UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO

DIVISIÓN ACADÉMICA DE INFORMÁTICA Y SISTEMAS

PROPUESTA DE MEDIDAS Y LINEAMIENTOS DE SEGURIDAD. CASO: CONSULTORIOS PSICOPEDAGÓGICOS DE LA UJAT

Trabajo recepcional bajo la modalidad de Tesis
que para obtener el grado de:

Maestro en Administración
de Tecnologías de la Información

Presenta:

Armando de Jesús Olán Crasbor

Directores de Trabajo Recepcional:

Dra. Martha Patricia Silva Payró
Dr. Pablo Pancardo García

Cuerpos Académicos o Grupos de Investigación de los Directores:

Gestión de Tecnologías de la Información
Sistemas Distribuidos

Línea de Generación y Aplicación del Conocimiento de la Maestría que alimenta la investigación:

Administración, Diseño e Implementación de Integración de Soluciones de TI.

Cunduacán Tabasco Octubre del 2019

Carta de autorización

El que suscribe, autoriza por medio del presente escrito a la Universidad Juárez Autónoma de Tabasco para que utilice tanto física como digitalmente la Tesis de Maestría **"Propuesta de medidas y lineamientos de seguridad. Caso: consultorios psicopedagógicos de la UJAT"**, de la cual soy autor y titular de los Derechos de Autor.

La finalidad del uso por parte de la Universidad Juárez Autónoma de Tabasco de la tesis antes mencionada, será única y exclusivamente para difusión, educación, sin fines de lucro; autorización que se hace de manera enunciativa más no limitativa para subirla a la Red Abierta de Bibliotecas Digitales (RABID) y a cualquier otra Red Académica con las que la Universidad tenga relación institucional.

Por lo antes mencionado, libero a la Universidad Juárez Autónoma de Tabasco de cualquier reclamación legal que pudiera ejercer respecto al uso y manipulación de la Tesis antes mencionada y para los fines estipulados en este documento.

Se firma la presente autorización en la Ciudad de Villahermosa, Tabasco a los 21 días del mes de octubre del año 2019.

AUTORIZO

C. Armando de Jesús Olán Crasbor

UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO

"ESTUDIO EN LA DUDA. ACCIÓN EN LA FE"

DAIS
11111000011

INSTITUTO JUÁREZ 1819-2019

Oficio No. 2418/2019/DAIS/D
21 de octubre de 2019

Dra. Martha Patricia Silva Payró
Profesor-Investigador
Presente

De acuerdo al artículo 46 fracción III del Reglamento General de Estudios de Posgrado Vigente, de la Universidad Juárez Autónoma de Tabasco, me permito informarle a Usted, que ha sido asignado director del trabajo de tesis titulado **"PROPUESTAS DE MEDIDAS Y LINEAMIENTOS DE SEGURIDAD. CASO: CONSULTORIOS PSICOPEDAGÓGICOS DE LA UJAT"**, a realizar por el **C. Armando de Jesús Olán Crasbor**, para obtener el grado de Maestro en Administración de Tecnologías de la Información.

Sin otro particular, aprovecho la ocasión para enviarle un afectuoso saludo.

Atentamente

UNIVERSIDAD JUAREZ AUTONOMA DE TABASCO

MTE. Oscar Alberto González González
Director

DIVISION ACADEMICA DE INFORMATICA Y SISTEMAS

C.c.p. MASI. Arturo Corona Ferreira.-Encargado del Despacho de la Coordinación de Posgrado.
Archivo.
Consecutivo.

Carretera Cunduacán-Jalpa Km. 1, Colonia Esmeralda, C.P. 86690. Cunduacán, Tabasco, México.
E-mail: direccion.dais@ujat.mx
Teléfonos: (993) 358 1500 ext. 6727; (914) 336 0616. Fax: (914) 336 0870

UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO

"ESTUDIO EN LA DUDA. ACCIÓN EN LA FE"

DAIS
11111000011

INSTITUTO JUÁREZ
1879-2019

Oficio No. 2419/2019/DAIS/D
21 de octubre de 2019

Dr. Pablo Pancardo García
Profesor-Investigador
Presente

De acuerdo al artículo 46 fracción III del Reglamento General de Estudios de Posgrado Vigente, de la Universidad Juárez Autónoma de Tabasco, me permito informarle a Usted, que ha sido asignado director del trabajo de tesis titulado **"PROPUESTAS DE MEDIDAS Y LINEAMIENTOS DE SEGURIDAD. CASO: CONSULTORIOS PSICOPEDAGÓGICOS DE LA UJAT"**, a realizar por el **C. Armando de Jesús Olán Crasbor**, para obtener el grado de Maestro en Administración de Tecnologías de la Información.

Sin otro particular, aprovecho la ocasión para enviarle un afectuoso saludo.

Atentamente

UNIVERSIDAD JUAREZ AUTONOMA DE TABASCO
21 OCT 2019

MTE. Óscar Alberto González González
Director

DIVISION ACADEMICA DE INFORMATICA Y SISTEMAS

C.c.p. MASI. Arturo Corona Ferreira.-Encargado del Despacho de la Coordinación de Posgrado.
Archivo.
Consecutivo.

Carretera Cunduacán-Jalpa Km. 1, Colonia Esmeralda, C.P. 86690, Cunduacán, Tabasco, México
E-mail: direccion.dais@ujat.mx
Teléfonos: (993) 358 1500 ext. 6727; (914) 336 0616; Fax: (914) 336 0870

Maestría CUMEX desde 2008
Consorcio de Universidades Mexicanas
UNA ALIANZA DE CALIDAD POR LA EDUCACIÓN SUPERIOR

UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO

"ESTUDIO EN LA DUDA. ACCIÓN EN LA FE"

DIVISIÓN ACADÉMICA DE INFORMÁTICA Y SISTEMAS

Cunduacán Tabasco 14 octubre 2019

En la Universidad Juárez Autónoma de Tabasco, de acuerdo al Reglamento de Estudios de Posgrado vigente, se revisó el trabajo de investigación titulado **"PROPUESTA DE MEDIDAS Y LINEAMIENTOS DE SEGURIDAD. CASO: CONSULTORIOS PSICOPEDAGÓGICOS DE LA UJAT"**, realizado por el **C. Armando de Jesús Olán Grasbor**, para obtener el Grado de Maestro en Administración de Tecnologías de la Información bajo la modalidad de Tesis.

Los integrantes del jurado, después de revisar el trabajo, lo declararon aceptado. Firmando la presente a los 14 del mes de octubre de 2019.

Dra. Marbella Araceli Gómez Lemus

MASI. Arturo Corona Ferreira

Dr. Herman Aguilar Mayo

UNIVERSIDAD JUAREZ AUTONOMA DE TABASCO
RECIBIDO
23 OCT. 2019
D.A.I.S.
COORDINACIÓN DE INV. Y POSGRADO

Carretera Cunduacán-Jalpa Km. 1, Colonia Esmeralda, C.P. 86690. Cunduacán, Tabasco, México.
E-mail: direccion.dais@ujat.mx
Teléfonos: (993) 358 1500 ext. 6727; (914) 336 0616; Fax: (914) 336 0870

DAIS
1111100001

UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO

"ESTUDIO EN LA DUDA. ACCIÓN EN LA FE"

DAIS
11111000011

INSTITUTO JUÁREZ
1879-2019

Oficio No. 2417/19/DAIS/D
21 de octubre de 2019

C. Armando de Jesús Olán Crasbor
Matrícula 172H11003

En virtud de que cumple satisfactoriamente los requisitos establecidos en el Reglamento General de Estudio de Posgrado vigente en la Universidad, informo a Usted que se autoriza la impresión del trabajo recepcional **"PROPUESTA DE MEDIDAS Y LINEAMIENTOS DE SEGURIDAD. CASO: CONSULTORIOS PSICOPEDAGÓGICOS DE LA UJAT"**, para presentar examen y obtener el Grado de Maestro en Administración de Tecnologías de la Información bajo la modalidad de Tesis.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente

UNIVERSIDAD JUAREZ AUTONOMA DE TABASCO

MTE. Óscar Alberto González González
Director

DIVISION ACADEMICA DE INFORMATICA Y SISTEMAS

C.c.p. MASI. Arturo Corona Ferreira.- Encargado del Despacho de la Coordinación de Posgrado.
Archivo.
Consecutivo.

Carretera Cunduacán-Jalpa Km. 1, Colonia Esmeralda. C.P. 86690. Cunduacán, Tabasco, México.
E-mail: direccion.dais@ujat.mx
Teléfonos: (993) 358 1500 ext. 6727; (914) 336 0616; Fax: (914) 336 0870

Agradecimientos

Agradecimientos a mis directores de tesis que me apoyaron en la realización de la misma y sin ellos este proyecto no hubiese sido posible.

Un agradecimiento especial a los psicólogos de la UJAT que aceptaron participar en este proyecto.

Dedicatorias

Dedicado a mi madre, que siempre me brindó su apoyo a lo largo de esta travesía.

Resumen

La seguridad de la información es un elemento que muchas empresas e instituciones a menudo pasan por alto, incluso, a veces no saben cómo implementar medidas de seguridad que resguarden la información sensible que poseen. En ese sentido, el principal objetivo de este trabajo de investigación es diseñar un modelo de seguridad, conforme al estándar ISO 27001, para los consultorios psicopedagógicos de la Universidad Juárez Autónoma de Tabasco. Los psicólogos de la UJAT manejan información sensible de la atención que realizan a sus pacientes en el día a día y, como resultado de la investigación se encontró que la información no se protege conforme a medidas o lineamientos que aseguren que la integridad de la misma no se ve afectada y qué, por lo tanto, la información se encuentre segura; ya que, si esta llegase a filtrarse o ser robada, representaría una enorme violación a la privacidad de los pacientes. Este proyecto se basa en el diseño de un modelo de seguridad, el cual implementa medidas y prácticas de seguridad a la información sensible que los psicólogos manejan para mantenerla protegida, y así tener la certeza de que dicha información se encuentra segura y bien resguardada.

Introducción

El proyecto de investigación tiene como objetivo diseñar un modelo de seguridad para los consultorios psicopedagógicos de la Universidad Juárez Autónoma de Tabasco, conforme al estándar 27001.

Para ello, se aplicó una encuesta a los psicólogos que laboran en la Universidad Juárez Autónoma de Tabasco y, de acuerdo a sus respuestas, se propone un modelo de acción que toma como base el estándar ISO 27001. Como resultado, se ha estructurado este reporte de investigación de la siguiente forma:

Capítulo 1. Antecedentes. En este apartado se muestran los datos de estudio del proyecto de investigación, citando diversos autores y poniendo ejemplos de métodos de seguridad en otras instituciones.

Capítulo 2. Marco Teórico. En este capítulo, se presenta la teoría necesaria para comprender el funcionamiento de las normas ISO empleadas en el proyecto de investigación, así como el vocabulario empleado en el mismo.

Capítulo 3. Aplicación de la metodología y desarrollo. En este capítulo se describen los pasos llevados a cabo en la obtención de resultados. En el caso de este proyecto de investigación, se muestra el proceso empleado para redactar la encuesta aplicada a los psicólogos de la UJAT, así como el proceso de aplicación.

Capítulo 4. Resultados. Se describen los resultados obtenidos producto de la aplicación de la metodología.

Capítulo 5. Conclusiones, recomendaciones y trabajos futuros. En este apartado se presentan las conclusiones obtenidas de todo el proyecto, así como recomendaciones para llevar a cabo una investigación y los trabajos futuros que puedan efectuarse, teniendo como fundamento esta investigación

Índice general

Índice de tablas ..... **¡Error! Marcador no definido.**

Índice de figuras xvi

Capítulo 1. Generalidades 1

1.1 Antecedentes 1

1.2 Planteamiento del problema 4

1.2.1 Definición del problema 4

1.2.2 Delimitación de la investigación 5

1.2.3 Preguntas de investigación 6

1.2.4 Objetivos 6

1.3 Justificación 7

1.4 Metodología utilizada 9

Capítulo 2. Marco teórico 11

2.1 Marco referencial 11

2.2 Marco conceptual 12

2.2.1 ISO 27001 12

2.2.2 ISO/IEC 27002 15

2.2.3 Seguridad de la información 16

2.2.4 Información sensible 17

Capítulo 3. Aplicación de la metodología y desarrollo 20

3.1 Tipo y diseño de investigación 20

3.2 Depuración de la población 21
3.3 Diseño de instrumentos 22
3.4 Información general 23
3.5 Aplicación de la prueba piloto 25
3.6 Aplicación del instrumento 25
3.7 Aplicación del cuestionario 26
Capítulo 4. Resultados 27
4.1 La población de estudio y consultas diarias 27
4.2 Medidas relativas a las prácticas de la seguridad de la información 27
4.3 Medidas relativas a las prácticas de la seguridad de la información 29
4.4 Acciones llevadas a cabo para preservar la información sensible 31
Capítulo 5.Propuesta de modelo de buenas prácticas de seguridad de la información 34
5.1 Introducción al modelo 34
5.2 Modelo de prácticas y lineamientos de Seguridad de la Información 35
Capítulo 6. Conclusiones, recomendaciones y trabajos futuros. 43
6.1 Conclusiones 43
6.2 Recomendaciones 45
6.3 Trabajos futuros 46
Referencias 47
Glosario 52
Apéndice A. Cuestionario aplicado a los psicólogos de la UJAT 53

Índice de tablas

Tabla 1 Escala de resguardo de información 24

Tabla 2 Divulgación de las buenas prácticas de seguridad de la información 28

Tabla 3 Confianza en la seguridad de la UJAT 29

Tabla 4 Medidas y directrices..... 38

Índice de figuras

Figura 1 Esquema Plan-Do-Act-Check 14

Figura 2 Pasos esenciales del model*o* 35

Figura 3 Esquema de departamentos 37

Capítulo 1. Generalidades

1.1 Antecedentes

En la actualidad, las instituciones y organizaciones hacen un uso intensivo de las Tecnologías de la Información (TI), Areitio (2008) menciona que es necesario integrar políticas y medidas de seguridad a los sistemas informáticos en red que garanticen el desarrollo y sostenibilidad del negocio, manteniendo la confidencialidad, la integridad, la disponibilidad y la usabilidad autorizada de la información. Lo anterior adquiere especial importancia y pone en consideración la necesidad de profesionales capaces de asegurar y mantener la seguridad de la información en los sistemas, ante las amenazas del presente y del futuro.

La seguridad de la información es un proceso en el cual se da cabida a un creciente número de elementos: aspectos tecnológicos, de gestión-organizacionales, de recursos humanos, de índole económica, de negocios, de tipo legal, de cumplimiento, entre otros; Areitio refiere que abarcan no sólo aspectos informáticos y de telecomunicaciones, sino también aspectos físicos, medioambientales, humanos, etc.

Como menciona Voutssas (2010), la información es un activo muy valioso para casi todas las organizaciones; para algunas de ellas es su activo más valioso y por ello se invierten considerables recursos en crearla, administrarla, mantenerla, distribuirla, etcétera.

Benavides, Enríquez y Solarte (2015) mencionan que tanto los análisis como la evaluación de riesgos, así como la verificación de controles de seguridad existentes, las

pruebas con software y el monitoreo de sistemas de información permiten establecer el estado actual de la organización, identificar las causas de cualquier vulnerabilidad y proponer soluciones de control, lo cual permite su mitigación.

Para poder asegurar la correcta administración de la seguridad de la información, Mendoza (2014) señala que se debe establecer y mantener acciones que cumplan con los tres requerimientos de mayor importancia para la información, que son la confidencialidad, la integridad y la disponibilidad.

En la actualidad se pueden encontrar organizaciones tales como Organizaciones no Gubernamentales (ONG) u organizaciones educativas como universidades, que afirman les preocupa la seguridad de la información, pero que carecen de personal formado para la seguridad, no disponen de un presupuesto explícito para tal fin o que no investigan los incidentes de seguridad, o bien creen que su negocio carece de interés para cualquier atacante potencial. Areitio (2008) afirma que este tipo de actitudes en cuanto a la seguridad ayuda a que los atacantes utilicen estas empresas para sus fines lucrativos y delictivos.

Tarazona (2007) menciona que las organizaciones públicas o privadas, así como las personas, dependen de cierta manera de la tecnología de la información como una herramienta esencial para lograr sus objetivos de negocio o para poder desarrollar actividades en su vida cotidiana; al mismo tiempo, todos tienen que enfrentarse con una amplia gama de amenazas y vulnerabilidades asociadas a los entornos informáticos de hoy.

La seguridad de la información se establece en las organizaciones independientemente del giro de estas, y es que la información es uno de los elementos más importantes, el cual, si se hace mal uso del mismo, puede acarrear problemas graves tanto para la organización como para los miembros de ésta.

Como se mencionó anteriormente, existen organizaciones como las escuelas o en este caso universidades, que guardan información sensible de forma física y lógica acerca de los alumnos que asisten a dicha institución, por ejemplo, archiveros o servidores localizados en el área designada para los mismos. Desde información personal como la edad o el año y fecha de nacimiento, hasta el nombre de sus padres y tutores o la dirección de su domicilio actual.

La información debe ser protegida de manera tal que solamente la persona que va a hacer uso y manejo de la información tenga acceso a ella. Utilizando un autenticador de personal para acceder a la sala de servidores donde se guarda la información es un buen primer filtro. Seguido de esto, otro autenticador en la máquina donde se resguarda la información y, para mayor seguridad, los datos estarán encriptados usando los niveles más altos de encriptación para que, si logran robar los datos, estos no sean tan fáciles de consultar por parte de los ladrones.

En este sentido, se necesita tener los estándares adecuados de seguridad tanto a nivel software, como hardware y a nivel estructural para asegurar que la información está a salvo.

1.2 Planteamiento del problema

1.2.1 Definición del problema

Dentro de la Universidad Juárez Autónoma de Tabasco (UJAT) se trabaja de manera directa con los alumnos que sufren trastornos de índole psicológica, mental o problemas de conducta, brindando ayuda psicológica en todas sus Divisiones Académicas, con el fin de brindarles el apoyo necesario en cualquiera que sea la situación que estén sobrellevando, independientemente de su grupo o clase social.

Sin importar la gravedad de la situación por la cual los alumnos atendidos estén pasando en ese momento, la institución tiene la obligación de proteger sus datos e información que se genere consulta a consulta.

El 22 de febrero del año 2019, se efectuó una entrevista con los psicólogos de las distintas Divisiones Académicas que laboran en la UJAT quienes muestran preocupación por el resguardo de la información, refiriendo que carecen de las herramientas o la capacitación necesarias para ejercer prácticas viables de seguridad de la información o, en ciertos casos, hicieron mención de que su organización no es blanco para un tipo de ataque.

Los problemas con los que se enfrentan van desde equipos de cómputo que tienen fallos de hardware o software, lo que provoca que la información que almacenaban se pierda por completo o realizan prácticas que ponen en riesgo el almacenamiento y resguardo de la información. Por lo anterior, son susceptibles de que su información sea robada, ya sea de forma física (robo del equipo) o digital (sustracción de archivos mediante internet o USB).

La institución actualmente, cuenta con una serie de lineamientos de seguridad que se encuentran publicados en la “Gaceta Juchiman” del 13 de Julio del año 2018, en la cual se exponen prácticas con base en la seguridad de la información, en la cual se menciona el registro de los equipos de cómputo externos a la organización, que los equipos de cómputo serán otorgados por la institución misma a los colaboradores de la UJAT, el manejo de las contraseñas y que toda modificación a la red, tanto al hardware como a los sitios web de la institución están a cargo del Departamento de Tecnologías de la Información e Innovación (DTII). Sin embargo, dichos lineamientos no cuentan con la debida difusión, por lo que los usuarios ignoran por completo que existen estas medidas de seguridad (Gaceta Juchimán, 2018).

En lo que refiere al último informe de actividades de la institución, concretamente el 3er Informe de Actividades, UJAT (2018), no hace mención acerca de la seguridad de la información o hacia algún plan de medidas y lineamientos de seguridad de la información.

1.2.2 Delimitación de la investigación

Alcances

Las sugerencias de mejora del funcionamiento de seguridad a nivel lógico, abarcan el empleo herramientas para el respaldo de la información.

Limitaciones

La configuración del hardware o software no estuvo contemplada para este proyecto.

El abordaje de la información fue a través de la perspectiva de los psicólogos que laboran en la UJAT.

No se consultó con las autoridades universitarias.

1.2.3 Preguntas de investigación

¿Cuál es la condición de la seguridad de la información de los consultorios psicopedagógicos en la UJAT?

¿Los datos que actualmente se encuentran almacenados en los equipos de cómputo de los consultorios psicopedagógicos están seguros y libres de algún posible ataque?

¿Se hace uso de las directrices expuestas en la normativa ISO 27001 en materia de la seguridad de la información en los consultorios psicopedagógicos de la UJAT?

1.2.4 Objetivos

Objetivo general

Diseñar un modelo de seguridad para los consultorios psicopedagógicos de la Universidad Juárez Autónoma de Tabasco, conforme al estándar 27001.

Objetivos específicos

1. Diagnosticar el nivel de uso de las medidas relativas a las prácticas de seguridad de la información con base en el estándar 27001 en los consultorios psicopedagógicos de la UJAT.
2. Diagnosticar el nivel de uso de las medidas relativas al resguardo de la información con base en el estándar 27001 en los consultorios psicopedagógicos de la UJAT.

3. Diagnosticar el nivel de uso de las medidas relativas a la información sensible, con base en el estándar 27001 en los consultorios psicopedagógicos de la UJAT.

1.3 Justificación

Dado los nuevos avances tecnológicos en materia de resguardo de información como es el almacenamiento en la nube; las organizaciones, empresas e instituciones deben siempre estar a la vanguardia para asegurar que la información sensible que manejan se encuentre segura de cualquier intento de robo o sabotaje por parte de personas u otras organizaciones con intenciones cuestionables.

Debido a este tipo de amenazas, es importante que las instituciones educativas cuenten con certificaciones de seguridad adecuadas que aseguren que dicha información se encuentra resguardada y segura ante cualquier tipo de peligro.

Esta investigación está enfocada en un grupo de 10 psicólogos que laboran en la UJAT, los cuales brindan apoyo a alumnos de la UJAT que pasan o han pasado por momentos difíciles, razón por la que existen casos en donde se debe guardar confidencialidad acerca de la ubicación, identidad o simplemente llevar un control y registro de las personas a las que se les brinda apoyo. Dicha información debe estar asegurada y resguardada ya que, de ser robada, se violentaría el derecho de confidencialidad del alumno y el derecho a decidir qué es lo que quiere y no quiere hacer público.

Anteriormente la UJAT no contaba con lineamientos de seguridad publicados en algún documento o gaceta oficial de la propia institución. Actualmente, el documento “Decreto de los lineamientos generales en el uso de las tecnologías de la información y

la comunicación de la Universidad Juárez Autónoma de Tabasco" de la Gaceta Juchimán (2018) cuenta con una descripción detalla de todas las normativas y lineamientos de uso las tecnologías, así como prácticas de seguridad enfocadas a la información

Como punto de referencia para esta investigación se está tomando en cuenta la normativa ISO 27001.

La ISO 27001 es una norma internacional que fue emitida por la Organización Internacional de Normalización (ISO) y la Comisión Internacional Electrotécnica (IEC por sus siglas en inglés). La ISO/IEC 27001 fue preparada por el Comité Técnico Conjunto ISO/IEC JTC 1, Tecnología de la información (ISO 27001, 2013).

La norma ISO 27001 (2013), se trata de la segunda edición de dicha norma y cancela y reemplaza a la primera edición (ISO/IEC 27001:2005), la cual ha sido técnicamente revisada.

Como dice Calder (2017) la norma ISO 27001 es el plan para gestionar la seguridad de la información en línea con los requisitos reglamentarios, contractuales y empresariales de una organización.

Es por eso que la principal filosofía de la norma ISO 27001 está basada en la gestión de los riesgos, investigando dónde están los mismos y luego tratarlos de manera sistemática.

La propia normativa ISO 27001 (2013) menciona que la organización debe establecer, implementar, mantener y continuamente mejorar un sistema de administración de seguridad de la información, de acuerdo con los requerimientos de este estándar internacional.

La implementación de los lineamientos la normativa anteriormente expuesta es una buena opción para el resguardo de la información confidencial y sensible, debido a todos los elementos que abarca, haciendo de esta organización una organización segura y confiable tanto para sus miembros como para las personas a las que se les está prestando apoyo.

1.4 Metodología utilizada

La metodología para utilizar en el presente trabajo de investigación es la cuantitativa. Malhotra (2004) explica que la metodología de investigación cuantitativa es aquella que busca cuantificar los datos y, por lo general, aplicar alguna forma de análisis estadístico.

Etapas de la metodología

En la primera etapa se llevó a cabo una reunión con los usuarios, en este caso, los psicólogos de las Divisiones Académicas de la UJAT, en la cual se les expuso el propósito de esta investigación y las metas que planeaban alcanzarse. Posteriormente se aplicó una encuesta para así recabar la información necesaria para el proyecto de investigación. Una vez hecho esto se realizó un análisis en el cual se identificó que medidas y lineamientos eran útiles, y cuales no estaban funcionando, para que, conforme a este análisis, se hiciera una propuesta con nuevos modelos y lineamientos de seguridad que pudieran ser aplicados.

Técnicas de recolección de datos

La técnica de recolección de datos aplicada para esta investigación es la encuesta, en la cual se recopilan datos mediante un cuestionario diseñado con anterioridad y la

información recogida se entrega en forma de tablas, trípticos o tablas. Los datos obtenidos se dirigen a una muestra representativa.

Capítulo 2. Marco teórico

2.1 Marco referencial

Baldecchi (2014) explica todos los elementos de un Sistema de Gestión de Seguridad de la Información (SGSI) para su correcta implementación, presentando los procesos y conceptos generales de un SGSI. De igual manera, se presenta una descripción de lo que es un SGSI, y parte desde los conceptos básicos de la ISO 27001 y la seguridad de la información, hasta la descripción de las etapas de implementación de la norma ISO y la implementación de esta.

Igualmente trata el tema de gestión de riesgos y cómo deben ser evaluados según el uso de una matriz de riesgo, así como el uso de una matriz de declaración de aplicabilidad o SOA e incluso trata el tema de auditorías internas, planes de continuidad de negocio y revisiones gerenciales.

How to achieve 27001 Certification. An example of Applied Compliance Management.

Este libro está dirigido principalmente a la oficina del jefe de seguridad, administración de seguridad y profesionales de la seguridad encargados de establecer y mantener un programa de administración de la seguridad. Sigurjon & Willet (2008) toman como objetivo primario en este libro el desarrollar un Sistema de Administración de Seguridad de la Información (ISMS por sus siglas en inglés), que permita a la organización obtener la certificación ISO 27001.

Fundamentos de ISO 27001 y su aplicación en las empresas.

En este artículo se describe los fundamentos de la norma ISO 27001 y como se aplica en las organizaciones. También se presenta la implementación de la norma en una organización. Se explica que la norma se puede implementar en una empresa para obtener la certificación o para perfeccionar algunos aspectos de la seguridad en la empresa. De igual manera, se indica cómo implementar estas buenas prácticas en empresas pequeñas que no pueden realizar la certificación.

IT Governance: A Manager's Guide to Data Security and ISO 27001 / ISO 27002

Este es un libro el cual examina los estándares de las mejores prácticas de conformidad y seguridad de la información. Calder & Watkins (2008) escriben este libro especialmente para compañías que buscan proteger y ampliar el manejo de sus sistemas de seguridad de la información, les permite asegurar que sus estrategias de seguridad en TI están coordinadas, coherentes son exhaustivas y económicos.

2.2 Marco conceptual

2.2.1 ISO 27001

La normativa ISO 27001 es una especificación para un Sistema de Manejo de la seguridad de la información. Calder (2011) menciona que la normativa está diseñada para su uso en todo tipo de organizaciones y en cualquier sector, como empresas comerciales, agencias gubernamentales o empresas no lucrativas. Es un sistema de administración. No una especificación tecnológica y esto se refleja en su título formal, el cual es “Seguridad de la información – Técnicas de seguridad de la información – Sistemas de Administración de seguridad de la Información”.

Esta normativa ISO, es una solución de continua mejora, con base en la cual se puede desarrollar un Sistema de Gestión de Seguridad de la Información o SGSI, el cuál permita evaluar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información de una organización.

Ladino, Villa y López (2011) explican que, antes de solicitar una auditoria, (dado que la normas ISO 27000 son certificables mediante auditorías realizadas por empresas dedicadas a ello), se debe contar con un Sistema de Gestión de la Seguridad de la Información (SGSI). El SGSI debe estar implementado con meses de anticipación.

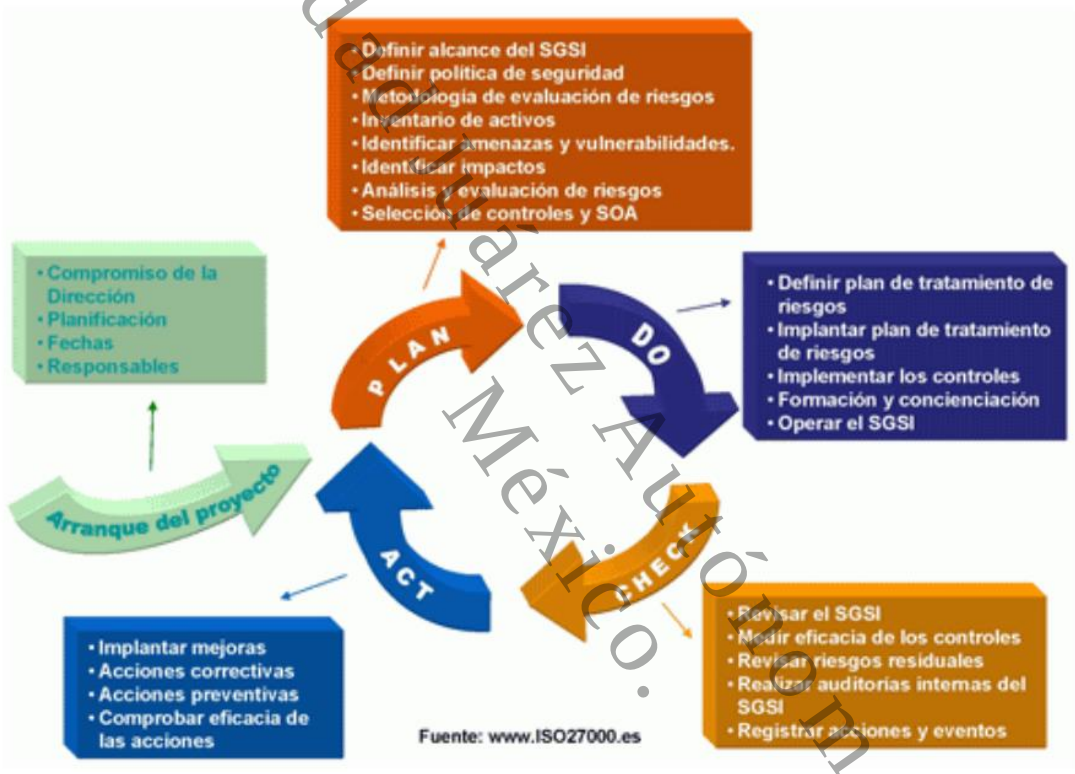
El Sistema de Gestión de la Seguridad de la Información ayuda a establecer políticas y procedimientos en relación con los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir. De igual manera, establece controles y estrategias adecuadas para eliminar o minimizar dichos peligros.

La ISO 27001 es un sistema que se basa en enfoques, a su vez basado en el ciclo de mejora continua o de Deming. Dicho ciclo consiste en Planificar-Hacer-Verificar-Actuar, por lo que se le conoce también como ciclo PDCA (acrónimo de sus siglas en inglés Plan-Do-Check-Act).

Este proceso Plan-Do-Check-Act se aplica para estructurar todos los procesos del SGSI, el cual toma como elementos de entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas, y a través de acciones y procesos que son necesarios se producen resultados de seguridad de la información, los cuales cumplen con estas expectativas.

Trasladando las necesidades de un SGSI a las necesidades planteadas por la ISO 27001, el ciclo PDCA se dividiría en los siguientes pasos, cada uno de ellos ligado a una serie de acciones expuestas en la figura 1 (ver figura 1):

Figura 1
Esquema Plan-Do-Act-Check



Nota: Ladino, López y Villa (2011).

Fases de un SGSI basado en la norma 27001

La norma ISO 27001 establece las siguientes fases para elaborar un SGSI:

1. Análisis y evaluación de riesgos.
2. Implementación de controles.
3. Definición de un plan de tratamiento de los riesgos o esquema de mejora.
4. Alcance de gestión.

5. Contexto de la organización.
6. Partes interesadas.
7. Fijación y medición de objetivos.
8. Proceso documental.
9. Auditorías internas y externas

2.2.2 ISO/IEC 27002

La norma ISO 27002 (denominada ISO 17799 anteriormente) es una normativa para la seguridad de la información publicada por la comisión electrotécnica internacional.

Esta norma ISO proporciona diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información.

Calder (2011) explica que el ISO 27002 es un “Código de prácticas”. Provee un marco de referencia aceptado de manera internacional de las mejores prácticas de la administración de la seguridad de la información e interoperabilidad de sistemas. También proporciona la dirección a tomar para la implementación de un SGSI capaz de la certificación, el cual un auditor externo puede referir. No provee las bases de un esquema de certificación internacional.

Es importante señalar, como nos dicen Calder & Watkins (2015) que el ISO 27002 provee las mejores prácticas internacionales en materia de controles de seguridad de la información, pero no está necesariamente actualizada a los cambios más recientes del entorno de la seguridad de la información. La velocidad con la cual la seguridad de la información evoluciona y continúa evolucionando, significa que algunas de las directrices

de la norma ISO 27002 pueden ser inadecuadas para lidiar con las más recientes amenazas o vulnerabilidades.

Lo anterior no invalida la norma ISO 27002, simplemente crea una oportunidad para que el facultativo vaya más allá de la norma ISO 27002, cuando sea necesario.

Esta norma se encuentra enfocada a cualquier tipo de empresa, independientemente de su tamaño, tipo o naturaleza. La norma ISO 27002 se organiza en base a 14 dominios, 35 objetivos de control y 114 controles.

El principal objetivo de la ISO 27002 es establecer directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización.

2.2.3 Seguridad de la información

Del Carmen, Enríquez y Solarte (2015) explican que la seguridad de la información tiene relación con las medidas preventivas aplicadas cuyo fin es el de salvaguardar y proteger la información bajo confidencialidad, disponibilidad e integridad. La información se presenta en diversos formatos y medios tanto físicos como electrónicos, es por eso que las organizaciones deben adoptar y adaptar metodologías para proteger los archivos y registros, mantener en funcionamiento una infraestructura tecnológica adecuadas que sirvan para la custodia y salvaguarda de la información.

Antonio y Clavijo (2006) mencionan que la seguridad de la información se compone de tres principios esenciales, los cuales son: integridad, confidencialidad y disponibilidad.

El principio de integridad nos permite garantizar que la información no ha sido alterada bajo ningún aspecto, convirtiéndola en el primer principio en ser aplicado.

El segundo principio es el de la confidencialidad de la información, el cual tiene como propósito el asegurar que sólo la persona con los permisos suficientes acceda a la información que se quiere distribuir.

El tercer y último principio en ser aplicado es el principio de la disponibilidad, el cual se aplica una vez se ha asegurado que la información integra llega a los usuarios o destinatarios autorizados. Una vez hecho esto se debe garantizar que llegue en el momento oportuno. Para que una información se pueda utilizar, deberá estar siempre disponible.

Además de todo los principios anteriormente mencionados, Antonio y Clavijo (2008) mencionan que es importante que todos los empleados de la compañía en la cual se están implementado dichos principios tomen conciencia sobre el manejo seguro de la información, ya que de nada sirve un sistema de seguridad de suma complejidad si los empleados, por dar un ejemplo, facilitan su usuario y contraseña a personas ajenas a la empresa, dando pie con esto a brechas de seguridad y posibles ataques o filtraciones de información crítica al exterior de la compañía.

2.2.4 Información sensible

Se le denomina información sensible a toda la información privada de un individuo, empresa o institución. La información sensible incluye todos los datos cuya divulgación puede perjudicar a la persona o entidad en cuestión, en caso de caer en las manos equivocadas.

Areito (2008) hace mención de que, la seguridad pasó de utilizarse para preservar los datos clasificados del gobierno a tener una aplicación de dimensiones inimaginables que incluye tantas transacciones financieras, acuerdos de contratos, comercio y negocios por internet, domótica y computación ubicua.

La información sensible no se trata solo de datos personales, en este término también se pueden incluir a información de una empresa cuya divulgación pueda perjudicar a un negocio. Dicha información puede incluir secretos comerciales, marketing y planes de ventas, planes de nuevos productos, patentes, información de proveedores y clientes, etc.

Por otra parte, la información no sensible es el nombre de la información que no está sujeta a protección especial y que puede compartirse con cualquier persona. Esto incluye la información que es de conocimiento público. En lo que respecta a las empresas e instituciones, cualquier persona interesada puede solicitar el acceso o la divulgación de esa información no sensible y, a menudo, se establecen procedimientos formales para hacerlo. La accesibilidad a los registros públicos bajo el control del gobierno es una parte importante de la transparencia gubernamental.

Con respecto a los riesgos presentados en la información sensible, es responsabilidad del propietario o de quien esté a cargo de la misma. En el caso de una persona, siempre debe estar vigilante sobre los datos, puesto que los riesgos son altos y las consecuencias graves. La información sensible en manos de personas mal intencionadas, puede ser usada para cometer delitos, robar dinero o cuentas bancarias, etc. El objetivo de la denominada ingeniería social, es el conseguir este tipo de

información. La ingeniería social es una técnica de hacking que consiste en la manipulación de usuarios legítimos para obtener información confidencial o privilegios de acceso a sistemas de información.

La tecnología puede ser una aliada para la protección de la información, sin embargo, su uso también incluye grandes riesgos.

En cuanto a medidas de protección, lo ideal es no mantener datos importantes en soportes o lugares que sean de fácil acceso para terceros. Si se almacena este tipo de información sensible, utilizar técnicas o herramientas de cifrado que los hagan de difícil acceso.

Capítulo 3. Aplicación de la metodología y desarrollo

3.1 Tipo y diseño de investigación

Para el desarrollo de esta investigación, se hizo uso del tipo de investigación cuantitativa la cual, según Tamayo (2007) utiliza la recolección y el análisis de datos para contestar preguntas de investigación y probar las hipótesis establecidas previamente, y confía en la medición numérica, el conteo y frecuentemente el uso de estadística para establecer con exactitud patrones de comportamiento en una población.

La metodología cuantitativa de acuerdo con Tamayo (2007) consiste en el contraste de teorías ya existentes a partir de una serie de hipótesis surgidas de la misma, siendo necesario obtener una muestra, ya sea en forma aleatoria o discriminada, pero representativa de una población o fenómeno objeto de estudio.

El diseño de la investigación fue el no experimental. Dzul (2010) refiere que el diseño de investigación no experimental es aquel que se realiza sin la manipulación deliberada de las variables. Se fundamenta en la observación de los fenómenos tal y como se dan en su contexto natural para después ser analizados.

También menciona que este tipo de investigación se basa en categorías, conceptos, variables, sucesos, comunidades o contextos que ya ocurrieron o se llevaron a cabo sin la intervención directa del investigador. Es por esto, que también se le conoce como investigación “ex post facto”. Al observar las variables y relaciones entre estas en su contexto.

3.2 Depuración de la población

Para el desarrollo de la investigación, la población a tomar en cuenta para su estudio fueron los psicólogos de la UJAT que imparten consultas psicopedagógicas en las distintas Divisiones Académicas de la institución, las cuales son:

1. División Académica de Educación y Artes (DAEA)
2. División Académica de Ciencias de la Salud (DACS)
3. División Académica de Informática y Sistemas (DAIS)
4. División Académica de Ciencias Básicas (DACB)
5. División Académica de Ingeniería y Arquitectura (DAIA)
6. División Académica Multidisciplinaria de Comalcalco (DAMC)
7. División Académica de Ciencias Económico Administrativas (DACEA)
8. División Académica de Ciencias Agropecuarias (DACA)
9. División Académica de Ciencias Biológicas (DACB)
10. División Académica de Ciencias Sociales y Humanidades (DACSH)
11. División Académica Multidisciplinaria de los Ríos (DAMR)

Como se mencionó con anterioridad, la población del estudio consistió en los psicólogos de la UJAT los cuales laboran en las Divisiones Académicas de la misma universidad, siendo un total de 10 individuos los cuales fueron encuestados. Del total, 7 se trataron de mujeres, lo que representa un 70% de la población total de encuestados, el restante 30%, son hombres.

3.3 Diseño de instrumentos

Como instrumento de recolección de información se utilizó el cuestionario. Como describen Meneses y Rodríguez (2011) un cuestionario es el instrumento estandarizado que se utiliza para la recogida de datos durante el trabajo de campo de algunas investigaciones cuantitativas, fundamentalmente, las que se llevan a cabo con metodologías de encuestas.

Dentro del cuestionario, se hace uso de un tipo de escala en particular de tipo Likert, la cual según Matas (2018) es un instrumento psicométrico en el cual el encuestado debe indicar su acuerdo o desacuerdo sobre una afirmación, ítem o reactivo, lo cual se realiza a través de una escala ordenada y unidimensional.

Para el diseño del cuestionario se consideró el uso de tres tipos de preguntas, preguntas de opción múltiple, preguntas abiertas y cuadros de intensidad llamados escala tipo Likert con el fin de recabar la máxima información posible de manera fácil y rápida, teniendo en cuenta que este tipo de preguntas son más fáciles de interpretar y graficar. Tanto en las preguntas de opción múltiple como en la encuesta con escala tipo Likert, los encuestados no tienen que escribir sus ideas, solo deben seleccionar la alternativa que se acople de la mejor manera a su forma de pensar, lo cual toma menos tiempo. Las preguntas abiertas por otro lado, toman más tiempo que las preguntas anteriores puesto que los encuestados deben pensar como plasmar de la mejor manera sus pensamientos y opiniones, es por eso que este tipo de preguntas se mantuvo en el mínimo, con solamente tres de ellas en todo el cuestionario.

3.4 Información general

Una vez analizado el instrumento para la recolección de datos, se concluyó el estructurar el cuestionario en cinco secciones: Datos personales, datos laborales, Diagnósticos relativos a la seguridad de la información usando la escala tipo Likert, Medidas relativas a las prácticas de seguridad de la información, Resguardo de la información y acciones llevadas a cabo para preservar la información sensible.

Bloque 1. Datos personales

En este bloque, los encuestados indican su edad y género. Dado que es una encuesta anónima y confidencial, el nombre no es requerido.

Bloque 2. Datos Laborales

En este bloque se pregunta a qué División Académica pertenece el entrevistado, su grado académico, los años laborados en la UJAT, si trabaja en otra institución, esto pensando en la posibilidad de que cargue consigo algún tipo de información en el trayecto de una institución a otra, y el promedio de consultas al día.

Bloque 3. Medidas relativas a las prácticas de seguridad de la información

Este bloque se compone de dos preguntas: En la primera se pregunta cuantas consultas se realizan a mujeres, esto para sacar un promedio de hombres y mujeres atendidos diariamente. Por último, se cuestiona acerca de algún área segura en la oficina del encuestado que permita resguardar la información, el cual es una pregunta cerrada de “si y no”.

Bloque 4. Resguardo de la información

En este bloque se compone de 5 afirmaciones utilizando la escala de Likert para medir el nivel de conformidad del encuestado. Las preguntas se describen a continuación en la tabla 1 (ver tabla 1).

Tabla 1
Escala de resguardo de información

La institución hace difusión de las buenas prácticas de seguridad de la información.	Para conocer si el encuestado piensa que la UJAT muestra interés en la seguridad de la información y hace campañas de difusión de la misma.
Conozco las prácticas de la institución en cuanto a seguridad de la información	Para saber si el encuestado sabe cómo procede la UJAT en caso de algún incidente relativo a la seguridad de la información.
Tengo claros los procedimientos a llevar cabo cuando se presenta algún incidente que involucre la integridad de mi información	Conocer si el encuestado sabe cómo reaccionar ante los incidentes que pongan en peligro la seguridad de la información.
Se cómo reportar cualquier incidente que involucran la seguridad de mi información	Conocer si el encuestado tiene conocimiento de a quién dirigirse en caso de que su información se vea comprometida
Considero que la institución posee un ambiente propicio para la seguridad y resguardo de mi información.	Conocer si el encuestado considera que la UJAT posee los lineamientos adecuados para considerar su información segura.

Bloque 5. Acciones llevadas a cabo para preservar la información sensible

Este bloque consta de cuatro interrogantes, una pregunta de opción múltiple y tres preguntas abiertas. En la primera pregunta “¿Dónde suelo resguardar la información de mis pacientes?” se busca conocer dónde suelen resguardar la información las personas encuestadas, esto para evaluar la seguridad del método de resguardo.

Las últimas tres interrogantes son abiertas, en las cuales se busca conocer la opinión de los encuestados acerca de métodos de seguridad, acciones a llevar acabo en

caso de incidentes relacionados con la seguridad de la información y las dificultades que encuentran para mantener su información segura.

3.5 Aplicación de la prueba piloto

Se seleccionó a la población de la DAIS para la aplicación de la prueba piloto. La prueba se dividió en dos etapas. En la primera etapa se les dio un cuestionario a cada persona para que estos lo leyeran y corroboraran que su contenido era claro y entendible, y disiparan sus dudas con respecto al mismo.

En dicha prueba no hubo ningún detalle que reportar, por lo que se procedió con la aplicación del cuestionario, en donde los participantes debían responder el cuestionario. La aplicación de este cuestionario se llevó a cabo sin incidente alguno y una vez confirmado que la encuesta es viable, se procedió a su aplicación a la población de estudio a la cual está dirigida.

3.6 Aplicación del instrumento

Reunión con la población de estudio

El día 22 de febrero del año 2019, se llevó a cabo una reunión con los psicólogos que imparten consultas en las diferentes divisiones académicas de la UJAT. En dicha reunión se les explicó a los presentes el tema principal de la investigación; así mismo, ellos hicieron comentarios acerca del estado actual de la seguridad de la información en su entorno laboral.

Entre los comentarios más destacados se encuentran:

1. No conocen acerca de medidas y lineamientos de seguridad de la información en general.

2. No tienen conocimientos acerca de cómo resguardar su información de manera segura para evitar extravíos o robo de información.
3. Sus equipos de cómputo no reciben el mantenimiento adecuado y, en caso de alguna falla, la información ahí almacenada se pierde para siempre.

Al final de la reunión se acordó que se les realizaría un cuestionario para conocer las medidas y procesos de seguridad de la información que operan en sus centros de trabajo.

3.7 Aplicación del cuestionario

El día 22 de marzo del presente año, los psicólogos que prestan sus servicios en la UJAT fueron parte de un seminario, en el cual discuten acerca de temas referentes a su campo laboral, es por eso que se acordó la aplicación de la encuesta en ese día antes del inicio del ya mencionado seminario, puesto que se encontrarían reunidos todos ellos y, de esta manera, se facilitaría la aplicación del mismo.

La duración total de la aplicación del cuestionario fue de aproximadamente 45 minutos. Al único participante que no asistió se le envió por medio de correo electrónico el cuestionario, el cual respondió sin contratiempo, reuniendo así a la totalidad de la población de estudio.

Capítulo 4. Resultados

A continuación, se presentan los resultados de la aplicación del cuestionario aplicado a los psicólogos de la UJAT. Se analizan las 4 secciones del cuestionario anteriormente mencionado.

4.1 La población de estudio y consultas diarias

La población total del estudio consta de 10 personas que se dedican a impartir consultas psicológicas a los alumnos de las Divisiones Académicas de la UJAT. De las 10 personas a las que se les aplicó el cuestionario, 7 son mujeres lo cual representa el 70% de la población, el 30% restante son hombres.

Al día, se realizan 42 consultas, la mayor cantidad de consultas realizadas en un día son cinco, lo cual representa un 11.90% de las consultas diarias realizadas.

Respecto a las consultas impartidas a mujeres, a diario se realizan 31 consultas, lo cual representa el 71.80% del total de consultas diarias realizadas en general. Dentro de este mismo promedio de atención hacía mujeres, cinco es el mayor número de mujeres atendidas en un día, lo cual representa el 16.12% de la población total atendida solamente ese día.

4.2 Medidas relativas a las prácticas de la seguridad de la información

En lo relativo a las áreas seguras dentro de los consultorios psicopedagógicos de la UJAT, 50% de la población actualmente posee un área segura para el resguardo de la información, mientras que el 50% restante no cuenta con esta área.

En la tabla 2 (ver tabla 2) se muestra el porcentaje de opinión de la población.

Tabla 2

Divulgación de las buenas prácticas de seguridad de la información

Totalmente en desacuerdo	*60%*
Bastante de acuerdo	*20%*
Algo en desacuerdo	10%
Algo de acuerdo	10%

Conocimiento de las prácticas de la institución en cuanto a la seguridad de la información.

En cuanto al conocimiento de las prácticas que la institución lleva a cabo en materia de seguridad de la información, 40% de la población total no tiene conocimiento de este tipo de prácticas, 40% tiene pocos conocimientos acerca de las prácticas ya mencionadas, 10% tiene conocimientos suficientes en cuanto a las prácticas de la institución, mientras que el 10% restante posee los conocimientos íntegros de las prácticas de seguridad de la información de la institución.

Claridad de los procedimientos a llevar a cabo en caso de un incidente que involucre la integridad de mi información.

Referente a la claridad de los procedimientos a llevar a cabo en caso de un incidente que involucre la integridad de mi información, un 10% de la población no tiene claro este tipo de procedimientos, el 60% tiene algo claro acerca de los mismos, 10% de los encuestados esta algo de acuerdo con la claridad de los procedimientos mientras que el 20% restante tiene claros los procedimientos a llevar a cabo.

Reporte de incidentes

Dos de los encuestados saben cómo reportar alguna incidencia de esa índole, mientras uno solo tiene prácticamente todos los conocimientos y solo necesita reafirmar sus conocimientos. Por otro lado, dos de los encuestados tienen aún dudas acerca de cómo reportar incidentes y de los cuatro restantes dos definitivamente desconocen como reportar, y los dos restantes tienen dudas acerca de la formulación de un reporte.

Confianza en la seguridad de la UJAT

En la tabla 3 se muestra el nivel de confianza que tienen los psicólogos al dejar su información en la UJAT (ver tabla 3).

Tabla 3
Confianza en la seguridad de la UJAT

Me siento confiado de que la información que dejo en la UJAT está segura	Personas que respondieron
Algo de acuerdo	2 personas (20%)
Bastante de acuerdo	2 personas (20%)
Algo en desacuerdo	2 personas (20%)
Totalmente en desacuerdo	3 personas (30%)
Nunca	1 persona (10%)

4.3 Medidas relativas a las prácticas de la seguridad de la información

Clasificación de la información

En el ámbito de la clasificación de la información, el 60% de la población de estudio realiza está práctica, aunque no de manera habitual, teniendo solo tres personas que realizan está práctica comúnmente y solo una persona no la tiene en práctica.

Respaldo de la información

En lo que respecta al respaldo de la información, 60% de la población realiza esta tarea, pero no la lleva a cabo de forma habitual. 10% de la población realiza esta actividad casi siempre, mientras que el 20% de la población no realiza está práctica de manera habitual y el 10% restante no lleva a cabo esta práctica en absoluto.

Protección de documentos

En lo que uso de contraseñas para protección de documentos se refiere, el 60% de la población no utiliza una contraseña, el 20% la usa muy de vez en cuando, 10% en algunos casos y el 10% restante, utiliza, por lo general, contraseñas para resguardo y protección de sus documentos.

Uso de antivirus

30% de la población hace uso de un antivirus para proteger sus computadoras, sin embargo, 30% de la población no hace uso de un programa antivirus mas no de manera exhaustiva. 20% de la población, sin embargo, no utilizan antivirus en sus computadoras.

Documentación importante a la vista en el escritorio

En lo que consta a la política de escritorio limpio, 50% de la población encuestada casi nunca deja documentación importante a la vista en su escritorio, sin embargo, 20% deja documentos a la vista a veces, y el otro 20% siempre deja documentación en su escritorio a la vista. El 10% restante mantiene sus documentos fuera del alcance de la vista de otras personas ajenas a su lugar de trabajo.

Documentación importante a la vista en el escritorio de la computadora.

En cuanto al escritorio de la computadora, 20% de la población nunca deja documentos importantes a la vista, mientras que 30% de la población casi nunca deja

documentación a la vista. 30% a veces deja documentación importante a la vista en su escritorio mientras que el 20% restante siempre deja documentación a la vista de otras personas.

Mantenimiento del equipo de cómputo

50% de la población indica que su equipo de cómputo recibe mantenimiento a veces, solo 20% de la población asegura que el mantenimiento es frecuente o casi siempre, mientras que la mitad dice que a veces. El 30% restante no recibe mantenimiento en sus equipos de cómputo.

Frecuencia de incidentes que ponen en riesgo la seguridad de la información

Referente a la frecuencia de los incidentes que ponen en riesgo la seguridad de la información, el 20% de la población nunca ha sufrido incidentes que pongan en riesgo la seguridad de la información, mientras que el 10% casi nunca ha sufrido incidentes. 40% de la población a veces sufre incidentes y el 30% restante casi siempre sufre incidentes que ponen en riesgo la seguridad de la información

4.4 Acciones llevadas a cabo para preservar la información sensible

Resguardo de la información de los pacientes

El 50% de los participantes del cuestionario indican que la computadora de oficina es donde resguardan la información de sus pacientes, seguido de las memorias USB con un 40%, y la nube con un 10%.

Resguardo físico de la información de los pacientes

La información física de los pacientes se realiza de igual manera tanto en escritorios como en lockers, ambos con 40%, mientras que el 20% restante utiliza gabinetes.

En cuanto al área de preguntas abiertas, este se compuso de tres cuestionamientos, los cuales eran:

1. ¿Qué acciones llevaría a cabo en caso de sufrir un incidente donde su información se viese comprometida?
2. ¿Qué dificultades encuentra usted para mantener segura la información en su lugar de trabajo?
3. ¿Quién es el responsable de brindar mantenimiento al equipo de cómputo?

Para la primera pregunta, un 20% de la población respondió con un “No sé”, mientras que 10% habla acerca de hacer uso de sus respaldos. 10% de la población participante avisaría a su jefe inmediato mientras que otro 10% habla de ir con soporte técnico. 20% más avisaría a su jefe inmediato. También se habla de exponer un oficio donde no se ha resguardado debido a la falta de apoyo, esto por un 10% de la población. Mientras que otro 10% habla de acudir a una persona profesional del área de seguridad y de confianza para su ayuda. Por último, el 20% restante reportaría a la persona que tomó la información.

Para la segunda pregunta, 40% de la población no tiene ninguna dificultad para mantener segura su información, 20% de la población se preocupa acerca de la seguridad física de la información, pues consideran que su lugar de trabajo no es del todo seguro para el resguardo de la información misma. 20% más de la población alude a que la

computadora que utiliza para almacenamiento de la información está en red y eso presenta una brecha de vulnerabilidad. 10% menciona que no cuenta con apoyo físico como memorias USB para uso laboral, mientras que otro 10% de la población explica que no tiene una computadora personal sino se trata de un equipo compartido.

Por último, para la 3er pregunta, el 90% de la población está de acuerdo en que el responsable del mantenimiento de los equipos de cómputo es el equipo de soporte técnico del centro de cómputo de su respectiva División Académica. Solamente una persona expresa que ella misma es la encargada de dar soporte a su equipo.

Capítulo 5. Propuesta de modelo de buenas prácticas de seguridad de la información

En esta sección se presenta el modelo propuesto que facilita el proceso de creación de políticas de seguridad de la información a nivel lógico en la UJAT. Después de realizar el estudio en el cual se identificó que el principal problema que sufren los psicólogos no es el resguardo, sino el aseguramiento de la información.

Derivado de esto, y como complemento a lo anterior, otro de los problemas al os que se enfrentan los psicólogos de la UJAT es que no pueden hacerse cargo de la implementación de medidas y lineamientos de seguridad que estén basados en la norma ISO 27001. Es por esto que se ha optado por recurrir a una solución a mayor escala.

La propuesta a considerar para tratar este problema se propone la creación de un Sistema de Gestión de Seguridad de la Información (SGSI).

Un SGSI, como explican Betín, Martelo y Madera (2014) consiste en un conjunto de políticas usadas para definir, construir, desarrollar y mantener la seguridad del equipo basado en hardware y recursos de software.

5.1 Introducción al modelo

El modelo que se propone en este capítulo tiene inspiración en dos vertientes principales, las cuales son:

El artículo titulado “Software para Gestión documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI)”.

En este artículo Betín, Martelo y Madera (2014) se expone el caso del desarrollo de un software el cual contribuye al control de los documentos que se generan a partir

del proceso de implantación de un Sistema de Gestión de Seguridad de la Información (SGSI). Este software permite la recepción, administración y organización de la documentación generada en el proceso de implantación del SGSI.

Experiencia propia dando la estancia profesional en la consultoría de TI IntegraIt.

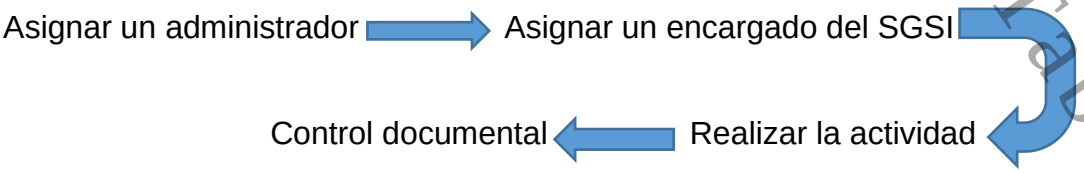
Como parte del programa de estudios de la maestría en Administración en Tecnologías de la Información, se realizó una estancia profesional en la empresa IntegraIT, la cual opera bajo el marco normativo de la norma ISO 27001. Al estar de apoyo en el área de Sistema de Gestión de la Información, tuve un contacto cercano con muchas de las prácticas y lineamientos de seguridad empleados en la empresa para mantener la información segura e integra. Lineamientos y prácticas en las cuales se basa el modelo propuesto para este trabajo de investigación.

5.2 Modelo de prácticas y lineamientos de Seguridad de la Información

Este modelo abarca 4 pasos esenciales, organizadas bajo el orden de trabajo de Plan-Do-Check-Act (PDCA), como explican Betín, Martelo y Madera (2014) esto permite al modelo estar en conformidad con un sistema de gestión.

En la figura 2 (ver figura 2) se muestran los pasos a seguir en el modelo propuesto.

Figura 2
Pasos esenciales del modelo



Nota: Elaboración propia con base en Betín, Martelo y Madera (2014)

1) Asignar un administrador: Un administrador es un elemento importante del modelo, pues debe tratarse de un individuo con vastos conocimientos en las medidas y directrices de la ISO 27001, y supervisara todo lo referente a la implementación de la misma. Así mismo, el encargado del SGSI debe reportar periódicamente en un lapso de tiempo determinado por el mismo administrador, los niveles y la frecuencia de los incidentes ocurridos en el área. Asimismo, el administrador es el encargado de realizar auditorías periódicamente, para así determinar qué tan buen o mal desempeño tiene el SGSI.
2) Asignar un encargado del SGSI: La segunda fase del modelo es asignar un encargado del SGSI, el cual tendrá como tarea el monitoreo y la implementación de las directrices que conforman este modelo (que se expondrán más adelante).
3) Realizar la actividad: Se establecen los parámetros y lineamientos del modelo en cuestión, se monitorean los resultados y, si se debe modificar algún parámetro se modifica.
4) Control documental: Dado que el modelo se centra principalmente en el resguardo y protección de documentos tanto de manera física y lógica, se deberá llevar un control de los mismos, verificando la vigencia de cada documento y, en caso de está vigencia haber vencido, destruir el documento acorde a las medidas establecidas.

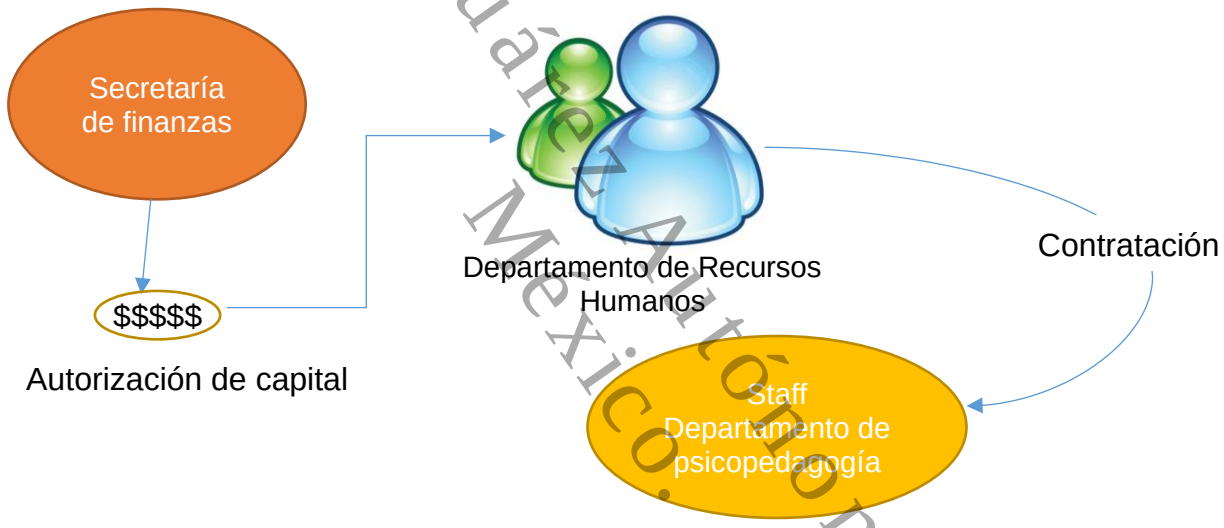
Consideraciones a tomar en cuenta

Para la implantación del modelo, se proponen dos nuevas plazas de trabajo, las cuales son administrador del SGSI y el encargado del SGSI, lo cual se traduce en la creación de dos nuevas fuentes de empleo en la UJAT, para lo cual se verían

involucradas dos nuevas áreas de la organización las cuales tendrían la tarea de evaluar los nuevos puestos y el salario a considerar para los mismos. Estás áreas son la secretaria de finanzas y el departamento de recursos humanos.

En la figura 3 (ver figura 3) se muestra la relación de estas áreas con el modelo propuesto.

Figura 3
Esquema de departamentos



En la tabla 4 (ver tabla 4) se describen las directrices y medidas con las cuales se define el modelo propuesto a través de este capítulo. Se toma en cuenta tanto la participación del SGSI como de los usuarios, en este caso los psicólogos de la UJAT. Las políticas y medidas aquí propuestas tienen su base en la norma ISO 27001 (2013).

Tabla 4
Medidas y directrices

Políticas de seguridad de la información.	
Políticas para la seguridad de la información. ISO 27001 (2013).	Un conjunto de políticas de seguridad de la información debe ser definidas, aprobadas por la administración, publicadas y comunicadas a los empleados.
Revisión de Políticas para la seguridad de la información. ISO 27001 (2013).	Las políticas de seguridad de la información deben ser revisadas en intervalos planeados o si cambios significativos ocurren para asegurar su continuidad, adecuación y efectividad.
Control de Usuarios	
Registro de Usuarios	Se debe llevar un proceso de registro formal de los usuarios para así asegurar el poder otorgar los derechos de acceso.
Control de Usuarios en los equipos de cómputo.	El encargado del SGSI, debe crear dos tipos de usuario en el equipo de cómputo a utilizar por el trabajador; un usuario Administrador el cual es usado exclusivamente por el área de SGSI, y otro para el uso del trabajador, el cual debe colocar una contraseña de acuerdo a las directrices establecidas.
Permisos de acceso a Usuarios a los repositorios de información.	El acceso de los usuarios a la información debe ser implementado para conceder o revocar el acceso.
Manejo de la información confidencial de los usuarios (Información de autenticación).	El manejo y asignación de la información de autenticación de los usuarios debe ser controlada y almacenada por el encargado del SGSI y utilizando métodos de encriptación en los archivos.
Administración de los privilegios del usuario.	La asignación de los privilegios del usuario debe revisarse en intervalos establecidos de manera regular.
Clasificación de la información.	
Clasificación de la información. ISO 27001 (2013).	Control La información debe ser clasificada en términos de valor, criticalidad y sensibilidad a modificaciones sin autorización.
Etiquetado de la información	Los archivos creados por los usuarios tendrán un etiquetado especial el cual debe ser discutido por el administrador, el encargado del SGSI y los mismos usuarios.

Tabla 4
Medidas y directrices (Continuación).

Responsabilidades del usuario	
Uso de la información secreta de autenticación. ISO 27001 (2013).	Los Usuarios serán requeridos a seguir las prácticas de la organización en el uso de la información secreta de autenticación.
Control de la información.	El encargado del SGIS deberá llevar un control en el cual monitoree continuamente los archivos creados y debidamente etiquetados, para así poder acceder con facilidad a los mismos. Dicho control debe estar debidamente encriptado para evitar accesos no autorizados.
Controles de acceso	
Restricciones de acceso a la información.	El acceso a la información y a los sistemas de información debe ser restringido y controlado para los usuarios de acuerdo a las políticas de control de acceso.
Sistema de control de contraseñas.	El sistema de control de contraseñas debe asegurar contraseñas de calidad, alfanuméricas de más de 10 caracteres.
Seguridad perimetral	
Perímetro de seguridad física.	Perímetros de seguridad deben ser definidos y utilizados para proteger las áreas donde se resguarda la información sensible.
Control de físico de entradas.	Las áreas seguras deben estar debidamente protegidas con controles de acceso que aseguran la entrada únicamente al personal autorizado.
Consultorios y oficinas seguras.	Seguridad física para las oficinas y consultorios psicopedagógicos debe ser diseñada y aplicada.
Acceso a los consultorios y oficinas.	El acceso a las oficinas y consultorios debe ser exclusivo de los psicólogos. Esto para evitar accesos no autorizados que pongan en peligro la integridad de la información.
Equipo	
Activos	Los equipos, la información o el software no debe ser transportado fuera del área laboral sin los permisos pertinentes.
Desechar o reutilizar equipos.	Todos los equipos que contengan medios de almacenamiento y que están en planes de reutilización, deben ser debidamente revisados y verificar que ningún tipo de información sensible ha quedado almacenada.

Tabla 4

Medidas y directrices (Continuación).

Política del escritorio y pantalla limpia.	Se debe adoptar una política de documentos en papel y de escritorio virtual limpio.
Protección contra el Malware	
Controles contra el Malware.	Controles de detección, prevención y recuperación en contra del Malware deben ser implementadas y deben combinarse apropiadamente y a conciencia con el usuario.
Respaldos	
Respaldos de información.	Respaldos de la información deben ser revisados con regularidad de acuerdo con una política de respaldo.
Administración de la seguridad de red	
Controles de red	Las redes deben ser administradas y controladas para proteger la información en sistemas y aplicaciones.

Nota: Elaboración propia con base en la norma ISO 27001 (2013).

Consideraciones generales

En primera instancia, se sugiere se hagan reuniones periódicas (cada mes, o de manera bimestral, según se convenga) con los psicólogos en la cual se discutan los siguientes tópicos:

1. ¿Cuántas veces han hecho un resguardo de su información sensible en el periodo preestablecido?

2. Los incidentes referentes a la seguridad de la información ocurridos durante ese periodo específico.

3. Plática referente a la seguridad de la información, en la cual se haga hincapié en la importancia de las prácticas de la seguridad de la información.

4. Dinámicas en las cuales los psicólogos puedan participar para así reafirmar sus conocimientos acerca de la seguridad de la información.

Y por parte de la institución, realizar campañas de difusión de la seguridad de la información para así mantener informada acerca del tema a la población que ahí labora.

En segunda instancia, se propone un listado de buenas prácticas de seguridad de la información el cual está previsto para el resguardo de la integridad de la seguridad de la información.

Seguridad Física y Perimetral

1. No consumir alimentos en el área de escritorio, esto para evitar derrames de líquido o comida en los equipos de cómputo o documentos importantes.

2. Revisar que los seguros de los lockers y escritorios funcionen correctamente. En caso contrario, reemplazarlos.

3. Se debe llevar un control de acceso a la oficina. De igual manera, la llave para el acceso a la misma solo debe poseerla el trabajador y un superior, esto para evitar que cualquier otra persona ajena a la misma oficina tenga acceso.

Información Lógica

1. Respaldar la información periódicamente en un repositorio de uso personal. Esto con el fin de que la información ahí almacenada este en constante actualización.

2. Proteger documentos o carpetas importantes con contraseñas.

3. No utilizar contraseñas sencillas. Esto para evitar que personas ajenas al entorno adivinen la contraseña y sustraigan la información.

4. Realizar mantenimiento preventivo y correctivo de manera constante a los equipos de cómputo. Esto para evitar errores irreversibles en las computadoras que pongan en peligro la integridad de la información que ahí se almacena.

5. Llevar un control y seguimiento de los incidentes referentes a la seguridad de la información que se han presentado recientemente, y aplicar medidas para evitar que los mismos se repitan.

Capítulo 6. Conclusiones, recomendaciones y trabajos futuros.

6.1 Conclusiones

En conclusión, se creó un modelo de buenas prácticas de seguridad de la información, acorde a las necesidades de los consultorios psicopedagógicos de la UJAT. Cabe resaltar que el modelo propuesto en este trabajo de investigación tiene como base la norma ISO 27001. Entre las medidas propuestas se encuentra el control de usuarios, la seguridad de la red, protección contra el malware y resguardo y protección de la información.

Diagnosticando el nivel de uso de las medidas relativas a las prácticas de seguridad de la información con base en el estándar 27001 en los consultorios psicopedagógicos de la UJAT, que es el primer objetivo específico, se concluye que, si bien se utilizan medidas para la seguridad de la información que se mencionan en la norma ISO 27001, como lo son el uso del malware, y en algunos casos en concreto, el uso de áreas seguras para el resguardo de la información, lo cierto es, que estas medidas de seguridad resultan insuficientes para proveer seguridad a la información, sobre todo a la información sensible.

Haciendo un segundo diagnóstico del nivel de uso de las medidas relativas al resguardo de seguridad de la información, se llegó a la conclusión de que los psicólogos que laboran en la UJAT si hacen resguardos de su información. Tanto la información general como la información sensible se resguarda, sin embargo, resguardar la información no es lo mismo que asegurar la información. Y es en este último punto donde se tiene que hacer un énfasis especial, puesto que lo deseable en este caso es que la información se encuentre tanto resguardada como asegurada.

Realizando un último diagnóstico, esta vez del nivel de uso de las medidas relativas a la información sensible con base en el estándar 27001, podría llegarse a una conclusión similar a lo anteriormente mencionado. La información se resguarda, mas no está asegurada. Y mucho menos está asegurada conforme a algún tipo de estándar o normativa ISO.

Hablando ahora de la condición de la seguridad de la información de los consultorios psicopedagógicos en la UJAT y tomando como referencia la escala de Likert utilizada en el cuestionario aplicado a los psicólogos de la UJAT (ver Apéndice A), en la cual 1 es muy mala y 5 es excelente, se concluye que 1, muy mala. Debido principalmente al desconocimiento de los psicólogos en este ámbito. Si bien están conscientes de la importancia de la seguridad de la información, no cuentan con los conocimientos necesarios para que la información que manejan, sobre todo la información de carácter sensible, se encuentre segura y resguardada ante cualquier posible percance.

Lo que nos lleva entonces a los datos que actualmente se encuentran almacenados en los equipos de cómputo de los consultorios psicopedagógicos, los cuales no están seguros y libres de algún posible ataque. Como gran parte de la población sujeta al cuestionario expuso en el mismo, sienten que su información no está segura en la UJAT, aunado a que varios de ellos no poseen buena seguridad perimetral, se concluye que los equipos de cómputo no están seguros.

Y esto nos lleva a un tercer punto, el cual es el uso de las directrices expuestas en la normativa ISO 27001 en los consultorios psicopedagógicos de la UJAT, y es que

actualmente no se hace uso de directrices o normas expuestas en la normativa ISO 27001 o alguna normativa en general.

Para concluir, los consultorios psicopedagógicos de la UJAT no cuentan con las medidas y directrices adecuadas que aseguren que la información allí almacenada se encuentra libre de ataques u otros incidentes. Esto debido principalmente a que en la actualidad no se sigue ningún modelo de prácticas de seguridad, ya sea que el mismo esté o no basado en algún tipo de normativa ISO o similares.

Los métodos y medidas de seguridad que actualmente se utilizan en los consultorios son, en la mayoría de los casos, aplicados por los mismos psicólogos de utilizando únicamente el sentido común.

Es por eso que la aplicación del modelo propuesto servirá, sobre todo, para crear confianza en los psicólogos y que ellos sientan que su información se encuentra resguardada de manera correcta y eficaz y que, sobre todo, se encuentra segura.

6.2 Recomendaciones

La ISO 27001 puede ser utilizada en conjunto con las normas ISO 27002, ISO 27003 e ISO 27004, por lo tanto, se podría construir otro modelo de buenas prácticas de seguridad de la información implementando todas las prácticas y lineamientos expuestas en todas las normas ISO anteriormente mencionadas.

Realizar campañas de divulgación a los psicólogos de la UJAT acerca de los peligros a los que se está expuesto cuando se navega en la internet, como lo son el *phishing* o el *scam.*

Darles a los psicólogos cursos de capacitación en los cuales les enseñen las medidas básicas de seguridad para el resguardo y aseguramiento de su información.

Realizar monitoreos constantes del estado actual de los equipos de cómputo utilizados por los psicólogos para asegurar que estos cumplen con los estándares de seguridad de la información adecuados.

Hacer uso de los programas antivirus y hacer escaneos a los equipos de cómputo con regularidad.

6.3 Trabajos futuros

Extender este mismo estudio a otras áreas de la institución que no cuenten con los modelos correspondientes para el resguardo y aseguramiento de la información sensible, implementando las demás normativas de la familia ISO 27000.

En dado caso que las áreas en las que se realiza el estudio ya cuenten con un modelo de buenas prácticas de seguridad de la información, analizarlo, estudiarlo y, a priori, realizar otro modelo basándose en el modelo anterior. Un modelo más actualizado que cubra las amenazas más actuales y, después de realizar las pruebas y las comparativas correspondientes, implementarlo.

Referencias

Antonio, C. y Clavijo, D. (2006). Políticas de seguridad informática. *Entramado*, *2*(1), 86-92. Recuperado de https://www.redalyc.org/pdf/2654/265420388008.pdf

Areitio, J. (2008). *Seguridad de la información*. (1er ed.). Madrid: Paraninfo. Recuperado de https://books.google.com.mx/books?id=_z2GcBD3deYC&printsec=frontcover&dq=Seguridad+de+la+informaci%C3%B3n.&hl=es-419&sa=X&ved=0ahUKEwj6uZPS2_nkAhUCRa0KHeywCrEQ6AEILjAB#v=onepage&q=Seguridad%20de%20la%20informaci%C3%B3n.&f=false

Baldecchi, R. (2014) *Implementación efectiva de un SGSI ISO 27001*. Ponencia presentada en la reunión del V Congreso Internacional sobre Gobierno, Riesgos, Auditorias y Seguridad de la información, Santiago, Chile.

Benavides, M., Enríquez, E. y Solarte, F. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL*, *28*(5), 493-506. Recuperado de http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

Betín, A., Madera, J. y Martelo, R. (2014). Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI). *Información Tecnologíca, 26*(2), 129-133. doi: 10.4067/S0718-07642015000200015

Calder, A. & Watkins, S. (2008). *IT Governance: A Manager's Guide to Data Security and ISO 27001 / ISO 27002.* (4th ed.). Londres: Kogan Page. Recuperado de

https://epdf.pub/it-governance-a-managers-guide-to-data-security-and-iso-27001-iso-27002.html

Calder, A. (2011). *ISO 27001 and ISO 27002. Implementing Information Security based on ISO 27001/ISO 27002 A Management Guide.* (1st ed.). Reino Unido: Van Haren Recuperado de https://books.google.com.mx/books?id=0hJADwAAQBAJ&pg=PT19&dq=iso+27001&hl=es-419&sa=X&ved=0ahUKEwiN_aDV4fnkAhVOOK0KHSdNAEsQ6AEIQzAD#v=onepage&q=iso%2027001&f=false

Calder, A. & Watkins, S. (2015). *IT Governance: An International Guide to Data Security and ISO27001/ISO27002*. (6th ed.) Gran Bretaña: Kogan Page Publishers. Recuperado de https://books.google.com.mx/books?id=OctwCgAAQBAJ&printsec=frontcover&dq=IT+Governance:+An+International+Guide+to+Data+Security+and+ISO27001/ISO27002&hl=es-419&sa=X&ved=0ahUKEwi1zZHh4vnkAhUHeKwKHXCkClcQ6AEILDAA#v=onepage&q=IT%20Governance%3A%20An%20International%20Guide%20to%20Data%20Security%20and%20ISO27001%2FISO27002&f=false

Calder, A. (2017). *Nueve pasos para el éxito: Una visión de conjunto para la aplicación de la ISO 27001:2013.* (1era ed.). Reino Unido: IT Governance Ltd. Recuperado de

https://books.google.com.mx/books?id=BxU3DwAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Dzul, M. (2010). *Aplicación básica de los métodos científicos. "Diseño no-experimental".* Ponencia presentada en la Asignatura de Fundamentos de la metodología de la Universidad Autónoma del Estado de Hidalgo. Hidalgo. México.

International Organization for Standardization [ISO]. (2013). *ISO/IEC 27001*. Suiza. ISO. Recuperado de www.iso.org

Ladino, A., López, E. y Villa, S. (2011). Fundamentos de ISO 27001 y su aplicación en las empresas. *Scientia Et Technica*, *18*(47), 334-338. Recuperado de http://www.redalyc.org/articulo.oa?id=84921327061.

Martelo, R., Maza, D. y Tovar, L. (2017). Modelo Básico de Seguridad Lógica. Caso de Estudio: el Laboratorio de Redes de la Universidad de Cartagena en Colombia. *Información Tecnológica*, *29*(2), 3-11. Doi: 10.4067/S0718-07642018000100002

Matas, A. (2018). Diseño del formato de escalas tipo Likert: un estado de la cuestión. *Revista Electrónica de Investigación Educativa*, *20*(1), 39-47. Recuperado de https://doi.org/10.24320/redie.2018.20.1.1347.

Malhotra, K. (2004). *Investigación de mercados: un enfoque aplicado.* Recuperado de https://books.google.com.mx/books?id=SLmEblVK2OQC&pg=PA137&dq=investigacion+cuantitativa&hl=es-419&sa=X&ved=0ahUKEwjIk-H8p_vkAhVDvFkKHadfBTEQ6AEIUjAG#v=onepage&q=investigacion%20cuantitativa&f=false

Mendoza, A. (2014). *Seguridad de la Información: Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica.* (1er ed.). Guatemala: Universidad de San Carlos en Guatemala. Recuperado de https://books.google.com.mx/books?id=xKkYBgAAQBAJ&printsec=frontcover&dq=seguridad+de+la+informacion&hl=es-419&sa=X&ved=0ahUKEwiA3e-7tqHkAhVMR60KHdlpA6kQ6AEINTAC#v=onepage&q&f=false.

Meneses, J. y Rodríguez, D. (2011) *El cuestionario y la entrevista.* (1er ed.) Cataluña: Universidad Oberta de Catalunya. Recuperado de http://femrecerca.cat/meneses/files/pid_00174026.pdf.

Thor, S. & Willett, K. (2008). *How to Achieve 27001 Certification. An example of Applied Compliance Management.* (1st ed.). New York: Auerbach Publications. Recuperado de https://books.google.com.mx/books?id=IjVh6o1nuYwC&printsec=frontcover&dq=How+to+Achieve+27001+Certification.+An+example+of+Applied+Compliance+Management&hl=es-419&sa=X&ved=0ahUKEwj1qLr-6PnkAhVBIqwKHaHFAAkQ6AEILDAA#v=onepage&q=How%20to%20Achieve%2027001%20Certification.%20An%20example%20of%20Applied%20Compliance%20Management&f=false

Tamayo, M. (2007). *El proceso de la investigación científica*. (4ta ed.). México: Limusa. Recuperado de https://books.google.com.mx/books?id=BhymmEqkkJwC&printsec=frontcover&dq=El+proceso+de+la+investigaci%C3%B3n+cient%C3%ADfica&hl=es-

419&sa=X&ved=0ahUKEwjF8N6I6fnkAhUEC6wKHa7ZCYIQ6AEIKTAA#v=onepage&q=El%20proceso%20de%20la%20investigaci%C3%B3n%20cient%C3%ADfica&f=false

Tarazona, C. (2007) *Amenazas Informáticas y Seguridad de la Información*. New York: Hein Online. Recuperado de https://heinonline.org/HOL/LandingPage?handle=hein.journals/dpencrim28&div=29&id=&page=&t=1561421216.

Universidad Juárez Autónoma de Tabasco. [UJAT]. (2018) Decreto de los lineamientos generales en el uso de las tecnologías de información y comunicación de la Universidad Juárez Autónoma de Tabasco. *Gaceta Juchimán, 7*(86), 3-21. Recuperado de http://gacetajuchiman.ujat.mx/2018/09/26/gaceta-juchiman-version-electronica-ano-7-no-86-junio-de-2018/

Universidad Juárez Autónoma de Tabasco. [UJAT]. (2018a). Tercer Informe de Actividades 2018. México. UJAT. Recuperado de ujat.mx/rectoria/24286.

Voutssas, J. (2010). Preservación documental digital y seguridad informática, *Scielo*, *24*(50), 127-155. Recuperado de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008.

Glosario

E

Ex post facto: Después de hecho.

I

ISO: Organización Internacional de Normalización.

S

SGSI: Sistema de Gestión de Seguridad de la Información.

SOA: Arquitectura orientada a servicios.

U

UJAT: Universidad Juárez Autónoma de Tabasco.

Apéndice A. Cuestionario aplicado a los psicólogos de la UJAT

1. Número_____

Cuestionario de seguridad de la información

Instrucciones: El propósito del siguiente cuestionario es conocer las medidas y procesos de seguridad de la información que operan en su centro de trabajo. Su participación es totalmente voluntaria, anónima y confidencial y no le tomará más de 20 minutos.

I. Datos Personales

2. Edad: _____

3. Género: Masculino ( ) Femenino ( )

II. Datos laborales

4.División Académica: _____

5. Grado Académico: Licenciatura ( ) Maestría ( ) Doctorado ( )

6. ¿Cuántos años ha laborado en la UJAT? _____

7. ¿Trabaja en otra institución? _____

8. En promedio, ¿cuántas consultas realiza al día? _____

III. Resguardo de la información. Indique con un Si o un No según considere sea la respuesta correcta.

9. En promedio de atención diaria, ¿Cuántas consultas son realizadas a mujeres?

_____

10. ¿Posee un área segura dentro de su oficina que me permita resguardar mi información?

Si ( ) No ( )

III. Indique en qué medida está de acuerdo o en desacuerdo con las siguientes afirmaciones relativas a la seguridad de la información por parte de la UJAT. (Marque con una X la respuesta que refleje su opinión).

Totalmente en desacuerdo (1), Algo en desacuerdo (2), Algo de acuerdo (3), Bastante de acuerdo (4), Totalmente de acuerdo (5).	**1**	**2**	**3**	**4**	**5**
11. La institución hace difusión de las buenas prácticas de seguridad de la información.					
12. Conozco las prácticas de la institución en cuanto a seguridad de la información					
Totalmente en desacuerdo (1), Algo en desacuerdo (2), Algo de acuerdo (3), Bastante de acuerdo (4), Totalmente de acuerdo (5).	**1**	**2**	**3**	**4**	**5**
13. Tengo claros los procedimientos a llevar cabo cuando se presenta algún incidente que involucre la integridad de mi información					
14. Se cómo reportar cualquier incidente que involucra la seguridad de mi información					
15. Me siento confiado de que la información que dejo en la UJAT está segura					

IV. Indique en qué medida se cumplen las siguientes afirmaciones relativas a las prácticas de seguridad de la información. (Marque con una X la respuesta que represente su opinión).

Nunca (1), Casi nunca (2), A veces (3), Casi siempre (4), Siempre (5)	**1**	**2**	**3**	**4**	**5**
16. Suelo clasificar mi información					
17. Hago respaldos de mi información con regularidad					
18. Protejo mis documentos utilizando contraseñas					
19. Hago uso de un de programa antivirus para proteger mi equipo					
20. Suelo dejar a la vista documentación importante en mi escritorio					
21. Suelo dejar a la vista documentos de importancia en la pantalla de mi computadora					
22. Con qué frecuencia se realiza mantenimiento a mi equipo de cómputo					
23. Con qué frecuencia se presentan incidentes que ponen en riesgo la seguridad de la información					

V. Por favor conteste las siguientes preguntas.

24. ¿Dónde suelo resguardar la información de mis pacientes?

25. Memoria USB ( )
26. Disco duro Externo ( )
27. Computadora de oficina ( )
28. La nube (Dropbox, Google drive, etc) ( )
29. Dispositivo móvil ( )

30. ¿En dónde resguardo físicamente mí información?

31. Escritorio ( )
32. Gabinete ( )
33. Armarios ( )
34. Lockers ( )
35. No la resguardo ( )
36. Otros _____
37. ¿Qué acciones llevaría a cabo en caso de sufrir un incidente donde su información se viese comprometida?

_____
_____
_____

38. ¿Qué dificultades encuentra usted para mantener segura la información en su lugar de trabajo?

_____
_____
_____

39. ¿Quién es el responsable de brindar mantenimiento a los equipos de cómputo?

_____
_____
_____