (Baquero, 2015)

Este método permitió hacer un análisis específico del comportamiento del sistema, examinando el panorama en el cual se desenvuelve el mismo, implementando la auditoría informática para analizar los peligros que logren existir y cómo tienen la posibilidad de solucionar.

2.1.2.3 Método Análisis y Síntesis

Estos dos métodos teóricos cumplen funcionalidades relevantes en la Indagación Científica. Por una parte, el análisis es un procedimiento teórico por medio del cual un todo complejo se descompone en sus distintas partes y cualidades. Por otro lado, la síntesis establece mentalmente la unión en medio de las partes previamente analizadas y permite hallar las interacciones fundamentales y propiedades en general entre ellas. (Santiesteban, 2014)

Análisis y síntesis son dos actividades simétricamente contrapuestas, el análisis significa disolución, descomposición en partes, sin embargo, la síntesis compone o forma un todo con recursos varios. En la síntesis sin embargo se parte de recursos diferentes, el motivo halla sus interacciones y se acaba con la integración de los elementos en un solo grupo o sistema conceptual. (Baena, 2017)

Este método es considerado como una actividad que se debería de hacer de forma elemental, cuando se ha definido el problema a investigar. Tiene que ver con la investigación sistemática de lo cual se pudo indagar en relación con un

asunto. Para lo que se ha trabajado con el procedimiento teórico análisis síntesis de lo estudiado en el marco teórico, una vez analizadas las variables declaradas.

2.1.3 Técnicas – Instrumentos de investigación

2.1.3.1 Observación

Pertenece a los primeros procedimientos científicos usados en la investigación y se usa para la obtención de información primaria sobre los objetos investigados o para la comprobación experimental de las hipótesis. La observación científica es sistemática, consciente y objetiva. Es un método de gran trascendencia debido a que posibilita la explicación auténtica de conjuntos sociales y escenas culturales que tienen la posibilidad de ser usadas para la especificación, evaluación e interpretación en el campo en que se lleva a cabo. (Chávez, 2019)

Hay diferentes tipos de observación, dependiendo del nivel en que el científico se implica con lo visto, poseemos observación fácil: no regulada, participante y no participante. La mayoría de nuestros propios conocimientos los obtenemos de una observación no regulada, así sea con colaboración o a falta de ella. (Paz G. B., 2017)

2.1.3.2 La entrevista

La entrevista es una técnica de colección de información por medio de una plática profesional. Además de adquirirse datos acerca de lo cual se investiga, la entrevista engloba gran trascendencia a partir de la perspectiva educativa y formativa para el investigador. Los resultados a conseguir en la tarea dependen en gran medida del grado de comunicación entre el investigador y los participantes en la misma. (Blanco, 2015)

Esta técnica de investigación permite tener un enfoque concreto con el tipo de información que se va a estudiar a través de un marco de consulta social, el intercambio de información oral entre dos o varias personas, con el fin de garantizar una mejor comprensión del tema de estudio extrayendo información significativa. (Feijóo, 2016).

La entrevista es una técnica en la que una persona (entrevistador) solicita información de otra o de un conjunto para obtener datos acerca de un problema definido. Hay diversos tipos de entrevista, en medio de las cuales las más comunes son: la entrevista semiestructurada para obtener información específica por medio de un guion que da cierta flexibilidad, entrevista focalizada es un tipo de entrevista con ausencia de dirección que progresa a partir de preguntas abiertas hasta preguntas cada vez más estructuradas, entrevista en profundidad una serie de conversaciones libres en las que el investigador parte de un objetivo explícito. Otro modo de entrevista es la entrevista centrada en el problema, por medio de una guía de entrevista que añade preguntas y estímulos narrativos es viable recoger datos biográficos en relación a cierto problema. (Valenzuela, 2017)

La entrevista se aplicó de manera presencial al Decano de la Institución junto a tres docentes de la misma, con preguntas abiertas obteniendo información variada sobre el uso y la protección de datos personales dentro de la Institución, teniendo en cuenta el procedimiento que tiene la institución para la protección de datos.

2.1.3.3 Encuesta

La encuesta constituye en un procedimiento de indagación que se dirige hacia una muestra representativa de un colectivo, denominado población, sobre el que se emplean un grupo de métodos estandarizados por medio de los que realizar una medición alrededor de ciertas dimensiones sobre las que se precisa conseguir entendimiento objetivo. (Martínez, Medina, & Domínguez, 2018)

La encuesta es una herramienta popular y fundamental al realizar una investigación, se puede definir como un cuestionario de diferente soporte ya sea de forma digital o a través de un documento escrito con preguntas formuladas con un objetivo específico que se debe aplicar a varias personas ya designadas dentro del área a investigar (Aurtenetxe, 2019).

La encuesta se hizo de forma personal a todos los docentes de la Uleam Extensión El Carmen, formulando preguntas que permitieran a los encuestados comunicar el conocimiento que tienen sobre los ataques informáticos y el uso de la tecnología.

2.1.3.4 Población

Una población es el conjunto de todos los recursos que se proponen para obtener una medida característica. Frente a la incapacidad de aprender toda la población se selecciona un subgrupo de recursos representativos poblacional que constituye lo cual se llama muestra. (Rodriguez, 2015)

Para esta investigación se tomó una población equivalente a 68 docentes trabajando actualmente en la Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen.

2.1.3.5 Muestreo

Uno de los más importantes fines de los estudios e indagaciones científicas es hacer generalizaciones desde una muestra. La muestra es un subconjunto de los miembros de una población, mientras tanto que la población comprende todos los miembros de un conjunto. Suele ser costoso y necesita enorme inversión de tiempo evaluar a toda la población de interés debido a que se debería tener identificada a la población y a sus miembros para formar una muestra y generalizar los resultados a toda la población. (Cruz del Castillo & Olivares, 2014)

En este trabajo de investigación se tomó una muestra de 19 docentes, haciéndose una muestra discrecional, por cuestiones de trabajo los docentes estaban ocupados.

2.1.4 Resultados de la investigación de campo.

2.1.4.1 Entrevista

Preguntas	Comentarios
1. ¿Dispone de un software o programa antivirus que proteja su dispositivo móvil en el cual usted realiza sus actividades de docentes?	Dos de las tres personas entrevistadas determinó no disponer una herramienta de protección contra virus en su dispositivo móvil, mientras una de ella, tiene y utiliza esta herramienta para el cuidado de su información.
2. ¿Qué conocimiento tiene sobre los ataques informáticos dentro del ámbito laboral?	Entre las respuestas encontramos el muy poco conocimiento sobre ataques, la información básica de estos y también solo la existencia de ataques informáticos, pero sin base.
3. ¿Conoce sobre el termino Ciberseguridad?	Declararon dos entrevistados tener conocimiento sobre la ciberseguridad que se utiliza para proteger información pública y privada, mientras que el otro entrevistado declaró no tener conocimiento sobre este.
4. ¿Tiene algún conocimiento previo a la Criptografía?	Todos los entrevistados consideraron no tener algún conocimiento o referencia de conocimiento sobre la criptología.
5. ¿Conoce lo que es una amenaza, una vulnerabilidad y un riesgo?	Dos de los entrevistados conocen la definición de estos términos, siendo uno de ellos aquel que no tiene conocimiento de estos.

<p>6. ¿Conoce sobre los ataques informáticos internos o externos que se pueden dar en la Universidad?</p>	<p>Solamente uno de los entrevistados tiene el conocimiento de ataques que se pueden dar en la universidad, dando como referencia la nota de los alumnos, mientras que los otros dos no sabían que esto puede suceder.</p>
<p>7. ¿Conoce sobre las vulnerabilidades que se expone un docente al compartir información por WhatsApp?</p>	<p>Un entrevistado conoce el peligro permanente que existe en todas las redes sociales y recomienda no brindar datos personales o privados en esta. Mientras que dos de ellos no conocen lo vulnerables que son utilizándolas de manera inapropiada.</p>
<p>8. ¿Ha existido algún ataque informático que haya perjudicado a usted como docente dentro de la institución?</p>	<p>Todos mencionaron no haber sufrido algún tipo de ataque informático ni como docente ni como institución.</p>
<p>9. ¿Conoce si dentro de la Universidad se manejan políticas para proteger la seguridad de la información de los docentes? ¿Cuáles son esas políticas?</p>	<p>Un docente conoce las políticas de seguridad como las contraseñas privadas, red de docente privada, uso personal de los equipos de cómputo docencia, siendo los dos faltantes quienes no tenían conocimiento de esta política.</p>
<p>10. ¿Se permite el acceso a los servidores a todo personal?</p>	<p>Todos saben que cada quien tiene su rol y sus permisos por lo tanto no se le permite el acceso</p>

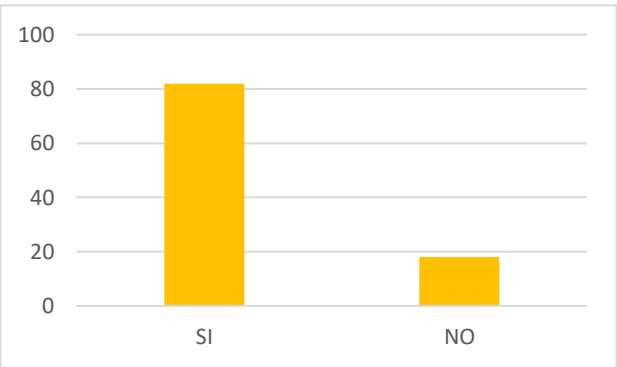
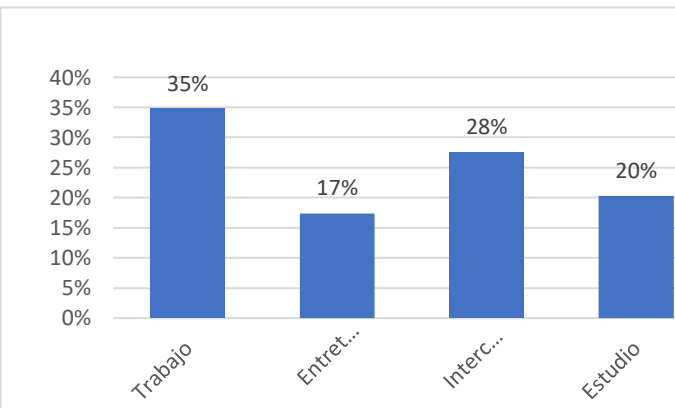
	a todos, solo al personal del departamento de administración.
11. ¿Qué tipo de ataque de seguridad usted ha enfrentado y qué hizo usted para resolverlo?	Ninguno de los entrevistados se ha enfrentado a un ataque de seguridad.
12. ¿Maneja usted cursos de actualización o políticas de seguridad para enfrentarse a la inseguridad constante que se produce a través de Ciberataques?	Uno de los entrevistados acepta que maneja cursos académicos de permanente actualización, mas ahora en la era digital.

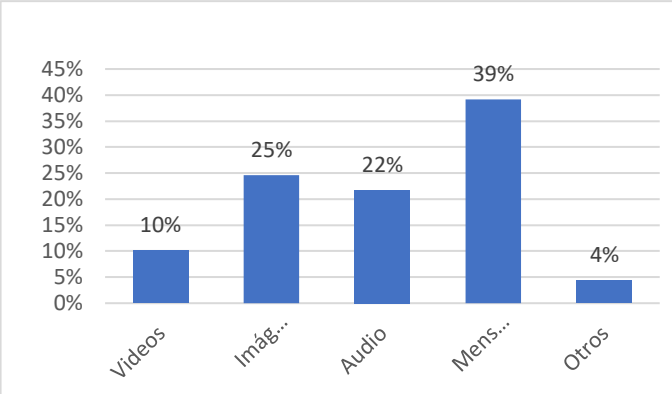
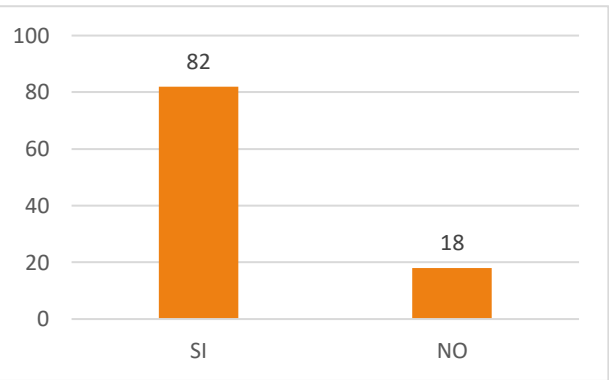
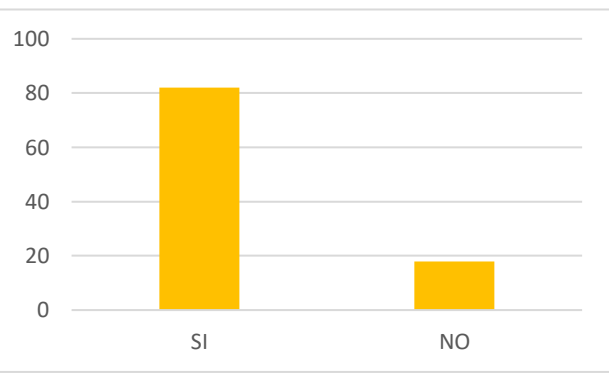
2.1.4.1.1 Interpretación de la Entrevista

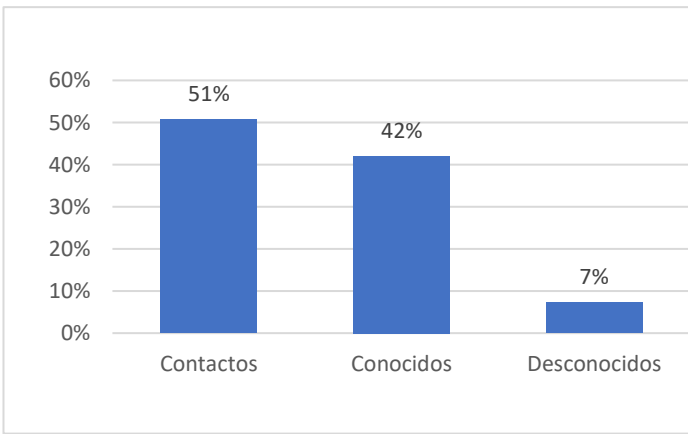
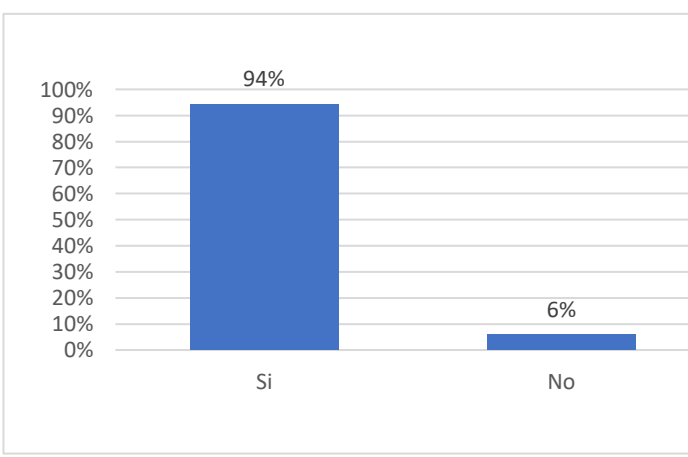
Al analizar las respuestas obtenidas mediante la entrevista a tres docentes sobre la protección de datos y la seguridad informática, se puede argumentar que; no todos usan lo que es un software para proteger su dispositivo, los conocimientos que se tiene sobre los ataques informáticos son muy pocos y básicos, se desconocen los términos como Ciberseguridad, Criptografía, sin saber diferenciar entre un riesgo informático, una vulnerabilidad y amenaza informática. Se desconocen las vulnerabilidades que se exponen al compartir información o datos, además se desconocen las políticas de seguridad básicas.

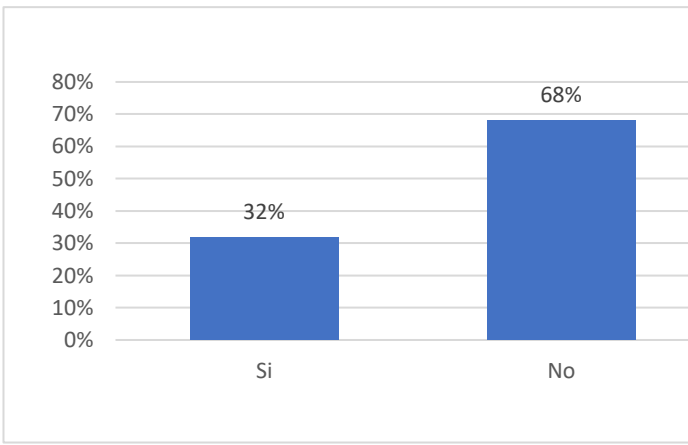
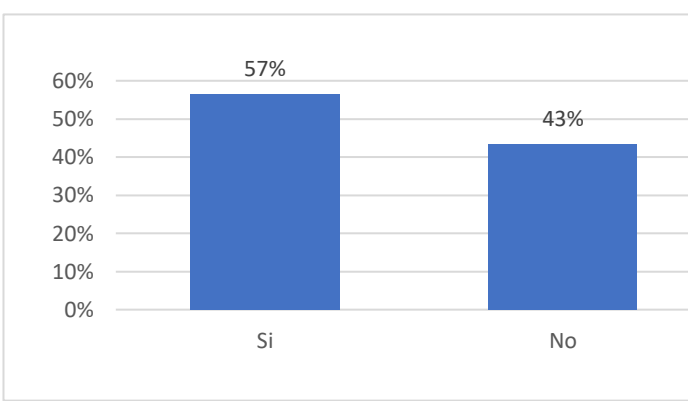
2.1.4.2 Encuesta a Docentes

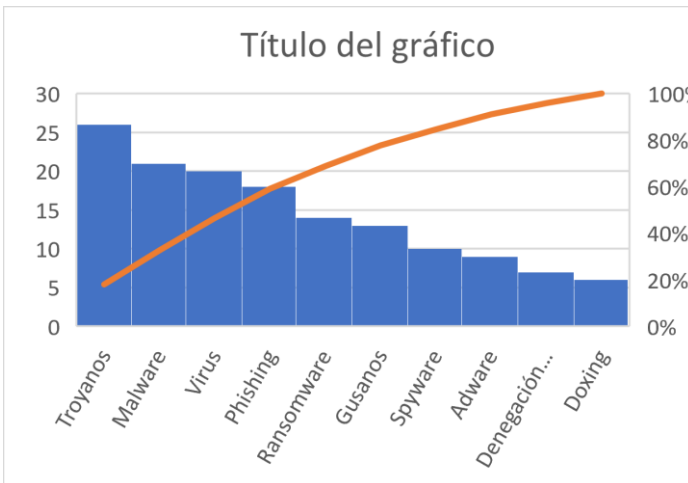
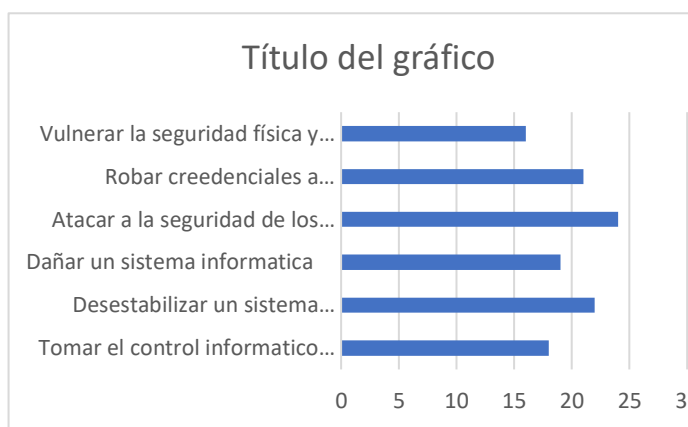
La presente encuesta tiene como objetivo reunir información seria y confiable acerca del Perfil del Docente de la Universidad Laica "Eloy Alfaro de Manabí" Extensión El Carmen, relacionada con la utilidad e importancia de los ataques informáticos.

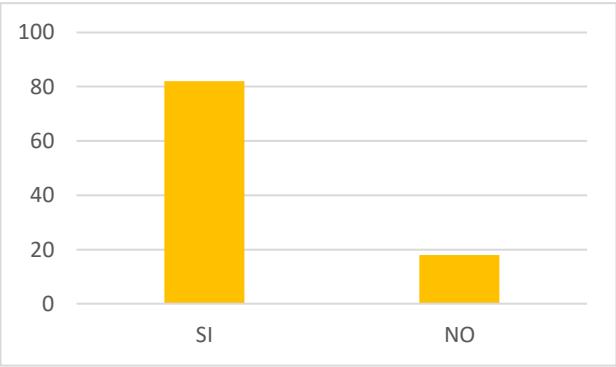
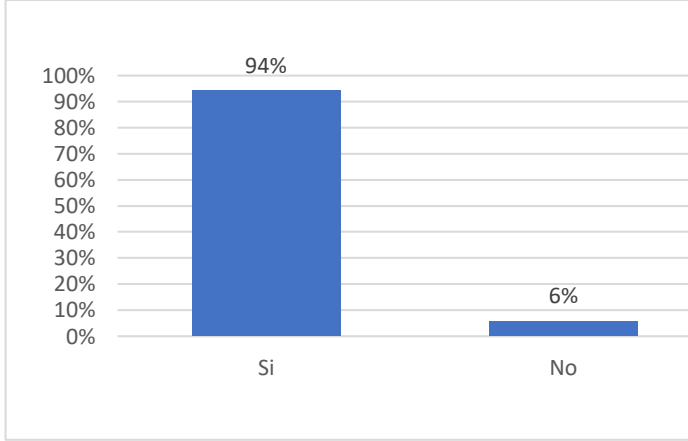
Preguntas	Gráficas	Análisis										
¿Usted utiliza la herramienta WhatsApp?	 <table border="1"> <caption>Gráfica: ¿Usted utiliza la herramienta WhatsApp?</caption> <thead> <tr> <th>Respuesta</th> <th>Porcentaje</th> </tr> </thead> <tbody> <tr> <td>SI</td> <td>80%</td> </tr> <tr> <td>NO</td> <td>20%</td> </tr> </tbody> </table>	Respuesta	Porcentaje	SI	80%	NO	20%	En su totalidad los docentes utilizan la herramienta WhatsApp.				
Respuesta	Porcentaje											
SI	80%											
NO	20%											
¿Con qué fin usa usted WhatsApp?	 <table border="1"> <caption>Gráfica: ¿Con qué fin usa usted WhatsApp?</caption> <thead> <tr> <th>Fin</th> <th>Porcentaje</th> </tr> </thead> <tbody> <tr> <td>Trabajo</td> <td>35%</td> </tr> <tr> <td>Entret...</td> <td>17%</td> </tr> <tr> <td>Interc...</td> <td>28%</td> </tr> <tr> <td>Estudio</td> <td>20%</td> </tr> </tbody> </table>	Fin	Porcentaje	Trabajo	35%	Entret...	17%	Interc...	28%	Estudio	20%	La mayor parte de los docentes usan la herramienta con fines laborales.
Fin	Porcentaje											
Trabajo	35%											
Entret...	17%											
Interc...	28%											
Estudio	20%											

<p>De los siguientes recursos, señale cuáles usted utiliza más</p>	 <table border="1"> <thead> <tr> <th>Recurso</th> <th>Porcentaje</th> </tr> </thead> <tbody> <tr> <td>Videos</td> <td>10%</td> </tr> <tr> <td>Imágenes</td> <td>25%</td> </tr> <tr> <td>Audio</td> <td>22%</td> </tr> <tr> <td>Mensajes de texto</td> <td>39%</td> </tr> <tr> <td>Otros</td> <td>4%</td> </tr> </tbody> </table>	Recurso	Porcentaje	Videos	10%	Imágenes	25%	Audio	22%	Mensajes de texto	39%	Otros	4%	<p>La mayor parte de los docentes usan lo que son mensajes de textos al momento de compartir información.</p>
Recurso	Porcentaje													
Videos	10%													
Imágenes	25%													
Audio	22%													
Mensajes de texto	39%													
Otros	4%													
<p>¿El uso constante del WhatsApp, le parece útil aplicarlo en su docencia?</p>	 <table border="1"> <thead> <tr> <th>Respuesta</th> <th>Cantidad</th> </tr> </thead> <tbody> <tr> <td>SI</td> <td>82</td> </tr> <tr> <td>NO</td> <td>18</td> </tr> </tbody> </table>	Respuesta	Cantidad	SI	82	NO	18	<p>La mayoría de docentes le parece útil aplicar el uso del WhatsApp en la hora de su docencia.</p>						
Respuesta	Cantidad													
SI	82													
NO	18													
<p>¿Cree usted que es importante la protección de los datos personales en WhatsApp?</p>	 <table border="1"> <thead> <tr> <th>Respuesta</th> <th>Cantidad</th> </tr> </thead> <tbody> <tr> <td>SI</td> <td>82</td> </tr> <tr> <td>NO</td> <td>18</td> </tr> </tbody> </table>	Respuesta	Cantidad	SI	82	NO	18	<p>En su totalidad están de acuerdo que la protección de los datos sea importante.</p>						
Respuesta	Cantidad													
SI	82													
NO	18													

<p>¿Con quienes usted interactúa más por medio de WhatsApp con diferentes tipos de información?</p>	 <table border="1"> <thead> <tr> <th>Tipo de contacto</th> <th>Porcentaje</th> </tr> </thead> <tbody> <tr> <td>Contactos</td> <td>51%</td> </tr> <tr> <td>Conocidos</td> <td>42%</td> </tr> <tr> <td>Desconocidos</td> <td>7%</td> </tr> </tbody> </table>	Tipo de contacto	Porcentaje	Contactos	51%	Conocidos	42%	Desconocidos	7%	<p>La mayor parte de los docentes tienen interacción con contactos ya registrados en el dispositivo.</p>
Tipo de contacto	Porcentaje									
Contactos	51%									
Conocidos	42%									
Desconocidos	7%									
<p>¿Cree usted que pueden existir vulnerabilidades en WhatsApp al momento de compartir información?</p>	 <table border="1"> <thead> <tr> <th>Respuesta</th> <th>Porcentaje</th> </tr> </thead> <tbody> <tr> <td>Si</td> <td>94%</td> </tr> <tr> <td>No</td> <td>6%</td> </tr> </tbody> </table>	Respuesta	Porcentaje	Si	94%	No	6%	<p>La mayoría de los docentes tiene el conocimiento de la vulnerabilidad que puede existir al momento de compartir información.</p>		
Respuesta	Porcentaje									
Si	94%									
No	6%									

<p>Cuando usted recibe información por WhatsApp, al ser un número desconocido ¿Usted abre el enlace compartido?</p>	 <table border="1"> <thead> <tr> <th>Respuesta</th> <th>Porcentaje</th> </tr> </thead> <tbody> <tr> <td>Si</td> <td>32%</td> </tr> <tr> <td>No</td> <td>68%</td> </tr> </tbody> </table>	Respuesta	Porcentaje	Si	32%	No	68%	<p>La mayor parte de los docentes tiene precaución al momento de abrir un mensaje, enlace o link de algún número desconocido.</p>
Respuesta	Porcentaje							
Si	32%							
No	68%							
<p>¿Conoce usted los distintos ataques informáticos que existen?</p>	 <table border="1"> <thead> <tr> <th>Respuesta</th> <th>Porcentaje</th> </tr> </thead> <tbody> <tr> <td>Si</td> <td>57%</td> </tr> <tr> <td>No</td> <td>43%</td> </tr> </tbody> </table>	Respuesta	Porcentaje	Si	57%	No	43%	<p>En su totalidad los docentes conocen sobre los distintos ataques informáticos.</p>
Respuesta	Porcentaje							
Si	57%							
No	43%							

<p>De la siguiente lista de ataques informáticos, señale los que usted conoce</p>	 <table border="1"> <caption>Título del gráfico</caption> <thead> <tr> <th>Ataque</th> <th>Número de docentes</th> </tr> </thead> <tbody> <tr><td>Troyanos</td><td>26</td></tr> <tr><td>Malware</td><td>21</td></tr> <tr><td>Virus</td><td>20</td></tr> <tr><td>Phishing</td><td>18</td></tr> <tr><td>Ransomware</td><td>14</td></tr> <tr><td>Gusanos</td><td>13</td></tr> <tr><td>Spyware</td><td>10</td></tr> <tr><td>Adware</td><td>9</td></tr> <tr><td>Denegación...</td><td>7</td></tr> <tr><td>Doxing</td><td>6</td></tr> </tbody> </table>	Ataque	Número de docentes	Troyanos	26	Malware	21	Virus	20	Phishing	18	Ransomware	14	Gusanos	13	Spyware	10	Adware	9	Denegación...	7	Doxing	6	<p>La mayoría de los docentes conocen los diferentes ataques informáticos.</p>
Ataque	Número de docentes																							
Troyanos	26																							
Malware	21																							
Virus	20																							
Phishing	18																							
Ransomware	14																							
Gusanos	13																							
Spyware	10																							
Adware	9																							
Denegación...	7																							
Doxing	6																							
<p>¿A qué considera usted un ataque informático?</p>	 <table border="1"> <caption>Título del gráfico</caption> <thead> <tr> <th>Acción</th> <th>Número de docentes</th> </tr> </thead> <tbody> <tr><td>Vulnerar la seguridad física y...</td><td>16</td></tr> <tr><td>Robar credenciales a...</td><td>21</td></tr> <tr><td>Atacar a la seguridad de los...</td><td>24</td></tr> <tr><td>Dañar un sistema informatica</td><td>19</td></tr> <tr><td>Desestabilizar un sistema...</td><td>22</td></tr> <tr><td>Tomar el control informatico...</td><td>18</td></tr> </tbody> </table>	Acción	Número de docentes	Vulnerar la seguridad física y...	16	Robar credenciales a...	21	Atacar a la seguridad de los...	24	Dañar un sistema informatica	19	Desestabilizar un sistema...	22	Tomar el control informatico...	18	<p>En su mayor parte los docentes consideran que un ataque informático es atacar a la seguridad de los datos o información de los usuarios.</p>								
Acción	Número de docentes																							
Vulnerar la seguridad física y...	16																							
Robar credenciales a...	21																							
Atacar a la seguridad de los...	24																							
Dañar un sistema informatica	19																							
Desestabilizar un sistema...	22																							
Tomar el control informatico...	18																							

<p>¿Le gustaría a usted tener información de que tratan los ataques informáticos y como evitarlos?</p>	 <table border="1"> <thead> <tr> <th>Respuesta</th> <th>Porcentaje</th> </tr> </thead> <tbody> <tr> <td>SI</td> <td>80%</td> </tr> <tr> <td>NO</td> <td>20%</td> </tr> </tbody> </table>	Respuesta	Porcentaje	SI	80%	NO	20%	<p>En su totalidad los docentes están interesados en tener información sobre los ataques informáticos.</p>
Respuesta	Porcentaje							
SI	80%							
NO	20%							
<p>Sería factible de que usted posea una guía digital para conocer y enfrentar los diferentes tipos de ataques informáticos</p>	 <table border="1"> <thead> <tr> <th>Respuesta</th> <th>Porcentaje</th> </tr> </thead> <tbody> <tr> <td>Si</td> <td>94%</td> </tr> <tr> <td>No</td> <td>6%</td> </tr> </tbody> </table>	Respuesta	Porcentaje	Si	94%	No	6%	<p>En su mayor parte los docentes están de acuerdo obtener en poseer un manual digital para conocer y evitar los ataques informáticos.</p>
Respuesta	Porcentaje							
Si	94%							
No	6%							

2.1.4.2.1 Interpretación de Encuesta

De acuerdo con la encuesta realizada a los docentes de la ULEAM Extensión El Carmen, en su mayor parte utilizan la herramienta WhatsApp con fines laborales, aplicándolo en su docencia mediante mensajes de textos. Según la pregunta 7 tienen el conocimiento de que puede existir vulnerabilidad al momento de compartir información, sin embargo, se desconoce cómo evitar este tipo de problemas, en su totalidad saben lo que es un ataque informático y los diferentes ataques informáticos existentes, y sería factible que tengan un manual digital para tener mayor conocimiento.

2.2 Análisis de resultados

Considerando los resultados de los instrumentos utilizados podemos dar a conocer que los docentes de la ULEAM Extensión El Carmen desconocen sobre los términos de la seguridad informática. No cuentan con un software para proteger su dispositivo ante cualquier amenaza y esto conlleva a tener un riesgo en la pérdida o duplicación de la información. Por su parte el encargado del departamento de administración menciona las políticas de seguridad que tiene la institución, sin embargo, los docentes desconocen estas políticas, por ello se considera importante realizar una mayor difusión para sean aplicadas y así tener mayor seguridad de la información.

Por tal motivo se hace factible y se plantea realizar una auditoría con algún tipo de metodología que dará resultados más concretos lo que determinará acciones a realizar como por ejemplo la elaboración de una guía o un manual de buenas prácticas para la seguridad y protección de la información.

CAPÍTULO III

3 DESARROLLO DE LA PROPUESTA

3.1 Antecedentes

3.1.1 Reseña Histórica de la Universidad Laica “Eloy Alfaro de Manabí” Extensión El Carmen

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. Olíver 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. (<https://carreras.uleam.edu.ec/elcarmen/resena-historica-2/>)

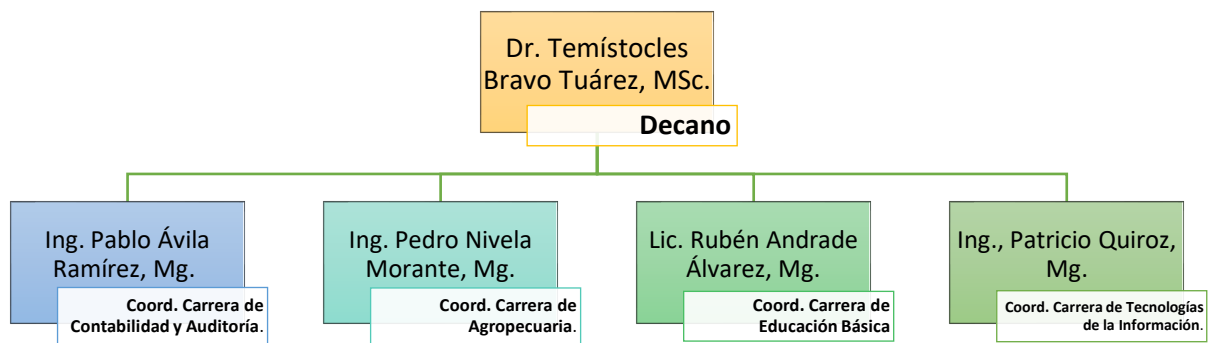
3.1.2 Misión

Formar profesionales competentes y emprendedores desde lo académico, la investigación, y la vinculación, que contribuyan a mejorar la calidad de vida de la sociedad.

3.1.3 Visión

Ser un referente nacional e internacional de Institución de Educación Superior que contribuye al desarrollo social, cultural y productivo con profesionales éticos, creativos, cualificados y con sentido de pertinencia.

3.2 Organigrama



3.3 Programa de Auditoria

Programa de Auditoria al cumplimiento de políticas de seguridad de la información en las comisiones de la Universidad Laica “Eloy Alfaro de Manabí” Extensión El Carmen		
Objetivo: Verificar el cumplimiento de políticas de seguridad de la información a los docentes del área de Ingeniería en Sistemas.		
TÉCNICAS Y PROCEDIMIENTOS	REFERENCIA	FECHA
1. Investigar sobre la seguridad de información y protección de datos personales.	PT1	01/05/2022
2. Revisar metodología ISO 27001 y sus fases de ejecución e implementación.	PT2	
3. Definir números de docentes que se evaluarán	PT3	19/06/2022
4. Definir activos: - Datos personales - WhatsApp	PT4	23/06/2021
5. Definir riesgos - Phishing - Virus - Ransomware	PT5	

6. Elaborar el diseño de instrumentos de auditoría	PT6	
7. Aplicar los instrumentos de investigación.	PT7	
8. Tabular y análisis de los datos		
9. Identificar las salvaguardas		
10. Realizar un manual de buenas prácticas		

3.4 Informe de Auditoria

En el presente informe se detallan los resultados de la Auditoría Informática aplicada a los docentes de la Universidad Laica “Eloy Alfaro Manabí” Extensión El Carmen; especificando los riesgos y vulnerabilidades de seguridad de la información en el procesamiento de datos de los docentes de la institución, de igual manera detallando las soluciones o medidas que se deben aplicar o tomar para poder prevenir este tipo de incidentes en todas partes; de esta forma se logra disminuir el impacto de algún riesgo presente hasta cierto punto.

3.4.1 Dirigido a:

Este informe de Auditoría Informática de la Seguridad de Información va dirigido a la Universidad Laica “Eloy Alfaro de Manabí” Extensión El Carmen.

3.5 Objetivo

Realizar una Auditoria de seguridad informática dando evidencia a la vulnerabilidad de los datos personales en docentes de la “Universidad Laica Eloy Alfaro de Manabí Extensión en El Carmen” en la Red social WhatsApp, debido a los ataques informáticos que acontecen diariamente.

3.6 Personal relacionado

Para el desarrollo de esta Auditoría Informática de Seguridad de Información se tomó como referencia los docentes de la Universidad Laica “Eloy Alfaro de Manabí” Extensión El Carmen, para analizar los riesgos del manejo de información de índole personal y así evaluar la seguridad que tienen en el uso de la red WhatsApp.

3.7 Alcance

En la presente Auditoría Informática de Seguridad de Información aplicada a los docentes de la Universidad Laica “Eloy Alfaro de Manabí” Extensión El Carmen, con el objetivo de analizar los riesgos del manejo de información de índole personal y así evaluar la seguridad de la información que tienen en el uso de la red WhatsApp.

Como parte importante de esta Auditoría Informática se aplicó la metodología ISO 27001 que tiene como objetivo analizar y gestionar los riesgos basados en los procesos para garantizar buenas prácticas de Seguridad de la Información, resulta muy útil el análisis y gestión de riesgos basados en los procesos ya que evalúa y controla a la organización en relación con los diferentes riesgos a los que se encuentra sometido el sistema de información.

También se utiliza como relación la política institucional ubicada en la página oficial de la Universidad ULEAM, para la herramienta de evaluación de auditoría se utiliza como referencia la sección Política de Seguridad de la Información, según el manual se realizó preguntas a los docentes de la institución sobre el conocimiento de los riesgos informáticos y el uso de los datos personales, para evaluar su seguridad al utilizar la red.

3.8 Definir Activos

Datos Personales

- Sin duda, la protección de datos también debe adaptarse a las nuevas realidades que impone la inteligencia artificial. En cambio, la IA debe programarse por defecto y por diseño para que su aplicación sea compatible con el respeto a la privacidad. Lo que no podemos ignorar es que, con el avance de la inteligencia artificial, el procesamiento de datos aumentará considerablemente, convirtiéndose en un uso a gran escala y rápido. Lo mismo ocurrirá con los riesgos conexos. Cuantos más datos se utilicen, especialmente en volúmenes tan grandes, mayor será el potencial de violación de la privacidad de los ciudadanos. (Herrera, 2022)
- La denominada protección de datos personales se entiende como la protección jurídica de las personas en lo que respecta al tratamiento de sus datos personales, o en su defecto, la protección de los ciudadanos frente a un posible uso no autorizado por parte de terceros. Datos fáciles de tratar, información identificable preparada para afectar a su entorno personal, social o profesional en el contexto de su privacidad, afectando directamente los derechos fundamentales de alto contenido. (Conde, 2016)
- Las preocupaciones sobre la recopilación de datos personales y su pérdida de control han surgido al mismo tiempo que los avances tecnológicos permiten la automatización del procesamiento de datos personales. Desde sus inicios, una de las características fundamentales de los dispositivos tecnológicos ha sido el aumento exponencial de la posibilidad de almacenar información personal. El desarrollo de las tecnologías de la información ha hecho posible recopilar y guardar datos ilimitados de una misma persona sin limitaciones de espacio, realizando un verdadero catálogo de su vida a través de la interrelación de todos los datos existentes. (Garriga, 2016)

WhatsApp

- Es el servicio de mensajería más utilizado en América Latina y partes de Europa, diseñado para teléfonos Android e IOS. Permite enviar texto, audio, ubicación en tiempo real, imágenes y video a través de sus usuarios, también tiene la capacidad de realizar llamadas de voz IP y videollamadas. Sin embargo, los usuarios se cansan de los colores y temas únicos de WhatsApp y optan por instalar aplicaciones de terceros como: WhatsApp Plus, WhatsApp Blue, OGWhatsApp, YOWhatsApp, GBWhatsApp, entre otras. Todas estas aplicaciones modificadas (MOD) no oficiales que ofrecen ciertas funciones que no existen en la aplicación oficial, y aunque puede parecer interesante tener más funciones, la privacidad no es una de ellas. La aplicación funciona como la original, pero es monitoreada por terceros dándole el permiso para espiar lo que haces fuera de la aplicación, obtener videos, imágenes entre otros archivos. (Iñiguez, 2020)

3.9 Definir Riesgos

Phishing

- El phishing es una técnica utilizada para engañar a las personas para que revelen información personal confidencial, como números de seguro social, números de cuentas, contraseñas, entre otros datos. Los estafadores a menudo se hacen pasar por amigos y les envían un mensaje con un enlace a una página de inicio de sesión falsa. Una vez que los usuarios ingresan sus datos en páginas falsas, esa información se utilizará para propagar spam o virus. (Yada, 2015)
- Si tienen éxito, los phishers pueden robar mucho dinero en sí mismo o vender información de usuario a otros delincuentes. La página de phishing debe ser muy similar a la página real para poder engañar a los usuarios. Por esta razón, los phishers a menudo usan un método llamado Engaño Visual. Por lo tanto, debería ser posible detectar páginas de phishing mediante análisis de similitud visual de páginas sospechosas con páginas web reales. (Park, Chen, Atiquzaman, Lee, & Yeo, 2016)

Virus

- Es un pequeño programa escrito intencionalmente para instalarse en el dispositivo de un usuario sin el consentimiento o permiso del usuario. Se dice que es un programa parásito ya que ataca el archivo o sector de arranque con el nombre en inglés (Boot) y se replica para seguir extendiéndose a otros dispositivos. Algunos se limitan a la replicación, mientras que otros pueden afectar al sistema. Los virus tienen diferentes propósitos: algunos solo infectan, algunos cambian datos, algunos eliminan, algunos destruyen hardware, algunos destruyen software, algunos solo muestran un mensaje, pero todos persiguen un propósito común de "propagación". (López Y. M., 2010)
- Un virus es un software malicioso diseñado para alterar el funcionamiento normal de un dispositivo sin el permiso o el conocimiento del usuario. Los virus a menudo reemplazan los archivos ejecutables con otros archivos que están infectados por su código y tienen la capacidad de replicarse. Para ello, una vez que se ejecuta un programa infectado por virus, algo que seguramente el usuario desconoce, se carga en memoria y toma el control del sistema operativo, infectando el programa llamado a ejecutar y añadiéndole código de virus, dando como resultado su untado. (Pérez J. C., 2016)

Ransomware

- El ransomware es un hack particularmente dañino, es un ataque pirata conocido como malware, puede infectar dispositivos aleatoriamente a través de sitios web visitados o dirigirse directamente a individuos u organizaciones a través de correos electrónicos cuidadosamente elaborados. Los piratas informáticos pueden llegar a investigar cuidadosamente las cuentas y relaciones de las redes sociales para asegurarse de que se abran los correos electrónicos y los archivos adjuntos. Una vez que el ransomware ingresa a una computadora o sistema informático, bloquea al usuario o cifra los archivos para que no puedan leerse sin la clave digital. (Gary, 2018)
- Los ataques de ransomware operados por humanos pueden ser muy sofisticados. Cualquier ataque comienza con el acceso inicial. Puede ser para acceder a la red interna a través de VPN, los troyanos se entregan a través de phishing selectivo, shells web implementados a través de vulnerabilidades de aplicaciones públicas e incluso ataques a la cadena de suministro. Si un atacante obtiene las credenciales de administrador del dominio, puede acceder fácilmente al servidor de copia de seguridad y eliminar todas las copias de seguridad disponibles. Eso es todo, por lo que la empresa víctima no tiene más remedio que pagar el rescate. (Skulkin, 2022)

3.9.1 Diseño de instrumentos

El cuestionario de 36 preguntas se encuentra dividido en tres riesgos de la siguiente manera: 12 preguntas referentes al grupo de riesgo PHISHING, 12 que conforman al riesgo de VIRUS, y 12 al grupo de riesgo RANSOMWARE. Una vez recolectada la información necesaria de cada docente registrado en la extensión y al haber finalizado de llenar los cuestionarios de identificación de riesgos se procedió a tabular en una matriz de Excel cada riesgo.

CUESTIONARIO PARA IDENTIFICAR RIESGOS VINCULADOS A LA PROTECCIÓN DE DATOS PERSONALES EN DOCENTES DE ULEAM EXT. EL CARMEN			
RIESGO: PHISHING		SI	NO
1	¿Revisa usted el propietario de algún tipo de correo antes de abrirlo?		
2	¿Instaló usted WhatsApp desde las tiendas oficiales?		
3	Al instalar y ejecutar WhatsApp, ¿Leyó y analizó las políticas y condiciones?		
4	¿Ingresaría usted datos personales en una página sin saber su procedencia lícita?		
5	¿Ha llenado formularios con información personal?		
6	¿Ha recibido usted mensajes requiriendo códigos ilegales para autenticación de WhatsApp ?		
7	¿Ha podido identificar en algún momento un contacto de con mensajes fraudulento?		
8	¿Ha sido víctima de fraudes por medio de WhatsApp donde se le piden sus datos personales?		
9	¿Cree usted que los archivos que comparte por medio de WhatsApp están expuestos?		
10	¿Abre usted archivos adjuntos a mensajes sospechosos antes de comprobar que sean legítimos?		
11	¿Tiene usted instalado software de seguridad como antivirus en su dispositivo?		
12	¿Mantiene usted el Sistema operativo y software de su dispositivo actualizados?		

CUESTIONARIO PARA IDENTIFICAR RIESGOS VINCULADOS A LA PROTECCIÓN DE DATOS PERSONALES EN DOCENTES DE ULEAM EXT. EL CARMEN				
RIESGO: VIRUS			SI	NO
1	¿Conoce usted qué son los virus informáticos?			
2	¿Conoce usted los tipos de virus informáticos que existen?			
3	¿Tiene usted instalado en su dispositivo un antivirus?			
4	¿Sabe usted distinguir un virus informático mientras está usando WhatsApp?			
5	¿Actualiza de manera correcta y precisa el antivirus en sus dispositivo?			
6	¿Suele usted abrir archivos o documentos en WhatsApp aun cuando no sabe de quien provienen?			
7	¿Cuando recibe archivos de un remitente desconocido en WhatsApp, los descargas?			
8	¿Descarga y ejecuta usted cualquier tipo de archivos en su dispositivo?			
9	¿Podría usted identificar cuando está ante un virus informático mientras usa WhatsApp?			
10	¿Conoce usted las formas de propagación de los virus informáticos ?			
11	¿Usa usted la aplicación de WhatsApp en su dispositivo que sea descargada desde las tiendas oficiales?			
12	¿Conoce usted si su dispositivo está expuesto a contraer un virus informático mientras usa WhatsApp?			





CUESTIONARIO PARA IDENTIFICAR RIESGOS VINCULADOS A LA PROTECCIÓN DE DATOS PERSONALES EN DOCENTES DE ULEAM EXT. EL CARMEN				
RIESGO: RANSOMWARE			SI	NO
1	¿Conoce usted que un ransomware de bloqueo afecta las funciones básicas de su dispositivo?			
2	¿Tiene usted en su dispositivo instalado un paquete de antivirus de buena popularidad?			
3	¿Realiza actualizaciones de la versión del antivirus de manera eficaz que usa en su dispositivo?			
4	¿Realiza análisis de vulnerabilidades para ayudarlo a revelar si hay un intruso en el sistema?			
5	¿Ha recibido alertas de parte de su antivirus reportando actividades maliciosas?			
6	¿Ha realizado usted actualizaciones recientes del sistema operativo que usan su dispositivo?			
7	¿Al momento de usted instalar un programa en su dispositivo le da la debida atención a los premisos que estos requieren?			
8	Cuando usted usa WhatsApp, ¿Se ha percatado de aplicaciones que se ejecuten en segundo plano?			
9	Cuando usted recibe mensajes inesperados mediante WhatsApp, ¿revisa el contacto antes de abrirlos?			
10	En los grupos de WhatsApp con sus estudiantes ¿se encarga de restringir mensajes de desconocidos?			
11	¿Realiza usted respaldos en la nube de su información de manera periodica?			
12	¿Su versión de WhatsApp se encuentra actualizada?			

3.9.2 Tabulación

La tabulación se realizó en una hoja electrónica de Excel, una encuesta aplicada a 15 docentes que se organizó por carreras y se procedió analizando las preguntas con sus respectivas respuestas de la siguiente manera: organizadas de negativa y positiva, definiendo el porcentaje negativo de riesgo que tiene cada carrera por vulnerabilidad se calcula dividiendo las preguntas positivas y negativas, valorando 1 como positivo y 0 como negativo luego se suman cuantos docentes por carrera afirmaron que pueden sobrellevar si llegan a sufrir algún tipo de riesgo (SI) siempre y cuando la pregunta este valorada en 1, caso contrario si la pregunta está valorada en 0 contara cómo negativa y la sumatoria de docentes que no podrían sobrellevar las instancias de los riesgos (NO) siempre y cuando la pregunta este valorada en 0, caso contrario si la pregunta está valorada en 1 contara cómo positiva de esta forma se realiza la sumatoria y se divide por las preguntas planteadas que en este caso cada riesgo contiene 12 preguntas, inmediatamente se multiplica por 100 y se divide por el número total de docentes de esa carrera que respondieron al cuestionario.

PLATAFORMA WHATSAPP											DOCENTES														
CUESTIONARIO PARA IDENTIFICAR RIESGOS VINCULADOS A LA PROTECCIÓN DE DATOS PERSONALES EN DOCENTES DE ULEAM EXT. EL CARMEN																									
RIESGO: PHISHING											P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	
1	¿Revisa usted el propietario de algún tipo de correo antes de abrirlo?											1	1	1	1	1	1	1	1	0	1	1	1	1	1
2	¿Instaló usted WhatsApp desde las tiendas oficiales?											1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	Al instalar y ejecutar WhatsApp, ¿Leyó y analizó las políticas y condiciones?											0	0	0	0	1	1	1	1	0	1	0	1	0	0
4	¿Ingresaría usted datos personales en una página sin saber su procedencia lícita?											0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	¿Ha llenado formularios con información personal?											1	1	0	1	1	1	1	1	0	1	1	1	1	1
6	¿Ha recibido usted mensajes requiriendo códigos ilegales para autenticación de WhatsApp?											1	0	1	1	0	1	0	1	0	0	0	0	0	0
7	¿Ha podido identificar en algún momento un contacto de con mensajes fraudulentos?											1	0	1	0	1	1	1	0	1	1	1	0	1	1
8	¿Ha sido víctima de fraudes por medio de WhatsApp donde se le piden sus datos personales?											1	0	0	1	0	0	0	0	0	0	0	0	0	0
9	¿Cree usted que los archivos que comparte por medio de WhatsApp están expuestos?											1	1	1	1	1	1	1	1	0	0	1	1	1	1
10	¿Abre usted archivos adjuntos a mensajes sospechosos antes de comprobar que sean legítimos?											1	1	1	0	1	1	1	1	1	1	1	1	1	1
11	¿Tiene usted instalado software de seguridad como antivirus en su dispositivo?											1	1	1	1	1	1	1	0	1	0	1	0	1	1
12	¿Mantiene usted el Sistema operativo y software de su dispositivo actualizados?											1	1	1	1	1	1	1	1	1	1	1	1	1	1

De la aplicación de matriz de riesgos los datos obtenidos fueron:

LEYENDA							
		GRAVEDAD (IMPACTO)					
		MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO	
		1	2	3	4	5	
APARICIÓN (probabilidad)	MUY ALTA	5	5	10	15	20	25
	ALTA	4	4	8	12	16	20
	MEDIA	3	3	6	9	12	15
	BAJA	2	2	4	6	8	12
	MUY BAJA	1	1	2	3	4	5
	Riesgo muy grave. Requiere medidas preventivas urgentes. No se debe iniciar el proyecto sin la aplicación de medidas preventivas urgentes y sin acotar sólidamente el riesgo.						
	Riesgo importante. Medidas preventivas obligatorias. Se deben controlar fuertemente las variables de riesgo durante el proyecto.						
	Riesgo apreciable. Estudiar económicamente si es posible introducir medidas preventivas para reducir el nivel de riesgo. Si no fuera posible, mantener las variables controladas.						
	Riesgo marginal. Se vigilará aunque no requiere medidas preventivas de partida.						



MATRIZ DE RIESGOS

Plataforma: WhatsApp

RIESGO	APARICIÓN	GRAVEDAD	VALOR DE	NIVEL DEL RIESGO
Phishing	3	3	9	Importante
Virus	3	2	6	Apreciable
Ransomware	3	6	18	Muy grave

3.10 Hallazgos

En la auditoría informática de seguridad de la información realizada a los docentes de la extensión El Carmen, cada cuestionario elaborado fue examinado cuidadosamente, se extrajo las causas principales por la que se produciría una vulnerabilidad en la seguridad en el manejo de información de cada docente. En la siguiente tabla podemos encontrar las causas principales por las cuales tenemos un nivel **MUY GRAVE** de riesgo en cada docente, también se muestra el gráfico en donde se representa el nivel de riesgo y seguridad de cada una según el riesgo.

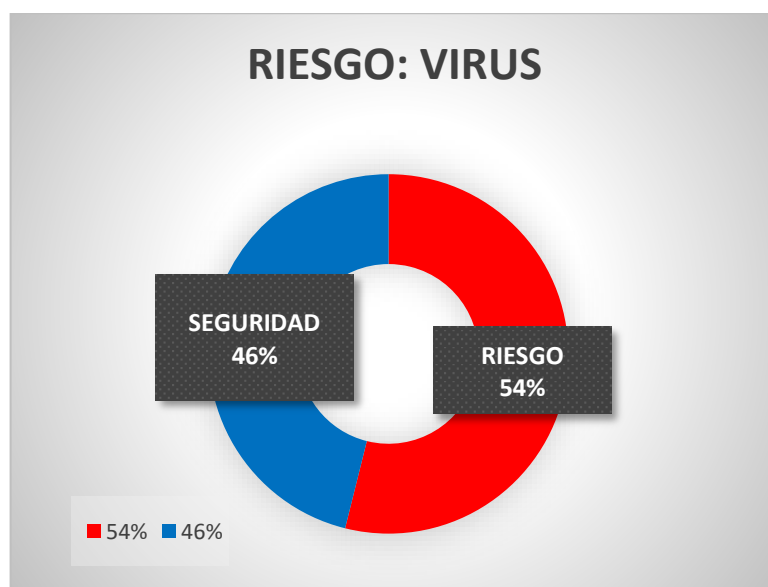
RIESGO	CAUSA
RANSOMWARE	<ul style="list-style-type: none">• Los docentes no conocen que un ransomware de bloqueo afecta las funciones básicas de su dispositivo.• Los docentes no realizan análisis de vulnerabilidades para ayudarse a revelar si hay un intruso en el sistema.• Los docentes no han realizado las actualizaciones recientes del sistema operativo que usan su dispositivo• Al momento de instalar un programa en su dispositivo los docentes no le dan la debida atención a los permisos que estos requieren• Cuando los docentes usan WhatsApp, No se han percatado de aplicaciones que se ejecutan en segundo plano• En los grupos de WhatsApp con sus estudiantes No se encarga n de restringir mensajes de desconocidos• No realizan respaldos en la nube de su información de manera periódica.

INTERPRETACIÓN: PHISHING



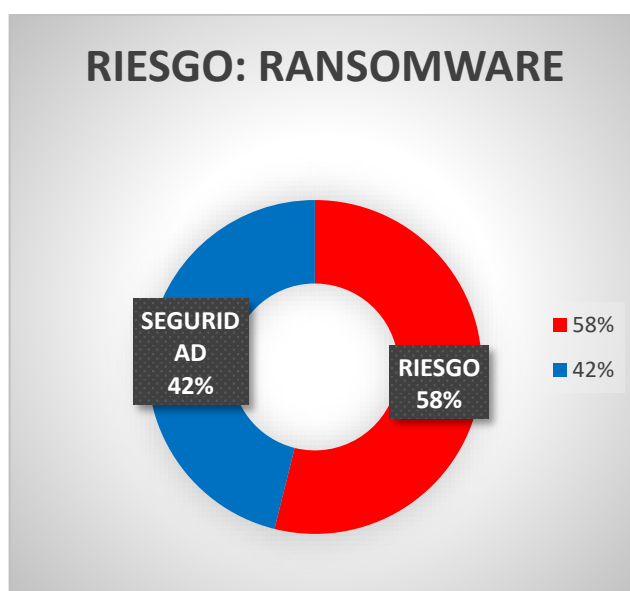
La evaluación de riesgos a todos los docentes de la Extensión El Carmen se pudo establecer que con relación al riesgo PHISHING más de la mitad de los docentes están preparadas para poder sobrellevar cuando sufran algún tipo de vulnerabilidad de este tipo, sin embargo, se debe tomar muy en cuenta a la otra mitad ya que tienen un porcentaje que supera el 46% y alcanzan un riesgo importante en poder sufrir algún tipo de conflicto.

INTERPRETACIÓN: VIRUS



La evaluación de riesgos a todos los docentes de la Extensión El Carmen se pudo establecer que con relación al riesgo VIRUS más de la mitad de los docentes no están preparadas para poder sobrellevar cuando sufran algún tipo de vulnerabilidad de este tipo ya que tienen un porcentaje que supera el 54% y alcanzan un riesgo apreciable en poder sufrir algún tipo de conflicto.

INTERPRETACIÓN: RANSOMWARE



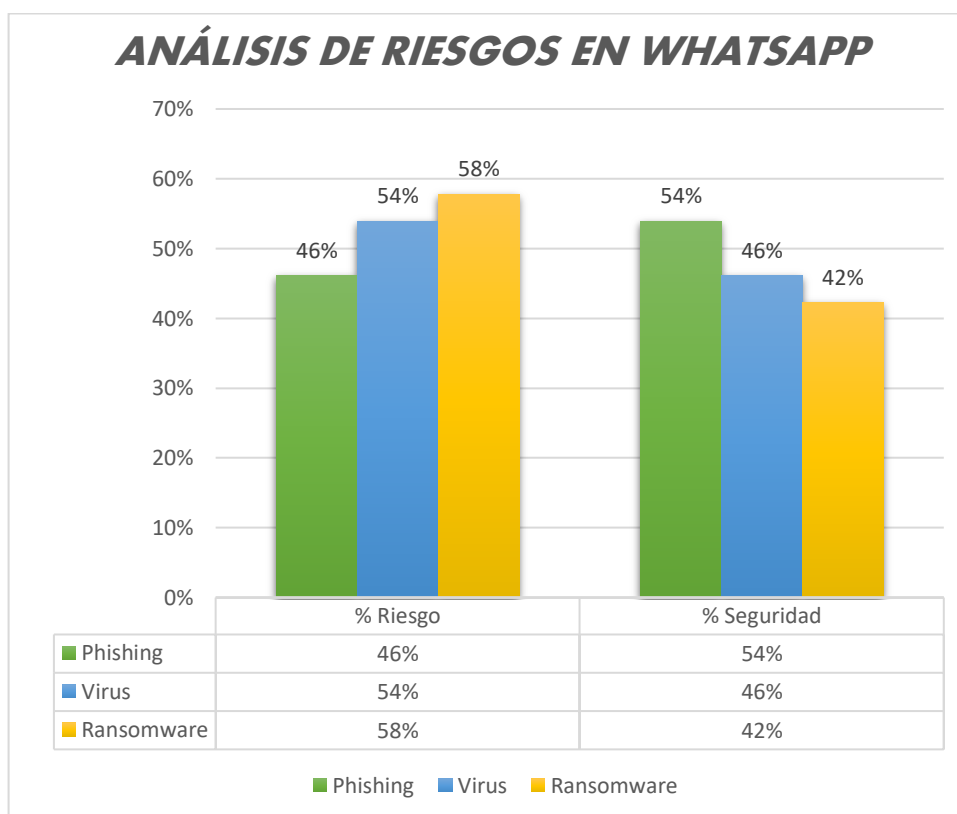
La evaluación de riesgos a todos los docentes de la Extensión El Carmen se pudo establecer que con relación al riesgo RANSOMWARE la mayoría de los docentes no están preparadas para poder sobrellevar cuando sufran algún tipo de vulnerabilidad de este tipo ya que tienen un porcentaje que supera el 58% y alcanzan un riesgo muy grave en poder sufrir algún tipo de conflicto, deben tomar medidas lo antes posible.

INTERPRETACION: ANÁLISIS DE RIESGOS EN WHATSAPP

La evaluación de riesgos de los docentes de la Extensión El Carmen se pudo establecer que con relación al riesgo RIESGOS EN WHATSAPP todos los docentes están en un peligro constante, ya que alcanzan un nivel de riesgo

importante, apreciable y muy grave por lo cual se deben tomar medidas inmediatas para poder saber cómo sobrellevar este tipo de vulnerabilidad.

En la auditoría informática de seguridad de la información realizada a los docentes de la Extensión El Carmen se diagnosticaron tres riesgos importantes que evalúan la seguridad de los datos de los docentes los cuales fueron phishing, virus y ransomware, se obtuvo como resultado que de los docentes evaluados la mayor parte están expuestas a que le puedan suceder cada uno de estos riesgos con un nivel de riesgo muy grave e importante requiriendo medidas preventivas urgentes para mantener controlados los peligros que se puedan presentar en la información de los docentes.



Luego examinar cada pregunta del cuestionarios por vulnerabilidad de cada docente de la extensión se logró apreciar lo siguiente, que todos están vulnerables a que les pueda ocurrir algún riesgo, en el grafico que se muestra que la mayoría de los docentes están expuestos a los riesgos establecidos cómo puede ser el phishing, virus o ransomware que en la mayoría de los docentes

superan un porcentaje del 50% señalando un nivel de riesgo muy grave e importante dando la advertencia que requieren de medidas preventivas urgentes para poder controlar que se cometan los riesgos encontrados y afecten de manera directa a la información de los docentes.

3.11 Conclusiones de la Auditoría

Al concluir con el proceso de auditoría se indica que es de mucha importancia desarrollar una auditoría de seguridad de la información entre periodos no muy lejanos en la Extensión El Carmen.

Es necesario considerar el riesgo que los docentes tienen para que pueda afectar de forma muy grave la información de cada uno de ellos, además se debe garantizar la integridad, eficiencia y calidad de información de carácter personal que cada uno maneja.

En la evaluación que se realizó a los 15 docentes de la Extensión El Carmen se revela el nivel actual de los docentes ante cómo actuar sobre un riesgo, esto es muy grave, ya que los docentes no tienen una idea clara de cómo sobrellevarlo, además de no seguir un control establecido que mejore el uso de la información que se maneja dentro de aplicaciones como WhatsApp y en los dispositivos tecnológicos.

3.12 Recomendaciones de la Auditoría

Para mantener de forma adecuada la información de carácter personal o institucional que manejan los docentes de la Extensión se recomienda seguir un proceso estricto para el manejo de esta

La finalidad de esta investigación juntamente con el informe es entregar una guía de buenas prácticas que ayude a que los docentes adapten a medidas diferentes, esto se lo puede revisar en el Anexo B.

4 CONCLUSIONES

Se puede concluir de esta investigación lo siguiente:

- Este trabajo de titulación se pudo soportar en bibliografía de autores expertos en el tema y con pocos años atrás de sus publicaciones .
- El diagnóstico se realizó con los docentes de la Universidad Laica Eloy Alfaro Extensión El Carmen, tomándose una muestra discrecional de 19 docentes por la falta de disponibilidad de algunos, siendo esta muestra la que permitió realizar un análisis de que la investigación tenía un fin factible.
- La auditoría se pudo aplicar a los docentes, teniéndose datos muy concretos que revelaron algunas falencias en la seguridad y manejo de datos de los docentes
- Así mismo se concluye que en la protección de datos algunos docentes no tienen conocimiento fundamentado en la seguridad de la información, por lo cual se propone poder usar una guía de buenas prácticas que se muestra como anexo en este documento.

5 RECOMENDACIONES.

Al terminar esta investigación se recomienda:

- Actualizar en futuras investigaciones datos de estudios de acuerdo con autores en esta área que puedan servir de referencia y soporte de investigaciones.
- Revisar de manera constante por parte de administradores de internet en cuanto al tráfico de uso de aplicaciones en especial de redes sociales que puedan conllevar a robo de datos
- Dejar abierta la posibilidad de poder realizar nuevas investigaciones en cuanto a periodos futuros que demuestren la evolución de la protección de datos conforme al cambio de las tecnologías usadas en este campo.

6 Bibliografía

Capacho , J. P., & Nieto Bernal, W. (2017). *Diseño de base de datos*. España: Universidad del Norte.

Celaya, L. A. (2014). *Cloud: herramientas para trabajar en la nube*. España: Editorial ICB.

Lerma Blasco, R., Murcia Andrés, J. A., & Mifsud Talón, E. (2013). *Aplicaciones web*. España: McGraw-Hill España.

Albacete, J. F. (2015). *Seguridad en equipos informáticos (MF0486_3)*. Málaga: IC Editorial.

Álvarez Heredia, F. (2016). *Calidad y auditoría en salud*. Bogotá: Ecoe Ediciones.

Alzate, A. T. (s.f.). *AUDITORIA DE SISTEMAS una vision practica*. Univ. Nacional de Colombia.

Andrés, D. M. (2014). *Aplicaciones ofimáticas (2a. ed.)*. Madrid: RA-MA Editorial.

Arias, Á. (2014). *Computación en la Nube*.

Arias, Á. (2014). *Computación en la Nube*. Galicia, España: IT Campus Academy.

Aseguramiento, C. d. (2018). *Guías de auditoría*. México: Instituto Mexicano de Contadores Públicos.

- Aurtenetxe, J. L. (2019). *Métodos y técnicas de investigación social*. España: Publicaciones de la Universidad de Deusto.
- Ávila, Ó. (24 de Mayo de 2011). *ContactoS*. Obtenido de <http://www2.izt.uam.mx/newpage/contactos/anterior/n80ne/nube.pdf>
- Ayjón, M. M. (2020). *LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN LA JUSTICIA PENAL*. Barcelona: J.M. BOSCH EDITOR.
- Baca Urbina, G. (2016). *Introducción a la Informática*. México: Grupo Editorial Patria.
- Baca Urbina, G. (2016). *Introducción a la Seguridad Informática*. Mexico: Grupo Editorial Patria.
- Baena Paz, G. M. (2017). *Metodología de la Investigación 3ra edición*. México: Grupo Editorial Patria.
- Baquero, J. (2015). *METODOLOGÍA DE LA INVESTIGACIÓN JURÍDICA*. Quito : Corporación de Estudios y Publicaciones.
- Baz Rodríguez, J. (2019). *Privacidad y protección de datos de los trabajadores en el entorno digital*. España: Wolters Kluwer España.
- Berenguel, J. (2016). *Desarrollo de aplicaciones web en el entorno servidor*. España: Renginfo S.A.
- Bermúdez Gómez, H. (2016). *Auditoría y control, reflexiones a la luz de la legislación*. Bogotá: Ediciones de la U.
- Beynon-Davies, P. (2014). *Sistemas de bases de datos*. España : Reverte S.A.
- Blanco Encinosa, L. J. (2008). Editorial Félix Varela.

Blanco Encinosa, L. J. (2008). Editorial Félix Varela.

Blanco, J. B. (2015). *METODOLOGÍA DE LA INVESTIGACIÓN JURÍDICA*.
Quito: Departamento Jurídico Editorial - CEP.

Blázquez, B. H. (2001). *Técnicas estadísticas de investigación social*. Madrid:
Días Santos S.A .

Borrego, D. D., Cantú, D., & Olivares, N. (2017). *Educación a Distancia Y Tic*.
EE.UU.

Burzaco Samper, M. (2020). *PROTECCIÓN DE DATOS PERSONALES*. Madrid:
Dykinson.

Caballero , Gónzales, C., & Clavero Garcia. (2016). *Sistemas de
almacenamiento*. España: Paraninfo S.A.

Cabello, A. L. (2014). *Desarrollo de aplicaciones web distribuidas*. España: IC
Editorial.

Calvo, N. d. (2014). *Gestión de archivos (transversal) (MF0978_2)*. Madrid:
Editorial CEP, S.L.

Candil, I. M. (2017). *Gestión de archivos: MF0978_2*. Cano Pina.

Carvalho, A. V. (2012). *Auditoría de inteligencia*. Asturias: Ediciones Trea.

Cazurro Barahona, V. (2020). *Antecedentes y fundamentos del Derecho a la
protección de datos*. Barcelona: J.M. BOSCH EDITOR.

Cazurro Barahona, V. (2020). *Antecedentes y fundamentos del Derecho a la
protección de datos*. España: J.M. BOSCH EDITOR.

- Chaparro, C. G. (2016). *CUADERNO DEL ALUMNO Gestión contable y gestión administrativa para auditoría Auditoría (MF0232_3)*. Madrid: Editorial CEP, S.L.
- Chaparro, C. G. (2016). *MANUAL Gestión contable y gestión administrativa para auditoría Auditoría (MF0232_3)*. Madrid: Editorial CEP, S.L.
- Chavarría Paniagua, C. (2014). *Auditoría administrativa*. México: Editorial Digital UNID.
- Chavarría Paniagua, C. (2015). *Auditoría Administrativa*. México: Editorial Digital UNID.
- Chávez, C. F. (2019). *METODOLOGÍA DE LA INVESTIGACIÓN ASÍ DE FÁCIL*. Córdoba, Argentina: El Cid Editor.
- Cierco, D. (2011). *Cloud computing: retos y oportunidades*. Madrid, España: Ideas.
- Comamala, J. P. (2015). RA-MA Editorial.
- Contreras, M. Á. (2016). *Desarrollo de aplicaciones web multiplataforma*. Ministerio de Educación de España.
- Cristea Uivaru, L. (2018). *La protección de datos de carácter sensible: Historia Clínica Digital y Big Data en Salud*. Barcelona: J.M. BOSCH EDITOR.
- Cuesta, M. J. (2014). *Gestión auxiliar de archivo en soporte convencional o informático (transversal) (UF0513)*. Madrid : Editorial CEP, S.L.
- Davara Rodríguez, M. Á.-D.-D. (2020). *Reglamento Europeo de Protección de Datos y la LOPDGDD: Todo lo que necesitas saber*. Madrid: Wolters Kluwer España.

- Dávila, G. (2014). *Metodología de la investigación*. México: Grupo Patria.
- Dávila, G. G. (2015). *Metodología de la investigación*. México: Grupo Editorial Patria.
- Derrien, Y. (2009). Marcombo.
- Derrien, Y. (2009). *Técnicas de la auditoría informática*. Barcelona : Marcombo.
- Domingo Herrero, R., & Estrella Sanchez, O. (2014). *Archivo y comunicación*. España: Paninfo S.A.
- Domínguez, A. G. (2016). *NUEVOS RETOS PARA LA PROTECCIÓN DE DATOS PERSONALES En la Era del Big Data y de la computación ubicua*. Madrid: Dykinson.
- Echeverría, P. M. (2017). *Internet Útil*. España: Ministerio de Educación de España.
- Elizondo, M. I. (2014). *Archivos históricos de Navarra. Tipología y documentación de los archivos*. Universidad Navarra.
- Feijóo, S. F. (2016). *Técnicas de investigación social y educativa*. Editorial UOC.
- Fernández Guerrero, J. (2014). *Sistemas de almacenamiento*. España: Elearning SL.A.
- Fernández Herrero, C. (2016). *UF1877 - Planificación de proyectos de implantación de infraestructuras*. España: Elearning S.L.
- Fernández, J. P. (2016). *Auditorías y continuidad de negocio*. Málaga: IC Editorial.

- Fernández, P. C. (2015). *UF2401 - Gestión de contenidos web*. España: Elearning S.L.
- Ferrer, M. J. (2015). *Implantación de aplicaciones web en entornos internet, intranet y extranet*. Madrid: RA-MA Editorial.
- García Dihigo, J. (2016). *Metodología de la investigación para administradores*. Bogotá, Colombia: Ediciones de la U.
- García, J. A. (2016). *HTML5, CSS3 y JQuery: curso práctico*. Madrid: RA-MA Editorial.
- García, M. G. (2015). *Fundamentos de Auditoria*. México: Grupo Editorial Patria.
- Gascó, G. E. (2013). Macmillan Iberia, S.A.
- Gascó, G. E. (2013). Macmillan Iberia, S.A.
- Gascó, G. E. (2013). *Seguridad Informatica*. España: Macmillan Iberia, S.A.
- Gómez Berenguel, J. L. (2016). *Desarrollo de aplicaciones web en el entorno servidor*. Madrid: Paraninfo S.A. Obtenido de <https://books.google.com.ec/books?id=gVGACwAAQBAJ&pg=PA67&dq=Herramientas+de+comunicaci%C3%B3n+y+colaboraci%C3%B3n+aplicaciones+web&hl=es&sa=X&ved=0ahUKEwipuJCpg6LnAhXOs1kKHTnWD2sQ6AEIMDAB#v=onepage&q=Herramientas%20de%20comunicaci%C3%B3n%20y%20colaboraci>
- Gómez Carretero, A. I.-G.-M.-R. (2018). *Calidad de Datos*. Madrid: RA-MA Editorial.
- Gonzalo, E. D. (2014). *Gestión de archivos. MF0978*. Editorial Tutor Formación.

- Granados La Paz, R. L. (2014). *Desarrollo de aplicaciones web en el entorno servidor (UF1844)*. Malaga: IC Editorial.
- Grijalbo Fernández, L. (2017). *Realización de auditorías e inspecciones ambientales, control de las desviaciones del SGA. UF1946*. Millan: Editorial Tutor Formación.
- Gualo Cejudo, F. -G.-C.-R. (2019). *Calidad de Datos*. Bogota: Ediciones de la U.
- Guerrero Logroño, R. M. (2017). *Sistemas de archivo y clasificación de documentos. ADGD0208*. Malaga: IC Editorial.
- Herrero, D. R., & Sánchez, Ó. E. (2014). *Archivo y comunicación*. Paraninfo S.A.
- Hincapie Saldarriaga, A. F.-S.-O. (2018). *LA CALIDAD DEL DATO EN LOS SISTEMAS DE INFORMACIÓN DE CONVIVENCIA Y SEGURIDAD CIUDADANA*. Cali: Programa Editorial Universidad del Valle.
- Hormigo, F. J. (2015). *Auditoría de las áreas de la empresa*. Málaga: IC Editorial.
- Jiménez, J. Z. (2013). *Aplicaciones web*. Macmillan Iberia, S.A.
- Jimenez, N. N., Povedano, N. A., García, S. R., & Gonsález, J. M. (2016). *TIC y recursos mediáticos en el aula de Primaria Colección: Didáctica*. España: Paninfo S.A.
- Kluwer, W. (2018). *Cómo sobrevivir al GDPR Todo lo que necesitas saber sobre protección de datos*. Madrid: Wolters Kluwer España.
- Lemos, P. L. (2015). *Cómo documentar un sistema de gestión de calidad según ISO 9001:201*. Madrid: Confemetal.

- López, F. F. (2015). *Sistemas de archivo y clasificación de documentos. UF0347. Tutor Formación* .
- Luna, A. C. (2014). *Creación de páginas web: HTML 5*. España : Editorial ICB.
- Mantilla Blanco, S. A. (2009). Ecoe Ediciones.
- Martín, M. I. (2014). *UF0347 - Sistemas de archivo y clasificación de documentos*. España: Elearning S.L.
- Martínez Sánchez, M. I.-M.-D. (2018). *Metodología de investigación para la educación y la diversidad*. Madrid: UNED - Universidad Nacional de Educación a Distancia.
- Marzo Portera, A. (2015). *Guía Práctica para la Protección de Datos de Carácter Personal*. Barcelona: Ediciones Experiencia.
- Marzo Portera, A. (2015). *La auditoría de seguridad en la protección de datos de carácter personal*. Barcelona: Ediciones Experiencia.
- Marzo Portera, A. (2015). *La Auditoría de Seguridad en la Protección de Datos de Carácter Personal*. Barcelona: Ediciones Experiencia.
- Marzo, A., Macho, A., & Quevedo, P. V. (2015). *La Auditoría de Seguridad en la Protección de Datos de Carácter Personal*. España: Ediciones Experiencia.
- Méndez Rodríguez , A., & Astudillo Moya, M. (2008). *Investigación en la era de la información* . México : Trillas S.A.
- Miguel, T. S. (2015). *Implantación de aplicaciones web en entornos internet, intranet y extranet* . España: Paninfo S.A.

- Molina, J. R., Valarezo, M. R., Honores, J. A., & Elizalde, R. C. (2017). *Utilitarios I. alcoy alicante*, España: Área de innovación y desarrollo.
- Mondelo, A. H. (2014). *Sistemas de archivo y clasificación de documentos: Técnicas y procedimientos*. España: Ideaspropias Editorial.
- Monroy Mejía, M. d.-N. (2018). *Metodología de la Investigación*. México: Grupo Editorial Éxodo.
- Morales, E. G. (2013). *Gestión de documentos en la e-administración*. Barcelona: UOC .
- Murcia, A. A. (2013). *Aplicaciones web*. España: McGraw-Hill España.
- Niño Rojas, V. M. (2019). *Metodología de la Investigación: diseño, ejecución e informe (2a. ed.)*. Bogotá: Ediciones de la U.
- Nsue, J. N. (2019). *Cómo organizar los archivos de los departamentos públicos de Guinea Ecuatorial: ejemplo de la Tesorería General: diseño de un sistema archivístico y de documentación institucional*. Editorial UOC.
- OCDE. (2017). *Perspectivas de la OCDE sobre la Economía Digital 2017*. México: OCDE.
- Oró Badia, R. (2015). *La protección de datos*. Barcelona: Editorial UOC.
- Oró Badia, R. (2015). *La protección de datos*. Barcelona: UOC.
- Ortiz , G. P., & Moreno, A. V. (2018). *La documentación conventual en el fondo diocesano de los archivos eclesiásticos de Mérida-Badajoz*. Ediciones Trea.

- P. C., C. M., & J. M. (2013). *Aplicaciones ofimáticas*. España: Macmillan Iberia, S.A.
- Palomares, F. C. (2017). *Gestión de servicios en el sistema informático: MF0490_3*. Madrid: Editorial CEP, S.L.
- Paz, G. B. (2017). *Metodología de la investigación (3a. ed.)*. México: Grupo Editorial Patria.
- Paz, G. M. (2014). *METODOLOGÍA DE LA INVESTIGACIÓN*. México: Grupo Editorial Patria.
- Paz, G. M. (2014). *METODOLOGÍA DE LA INVESTIGACIÓN*. México: Grupo Editorial Patria.
- Peinado, J. I. (2015). *Métodos, técnicas e instrumentos de la investigación criminológica*. Madrid : DYKISON, SL.
- Pérez Del Castillo, R., García Rodríguez, I., & González Ruiz, F. (2018). *Mantenimiento y evolución de sistemas de información*. Madrid: RA-MA Editorial FECHA.
- Pérez Rodríguez, M. D. (2017). *LEY DE PROTECCIÓN DE DATOS*. Málaga: Editorial ICB.
- Pérez Rodríguez, M. D. (2017). *Ley de Protección de datos (2a. ed.)*. España: Editorial ICB.
- Piattini Velthuis, M. (2015). *AUDITORÍA DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN*. Madrid: RA-MA Editorial.
- Piñar Mañas, J. (2019). *Código Protección de Datos*. Madrid: Wolters Kluwer España.

- Pozo, M. A. (2014). *MF0978_2 - Gestión de archivos*. España : Paraninfo S.A.
- Pretel, G. B. (2018). *La gestión del documento electrónico*. España: Wolters Kluwer España.
- Puertas, J. P. (2014). *Creación de un portal con PHP y MySQL*. España: RA-MA Editorial.
- Ramons, J. (2017). *Productividad en la nube*. Copyring.
- Ramos , J. (2017). *Productividad en la nube*. Copyring.
- Ramos Martín, A. (2014). *Aplicaciones web*. Paraninfo,SA.
- Ramos Martín, A. (2014). *Aplicaciones web*. España: Paraninfo.
- Ramos Martín, A., & Ramos Martín, M. J. (2014). *Aplicaciones Web*. Madrid: Paraninfo, S.A. Obtenido de <https://books.google.com.ec/books?id=43G6AwAAQBAJ&printsec=frontcover&dq=aplicaciones+web&hl=es&sa=X&ved=0ahUKEwia6s6BrMLIAhUEzlkKHSwvAPEQ6AEIJzAA#v=onepage&q&f=false>
- Ramos, J. (2012). *Productividad en la nube*. CopyRing.
- Razo, C. M. (2002). *Auditoría en sistemas computacionales*. Pearson Educación.
- Rebollo Delgado, L. (2014). *VIDA PRIVADA Y PROTECCIÓN DE DATOS EN LA UNIÓN EUROPEA*. Madrid: Dykinson.
- Recio Gayo, M. (2016). *PROTECCIÓN DE DATOS PERSONALES E INNOVACIÓN: ¿(IN)COMPATIBLES?* Madrid: Editorial Reus.

- Recio Gayo, M. (2019). *El ejercicio de los derechos de protección de datos y su aplicación práctica*. Madrid: Wolters Kluwer España.
- Rivas, G. A. (s.f.). *Auditoría informática*. Ediciones Díaz de Santos.
- Rodríguez, J. J. (2015). *MUESTREO Y PREPARACIÓN DE LA MUESTRA*. SL: Cano Pina.
- Rodríguez, M. D. (2015). *Gestión de archivos (MF0978_2) (2a. ed.)*. Editorial ICB.
- Rodríguez, María Dolores Pérez. (2016). *Archivos y documentación (2a. ed.)*. Editorial ICB.
- Romera, G. C. (2017). *Sistema operativo, búsqueda de información: Internet/Intranet y correo electrónico*. España : IC Editorial.
- Santiesteban Naranjo, E. (2014). *METODOLOGÍA DE LA INVESTIGACIÓN CIENTÍFICA*. Las tunas: Editorial Universitaria.
- Santiesteban Naranjo, E. (2014). *METODOLOGÍA DE LA INVESTIGACIÓN CIENTÍFICA*. Las Tunas: Editorial Universitaria.
- Santos, J. C. (2014). RA-MA Editorial.
- Santos, J. C. (2015). *Mantenimiento de la seguridad en sistemas informáticos*. Madrid: RA-MA Editorial.
- Santos, J. C. (2015). *Seguridad Informatica*. Madrid: RA-MA Editorial.
- Sanz, M. L. (2015). *Programación web en el entorno servidor*. España: RA-MA Editorial.

- Serrano, M. J. (2017). *Comunicación y atención al cliente 2.ª edición*. España: Paraninfo S.A. Obtenido de <https://books.google.com.ec/books?id=mdXLDgAAQBAJ&pg=PA84&dq=Herramientas+de+comunicaci%C3%B3n+y+colaboraci%C3%B3n+aplicaciones+web&hl=es&sa=X&ved=0ahUKEwipuJCpg6LnAhXOs1kKHTnWD2sQ6AEIJzAA#v=onepage&q=Herramientas%20de%20comunicaci%C3%B3n%20y%20colaboraci>
- Tapia Iturriaga, C. K.-M.-C. (2019). *Fundamentos de auditoría Aplicación práctica de las Normas Internacionales de Auditoría*. México: Instituto Mexicano de Contadores Públicos.
- Tejada, E. C. (2015). *Auditoría de seguridad informática*. Málaga: IC Editorial.
- Urbano López, M. d. (2015). *Administración y auditoría de los servicios Web*. Andalucía: IC Editorial.
- Urbina, G. B. (2016). *Introducción a la seguridad informática*. España: Grupo Editorial Patria.
- Valenzuela, C. -L. (2017). *GUIA PARA LA REDACCION DE UN PROYECTO DE INVESTIGACION*. Buenos Aires: Espacio Editorial.
- Vázquez, S. E. (2015). Tecnologías de almacenamiento de información en el ambiente digital. *Information storage technologies in the digital environment*.
- Venezuela, U. C. (2019). ORGANIZACION Y METODOS. *Metodología* .
- Vera, A. A. (2015). *Metodología de la investigación*. España: Athenaica Ediciones Universitarias.

Vieites, Á. G. (2015). *Auditoria de Seguridad Informatica* . Madrid: RA-MA Editorial.

Zofío, J. J. (2013). *Aplicaciones web*. Macmillan Iberia, S.A.

ANEXOS

ANEXO A: GUÍA DE BUENAS PRÁCTICAS PARA LA SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN.

ANEXO B: GUÍA DE ENTREVISTA PARA DOCENTES.

ANEXO C: GUÍA DE ENCUESTA PARA LOS DOCENTES.

ANEXO D: FICHA INFORMATIVA.

ANEXO E: CAPTURAS EVIDENCIA DE ENCUESTAS



**GUÍA DE BUENAS PRÁCTICAS PARA LA SEGURIDAD Y PROTECCIÓN DE
LA INFORMACIÓN**

**SEGÚN HALLAZGOS DE LA AUDITORÍA APLICADA EN LA
INVESTIGACIÓN DENOMINADA**

**AUDITORIA INFORMÁTICA PARA PROTECCIÓN DE DATOS
PERSONALES DE LOS DOCENTES DE LA “UNIVERSIDAD LAICA ELOY
ALFARO DE MANABI” EN EL CANTÓN EL CARMEN, PROVINCIA DE
MANABI**

AUTOR

Alfredo Leonardo Medranda Reyes

El Carmen, Enero 2023.

INTRODUCCIÓN.

El control de seguridad de los datos personales es cuestión y responsabilidad de las personas que los manipulan, más sin embargo pueden existir factores externos auspiciados por personas que manipulan programas o métodos para hacer que esta información sea divulgada y al hacerse esta acción puedan ser mal utilizadas, este riesgo se puede correr en distintos momentos y espacios donde se puedan desenvolver los implicados

De esta manera y una vez investigados elementos de uso del internet en la ULEAM Extensión en El Carmen usando sus datos personales de distintas plataformas y modos por parte de algunos docentes se puede llevar a cabo algunas observaciones que eviten la posible futura pérdida de información personal.

Este manual se presenta dando respuestas a los hallazgos encontrados en la auditoría y se espera que sea de mucha utilidad al aplicarlo, en especial al momento de usar aplicaciones como: WhatsApp Web, Facebook y otras redes sociales sensibles al blanco de pérdidas de información personal.

Objetivos.

- Dar a conocer a los docentes y personal de la ULEAM Extensión EL Carmen los lineamientos que se deben seguir al momento de manipular sus datos personales en especial los manejados desde sus ordenadores y móviles.
- Orientar a los docentes con el uso de algunas aplicaciones que permiten ser objetivo de ataques por parte de delincuentes que se pueden aprovechar de algunos eventos para poder delinquir.
- Difundir las buenas prácticas para la seguridad y protección de la información

PHISHING	
Objetivo del control	Prevenir que los docentes tengan altas posibilidades de ser víctimas de páginas fraudulentas o pérdida de información personal.
<ul style="list-style-type: none"> • Instalar un antivirus con anti-phishing, es necesario tenerlo actualizado y con las licencias en orden. • Mantener actualizado el dispositivo, la aplicación y los motores de búsqueda para que los atacantes no encuentren vulnerabilidad. • Atención a enlaces para poder reconocer si son sitios oficiales o no. • Antes de ingresar a cualquier enlace, verifique que el mismo utilice el protocolo https, ya que utiliza un cifrado basado en la seguridad de textos. • Mantener activada la verificación en dos pasos, para que quien entre a nuestra cuenta no tenga acceso a nuestra información. • Ignorar mensajes sospechosos, aunque vengan de algún conocido. Revisar y preguntarle directamente a esa persona el mensaje recibido fue enviado por su voluntad. 	

VIRUS	
Objetivo del control	Prevenir que los docentes tengan altas posibilidades de ser víctimas de programa maligno y mantener un entorno digital estable.
<ul style="list-style-type: none"> • Instalar un antivirus, está de más mencionarlo especialmente si el docente tiene hijos pequeños que utilizan el teléfono constantemente. 	

- No comparta su PIN de verificación en dos pasos con nadie.
- Facilita un correo electrónico en caso de que olvide su PIN.
- Si recibe una notificación de alerta para reestablecer tu código de verificación y tu no realizaste la solicitud, no accedas al enlace. Alguien debe estar intentando tener acceso a tu número telefónico sin tu consentimiento.
- Si un mensaje le parece poco habitual de un conocido, tome el tiempo de hacer preguntas que solo tu conocido pueda responder para verificar que sea seguro.
- Evita descargar aplicaciones de fuentes desconocidas y si llegas hacerlo evita conceder todos los permisos del dispositivo.

ADWARE	
Objetivo del control	Prevenir que los docentes tengan altas posibilidades de ser víctimas de publicidad maligna.
<ul style="list-style-type: none"> • Instalar un antivirus que cuente con la herramienta “bloquear publicidad no deseada”. • Considere poner la privacidad de su foto de perfil solo para contactos conocidos ya que los ciber atacantes pueden tomarla y tener acceso a su información mediante los motores de búsqueda. • Evite enviar información personal mediante esta aplicación, haciendo referencia a datos bancarios, dirección domiciliaria o correos que contengan información confidencial. • Tenga cuidado si se encuentra en una página que no inspira confianza, hacer clic en un botón o en una página emergente es suficiente para adquirir Adware. 	

- Si un mensaje le parece poco habitual de un conocido, tómese el tiempo de hacer preguntas que solo tu conocido pueda responder para verificar que sea seguro.
- Cuando acceda a WhatsApp Web, y ya haya dejado de utilizar esta herramienta, recuerde cerrar sesión desde su teléfono en “Dispositivos vinculados” tendrá la opción de cerrar todas las sesiones.
- Tiene la opción de activar las notificaciones de seguridad, es un código que tiene cada chat y en caso de este cambio, te llegara una notificación de que se accedió al chat desde otro nuevo dispositivo.

MANEJO DE SESIONES Y CONTRASEÑAS	
Objetivo del control	Concienciar a los docentes para que tengan precaución al dejar sesiones abiertas en las redes sociales y evitar dejar grabadas contraseñas.
<ul style="list-style-type: none"> • Considere siempre revisar el cierre de sesión en programas o aplicaciones que solicitan claves para el acceso • No grabe contraseñas cuando el navegador lo pida que lo haga, ya que si lo hace en especial en navegadores usadas en computadoras no personales esto puede ser objeto a que la usen de manera fraudulenta. • Evite al ingresar a un programa que alguien este cerca o analice su clave, así como colóquese fuera del alcance de cámaras que puedan grabar su acceso • En lo posible convine el ingreso a sus paginas privadas con pines enviados a su teléfono personal 	

Anexo B: GUÍA DE ENTREVISTA PARA DOCENTES..

ENTREVISTA

- 1. ¿Dispone de un software o programa antivirus que proteja su dispositivo móvil en el cual usted realiza sus actividades de docentes?**
 - No
 - No
 - Si
- 2. ¿Qué conocimiento tiene sobre los ataques informáticos dentro del ámbito laboral?**
 - Muy poco
 - Lo básico
 - Que existen ataques informáticos, existen los famosos hackers.
- 3. ¿Conoce sobre el termino Ciberseguridad?**
 - No
 - Si
 - Si, proteger la información pública y privada.
- 4. ¿Tiene algún conocimiento previo a la Criptografía?**
 - No
 - No
 - No
- 5. ¿Conoce lo que es una amenaza, una vulnerabilidad y un riesgo?**
 - Si
 - No
 - Si, riesgo es una amenaza existente, vulnerabilidad es peligro.
- 6. ¿Conoce sobre los ataques informáticos internos o externos que se pueden dar en la Universidad?**
 - No
 - No
 - Si, tenemos el conocimiento que puede haber ataques en las notas de los alumnos.
- 7. ¿Conoce sobre las vulnerabilidades que se expone un docente al compartir información por WhatsApp?**
 - No
 - No
 - Si, peligro permanente en todas las redes sociales, por esta razón no dar datos personales o privados.
- 8. ¿Ha existido algún ataque informático que haya perjudicado a usted como docente dentro de la institución?**
 - No
 - No
 - No, ha existido ni como docente ni como institución.

9. ¿Conoce si dentro de la Universidad se manejan políticas para proteger la seguridad de la información de los docentes? ¿Cuáles son esas políticas?

- Desconozco
- Desconozco
- Si, Contraseñas privadas, Red de docente privada, uso personal de los equipos de cómputo docencia.

10. ¿Se permite el acceso a los servidores a todo personal?

- No
- No
- No, solo personal del departamento de administración.

11. ¿Qué tipo de ataque de seguridad usted ha enfrentado y qué hizo usted para resolverlo?

- Ninguno
- Ninguno
- Ninguno

12. ¿Maneja usted cursos de actualización o políticas de seguridad para enfrentarse a la inseguridad constante que se produce a través de Ciberataques?

- No
- No
- Si, los académicos permanente actualización, mas ahora en la era digital.

ANEXO C:

ENCUESTA A DOCENTES

Preguntas
¿Usted utiliza la herramienta WhatsApp?
¿Con qué fin usa usted WhatsApp?
De los siguientes recursos, señale cuáles usted utiliza más
¿El uso constante del WhatsApp, le parece útil aplicarlo en su docencia?
¿Cree usted que es importante la protección de los datos personales en WhatsApp?
¿Con quienes usted interactúa más por medio de WhatsApp con diferentes tipos de información?
¿Cree usted que pueden existir vulnerabilidades en WhatsApp al momento de compartir información?
Cuando usted recibe información por WhatsApp, al ser un número desconocido ¿Usted abre el enlace compartido?

¿Conoce usted los distintos ataques informáticos que existen?

De la siguiente lista de ataques informáticos, señale los que usted conoce

¿A qué considera usted un ataque informático?

¿Le gustaría a usted tener información de que tratan los ataques informáticos y como evitarlos?

Sería factible de que usted posea una guía digital para conocer y enfrentar los diferentes tipos de ataques informáticos

ANEXO D:

FICHA INFORMATIVA.

CUESTIONARIO PARA IDENTIFICAR RIESGOS VINCULADOS A LA PROTECCIÓN DE DATOS PERSONALES EN DOCENTES			
RIESGO: PHISHING		SI	NO
1.	¿Revisa usted el propietario de algún tipo de correo antes de abrirlo?		
2.	¿Instaló usted WhatsApp desde las tiendas oficiales?		
3.	Al instalar y ejecutar WhatsApp, ¿Leyó y analizó las políticas y condiciones?		
4.	¿Ingresaría usted datos personales en una página sin saber su procedencia lícita?		
5.	¿Ha llenado formularios con información personal?		
6.	¿Ha recibido usted mensajes requiriendo códigos ilegales para autenticación de WhatsApp?		
7.	¿Ha podido identificar en algún momento un contacto de con mensajes fraudulento?		

8.	¿Ha sido víctima de fraudes por medio de WhatsApp donde se le piden sus datos personales?		
9.	¿Cree usted que los archivos que comparte por medio de WhatsApp están expuestos?		
10.	¿Abre usted archivos adjuntos a mensajes sospechosos antes de comprobar que sean legítimos?		
11.	¿Tiene usted instalado software de seguridad como antivirus en su dispositivo?		
12.	¿Mantiene usted el Sistema operativo y software de su dispositivo actualizados?		

CUESTIONARIO PARA IDENTIFICAR RIESGOS VINCULADOS A LA PROTECCIÓN DE DATOS PERSONALES EN DOCENTES			
RIESGO: VIRUS		SI	NO
1.	¿Conoce usted qué son los virus informáticos?		
2.	¿Conoce usted los tipos de virus informáticos que existen?		

3.	¿Tiene usted instalado en su dispositivo un antivirus?		
4.	¿Sabe usted distinguir un virus informático mientras está usando WhatsApp?		
5.	¿Actualiza de manera correcta y precisa el antivirus en su dispositivo?		
6.	¿Suele usted abrir archivos o documentos en WhatsApp aun cuando no sabe de quien provienen?		
7.	¿Cuándo recibe archivos de un remitente desconocido en WhatsApp, los descargas?		
8.	¿Descarga y ejecuta usted cualquier tipo de archivos en su dispositivo?		
9.	¿Podría usted identificar cuando está ante un virus informático mientras usa WhatsApp?		
10.	¿Conoce usted las formas de propagación de los virus informáticos?		

11.	¿Usa usted la aplicación de WhatsApp en su dispositivo que sea descargada desde las tiendas oficiales?		
12.	¿Conoce usted si su dispositivo está expuesto a contraer un virus informático mientras usa WhatsApp?		

CUESTIONARIO PARA IDENTIFICAR RIESGOS VINCULADOS A LA PROTECCIÓN DE DATOS PERSONALES EN DOCENTES			
RIESGO: RANSOMWARE		SI	NO
1.	¿Conoce usted que un ransomware de bloqueo afecta las funciones básicas de su dispositivo?		
2.	¿Tiene usted en su dispositivo instalado un paquete de antivirus de buena popularidad?		
3.	¿Realiza actualizaciones de la versión del antivirus de manera eficaz que usa en su dispositivo?		
4.	¿Realiza análisis de vulnerabilidades para ayudarle a revelar si hay un intruso en el sistema?		

5.	¿Ha recibido alertas de parte de su antivirus reportando actividades maliciosas?		
6.	¿Ha realizado usted actualizaciones recientes del sistema operativo que usan su dispositivo?		
7.	¿Al momento de usted instalar un programa en su dispositivo le da la debida atención a los premisos que estos requieren?		
8.	¿Al momento de usted instalar un programa en su dispositivo le da la debida atención a los premisos que estos requieren?		
9.	Cuando usted recibe mensajes inesperados mediante WhatsApp, ¿revisa el contacto antes de abrirlos?		
10.	En los grupos de WhatsApp con sus estudiantes ¿se encarga de restringir mensajes de desconocidos?		
11.	¿Realiza usted respaldos en la nube de su información de manera periódica?		
12.	¿Su versión de WhatsApp se encuentra actualizada?		

ANEXO E:

CAPTURA EVIDENCIA DE ENCUESTA A DOCENTES

