UNIVERSIDAD AUTÓNOMA DE ZACATECAS
"FRANCISCO GARCÍA SALINAS"
Unidad Académica de Ingeniería Eléctrica

TÍTULO DE LA TESIS:

Creación de Políticas de Seguridad de la Información a partir de un Análisis de Riesgos de los Activos de la Información dentro de la Unidad Académica de Psicología de la Universidad Autónoma de Zacatecas

Tesis para optar el grado de:
Maestro en Ingeniería y Tecnología Aplicada

NOMBRE DEL ESTUDIANTE:
Ing. En C. Tomás de Jesús Moreno Zamudio

Asesores:
Dr. Sodel Vázquez Reyes
MIA Santiago Villagrana Barraza

Co-Asesor:
Dr. Carlos Alberto Olvera Olvera

AGRADECIMIENTOS

Agradezco, en primera instancia, a Dios, por brindarme esta gran oportunidad y por haber colocado a las personas correctas en mi vida académica y profesional. A su vez, agradezco a mis padres, quienes me han enseñado siempre a alcanzar mis metas a través de esfuerzo y perseverancia; gracias siempre por las herramientas de vida que me han brindado.

Agradezco al CONACYT por el apoyo económico brindado durante la realización de este proyecto, y al mismo tiempo lo exhorto a seguir apoyando las causas de investigación científica en el país a pesar de los momentos difíciles; muchos no hubiésemos podido completar nuestra formación de Posgrado sin su valioso y oportuno apoyo, y en ese tenor, sería excelente que todos tuviéramos la misma oportunidad.

Agradezco a la Unidad Académica de Ingeniería Eléctrica, y especialmente a mi Honorable Universidad: La Máxima Casa de Estudios de Zacatecas, la Benemérita Universidad Autónoma de Zacatecas., institución de enorme calidad, que me ha brindado una formación integral durante más de 8 años, y que, sin ésta muchos de nosotros no tendríamos la oportunidad de seguirnos formando como profesionales de calidad.

Quiero agradecerles a mis asesores de tesis, quienes tuvieron la paciencia y la disposición de llevar a buen término este proyecto, sin duda alguna, ellos fueron parte esencial en este proceso académico, además de que son grandes colegas y amigos.

Agradezco a todos mis amigos que de alguna u otra forma estuvieron involucrados en mi proceso de formación, gracias por estar siempre en los momentos más importantes de mi vida académica y personal.

Agradezco también a los sinodales y lectores que se tomaron el tiempo de revisar este proyecto de tesis y de investigación, también formarán parte esencial para la culminación de este proceso que es importante para todos.

DEDICATORIA

Dedico esta tesis a todas las personas que han sido de suma importancia en mi vida profesional y personal.

A mi madre, que día a día me demuestra que los obstáculos que se presentan en la vida se pueden superar con disciplina, amor y esfuerzo.

A mi padre, que siempre me ha inculcado un espíritu de lucha y perseverancia.

A mi hermano, que me ha demostrado que a pesar de todo podemos contar uno con el otro.

A toda mi familia que, indirectamente han estado en procesos importantes de nuestras vidas.

A mis amigos: Alejandro Pérez, Pedro Morales, Erik Lixsandro, Ulises Saucedo, Erik Rosales, Isaac Ferrer, Oscar Paniagua, Alejandro Gaytán y Hamlet; quienes me han acompañado durante más de 15 años en mi vida. A Luis Aguirre, Bruno Esquivel, Juan Adame, Víctor Rodríguez, y en general, a todos los que forman parte de un gran equipo apodado “FUA”; sin duda alguna, son un ejemplo de lucha y orgullo universitario. A mis amigos que conocí en el ámbito Universitario: Roberto Valadez, Tarango, Cardiel, Carlos Castruita, Yazmín Alfaro, Rosalba Guerrero, Gerardina, y todos aquellos que han sido parte fundamental de mi formación personal, académica y profesional.

A la mujer que me acompañó durante 7 años de mi vida; quien fue un pilar importante en todo este proceso de mi formación.

A todos aquellos administrativos, trabajadores y universitarios en general que he tenido la fortuna de conocer, y que, algunos de ellos se han convertido en grandes amigos y ejemplo de trayectoria académica y profesional

A mis Asesores: Santiago Villagrana, Carlos A. Olvera Olvera y Sodel Vázquez, quienes siempre han sido un gran ejemplo para mí y que siempre han estado al pendiente de nuestro desempeño académico, e inclusive personal, gracias nuevamente.

A todas aquellas personas que han entrado a mi vida para cambiarla en un buen sentido; son personas que me han ayudado a crecer en todos los ámbitos.

RESUMEN

La Universidad Autónoma de Zacatecas cuenta con información sensible en distintos ejes; empezando desde información personal, de proyectos académicos y de manejo de recursos financieros, tecnológicos e institucionales. Toda esta información, constituye por naturaleza, una serie de activos que siempre serán importantes para cualquier organización educativa. En esta lógica, la presente investigación, nace del interés de implementar *Políticas de Seguridad de la Información* para poder gestionar adecuadamente los riesgos por parte del personal administrativo que tiene contacto directo con dichos activos de la información, específicamente dentro de la Unidad Académica de Psicología. El enfoque de la presente investigación es cuantitativo, utilizando el método no experimental, a través de un diseño transversal, donde la característica de recolección de datos se realizó en un único momento y fue de tipo descriptivo. Los resultados de la presente investigación muestran, a través de una matriz de análisis de riesgos, diferentes vulnerabilidades de los activos de la información de esta institución, herramienta que marcó la pauta para poder justificar adecuadamente las medidas de mitigación de riegos. Con base a esto, se realizó una búsqueda exhaustiva de buenas prácticas de seguridad de la información para exhibir una seria de recomendaciones que ayudarán a prevenir muchas de las vulnerabilidades y riesgos encontrados en cada activo de la información; todas estas recomendaciones se incorporaron a través de la creación de Políticas de Seguridad dentro del Área Administrativa de la Unidad Académica de Psicología de la Benemérita Universidad Autónoma de Zacatecas.

Palabras Clave: Seguridad de la Información, Gestión de la Seguridad de la Información, Políticas de Seguridad, Análisis de Riesgos.

ABSTRACT

The Autonomous University of Zacatecas has sensitive information on different axes; starting from personal information, academic projects and management of financial, technological and institutional resources. All this information constitutes, by nature, a series of assets that will always be important for any educational organization. In this logic, this research arises from the interest of implementing Information Security Policies to be able to adequately manage risks by administrative personnel who have direct contact with said information assets, specifically within the Academic Unit of Psychology. The focus of the present investigation is quantitative, using the non-experimental method, through a cross-sectional design, where the characteristic of data collection was carried out in a single moment and was descriptive. The results of the present investigation show, through a risk analysis matrix, different vulnerabilities of the information assets of this institution, a tool that set the standard to be able to adequately justify the risk mitigation measures. Based on this, an exhaustive search for good information security practices was carried out to display a series of recommendations that will help prevent many of the vulnerabilities and risks found in each information asset; All of these recommendations were incorporated through the creation of a Security Policy within the Administrative Area of the Academic Psychology Unit of the Benemérita Universidad Autónoma de Zacatecas.

Key Words: Information Security, Information Security Management, Security Policies, Risk Analysis.

Índice

Índice de Ilustraciones

Índice de tablas

Índice de Anexos

CAPÍTULO I: INTRODUCCIÓN

La globalización ha creado la necesidad de la utilización de las Tecnologías de la Información y Comunicación (TIC) dentro de las organizaciones modernas casi en su totalidad. Los procesos cotidianos dentro de éstas, apuntan a la optimización a través de las diferentes herramientas tecnológicas que la era de la información ofrece. En esta lógica, la Seguridad de la Información (SI) requiere colocarse en un eje prioritario para proteger los activos de Información dentro de las organizaciones, mismos que constituyen los pilares funcionales y primordiales dentro de éstas.

Al hablar de activos de información, no sólo hacemos énfasis en las tecnologías o situaciones técnicas, sino que se involucran diferentes conceptos que han sido abordados en temáticas relacionados con la Gestión de Riesgos. Así pues, el concepto de información, hace alusión a todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración (Cavalcanti, 2012). En este sentido, al hablar de Seguridad de la Información hacemos referencia al conjunto de procedimientos, estrategias y herramientas que permitirán garantizar 3 ejes primordiales: **Confidencialidad, Integridad y Disponibilidad.**

Para poder garantizar estos 3 ejes primordiales de la Seguridad de la Información, no basta con la implementación de tecnologías novedosas y potentes que garanticen la permanencia del activo más importante de una organización, sino que es necesario implementar ***Políticas de Seguridad*** que pongan de manifiesto los qué haceres del personal, tanto experto, como inexperto, para poder gestionar de manera adecuada los riesgos que están latentes para la información de cualquier organización. Así pues, una Política de Seguridad, según Borghello (2012), surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios

críticos, mismos que permiten a la compañía desarrollarse y mantenerse en su sector de negocios. Esta misma herramienta, se puede pasar a las organizaciones educativas, en donde la protección de datos y de los mismos activos de información, se ha convertido en una tarea crucial en los últimos años.

Hay diferentes metodologías para poder crear una Política de Seguridad en diferentes ámbitos o espacios. Sin embargo, se debe tener en cuenta, que, tal como lo explica Vega (2008), requiere no solamente conocer las amenazas a las que están expuestas la información y los recursos de una organización, sino también establecer el origen de las mismas, que pueden ser internas o externas a la organización. Es aquí donde se encuentra la importancia de realizar un análisis de riesgos de los activos de la información, para determinar el origen y conocer las amenazas que se perciben dentro de una organización, específicamente en las organizaciones educativas, en donde el personal administrativo está expuesto constantemente a estos riesgos de la seguridad de la información. A partir de esta importancia, y de saber diversas medidas que se requieren para integrar una protección adecuada, y de la problemática que yace en los diversos objetos de estudio, se pueden gestionar diversos riesgos.

1.1. PLANTEAMIENTO DEL PROBLEMA

Se pueden encontrar diversas problemáticas alusivas a la mala gestión de la seguridad de la información y de los impactos económicos, organizacionales y personales que subyacen de éste. Sin embargo, la problemática esencial que se aborda en la presente investigación hace un énfasis primordial en que no todas las organizaciones e instituciones en general tienen la capacidad de analizar los riesgos de sus activos de información y, por ende, no tienen la capacidad de implementar y proponer políticas de seguridad de la información que garanticen su desarrollo óptimo en cualquiera de sus ejes y/o departamentos. Así pues, partiendo de otra problemática más actual, se ha observado que, dentro de las organizaciones, específicamente en México, se hace un mal manejo y cuidado de la información dentro de éstas debido a que el avance tecnológico exige a las organizaciones

medidas de seguridad no sólo físicas y técnicas, sino que también se requiere una educación de seguridad, capacitación y concientización al personal que procesa y que está a cargo de la información. Así pues, ninguna institución educativa está exenta de este mal cuidado y uso de la información, y, por ende, de los riesgos que subyacen de ésta, así como de las amenazas, que por naturaleza adquiere cualquier activo de información, sin importar el área o departamento en donde se procese o utilice.

Si bien ya existen avances tecnológicos que ofrecen una protección amplia y efectiva, **es en el sector humano donde se encuentran vulnerabilidades impredecibles por naturaleza**, sobre todo en la gestión de los activos de información y lo que se maneja a partir de éstos. Así pues, el comportamiento de las organizaciones, es un eje importante para determinar las vulnerabilidades contextualizadas en la seguridad de la información. Esta afirmación se sustenta de manera clara y precisa a través de lo que afirma Chiavenato (2009), haciendo alusión a que el comportamiento organizacional (CO) es un campo del conocimiento humano extremadamente sensible a ciertas características de las organizaciones y de su entorno. Por tanto, es una disciplina que depende de las contingencias y las situaciones, así como de la mentalidad que existe en cada organización y de la estructura organizacional que se adopte como plataforma para las decisiones y las operaciones. Todo este constructo organizacional, se ve influido por los diferentes contextos y entornos que surgen y perduran dentro de cualquier organización o empresa, haciendo alusión a los procesos internos, el capital humano, modelos de negocio, etc. De los cuales, en su mayor parte, el personal y recurso humano juegan un papel predominante.

Dicho lo anterior, se desconocen, en muchas de las organizaciones educativas en México, medidas y normas que busquen preservar la información y que guíen al personal a tener un comportamiento adecuado a través de buenas prácticas para la protección ante ataques a los datos o algún activo de la información que sea utilizado por este mismo personal. En el caso de la Universidad Autónoma de Zacatecas, específicamente dentro de la Unidad Académica de Psicología, también se carece y se desconocen normas oficiales orientadas a la protección de datos y

seguridad de la información; esta información se constató a través de una reunión y entrevista, donde se informó que, en dicha Unidad Académica, y en la Universidad en general, no se cuenta con Políticas de Seguridad de la Información de manera oficial que pueda ayudar a los usuarios y a los administradores de la red y tecnología, a gestionar los riesgos de la información de una manera adecuada, por lo que la falta de certificación o capacitación y sobre todo de Políticas de Seguridad, imposibilita a la Universidad y a sus Unidades Académicas, en casos de riesgos en sus activos de información, tomar medidas adecuadas para poder preservarla y mantener los pilares ya antes mencionados.

Por esta razón, en la presente investigación se llevará a cabo una metodología adecuada para la creación de Políticas de Seguridad dentro del Área Administrativa de la Unidad Académica de Psicología de la Universidad Autónoma de Zacatecas, todo esto, tomando como primer punto de partida la realización de un Análisis de Riesgos de la Seguridad de la Información con metodologías ya propuestas por otros autores y organizaciones e instituciones expertas en el tema que aquí se aborda, tomando siempre la premisa de que la ausencia de Políticas de Seguridad de la Información, por lo regular, trae consecuencias graves para cualquier organización; una organización sin buenas prácticas, en general, no tendrá la noción de cómo utilizar adecuadamente las herramientas tecnológicas que tienen a su alcance, y, sobre todo, tener una guía de lo que se debe y no debe hacer con dichas herramientas. De ningunas situaciones está exenta el objeto de estudio que aquí se propone, por lo que se vuelve una problemática importante de estudiar y de atender.

1.2.1. Preguntas de Investigación

De la problemática detectada, subyacen las siguientes preguntas de investigación:

- ¿Cuáles son los principales riesgos y amenazas dentro de la Unidad Académica de Psicología de la Universidad Autónoma de Zacatecas que deben ser tomadas en cuenta para el diseño de Políticas de Seguridad para la Administración de Riesgos de la Seguridad de la Información?

- ¿Qué Activos de la Información son indispensables conocer para poder medir el Riesgo de la Seguridad de la Información dentro de la Unidad Académica de Psicología de la Universidad Autónoma de Zacatecas?
- ¿Cuáles son las principales buenas prácticas que se deben considerar incluir dentro de las Políticas de Seguridad de la Información para el Personal Administrativo partiendo del Análisis de Riesgos realizado en los activos de la información dentro de la Unidad Académica de Psicología de la Universidad Autónoma de Zacatecas?

1.2. JUSTIFICACIÓN

Las instituciones educativas en México y en el mundo, a lo largo de sus diferentes ejes históricos, han sufrido diversos ataques que han puesto, en cierta medida, en riesgo los datos e información más sensibles; y en esta misma lógica de ocurrencia de hechos, la Universidad Autónoma de Zacatecas también se ha visto afectada en algunas ocasiones. Dicho lo anterior, y dimensionando la relevancia que conlleva la Seguridad de la Información dentro de las instituciones educativas modernas, es de suma importancia evaluar y analizar las vulnerabilidades y riesgos que se pueden presentar dentro de éstas, para así poder proponer Políticas de Seguridad que conlleven a una Administración de Riesgos adecuada, y que permitan garantizar los 3 ejes primordiales ya antes mencionados, buscando así una reducción y anulación de los riegos y vulnerabilidades dentro de la Universidad Autónoma de Zacatecas, tratando siempre de salvaguardar los activos de información que, en este caso, la Unidad Académica de Psicología utiliza para poder llevar a cabo diferentes procesos esenciales. Es por eso que siempre será importante atender uno los factores más influyentes dentro del cumplimiento de los pilares de la Seguridad de la información, el cual hace alusión al sector humano dentro de los diferentes ejes organizacionales. En este sentido, la importancia de esta investigación yace en poder atender, a través de un mecanismo efectivo de mitigación de riesgos, lo que Chiavenato (2009) afirma a través de una analogía interesante entre los elementos socioculturales dentro de

una organización, y el funcionamiento del comportamiento existente dentro de las organizaciones, donde se hace alusión a los *aspectos visibles*: donde se encuentran aspectos relacionados con las estrategias, objetivos, políticas y procedimientos, estructura de la organización, autoridad formal, cadena de mando y tecnología, y a los *aspectos invisibles*: donde se visualizan aspectos relacionados con las percepciones, actitudes, normas del grupo, interacciones informales y conflictos interpersonales e intergrupales. A través de la observación y entendimiento de todos estos aspectos, es donde se puede dilucidar y dimensionar el impacto tan grande que tiene el factor humano dentro de cualquier organización, sobre todo en cuestiones de Seguridad de la Información, y es precisamente en este impacto, donde se sustenta la justificación esencial de esta investigación para poder establecer normas y medidas de seguridad que ayuden a brindar un panorama más amplio de los quehaceres por parte del personal de una organización para actuar y acatar puntualmente las actividades relacionadas con la prevención de riegos y protección de datos. Para poder establecer adecuadamente estas normas y/o Políticas, es necesario realizar un adecuado análisis de todos los factores y amenazas que pueden existir en los activos de la información de una organización, para así, sustentar, teórica y prácticamente la implementación de esas buenas prácticas según sea el contexto que se dé; por eso, para cualquier institución educativa, se vuelve totalmente necesario tener una adecuada gestión de riesgos que permita saber cuáles son las principales vulnerabilidades de sus activos de información y cuáles son las amenazas que podrían explotar las vulnerabilidades. En la medida que la institución tenga clara esta identificación de riesgos podrá establecer las medidas preventivas y correctivas viables que garanticen mayores niveles de seguridad en su información; el hecho de saber en dónde está parada la institución, en cualquier eje de los activos de la información marcará la pauta más importante para prevenir e implementar estrategias de protección de la seguridad de la información.

Dicho lo anterior, se puede enfatizar otro punto importante que justifica esta investigación, la cual hace alusión a la elaboración adecuada de las Políticas, partiendo de un análisis establecido con metodologías adecuadas al objeto de

estudio. En este caso, dentro de la Universidad Autónoma de Zacatecas, específicamente en la Unidad Académica de Psicología, resulta sumamente necesario establecer Políticas de Seguridad de la Información en el Personal Administrativo, ya que partiendo de que no hay normas bien establecidas para este rubro, la incorporación de éstas, podría en todos los sentidos y panoramas, utilizarse como una herramienta para concientizar al personal sobre los riesgos de seguridad y proporcionar pautas de actuación concretas, consolidando así acciones para poder mantener a una empresa en constante desarrollo. Así pues, todas las organizaciones requieren la coordinación de diferentes actividades de colaboradores individuales con el objetivo principal de efectuar transacciones planeadas con el entorno. Las aportaciones de cada persona a la organización varían en función no sólo de sus diferencias individuales, conocimientos y competencias, sino también de los sistemas utilizados por la organización (Chiavenato,2019). La coordinación de actividades a las que se hace alusión, sin duda alguna, se verá plasmada en normas y el fomento de buenas prácticas que conlleven al desarrollo óptimo de los procesos organizacionales; es decir, es de suma importancia en toda institución educativa, específicamente en la Unidad Académica de Psicología de la Universidad Autónoma de Zacatecas, la elaboración, y posteriormente, el seguimiento de Políticas de Seguridad de la Información para su Personal Administrativo.

1.3. HIPOTÉSIS

La identificación de las amenazas y riesgos de los activos de la información de la Unidad Académica de Psicología de la Universidad Autónoma de Zacatecas a través de la implementación de un Análisis de Riesgos, facilitará el proceso de la creación de Políticas de Seguridad de la Información para el Personal Administrativo de dicha Unidad Académica.

1.4. OBJETIVOS

General:

Diseñar Políticas de Seguridad para la Administración de Riesgos de la Seguridad de la Información a través de un Análisis de Riesgos de los activos de la información dentro de la Unidad Académica de Psicología de la Universidad Autónoma de Zacatecas

Específicos:

1. Caracterizar a la Unidad Académica de Psicología de la UAZ, en cuanto a qué información hay, quién la usa, personal y sindicatos, sistemas que se manejan, etc.
2. Analizar los Riegos de Seguridad de Información dentro de la Unidad Académica de Psicología de la Universidad Autónoma de Zacatecas.
3. Saber la Percepción de la Seguridad de la Información en los integrantes que tienen contacto con Tecnología dentro de la Unidad Académica de Psicología de la Universidad Autónoma de Zacatecas
4. Analizar algunas métricas del ISO/IEC 27000 vinculadas con el factor humano para ver la viabilidad de inclusión dentro de las Políticas de Seguridad de la Información aquí propuestas, tomando en cuenta también algunas métricas y metodologías implementadas por otros autores y/o instituciones en general.
5. Seleccionar algunas de las métricas analizadas, ya sea de del ISO/IEC 27000, o algunas otras adaptadas a partir de este estándar, que estén vinculadas con el factor humano para ver la viabilidad de inclusión dentro de las Políticas de Seguridad propuestas.

CAPÍTULO II: MARCO TEÓRICO

2.1. ANTECEDENTES

A lo largo del contexto histórico del concepto de Seguridad de la Información, se han realizado diferentes investigaciones, análisis y prácticas, en las cuales se ha puesto de manifiesto que el ser humano en general, juega un rol importante en las situaciones relacionadas con las vulnerabilidades de los activos de información en cualquier institución, organización o contexto. Estos actos van a depender del significado trascendental que se le dé a la información que se está manipulando, ya que, a través de ésta, se pueden generar diversas hipótesis, historias de vida y modelos económicos que le garantizarán su prevalencia y calidad de vida en los diferentes ejes de evolución

2.1.1. El Recurso humano dentro de las organizaciones

Hay muchos estudios realizados acerca del recurso humano dentro de las organizaciones, sin embargo, las que interesan para esta investigación, son aquellas que hacen alusión a las negligencias relacionadas al manejo de los datos instituciones. En este tenor, hay que visualizar que los ataques a la información dentro las organizaciones, tanto de forma física, lógica y/o digital, cada día son más comunes y despierta el interés de diferentes grupos de ciberdelincuentes. Varios estudios realizados afirman que el 75% de los ataques de seguridad son producidos a través del factor humano; por ejemplo, en fallos de configuración de las herramientas tecnológicas, o bien, por un mal uso del personal de la propia organización (Vieites, 2015). Así mismo, dentro de uno de los reportes sobre ciberseguridad (CISCO, 2019), se exhiben varios hallazgos clave alusivos al factor humano: los delincuentes online utilizan a los usuarios para instalar malware o contribuir a aprovechar los puntos débiles de la seguridad, por ejemplo, a través de correos electrónicos; el error humano es una realidad y, en la actualidad, existe una industria multimillonaria de delitos cibernéticos que apuesta al error. Necesita estar preparado para este error y poder responder rápidamente cuando sucede. En esta

lógica, se puede afirmar que el comportamiento negligente de los usuarios a la hora de usar Internet, sumado a las campañas selectivas de los enemigos, hace que muchos mercados verticales presenten un mayor riesgo de verse expuestos a malware en sitios web o a cualquier tipo de ataque que vulnere los 3 pilares esenciales de la Seguridad de la Información.

En otros estudios realizados dentro las organizaciones, mostrados por Dell Technologies (2011), el 56% de los empleados ha podido ingresar al edificio de su trabajo sin presentar tarjeta de acceso, en más de una oportunidad. Casi el 85% de esos trabajadores ha facilitado más de una vez el acceso de alguien que no conocía a sus oficinas. El 60% de los empleados aún conservan acceso a información que ya no requieren. Así mismo, se supo que, 7 de cada 10 empleados envía con frecuencia documentos de trabajo a su dirección de mail personal, lo que sugiere un riesgo y una mala práctica respecto a la seguridad de la organización. Tales resultados que muestra Dell Technologies (2011), provienen de una encuesta llevada a cabo por RSA, la División de Seguridad de la empresa EMC, entre trabajadores del sector privado y público en Boston, Washington D.C. y Buenos Aires. El foco de los analistas estuvo puesto en las actitudes y conductas de seguridad de acceso de cada miembro de las empresas y organizaciones, lo que conlleva a planificar diversas metodologías para mitigar riesgos de Seguridad de la Información relacionados con el factor humano, a través de implementación de manuales, capacitaciones y sensibilización respecto a estos temas, tomando en cuenta también las organizaciones educativas y universidades, y nunca perdiendo de vista que la seguridad de la información en cualquier organización es crucial para mantener su desarrollo constante. Así pues, han ocurrido una serie de eventos documentados en los cuales se exhibe que hay prácticas negativas por parte del sector humano que hace uso de la información y que, hay más antecedentes relacionados con diversos ataques en diversos contextos, mismos que forman parte de la justificación y del porqué es importante implementar y fomentar la seguridad de la información a través de diversas estrategias.

2.1.2. Ataques realizados a organizaciones

En el 2014, *PandaSecurity* anunció que varias empresas internacionales sufrieron ataques de Información de Seguridad. En mayo, los ciberdelincuentes accedieron a las cuentas de algunos empleados de eBay, lo que propició acceso a la red interna de la empresa, y por ende a la base de datos donde se tenía información de los usuarios, tal como teléfonos, direcciones, contraseñas y correos electrónicos. También informó que, la compañía financiera coreana, Korea Credit Bureau (KCB), fue víctima en enero de un ataque en el que le robaron 105,8 millones de cuentas de usuarios que incluían detalles de tarjetas de crédito, nombre y apellidos, teléfonos, direcciones e incluso números de pasaporte. En este caso no se utilizó malware para acceder a la información. El ladrón trabajaba para KBC y durante 11 meses copió toda la información y la vendió al que le ofertó mejor. Otro dato importante que aportó, es que Sony, en el 2014, también sufrió un ataque, causando estragos como una semana sin poder conectar las computadoras, borrado masivo de información, robo de todo tipo de información interna de la empresa, etc. Los atacantes también han publicado 5 películas que estaban aún sin estrenar y amenazaron con publicar más información confidencial.

En el 2016, el periódico digital *El País*, a través de la nota escrita de Mendiola Zuriarrain (2016), anunció que más de 60 millones cuentas en Dropbox fueron robadas. El servicio en la nube confirmó que recibieron diferentes reportes de usuarios que reportaban un correo spam recibido a las direcciones de Dropbox. La empresa, dio a conocer a través de un comunicado que la plataforma había sido hackeada. Este ataque se originó desde el 2012, tras el robo de las credenciales a un empleado, lo que propició acceso a la información de las personas que utilizan el servicio en la Nube.

Más recientemente, en el 2019, se presentaron varios ataques que pusieron en verdaderos problemas a diferentes organizaciones en el mundo. La empresa *ESET*, a través de un artículo realizado por Lubeck (2019), hizo un pequeño informe donde anunció la invasión a la privacidad de los usuarios en La Liga Nacional de Fútbol profesional (LFP) de España y su aplicación oficial. El organismo propietario de los derechos del fútbol de España fue multado tras ser acusado de utilizar la app para

espiar a través del micrófono de los dispositivos móviles de los usuarios con el objetivo de buscar transmisiones ilegales de los partidos. Otro dato interesante que informó ESET a través d este artículo, fue uno que tiene que ver directamente con el factor humano y con la vulnerabilidad emocional; los ataques que hacen uso de la ingeniería social siguen sumamente activos, principalmente aquellos que eligen plataformas como WhatsApp para distribuirse. En este período de tiempo se reportaron distintas campañas de phishing que prometían, por ejemplo, accesos a Spotify premium de forma gratuita, así como engaños más elaborados y que también hacían uso de la ingeniería social, pero que iban dirigidos a usuarios que habían sido víctimas del robo de un iPhone.

En el caso específico de México, las prácticas dañinas por medio de **software** y aplicaciones móviles (**malware**) han causan un impacto económico anual al país de 39,000 millones de pesos (3,000 millones de dólares), lo que equivale a casi dos veces la recaudación por el impuesto de 10% a los refrescos, según el reporte anual de ciberseguridad de Norton, realizado algunos años atrás. Esa pérdida económica refiere a los ataques detectados específicamente por incidentes de **phishing** (suplantación de sitios para obtener información), ingeniería social y ataques dirigidos para robar a empresas a través de los dispositivos de sus empleados (Chávez, 2013).

Tal como se puede observar, México también se ha visto involucrado en situaciones donde se ve comprometida la información de sus organizaciones y en donde tiene que poner principal énfasis en su ciberseguridad y seguridad de la información en general; dentro de las organizaciones mexicanas, se dan mucho los ataques avanzados, que están planeándose con tiempo, y que están incluso contemplando infiltrar gente y utilizando conocimiento de la organización y temas externos, y al final están teniendo un impacto importante. Pero el otro es el oportunístico, aquellos ataques que están buscando ver quién está desprotegido, y está generando grandes impactos a las organizaciones. Por ejemplo, el ramsonware, que es uno de los ataques que se viven con más frecuencia en México, no va dirigido a nadie, va a ver a quién cae, y a quien le cae tiene que sufrir las consecuencias y tiene que tener respaldo para que no le impacte (Bello, 2019).

Así mismo, se conoce que, en noviembre de 2019, ocurrió un ciberataque de secuestro de datos para demandar un pago por parte de 5 millones de dólares a Pemex, hecho que provocó una severa afectación a sus operaciones. Apenas el día 24 de febrero del 2020 se realizó un ataque a los sistemas operativos de la Secretaría de Economía, en donde los servidores de correos electrónicos y archivos resultaron dañados. Estos son problemas de seguridad nacional (De Haas Matamoros, 2020).

2.1.3. La Seguridad de la información en las organizaciones mexicanas

La Seguridad de la Información en México es un concepto al que no se le ha tomado mucha importancia. No hay mucha documentación relacionada con la implementación de Seguridad de Información dentro de las organizaciones mexicanas, aunque hay empresas que ofrecen servicios en este ámbito. El problema de la implementación de seguridad dentro de las organizaciones mexicanas yace, más que nada, en la concientización y cultura de la sociedad.

En términos de seguridad informática, México se encuentra lejos de los estándares mundiales. Mientras a nivel global las estrategias de ciberseguridad alineadas al negocio ya son un requerimiento estándar para 45% de las empresas, en México, sólo 19% de las compañías aplican este tipo de reglamentaciones, rezago que de acuerdo con el director de asesoría para la consultora Ernst & Young (EY), Christian Andreani, incrementa la probabilidad de las empresas mexicanas de sufrir un ciberataque (Chávez, 2014).

Este dato, no ha cambiado mucho en los últimos años, ya que, apenas en el 2019, Marcos Polanco, director de servicios estratégicos de Situm, la consultora de Telmex, expuso a la revista *Expansión* que México y sus empresas tienen grandes retos por delante: una estrategia de país no implementada, empresas poco preparadas y grandes vulnerabilidades, según se discutió en una sesión de la Cumbre de Negocios México en ese mismo año, que se celebró en Cancún en octubre. En este sentido, México ha ido avanzando, pero no a la velocidad que se necesita. Los atacantes están avanzando más rápido incluso a veces que las

organizaciones. A nivel país, la estrategia nacional falta implementarla, falta ver resultados tangibles. A nivel empresarial, hay distintos niveles. Hay empresas que están avanzando más rápido, como son por su naturaleza las del sector financiero, sin embargo, es muy dispar el nivel, las hay que tienen un nivel muy básico y están sufriendo las consecuencias de este tipo de situaciones. (Bello, 2019).

Un dato mucho más reciente, es el de que hay una batalla en el ciberespacio, y el Estado Mexicano enfrenta un grave rezago para hacer cumplir la ley en esta extensión virtual de la soberanía nacional. Es urgente preservar la seguridad de la nación también desde lo virtual, propiamente en el ciberespacio. Para ello, es requerido empezar por legislar. A partir de la reciente declaración del titular de la Secretaría de Seguridad y Protección Ciudadana, el doctor Alfonso Durazo Montaño, una de las necesidades legislativas en materia de seguridad que se promoverán en este periodo legislativo de sesiones, es una Ley de Ciberseguridad. La regulación de la ciberseguridad es ya un asunto legislativo prioritario (De Haas Matamoros, 2020).

A pesar de que la Seguridad de la Información está en “pañales” en México, el Gobierno Federal exige el máximo de Seguridad de los datos a través de leyes sustentadas y aprobadas en las distintas instancias. Una de éstas, y que tiene suma relevancia en cuanto a la Seguridad de la Información, es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), la cual es aplicable a todas las personas físicas o morales, del sector público y privado, tanto a nivel federal como estatal, que lleven a cabo el tratamiento de datos personales en el ejercicio de sus actividades, por lo tanto empresas como bancos, aseguradoras, hospitales, escuelas, compañías de telecomunicaciones, asociaciones religiosas, y profesionistas como abogados, médicos, entre otros, se encuentran obligados a cumplir con lo que establece esta ley. Además, tal como se mencionó con anterioridad, la regulación de la ciberseguridad poco a poco se va convirtiendo en un asunto legislativo, aunque aún hay mucho por avanzar en esta lógica. Sin duda alguna México tiene que ir avanzando en muchas cuestiones respecto a Ciberseguridad y Seguridad de la Información, y en el caso del Estado de Zacatecas no debe ser la excepción. Por ejemplo, en el Estado de Zacatecas,

aparte de seguir la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, se ha tratado de hacer esfuerzos por implementar proyectos como el que Gandaria (2019) señala, mismo que tiene que ver con la instalación de laboratorios de Ciberseguridad para la vigilancia de la red pública de internet y Deep Web por parte de la División Científica, cuyo objetivo es la prevención y atención de delitos, como la suplantación de identidad, pornografía, fraudes bancarios, ataques web, entre otros. Sin embargo, es una realidad que en Zacatecas todavía falta mucho camino por recorrer en estas cuestiones, desde el ámbito empresarial, hasta el ámbito educativo.

2.1.4. Ataques a la seguridad de la información en las universidades

Dentro de cualquier Universidad y por ende organización, existen activos que hacen referencia a cualquier cosa que tenga valor para ésta, tal como la información de cualquier índole. En esta lógica, cualquier Universidad es blanco de ser atacado para diferentes fines; ya sea por los activos tan relevantes que ésta contiene, o por la cantidad de equipos que ayudarían a los ciberdelincuentes a realizar ataques masivamente hacia otras organizaciones con diferentes fines económicos, sociales o políticos. Malvido (2010), afirma que hasta dos veces al mes requiere la policía a la Universidad que le entregue informes de conexiones a internet, y es que hay 'hackers' que utilizan su red informática para atacar a otros dispositivos y organismos. En esta lógica, afirma también que la red informática de la Universidad se ha convertido en una plataforma para los delitos informáticos, porque su capacidad de conexión es muy alta y por la gran cantidad de usuarios que la utilizan cada día.

En los últimos años, diversas Universidades han presentado ataques informáticos y ataques a su Seguridad de la Información. Estos ataques son polimorfos y multipropósito, haciendo más difícil detectarlos y generar planes de Contingencia o modelos de seguridad que los eviten. Por ejemplo, según *Obando Jaramillo (2015)* en Bogotá, un estudiante utilizando un software registrador de teclas (key loggers), capturó la contraseña de docentes para acceder al sistema de notas y poder alterarlas. Según Forbes (2018), las instituciones educativas ocupan el tercer lugar

a nivel mundial, en términos de vulnerabilidad en ciberseguridad. Y el foco de sus "atacantes" son esencialmente estudiantes. Un ejemplo que se relata en este mismo artículo, es el de un estudiante de 25 años, que fue condenado en febrero pasado por los delitos de acceso abusivo a sistema informático, violación de datos personales y uso de software malicioso, logró, a través de key loggers (registrador de teclas), descifrar las contraseñas de algunos profesores para ingresar a la plataforma de notas. Luego creó un correo electrónico clandestino, a través del cual contactó a estudiantes de varios cursos y les ofreció sus servicios.

El fraude se descubrió cuando una alumna recibió el correo de "soluciones académicas", en el cual le ofrecían subir la nota de sus parciales por un precio que oscilaba entre $70 y $90 mil. La joven puso en conocimiento de los hechos a las directivas de la universidad, que a su vez denunciaron ante las autoridades.

Nimnicht (2019), a través de una Encuesta lanzada por la empresa McAffe, la cual es una de las principales empresas de ciberseguridad a nivel mundial, informó que el 80% de los estudiantes han sido afectados por un ataque cibernético, o tienen un amigo / familiar que ha sido afectado, sin embargo, el 43% afirma que no creen que sean víctimas de un delito cibernético. Solo el 19% de los estudiantes toman medidas adicionales para proteger sus registros escolares y académicos en comparación con el 69% de los estudiantes que protegen proactivamente su información bancaria o financiera. En el primer trimestre de 2019, los ataques cibernéticos divulgados públicamente dirigidos al sector educativo aumentaron en un 50%, en comparación con el trimestre anterior. Más del 70% de los ataques cibernéticos desde enero hasta mayo de 2019 utilizaron el secuestro de cuentas o malware como el principal vector de ataque. Según la Fundación Universitaria Iberoamericana (FUNIBER, 2020), algunos de los datos ya mencionados, se ven ratificados a través de un estudio elaborado por la compañía experta en ciberseguridad Kaspersky, que detectó casi 1.000 ataques en más de 130 universidades de 16 países. Los atacantes emplean como cebo una página web idéntica a la original para captar a empleados y estudiantes. Estos introducen sus datos de acceso y credenciales que quedan a disposición del hacker.

En resumen, se puede afirmar que las universidades hoy en día son un blanco y una presa jugosa para los hackers y atacantes. Si bien es cierto que teniendo herramientas tecnológicas que puedan disminuir los ataques cibernéticos a las Universidades, es el factor humano el que sigue prevaleciendo para poner en riesgo la Seguridad de la Información dentro de éstas, y es menester y de suma importancia trabajas en la implementación de buenas prácticas y políticas que ayuden a gestionar adecuadamente los riesgos que subyacen de estos ataques.

2.1.5. Datos, antecedentes y caracterizaciones relevantes dentro de la Universidad Autónoma de Zacatecas.

2.1.5.1. Historia de la Universidad

La Universidad Autónoma de Zacatecas (UAZ), tiene origen el 13 de septiembre de 1774, cuando el H. Ayuntamiento de Zacatecas se dirigió al Virrey de la Nueva España, solicitando la creación de un Colegio. En base a diversas gestiones, se consiguió lograr la fundación de dicha escuela, impartiendo inicialmente cátedras de Latinidad, Retórica, Filosofía, Historia y Teología Eclesiásticas y retomando la constitución y el reglamento del Colegio de San Idelfonso de la ciudad de México para regir el Colegio llamado en aquella fecha “San Luis Gonzaga de Zacatecas”. Los padres jesuitas se encargaron de la dirección de este Colegio hasta que en 1832 se le dio el nombre de Instituto Literario, después se llamó Instituto Literario de García y luego Instituto Científico y Literario de Zacatecas, posteriormente Colegio del Estado, para después llamarse Instituto de Ciencias, que, al alcanzar su autonomía, se denominó Instituto de Ciencias Autónomo de Zacatecas (ICAZ) (Universidad Autónoma de Zacatecas [UAZ], 2018).

La UAZ, a lo largo de su eje histórico, ha sufrido cambios de diferente índole, empezando por su nomenclatura; de 1932 a 1837 llevaba como nombre “Casa de Estudios de Jerez, donde al ocupar la gubernatura del Estado el señor Francisco García Salinas promovió en 1832 la fundación de una Casa de Estudios donde se impartieron las cátedras de: latín, Dibujo, Bellas Artes, francés, Lógica, Geografía y Jurisprudencia (UAZ, 2018).

La Universidad Autónoma de Zacatecas “Francisco García Salinas” (UAZ), históricamente tiene un compromiso con la sociedad zacatecana, particularmente con los jóvenes universitarios, es en ese sentido que como lo expresa el Capítulo II, Artículo 4, en sus fracciones de la I a la V de la misma Ley Orgánica de la Universidad Autónoma de Zacatecas, la Universidad tiene como fines esenciales:

I. Impartir educación de modo que se obtenga la adecuada preparación del estudiante, para la eficacia de sus servicios a la sociedad como profesionista, técnico, catedrático universitario o investigador;
II. Organizar, realizar y fomentar la investigación científica, humanística y tecnológica de tal forma que comprenda lo universal, y en especial los problemas nacionales y regionales; proponiendo las soluciones que estime conducentes;
III. Extender y divulgar la ciencia, la tecnología, el arte y la cultura;
IV. Fortalecer a su cuerpo académico mediante la formación y actualización; y
V. V. Coadyuvar a que se erradique la marginación y la desigualdad social, mediante la universalidad del conocimiento y el desarrollo de los más elevados valores humanos, fortaleciendo así la soberanía y la identidad nacionales.

2.1.5.2. Estructura general de la Universidad.

La Universidad Autónoma de Zacatecas está compuesta por Áreas Académicas, y a su vez, éstas se subdividen en Unidades Académicas. En este tenor, la Universidad también requiere de trabajadores, tanto en el ámbito docente, como en el ámbito administrativo.

En el ciclo 2016-2017, según las Numeralias reportadas, la Universidad Autónoma de Zacatecas, cuenta con 2895 académicos, de los cuales 1459 son de tiempo completo, 508 de medio tiempo, 781 laborando horas clase y 147 en horas clase DE. Así mismo, la UAZ cuenta con 2,800 trabajadores, mismos que laboran en las distintas áreas administrativas y de intendencia. En cuanto a los alumnos, la universidad cuenta con 37395 alumnos, de los cuales 638 alumnos son de

educación media básica, 11463 alumnos de educación media superior, 23594 alumnos de licenciatura y 1700 alumnos de posgrado. Así mismo, la UAZ en el ciclo 2016-2017, contaba 1 plan de estudio de educación media básica, 2 planes de estudio de educación media superior, 39 programas académicos de licenciatura y 47 programas académicos de maestría, doctorado y especialidad. Así mismo, cuenta con 1 plantel de educación media básica, 13 planteles de educación media superior, 28 unidades académicas de licenciatura y posgrado y 4 centros de investigación.

2.1.5.3. Seguridad de la información dentro de la Universidad Autónoma de Zacatecas

En los últimos años, la Universidad Autónoma de Zacatecas, a través de la Coordinación de Informática y Telecomunicación y los departamentos que derivan de ésta, han hecho esfuerzos constantes para preservar y gestionar de manera adecuada los activos de información que hay en la Universidad, así como la configuración adecuada de sus redes, con la finalidad de mitigar riesgos y estableces una cultura de Seguridad de la Información. A través de algunas entrevistas, reuniones y auditorias, se han sabido de algunas vulnerabilidades y ataques que han puesto en riesgo los activos de la información de la Universidad en general, sin embargo, dicho departamento ha podido mitigar de manera oportuna dichas amenazas.

Algunas de las técnicas que la Universidad ha adoptado, es la implementación de estándares de calidad en los procesos que esta lleva, además de empezar a generar investigaciones y concientización de diferente índole. Además, otra acción de suma importancia, es la de la contratación de herramientas que logren proteger la infraestructura y la red que la Universidad utiliza; una de estas herramientas es la de FORTIGATE, herramienta que permite una infraestructura de seguridad simplificada de extremo a extremo, con la cual se logra, proteger toda la superficie de ataque desde la sede hasta las sucursales con seguridad avanzada, completar la visibilidad y el control en la nube que habilita aplicaciones seguras y la conectividad, permite ofrecer aplicaciones seguras, acceso a dispositivos y administración sin comprometer el rendimiento y la velocidad, implementar

información de amenazas avanzadas para detectar, prevenir y responder a malware sofisticado y mejorar el conocimiento de seguridad, proteger las aplicaciones web críticas de la empresa con un conjunto integrado de productos para detener las amenazas avanzadas, entre otras acciones dignas de implementar para mantener salvaguardados los activos físicos de la institución. Todo esto, lo hacen a través de un convenio con la empresa FORTINET, empresa que se dedica a proporcionar seguridad de redes, así como productos de acceso seguro que comparten inteligencia y trabajan en conjunto.

A pesar de los constantes esfuerzos por parte del personal de la Coordinación de Evaluación e Información Institucional para poder implementar esta cultura de seguridad de la información y ciberseguridad, sigue habiendo la problemática de que no hay una capacitación y concientización por parte del personal administrativo y gestor de la información, y los ataques, por más herramientas tecnológicas que se lleguen a implementar, vulneran el sector humano; esto ocurre desde la administración central hasta las Unidades Académicas existentes en la Universidad. Es aquí, donde se reitera y ratifica la importancia de esta investigación: la creación de Políticas de Seguridad de la Información, en donde se incluyan buenas prácticas respecto al salvaguardo de los activos de la información, y el implementarlas en cada Unidad Académica sería de gran ayuda para mitigar riesgos muy generales y esenciales.

2.1.6. La Universidad Autónoma de Zacatecas y ANUIES-TIC: Informe respecto a la Seguridad de la Información en Universidades Públicas.

La Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES) reúne a las principales Instituciones de Educación Superior (IES) de México, representando más del 90% de la matrícula de educación superior en México; se trata de una organización plural y no gubernamental que promueve el mejoramiento integral de las instituciones asociadas en los campos de la docencia, la investigación y la extensión de la cultura y los servicios.

Dentro esta Asociación de suma relevancia, se encuentra el Comité de Tecnologías de la Información y Comunicaciones (tic) de la ANUIES, denominado también “Comité ANUIES-TIC”, éste fue creado y avalado en diciembre de 2015, como un órgano para la participación y la coordinación entre las Instituciones de Educación Superior asociadas a la ANUIES, que asesora y promueve las mejores prácticas para el uso y el aprovechamiento de las TIC. El Comité ANUIES-TIC ha enunciado como ejes estratégicos las temáticas de Gobierno de Tecnologías de la Información, la Seguridad de la Información y la Gestión Interinstitucional con proveedores y prestadores de servicios de tic, y sin duda alguna, cada año se preocupa por mejorar las prácticas relacionadas a estos temas.

En el 2016, se realizó un estudio con un universo de 179 instituciones de educación superior, que forman parte de la Asociación Nacional de Universidades e Instituciones de Educación Superior en México (ANUIES), en el cual, la Universidad Autónoma de Zacatecas no aparece. Dentro de este informe, se muestran resultados alusivos a la Seguridad de la Información, pero aquellos que más interesan para la presente investigación hacen referencia a Política de seguridad alineada a los objetivos de la institución, Auditoría de seguridad de la información, Herramientas de seguridad de la información, Incidentes de seguridad de la información. Porcentaje de IES que considera la gestión de riesgos.

En el indicador de Políticas Seguridad, ANUIES (2016), se describe como parte fundamental de cualquier esquema de seguridad eficiente; aminoran los riesgos para la institución, y permite a los profesionales de ti actuar de manera rápida y acertada en caso de algún ataque informático. Indican a los usuarios la manera adecuada de usar un sistema, señalando lo que puede hacerse y lo que debe evitarse en una red de datos, contribuyendo a que no seamos “malos vecinos” sin saberlo. Los resultados que se obtuvieron en este indicador, respecto a la implementación de cada universidad incorporada a ANUIES, se muestran a través de la Ilustración 1.0.

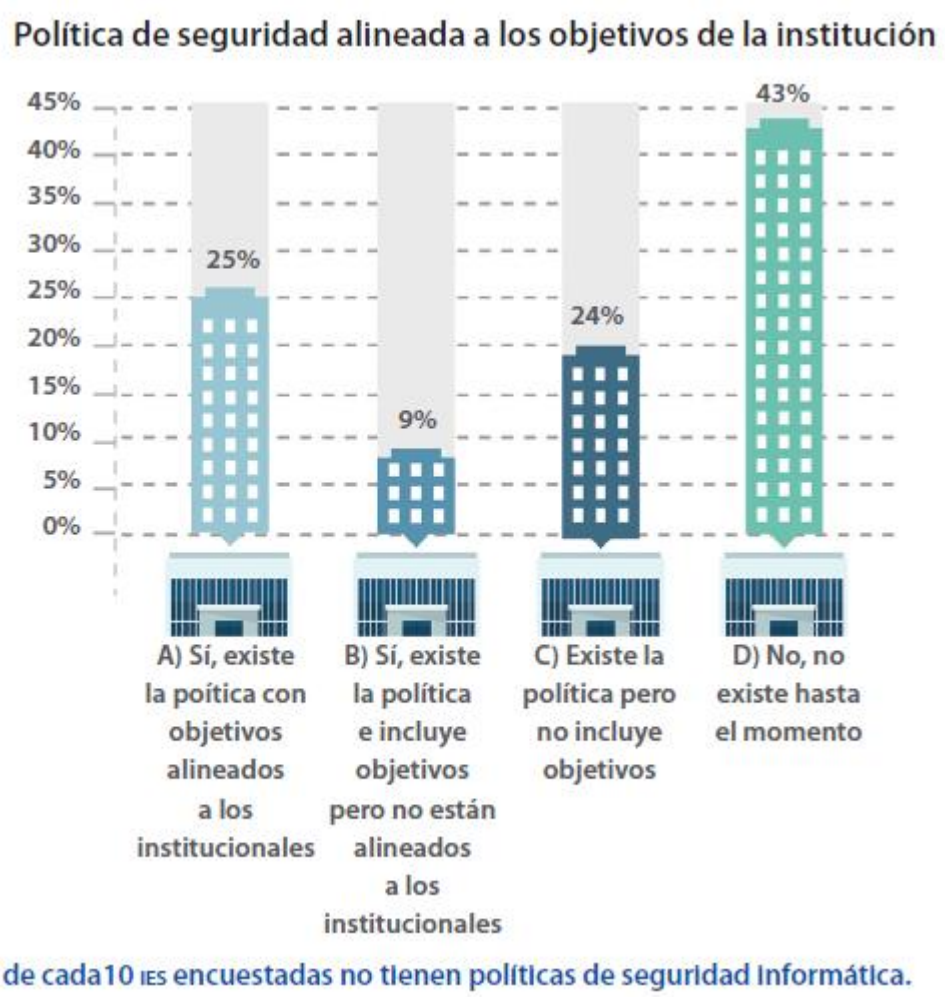
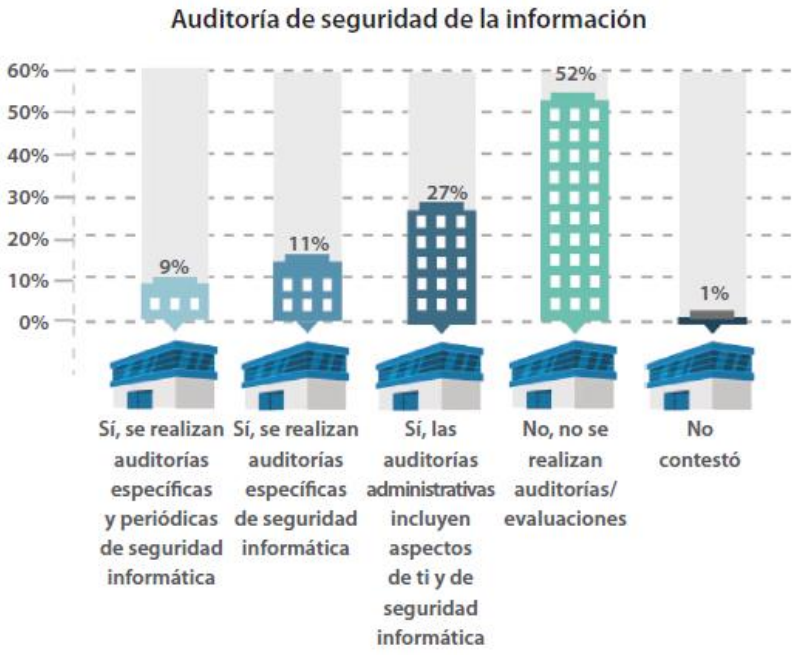


Ilustración 1. Uso de Políticas de Seguridad en IES según ANUIES

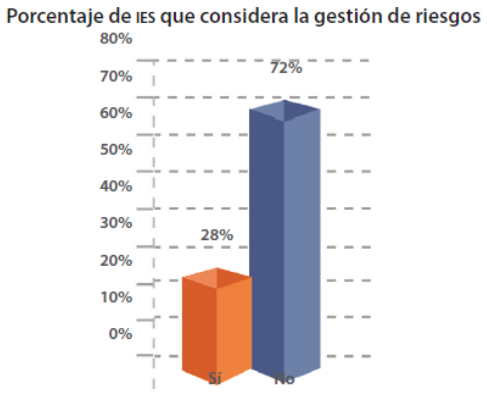
Así mismo, el indicador de Auditoría de Seguridad en las Universidades participantes, que hace referencia a las auditorías de seguridad informática, las cuales permiten la revisión de la implementación de la infraestructura de seguridad de la información y permiten identificar las áreas de oportunidad para reconocer las amenazas a las que se encuentra expuesta la institución, obtuvo los resultados mostrados en la Ilustración 2.0, en donde se exhiben las instituciones que siguen estas prácticas y las que no toman esta medida tan importante para la gestión de riesgos de los activos de información.



Nota: 5 de cada 10 IES encuestadas no realizan auditorías o evaluaciones de seguridad informática.

Ilustración 2. IES con auditoria de Seguridad según ANUIES

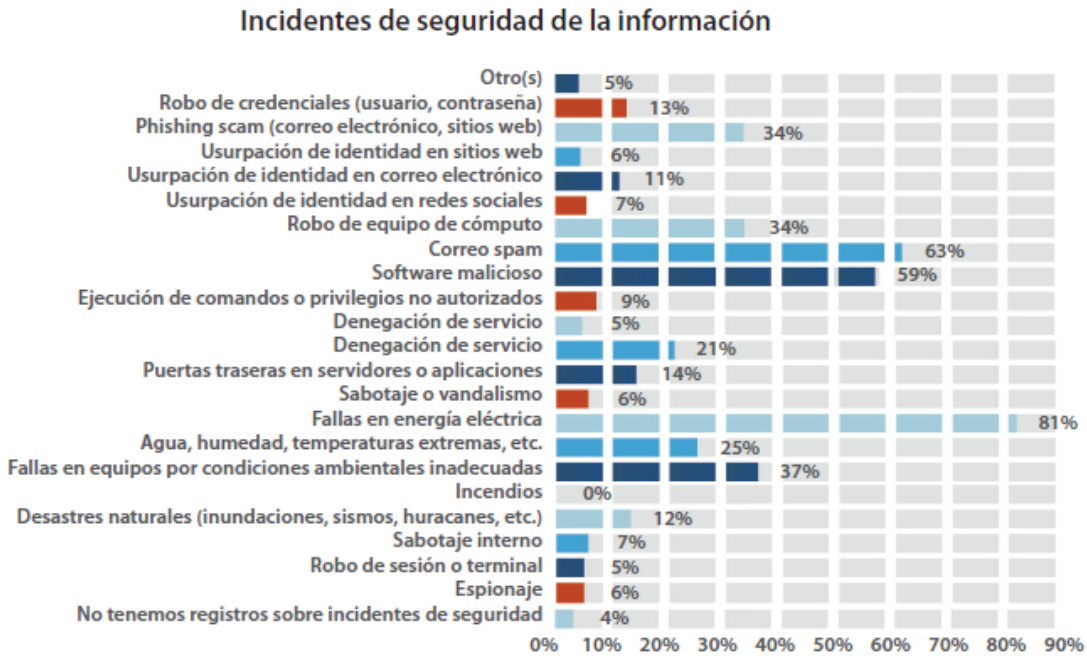
En cuanto al porcentaje de riesgos que hay en las Universidades estudiadas por ANUIES (2016), en la ilustración 3.0 se muestra un comportamiento bastante peculiar:



Nota: Casi 3 de cada 10 IES encuestadas consideran una o más metodologías o estándar de gestión de riesgos.

Ilustración 3. IES con Metodología de Gestión de Riesgos según la ANUIES.

Por último, en cuanto a los estudios realizados en el años 2016, los incidentes presentados en dichas Universidades, se constatan a través de la siguiente gráfica, donde se explica que las IES seleccionaron los ataques de seguridad informática a los que se han visto expuestas, siendo lo más frecuentes el correo *spam* (63%), *software* malicioso (59%), fallas de energía eléctrica (81%); también se observa que se presentan en las IES ataques informáticos como *Phishing scam* (34%), robo de equipo de cómputo (34%) y fallas de equipo por condiciones ambientales inadecuadas (37%). Esto se muestra en la Ilustración 4.0.



Nota: Los incidentes de seguridad que más reportan las IES son el correo *spam*, el *software* malicioso y las fallas de energía eléctrica.

Ilustración 4. Incidentes sobre Seguridad de la Información ocurridos en la IES según ANUIES

Fue hasta el año 2017, donde empezó a aparecer la Universidad Autónoma de Zacatecas en los informes de ANUIES-TIC, en donde, la Universidad reportó algunas cuestiones estadísticas respecto a las herramientas de seguridad de la información que utiliza, el presupuesto que deriva a las acciones para mitigar riesgos, los principales riesgos que encuentra, etc. Aunque el hecho de que la Universidad aparezca en este reporte es un gran avance, todavía hay mucho que trabajar para mitigar riesgos, empezando por la implementación y creación de

políticas de seguridad a nivel administrativo y en cada una de las Unidades Académicas; esto, como ya se mencionó con anterioridad, está ligado totalmente al factor humano.

Un estudio más reciente, realizado por el mismo ANUIES (2019), muestra datos muy interesantes, en donde las Universidades, durante los años que han ido transcurriendo, se han preocupado por implementar medidas de seguridad de la información, incluyendo, claro está, a la Universidad Autónoma de Zacatecas. Los resultados en los mismos indicadores, varían con significatividad. Este studio se realizó en un universo de las 195 instituciones de educación superior asociadas en 2019, que forman parte de la Asociación Nacional de Universidades e Instituciones de Educación Superior en México (ANUIES). ANUIES (2019), hace una comparación muy relevante, partiendo del año 2017; informa que la Política de seguridad que incluye objetivos alineados a los institucionales presenta un decremento en la tendencia entre las IES, a alinear sus políticas de seguridad con los objetivos de la institución. Además, a pesar de que hubo un decremento en algunos incidentes de seguridad de la información que se han presentado, a diferencia del año pasado, se han registrado también aumentos en los incidentes de seguridad, como: Robo de credenciales, phishing, usurpación de identidad en correo electrónico, correo electrónico spam, sabotaje o vandalismo, fallas por condiciones ambientales. Lo anterior, se expresa visualmente en las ilustraciones 5.0 y 6.0.

		2017	2018	2019	Variación
5.2 IES que tienen definida una política de seguridad que incluye objetivos alineados a los institucionales	No	58%	52%	56%	4%
	Sí	41%	48%	40%	-8%
	No contestó	2%	0%	2%	2%

Ilustración 5. Comparación por año (2017-2019) de las IES que tienen una politica de Seguridad de la Información.

		2017	2018	2019	Variación
5.17. Incidentes de seguridad que se han presentado en los últimos 12 meses en las IES	Otro(s).	15%	8%	12%	4%
	Robo de credenciales	26%	24%	31%	7%
	Phishing Scam	49%	45%	47%	2%
	Usurpación de identidad en sitios web	14%	13%	12%	-1%
	Usurpación de identidad en correo electrónico	22%	22%	27%	5%
	Usurpación de identidad en redes sociales	19%	17%	12%	-5%
	Robo de equipo de cómputo	58%	50%	47%	-3%
	Correo Spam	77%	74%	75%	1%
	Software malicioso	81%	77%	61%	-16%
	Ejecución de comandos o privilegios no autorizados	12%	15%	12%	-3%
	Denegación de servicio	25%	24%	22%	-2%
	Puertas traseras en servidores o aplicaciones	15%	14%	11%	-3%
	Sabotaje o vandalismo	14%	15%	16%	1%
	Fallas en energía eléctrica	83%	80%	80%	0%
	Agua, humedad, temperaturas extremas, etc.	43%	40%	42%	2%
	Fallas en equipos por condiciones ambientales inadecuadas	38%	35%	36%	1%
	Incendios	4%	2%	1%	-1%
	Desastres naturales (inundaciones, sismos, huracanes, etc.)	13%	19%	12%	-7%
	Sabotaje interno	5%	6%	4%	-2%
	Robo de sesión o terminal	5%	2%	5%	3%
	espionaje	5%	4%	4%	0%
	No tenemos registros sobre incidentes de seguridad	20%	17%	25%	8%

Ilustración 6. Comparación por año (2017-2019) de los incidentes de seguridad de la información que presentan las IES.

Tal como se muestra en la ilustración 5.0, la implementación de Políticas de Seguridad en las Universidades ha variado significativamente. Sin embargo, es importante poner énfasis que, en la Universidad Autónoma de Zacatecas, a pesar de que se ha buscado implementar normas y políticas, aún no se ha podido del todo, y mucho menos, en cada Unidad Académica. Así mismo, tal como lo muestra la ilustración 6.0, es importante poner atención en los diversos ataques y riesgos que

tienen la universidades e instituciones educativas; a través de los análisis de riesgos que se pudieran llegar a realizar, se puede saber dónde se está parado para poder ejercer acciones que mitiguen estos riesgos. Claro está, que una de estas acciones se puede orientar a la implementación de Políticas de Seguridad de la información en muchos de los casos, específicamente en aquellos casos que tengan que ver con el manejo de información por parte de los administrativos de alguna Unidad Académica o institución educativa en general. Para poder realizar estas dos últimas medidas que son esenciales para las instituciones educativas, se tiene que evocar a las investigaciones documentales específicamente del objeto de estudio, tal como se muestra en la sección siguiente.

2.1.7. Descripción breve de la Unidad Académica de Psicología de la Universidad Autónoma de Zacatecas.

Se han realizado diversas investigaciones documentales en donde se ha ido recopilando la información más relevante de la Universidad Autónoma de Zacatecas, específicamente en la Unidad Académica de Psicología. Según la información que otorga la Página Oficial de la Unidad Académica de Psicología de la UAZ (s.f.), ésta, dentro de su organigrama, se compone, en primera instancia, de un órgano colegiado correspondiente al H. Consejo de Unidad. De aquí se empiezan a desprender puestos administrativos que son de suma importancia para la institución educativa. Esta Unidad, dentro de su estructura interna, cuenta con un director, un/a coordinador/a administrativo, un/a coordinador/a de docencia, un/a coordinador/a de vinculación y extensión, un/a coordinador/a de investigación y posgrado, un/a responsable de Programa de la Licenciatura Campus Zacatecas, un/a responsable de la Maestría en Psicología Aplicada, un/a responsable de programa de la Maestría en Psicología Infantil, un/a responsable de programa de la Maestría en Estudios Psicoanalíticos, un/a responsable de Programa de la Especialidad en Psicología Organizacional. Cada uno de estos responsables y directores, tienen a su cargo uno o varios departamentos, y a su vez, están a cargo de más personas, conformando así un equipo administrativo de 49 trabajadores en total, dentro del Campus Zacatecas; cada uno de estas personas maneja activos de

la información, mismos que están expuestos a cualquier amenaza o riesgo de la Seguridad de la Información. El organigrama de toda la Unidad Académica de Psicología se muestra en la Figura 7.0. Cabe aclarar que, tal como se mencionó con anterioridad, dentro de la UAZ, existen más Unidades con características similares en sus organigramas.

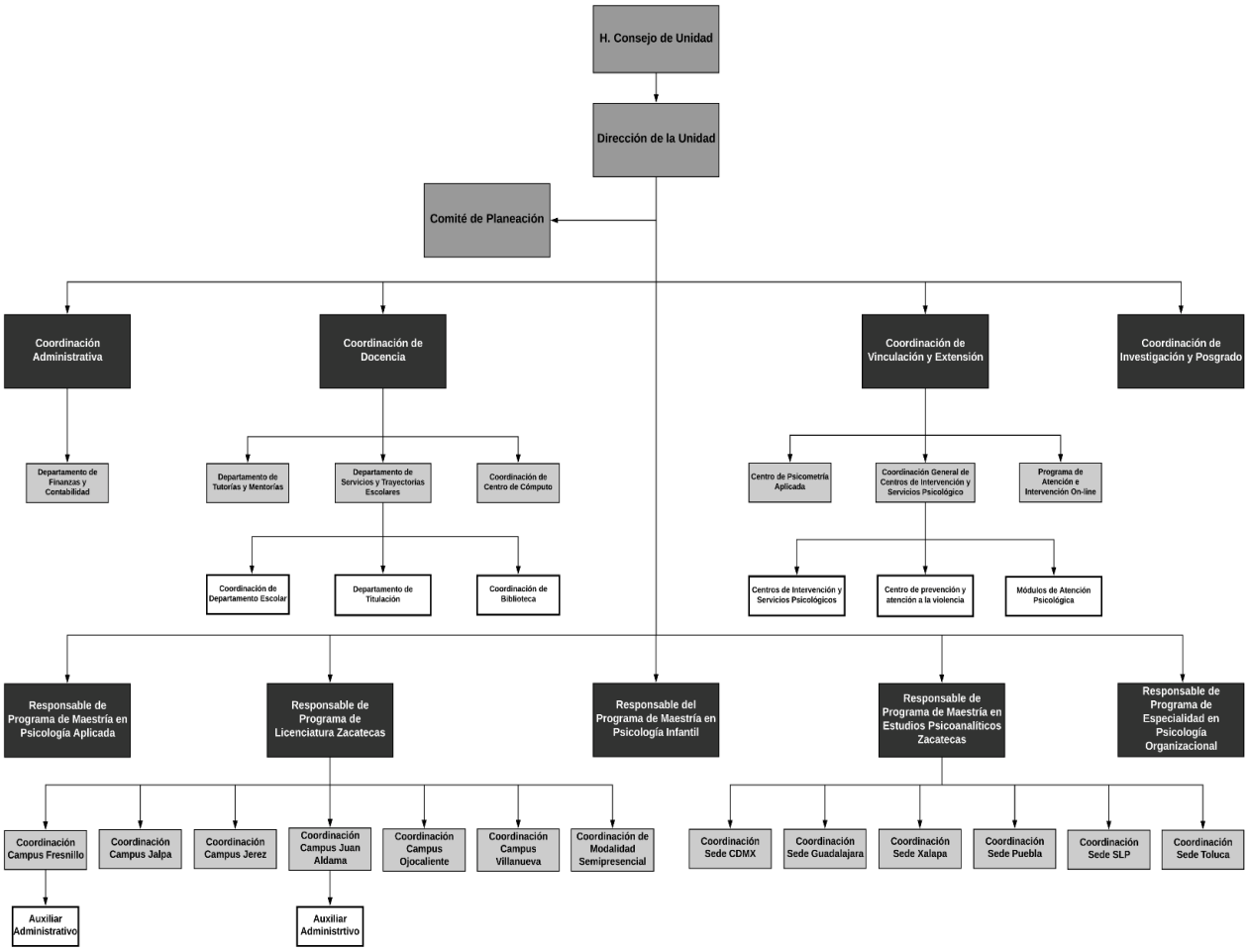


Ilustración 7. Organigrama General de la Unidad Académica de Psicología de la Universidad Autónoma de Zacatecas

Así mismo, la Unidad Académica de Psicología sede Zacatecas, cuenta con cuenta con 1403 alumnos y 138 profesores (Distribuidos en dos turnos), lo que sugiere también que cada uno de éstos, en conjunto con los administrativos, hacen uso de algunos activos de la información ubicados en la Administración central de esta Unidad Académica.

2.1.7.1. Principales Activos de la Información documentados en la Administración central de la Unidad Académica de Psicología

Según los últimos datos de la Coordinación de Infraestructura de la UAZ (2012-2017), la Unidad Académica de Psicología cuenta con diversos activos que se utilizan en oficinas, departamentos, aulas, y que inclusive, forman parte de la infraestructura general de la Unidad. Sin embargo, dentro de éstos, hay activos que son sumamente relevantes dentro de la Administración central, y que son, específicamente, activos de la información. Retomando la definición de un activo de información, el cual se mencionó con anterioridad, los principales activos de información documentados y que sirven para realizar un análisis de riesgos de la seguridad de la información son los que se muestran en las siguientes tablas.

Tabla 1. Activos de la Información registrados en el área del Almacén Administrativo

Activo de la Información	Descripción/Observaciones	Cantidad
Switch de Red	Para 8 puertos de Red. ENCORE	1

Tabla 2. Activos de la Información dentro de los Cubículos Administrativos

Activo de la Información	Descripción/Observaciones	Cantidad
Switch de Red	Para 8 puertos de Red. ENCORE	1
CPU con monitor integrado	Color negro, marca HP	16
CPU	Ensamblados marca HP	8
Laptop	Color negro Sony, ASUS	4
Cámara Digital	Canon	2
Impresora Lasser	JET, printer	3
Archivero	Metal, contiene diversos documentos.	4

Tabla 3. Activos de la Información dentro del Departamento Escolar

Activo de la Información	Descripción/Observaciones	Cantidad
Impresora	Ensamblada, EPSON	3
Impresora Lasser	JET PHP	2
CPU	Ensamblados marca HP	5

Tabla 4. Activos de la Información dentro de la Dirección

Activo de la Información	Descripción/Observaciones	Cantidad
Tableta digitalizadora	IPAD, motorola	1
CPU con monitor integrado	Color negro, HP.	1
CPU	Color negro, HP	1
Disco Duro	ADATA 500 GB	1
Impresora Multifuncional	Brother, color negro	3
IPAD	Apple	2
Cámara Digital	Samsumng, Color negro	1
Laptop	HP, color negro, 500 GB – DELL	2

Tabla 5. Activos de la Información dentro de la Recepción Administrativa

Activo de la Información	Descripción/Observaciones	Cantidad
Archivero	Color negro metálico. Contiene documentos diversos	5
CPU	Color negro Ensamblada, HP – JET	3
CPU con monitor integrado	Color negro	1
Impresora	HP	1
Impresora lasser	Lasser Jet 1022, JET	2

Tabla 6. Activos de la Información dentro de la Sala de Maestros

Activo de la Información	Descripción/Observaciones	Cantidad
Laptop	HP Probook 440 Color gris	1
Disco Duro	HITACHI 2TBG	1
Impresora Multifuncional	HP Color negro	1
Impresora	HP	1
Teléfono	Motorola inalámbrico	1

Tabla 7. Activos de la Información dentro de la Secretaria Académica

Activo de la Información	Descripción/Observaciones	Cantidad
Impresora multifuncional	Canon	1
Archivero	Color negro metálico. Contiene documentos diversos	6
CPU	HP	5
Videocámara	De 80 GB color gris	1
Teléfono	Panasonic inalámbrico	1
Impresora	Color negro, Samsung	2

Tabla 8. Activos de la Información dentro del Centro de Fotocopiado

Activo de la Información	Descripción/Observaciones	Cantidad
Tablet Digitalizadora	Color negro s/m	6
Microcomputadora portátil	Negras	8
CPU	HP – Ensamblado color negro	2
Archivero	Color negro metálico. Contiene documentos diversos	2

Tabla 9. Activos de la Información dentro del Área de Red

Activo de la Información	Descripción/Observaciones	Cantidad
Central telefónica	Conmutador	1
Switch para red	CISCO System	4

Tabla 10. Activos de la Información dentro de la Caja Administrativa

Activo de la Información	Descripción/Observaciones	Cantidad
CPU	ALASKA	1
Impresora Multifuncional	Xerox	2
Archivero	Color negro metálico. Contiene documentos diversos	1

Tabla 11. Activos de la Información dentro del Departamento de Contabilidad

Activo de la Información	Descripción/Observaciones	Cantidad
CPU	Ensamblada JET, Actkeck	2
Impresora Lasser	JET	2
Archivero	Color negro metálico. Contiene documentos diversos	1

Tabla 12. Activos de la Información dentro del Departamento de Responsable de Programa

Activo de la Información	Descripción/Observaciones	Cantidad
CPU	Ensamblada JET, Actkeck	1
Impresora Lasser	JET	1
Archivero	Color negro metálico. Contiene documentos diversos	2

Tabla 13. Activos de la Información dentro del Área de Posgrados

Activo de la Información	Descripción/Observaciones	Cantidad
CPU	Ensamblada JET, Actkeck	1
Impresora Lasser	JET	1
Archivero	Color negro metálico. Contiene documentos diversos	2

Tabla 14. Activos de la Información dentro del Departamento de Extensión y Vinculación.

Activo de la Información	Descripción/Observaciones	Cantidad
Laptop	Color negro	2
CPU	HP	2
Archivero	Color negro metálico. Contiene documentos diversos	2
Switch de red	Con 8 puertos de red	1

Tabla 15. Activos de la Información dentro del Departamento de Extensión y Vinculación.

Activo de la Información	Descripción/Observaciones	Cantidad
Laptop	Color negro	2
CPU	HP	2
Archivero	Color negro metálico. Contiene documentos diversos	2
Switch de red	Con 8 puertos de red	1

Esta información está documentado a través de diferentes documentos que se han recabado a lo largo de diversos procesos de conteo, investigación documental y entrevistas con los coordinadores de diversos departamentos y directores de dicha Unidad Académica.

2.1.8. Percepción de la Seguridad de la Información en trabajadores administrativos de la Unidad Académica de Psicología de la UAZ

Uno de los trabajos que se vuelven relevantes para entender un poco más el contexto de la presente investigación, es aquella alusiva a la percepción existente respecto a la Seguridad de la Información en los administrativos de la Unidad Académica de Psicología. Esto con la finalidad de poder reforzar la génesis de la presente investigación alusiva al análisis de riesgos.

Así pues, en esta investigación realizada por Moreno Zamudio et al. (2018), se buscó saber la percepción acerca de la Seguridad de la Información en trabajadores administrativo de la Licenciatura en Psicología de la Universidad Autónoma de Zacatecas. El desarrollo del mismo se llevó a cabo en tres fases: la primera consistió en una investigación documental; donde se recaudaron los datos generales de la Universidad y del Programa Psicología, la segunda en una investigación de campo; donde se aplicó el cuestionario para saber la percepción que se tiene acerca de los aspectos genéricos relacionados con la Seguridad de la Información en trabajadores administrativos del Programa Psicología de la UAZ, y la tercera la conformó la clasificación e interpretación de los datos que se obtuvieron a través del cuestionario aplicado y propuesto.

En esta investigación, la información a la que se tuvo acceso se consiguió a través de entrevistas, visitas a los responsables de ambos Programas y consultas a los sitios oficiales de la Universidad. El objeto de estudio, según los autores antes mencionados, fueron los trabajadores administrativos de la Licenciatura en Psicología de la Universidad Autónoma de Zacatecas.

Reseña de las dificultades de la Aplicación

Dentro de esta investigación se presentaron algunas dificultades, tales como que no fue posible aplicarles la encuesta a todos los administrativos de la Unidad Académica en mención, ya que algunos no estaban en la disposición de contestar, no se encontraron, o bien, los turnos diferían al momento de la aplicación y pilotaje. Sin embargo, se le aplicó a la mayoría de los trabajadores, mostrando en éstos un interés notorio y disposición al contestar.

Propuesta de indicadores para la percepción de la Seguridad de la Información.

El hablar del concepto de percepción se puede tornar un tanto complejo ya que se puede abordar desde una perspectiva psicológica, cognitiva o inclusive política. Pero, una definición genérica aplicada al contexto de la presente investigación, es la que da Vargas (1994), quien afirma que la percepción debe ser entendida como relativa a la situación histórico-social pues tiene ubicación espacial y temporal, depende de las circunstancias cambiantes y de la adquisición de experiencias novedosas que incorporen otros elementos a las estructuras perceptuales previas, modificándolas y adecuándolas a las condiciones.

Tal como se afirmó con anterioridad, el hablar de Seguridad de la Información abarca demasiados ejes que se miden de diferentes formas. En la presente investigación respecto a la percepción, partiendo de la definición anteriormente expuesta, se proponen tres indicadores relacionados con la temática central aquí tratada, tomando en cuenta que el sujeto de estudio tiene que, por naturaleza, manejar y administrar información en sus estaciones de trabajo, y que estos

indicadores marcarán la pauta para generar acciones futuras. Tales indicadores se definen en la Tabla 16.

Una vez aplicado el cuestionario al objeto de estudio descrito con anterioridad, se obtuvieron los siguientes resultados en cada indicador propuesto; cada uno de los indicadores responde a preguntas específicas relacionadas con la definición de cada uno de éstos. A continuación, se muestran algunas de las preguntas respondidas por cada indicador, brindando un panorama aproximado de la percepción que se tiene en ambos Programas de la UAZ.

Tabla 16. Propuesta de indicadores acerca de la Seguridad de la Información en trabajadores administrativos de los Programas de Ingeniería en Computación y Psicología de la Universidad Autónoma de Zacatecas

#	Indicador	Definición del Indicador
1	Percepción acerca de la importancia del manejo de datos e información institucional y de conocer acerca de la Seguridad de la Información.	Partiendo del hecho de que la información es el eje neurálgico de toda institución educativa, es necesario saber la percepción que se tiene por parte de los administradores acerca de la importancia en el manejo de datos, incluyendo la valoración que éstos le dan a la información, los conocimientos que tienen sobre la protección de datos, etc.
2	Percepción acerca del involucramiento de la institución y sus autoridades en temas de Seguridad de la Información	La Seguridad de la Información es un acto multidisciplinario y que involucra a todos los actores de una organización. El saber la percepción que tienen los administrativos acerca del involucramiento que tienen las autoridades e institución en general acerca de la seguridad de la información es sumamente importante para poder ejercer medidas desde un orden jerárquico. Este indicador abarca el saber a quién dirigirse, las acciones que se han tomados para prevención, etc.
3	Percepción acerca de la importancia de implementar de Buenas prácticas relacionadas con la seguridad de la Información	Otro aspecto sumamente importante de la Seguridad de la información son las buenas prácticas que se tienen de ésta. El saber la percepción en los administrativos que se tiene acerca de tomar acciones de prevención o no, marcará la pauta para implementar acciones de concientización en un futuro. Este indicador abarca todo lo que tiene que ver con la importancia de implementar medidas dentro de la estación de trabajo, como actualización de dispositivos, software, etc.

2.1.8.1. Percepción acerca de la importancia del manejo de datos e información institucional y de conocer acerca de la Seguridad de la Información.

Para poder entender la situación en la que se encuentra la Unidad Académica de Psicología y poder saber las percepciones más relevantes para este estudio, se analizaron los siguientes cuestionamientos, dando como resultado que, dentro del indicador alusivo a la importancia del manejo de datos e información institución y conocimiento acerca de la seguridad de la información, específicamente de lo que corresponde a la percepción del conocimiento del concepto de Seguridad de la Información, tal como se observa en la Ilustración 8, se obtuvo que en el Programa de Psicología un 58% sí lo conoce, mientras que un 42% no lo conoce. Así mismo, en esta investigación se pone de manifiesto la importancia del manejo de información que tiene el personal administrativo dentro de la institución. En la figura 9, se observa que la mayoría de los trabajadores consideran que la información que ellos manipulan o manejan tiene un valor alto de importancia, lo que sugiere que se debe poner atención en todos los activos que este personal administrativo maneja.

Pregunta: ¿Considera usted que conoce el concepto de Seguridad de la Información?

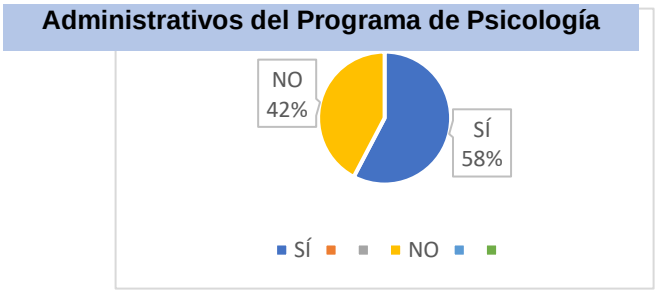


Ilustración 8. Percepción acerca del conocer el concepto Seguridad de la Información (Psicología)

Pregunta: Del 1 al 10, tomando al 10 como el valor de mayor importancia, y el uno como de menor, ¿Qué valor le daría a la información que maneja en su estación de trabajo?

Ilustración 9. Percepción acerca de la importancia de la información institucional (Psicología)

2.1.8.2. Percepción acerca del involucramiento de la institución y sus autoridades en temas de Seguridad de la Información.

Dentro de este indicador se puede observar en cuanto a los dos cuestionamientos observador en las Ilustración 10 y 11, que dentro de la Unidad Académica de Psicología no hay una percepción favorable referente a la protección de datos dentro de la institución, ya que 16 de 26 encuestados perciben que no hay una protección adecuada de los datos, mientras que el resto percibe que hay una protección medianamente adecuada, pero nunca hubo una percepción de una adecuada protección por completo. Para el caso del cuestionamiento que hace alusión a la frecuencia de implementación de capacitación y campañas de prevención sobre temas de la Seguridad de la Información se obtuvieron los siguientes resultados: En el caso del Programa de Psicología el 73% respondió que nunca han realizado este tipo de campañas, el 15% respondió que cada cambio de administración se hacía y el 12% respondió que cada año.

Pregunta: Del 1 al 5, considerando el 5 el valor más adecuado, y el 1 el menos adecuado. ¿Considera usted que su institución protege adecuadamente los datos e información que se manejan dentro de ésta?

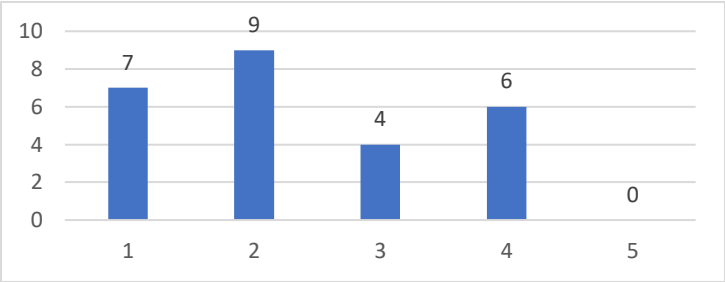


Ilustración 10. Percepción acerca de la Institución en cuanto a la protección de sus datos e información (Psicología)

Pregunta: ¿Con qué frecuencia se realizan campañas de prevención/difusión de buenas prácticas de Seguridad de la Información dentro de su área de trabajo?

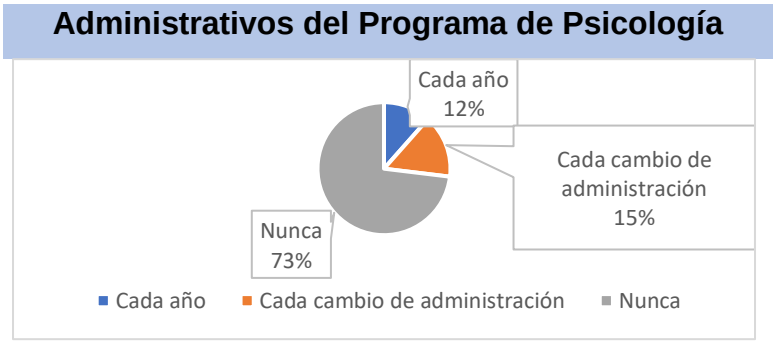


Ilustración 11. Percepción acerca de capacitación institucional sobre temas de Seguridad de la Información (Psicología)

2.1.8.3. Percepción acerca de la importancia de implementar de Buenas prácticas relacionadas con la seguridad de la Información

En el caso de este indicador, específicamente para los cuestionamientos de percepción acerca de la importancia de contar con Políticas de Seguridad y la Percepción de la importancia de estar capacitado en temas de Seguridad de la Información se obtuvieron los siguientes resultados, mismos que se visualizan en la Ilustración 12 y 13 respectivamente. Para la primera pregunta, en el Programa de Psicología se percibe con un 50% demasiado importante implementar y contar con Políticas de Seguridad de la Información, en seguida un 27% de los administrativos toman una importancia latente y el 23% considerablemente importante. Para el segundo cuestionamiento se obtuvieron los siguientes resultados: Un 54% de los administrativos considera importante estar capacitado en temas de Seguridad de la Información, mientras que un 19% lo toma como importante, un 19% como

considerablemente importante y un 8% no lo considera nada importante. Haciendo un análisis rápido, en el indicador del involucramiento institucional salieron porcentajes bajo de implementación de campañas de concientización y capacitación, siendo que los administradores en este indicador de buenas prácticas si lo consideran importante; este hecho marca la pauta para tomar acciones futuras dentro de las instituciones de la UAZ para tomar más importancia en la concientización de temas alusivos a la Seguridad de la Información.

Pregunta: ¿Qué tan importante considera usted el tener Políticas de Seguridad de la Información dentro de su institución de trabajo?

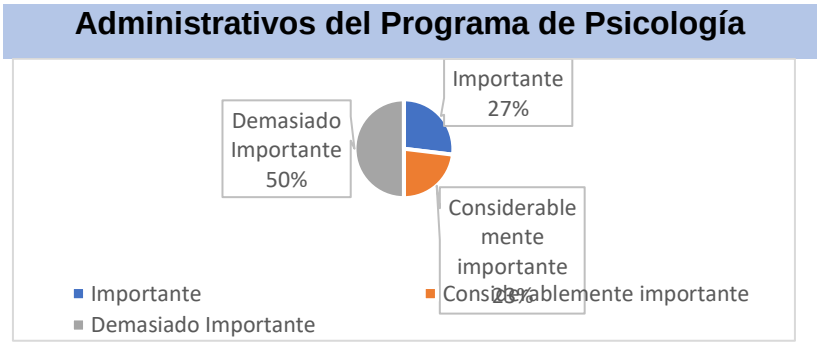


Ilustración 12. Percepción acerca de la importancia de contar con Políticas de Seguridad de la Información (Psicología)

Pregunta: ¿Qué tan importante es para usted estar capacitado y tener conocimiento sobre medidas de seguridad de la información dentro de su institución de trabajo?

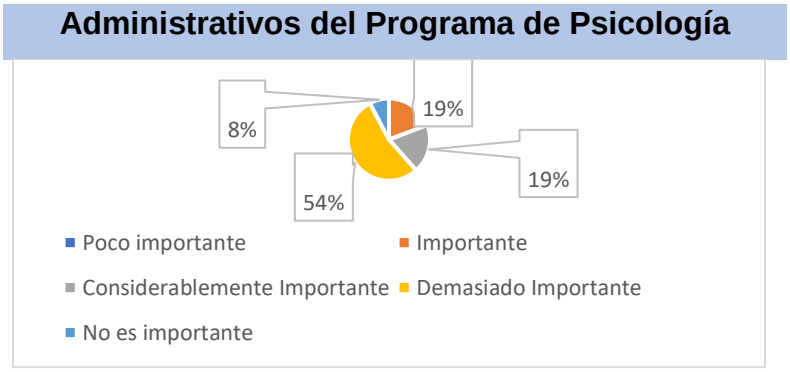


Ilustración 13. Percepción acerca de la importancia de estar capacitado en temas de Seguridad de la Información (Psicología)

A partir de esta investigación relacionado a la Percepción de la Seguridad de la Información en Personal Administrativo, también se puede observar y analizar la pertinencia y relevancia de la implementación de Políticas de Seguridad de la Información en esta Unidad. Es este tenor, el tener un panorama general de la percepción que tienen los administrativos dentro de una institución marcará la pauta importante para implementar acciones que ayuden a coadyuvar el uso de buenas prácticas e incrementar la Seguridad de la Información dentro de la Universidad Autónoma de Zacatecas. Tal como se pudo observar, en las Universidades públicas, específicamente dentro de las Unidades Académicas de la Universidad Autónoma de Zacatecas, hace falta implementar campañas de concientización y capacitación a su personal específicamente para temas relacionados con la Seguridad de la Información. Aunque los administrativos consideren importante el implementar Políticas de Seguridad de la Información y el estar informado acerca de aspectos que tienen que ver con delitos cibernéticos, protección de datos, entre otros, si no hay una coordinación jerárquica institucional difícilmente se pueden implementar acciones que mitiguen diversos riesgos. Tal como ya se ha comentado con anterioridad, la Seguridad de la Información es un aspecto que incluye diversos procesos, personas, entes y actores para poder llevarla a cabo adecuadamente; es necesario el involucramiento tanto de trabajadores, autoridades, docentes y alumnos de una universidad pública para poder conservar adecuadamente los tres pilares de la Seguridad de la Información a los cuales ya se hizo alusión dentro de este trabajo investigativo.

Así mismo, se pudieron apreciar otros cuestionamientos acerca de la percepción de la Seguridad de la Información, tal como la importancia que se percibe acerca de mantener actualizados los dispositivos o la creencia de haber sido víctima de ataques cibernéticos o Ingeniería Social, dando como resultados datos interesantes que señalan claramente el inicio para poder llevar a cabo planes que incrementen el uso de buenas prácticas y la implementación y seguimiento de Políticas relacionadas con la seguridad de la información, protección de datos y mitigación de riesgos.

2.2. BASES TEÓRICAS

La seguridad de la Información es un concepto muy amplio, en el cual se incluyen diversos factores que se han analizado a través del eje histórico y evolutivo del propio concepto. En este tenor, es de suma importancia abordar los conceptos claves que subyacen del término, abordándolo desde a un contexto teórico y práctico.

2.2.1. La Seguridad de la Información: Un breve recorrido teórico a los conceptos clave

El eje histórico y evolutivo de la humanidad, se ha regido siempre a través de la información. Desde las primeras civilizaciones, las sociedades y comunidades, buscaban transmitir su cultura a través de pinturas, monumentos, construcciones, etc. Desde estas primeras etapas, la Seguridad de la Información ya iba tomando presencia; por ejemplo, algunas pinturas rupestres, o artes abstractas, sólo tenían acceso a ciertas personas de la civilización, de tal forma que éstas eran un secreto vital e importante que regía a las comunidades de aquellas épocas.

Tal como lo afirma Borghello (2012), los descubrimientos arqueológicos marcan, sin duda, las más importantes pruebas de seguridad de los antiguos: las pirámides egipcias, el palacio de Sargón, el templo Karmak en el valle Nilo, el dios egipcio Anubi representado con una llave en su mano, etc. Así pues, podemos ver que, desde el eje evolutivo del hombre, la Seguridad de la Información ha sido de suma importancia.

Si nos situamos en un contexto actual, la Información es el activo más importante de cualquier organización; la información de toda empresa o institución, puede marcar la pauta para poder emprender nuevas ideas, mantener algún nivel o equilibrio, o simplemente para su buen funcionamiento. Actualmente, la información no sólo se concentra en datos físicos (documentos, archivos, papelería, etc.), sino que también, intervienen los datos digitales, en donde el uso adecuado de la tecnología es de suma importancia para poder conservar de manera adecuada la información de cualquier institución.

En esta lógica, la Seguridad de la Información implica proteger la información de riesgos que puedan afectarla, en sus diferentes formas y estados. Esto quiere decir entonces, que toma en cuenta a la tecnología, a las personas y a los procesos mediante sus principios más básicos: Confidencialidad, Integridad y Disponibilidad.

2.2.1.1. Confidencialidad

Dentro de toda institución u organización, muchos de los datos e información no son de acceso público. Así pues, para que la información esté segura, y sea tratada de una manera adecuada y sin riesgos, solamente las personas con autorización pueden conocer el contenido de ésta. Según la definición que nos da el Instituto Nacional de Ciberseguridad (INCIBE) de España, y reafirmando lo anteriormente descrito, la confidencialidad implica que la información es accesible únicamente por el personal autorizado. Es lo que se conoce como need-to-know. Con este término se hace referencia a que la información solo debe ponerse en conocimiento de las personas, entidades o sistemas autorizados para su acceso.

Un claro ejemplo de información que requieren confidencialidad son aquellos sistemas o accesos que necesitan alguna contraseña, los datos personales de los alumnos de las universidades, o bien, las nóminas de éstas. Si alguna de esta información sensible queda al acceso público, pueden hacer mal uso de ésta, y traería grandes consecuencias para cualquier institución.

2.2.1.2. Integridad

Al hablar de integridad de la información, se hace alusión a mantener la información sin alteraciones, y, por ende, mantener su valor original de cualquier índole. En esta lógica, cualquiera que tenga acceso a esta información, debe tener la certeza de que al consultarla contendrá los valores originales y que no ha sido alterada de alguna forma que pueda vulnerar la funcionalidad institucional.

Según la Academia Americana de Seguridad Informática, la información se puede alterar de diversas formas:

- Alteración de contenido en los documentos: Se realizan inserciones o sustituciones de partes de su contenido.

- Alteración en los elementos que soportan la información: Se realizan
- alteraciones en la estructura física y lógica donde la información se encuentra almacenada, por ejemplo, en los equipos de cómputo y en los servidores.

Por las razones que se enlistan anteriormente, es de suma importancia mantener la integridad total de la información y los datos que manejan en cualquier institución educativa, para que todos los elementos que componen la base de gestión de la información se mantengan en sus condiciones originales definidas por sus responsables y propietarios.

2.2.1.3. Disponibilidad

La disponibilidad, tal como su misma nomenclatura lo dice, permite que la información pueda estar disponible cuando sea necesaria. Hace alusión al acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran. Según el Instituto Nacional de Ciberseguridad, la disponibilidad de la información se refiere a que la información esté accesible cuando la necesitemos. Algunos ejemplos de falta de disponibilidad de la información son: cuando nos es imposible acceder al correo electrónico corporativo debido a un error de configuración, o bien, cuando se sufre un ataque de denegación de servicio, en el que el sistema «cae» impidiendo accesos legítimos. Ambos tienen implicaciones serias para la seguridad de la información.

Para poder garantizar estos 3 ejes esenciales de nuestros datos y nuestra información, es necesario tomar algunas medidas importantes a través de Normas como lo son el ISO/IEC 27001, la cual, según Mantilla Guerra (2018), es una norma desarrollada como modelo para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI) para cualquier tipo de organización. Permite diseñar e implantar un SGSI, en base a las necesidades, objetivos, requisitos de seguridad, los procesos, los empleados, el tamaño, los sistemas de soporte y la estructura de la organización. Esta norma ha sido estructurada metodológicamente para adaptarse al modelo "Planificar, Hacer, Verificar, Actuar" (Plan Do Check Act).

El concepto de Seguridad de la Información como tal, si bien está vinculado con el de Seguridad Informática, no debe confundirse, ya que este último sólo se encarga de la seguridad en contextos informáticos, sin embargo, la información puede encontrarse manifiesta en diversas formas, y no sólo de manera virtual o informática (Mendoza et al., 2016). El ser humano en general, siempre y cuando esté concientizado, da un significado más trascendental a la seguridad de la Información, ya que de ésta puede formular diversas hipótesis, historias de vida y modelos económicos que le garantizarán su prevalencia y calidad de vida en los diferentes ejes de evolución.

La Seguridad de la Información ayuda a proteger a las organizaciones de los posibles ataques que vulneren la confidencialidad y el trato de la información dentro de ésta. Esta protección hace referencia a la implementación de planes de contingencia que previenen y/o disminuyen el impacto negativo en situaciones de desastres naturales, cambios climáticos, fallas de diferente índole en las infraestructuras, vandalismo, robo, Ingeniería Social o cualquier situación que vulnere la integridad de la Información dentro de una organización. Así pues, al referenciar este concepto, también es menester hacer alusión a todo lo que subyace de él, desde el uso de las tecnologías, hasta los ataques cibernéticos y a la seguridad en general que surgen de las malas prácticas para salvaguardar los activos de toda organización.

2.2.2. Uso de las Tecnologías de la Información en las organizaciones y su relación con la Seguridad de la Información

En la era actual, las Tecnologías de la Información y Comunicación (TIC) proporcionan diversas opciones que acortan distancias entre la comunicación y los procesos cotidianos, afectando así a los mercados, estilos de vida y a la configuración y concepción de las sociedades como tal.

Las organizaciones no son excepción en el impacto que las TIC han venido a traer en esta nueva era. Existe una relación bidireccional entre la organización y sus sistemas de información. La organización está abierta a los impactos de los

sistemas de información y estos deben estar alineados con los objetivos de la organización (Restrepo, 2005).

Es bien sabido que en esta era de la información en la que vivimos, inminentemente requerimos hacer uso de diversas tecnologías que tenemos al alcance para poder eficientizar los procesos cotidianos, y, sobre todo, organizacionales. Así pues, tal como afirma (Cano Pita, 2018) las TICs son esenciales para mejorar la productividad de las empresas, la calidad, el control y facilitar la comunicación, entre otros beneficios, aunque su aplicación debe llevarse a cabo de forma inteligente. El mero hecho de introducir tecnología en los procesos empresariales no es garantía de gozar de estas ventajas. Para que la implantación de nueva tecnología produzca efectos positivos, hay que cumplir varios requisitos; tener un conocimiento profundo de los procesos de la empresa, planificar detalladamente las necesidades de tecnología de la información e incorporar los sistemas tecnológicos paulatinamente, empezando por los más básicos. Así mismo, partiendo de esta afirmación tan relevante, es de suma importancia tener buenas prácticas de la Seguridad de la Información para poder explotar adecuadamente los activos de la empresa.

2.2.3. Seguridad de la información en las organizaciones

Medina Iriarte (2006), afirma que la Seguridad de la Información puede ser vista desde su rol estratégico en los procesos de negocio, al identificar con qué recursos (organización, procesos, tecnología), se debe contar para alcanzar la efectividad entre las actividades de resguardo o protección de los activos de información y la habilitación del acceso apropiado a los mismos. En este sentido, la Seguridad de la Información es un aspecto sumamente importante en la relación que se establece entre el negocio, sus clientes, socios, proveedores y empleados.

Por otro lado, Rivera Ledesma (s.f.), define a la Seguridad de la Información como la preservación de confidencialidad, integración y disponibilidad de la información; además, también puede involucrar otras propiedades como autenticidad, responsabilidad, no repudiación y confiabilidad. Aquí ya se observa una definición más holística, en donde se abordan los pilares básicos para conservar los activos de una organización intactos, además de que involucra más el proceso del ser

humano y las buenas prácticas que se pueden desarrollar a través de normas, políticas o estándares.

En este tenor, una de las definiciones que incluyen de manera acertada las buenas prácticas y algunos estándares de suma relevancia, es la que otorga el Committee on National Security Systems (CNSS), éste define la seguridad de la información (InfoSec) como la protección de la información y los sistemas de información contra personas no autorizadas, acceso, uso, divulgación, interrupción, modificación o destrucción para proporcionar confidencialidad, integridad y disponibilidad. (CNSS, 2010). Se han utilizado diferentes concepciones y guías para la implementación de controles de seguridad de la información, los cuales hacen alusión a estándares que enlistan o detectan las vulnerabilidades de los activos en las organizaciones. Podemos hacer referencia a los estándares y normas como la ISO 1779, ISO 27000 e ISO/IES 27000.

Tal como lo señala González Tabares (2018), la norma ISO 17799 es un código de buenas prácticas para la Gestión de la Seguridad de la Información, esta norma surge como evolución histórica de la norma británica BS 7799 y actualmente existen varias adaptaciones de la misma que convergerán en un futuro próximo a las normas de la serie ISO 27000. La ISO 17799 introduce un cambio importante en los sistemas de gestión de la seguridad de la información ya que los aborda desde un punto de vista de continuidad de negocio y de mejora continua. Esta norma hereda muchos conceptos de la serie de normas ISO 9000 y subraya la seguridad entendida como proceso. Así mismo, la norma ISO/IEC 27000 contiene las mejores prácticas recomendadas en seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de Seguridad de la Información (SGSI).

Si bien estos estándares y normas hablan del involucramiento que tiene el ser humano, no lo ponen en un eje prioritario ante las posibles vulnerabilidades de Seguridad de la Información. Es pertinente incluir técnicas que ofrecen contramedidas ante la Ingeniería Social, tales como como la concientización y entrenamiento, cambios de comportamiento, capacitación, y todo aquello que se vea relacionado con el Recurso Humano para conservar una Seguridad de la

Información de las organizaciones; claro ejemplo de estas técnicas, sin duda alguna, tienen que ver con la implementación de Políticas de Seguridad de la Información, mismas que le darán una noción pertinente a los usuarios de qué hacer en caso de alguna contingencia relacionada a los datos en riesgo de una institución.

Dicho todo lo anterior, podemos dilucidar que el enfoque conceptual o definición teórica/práctica que se le quiera tomar respecto a la seguridad de la información y todo lo que yace de ésta, pone de manifiesto que es una necesidad en toda empresa y organización, y que, por ende, se debe tomar en cuenta el hecho de que cualquier activo de información de toda organización puede sufrir ataques o amenazas explotando diversas vulnerabilidades; desde el factor infraestructural, hasta el factor más complejo, haciendo alusión al factor humano. Todas estas buenas prácticas también hacen alusión a la implementación de Sistemas de Gestión de Seguridad de la Información, en donde también se ven inmiscuidos procesos relacionados con la creación y gestión de Políticas de Seguridad de la Información.

2.2.4. Sistema de Gestión de Seguridad de la Información

Un Sistema de Gestión de la Seguridad de la Información (SGSI), según el ISO-27001, es una estrategia que ayuda a establecer políticas y procedimientos en relación a 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. Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

Así pues, según el ISO27001, la Gestión de la Seguridad de la Información, se basa en 4 niveles primordiales:

2.2.4.1. Nivel 1 de un SGSI

Manual de seguridad: Sería el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades,

políticas y directrices principales específicamente del Sistema de Seguridad de la Información que se querrá implementar en una empresa o una institución.

2.2.4.2. Nivel 2 de un SGSI

Procedimientos: documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

2.2.4.3. Nivel 3 de un SGSI

Instrucciones, checklists y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

2.2.4.4. Nivel 4 de un SGSI

Son los registros que se hacen a través de documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos. De manera específica, ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos (en cualquier formato o tipo de medio):

Alcance del SGSI: ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).

Política y objetivos de seguridad: documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Procedimientos y mecanismos de control que soportan al SGSI: aquellos procedimientos que regulan el propio funcionamiento del SGSI.

Enfoque de evaluación de riesgos: descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables.

Informe de evaluación de riesgos: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.

Plan de tratamiento de riesgos: documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.

Procedimientos documentados: todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.

Registros: documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.

Declaración de aplicabilidad: (SOA -Statement of Applicability-, en sus siglas inglesas); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

Tal como se mencionó con anterioridad, una parte prioritaria dentro de un Sistema de Gestión de Seguridad de la Información yace en dos partes:

1. Realizar un Análisis de Riesgos de los activos de la información que hay en una institución o empresa.
2. Crear las Políticas que garanticen unos buenos hábitos, y éstas se darán a partir del Análisis de Riesgos realizado.

2.2.5. Análisis de Riesgos de la Seguridad de la Información

Como ya se había mencionado con anterioridad, el proceso de gestión de riesgos involucra cuatro actividades cíclicas:

- La identificación de activos y los riesgos a los que están expuestos
- El análisis de los riesgos identificados para cada activo
- La selección e implantación de controles que reduzcan los riesgos
- El seguimiento, medición y mejora de las medidas implementadas

Así pues, a partir estos pasos es como se puede llegar a la creación de una Política de seguridad más acertada. En este sentido, el análisis de riesgo, según Erb (2010) especifica que el primer paso en la seguridad de la información es el análisis de riesgo que tiene como propósito determinar los componentes de un sistema que requieren protección, sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo. Parte fundamental de la gestión de Riesgos, es precisamente el análisis de Riesgos.

Tal como lo afirma el Laboratorio de Redes y Seguridad de la UNAM (2014), un análisis de riegos proporciona herramientas útiles para cuantificar el riesgo y evaluar si este análisis es adecuado y tomar medidas para reducirlo, además intenta mantener un balance económico entre el impacto de los riesgos y el costo de las soluciones de un programa efectivo de seguridad destinadas a manejarlos. Existen diversas metodologías para un análisis y gestión de riesgos de la seguridad de la información. Los tipos de activos que se definen, los listados, descripciones y priorizaciones dependerán de las necesidades específicas de la institución u organización donde se implementará. Sin embargo, el proceso global es en gran parte similar en todas las metodologías de análisis de riesgos de la seguridad de la

información. Las fases genéricas de un análisis de riesgos de seguridad se muestran en la Ilustración 14.

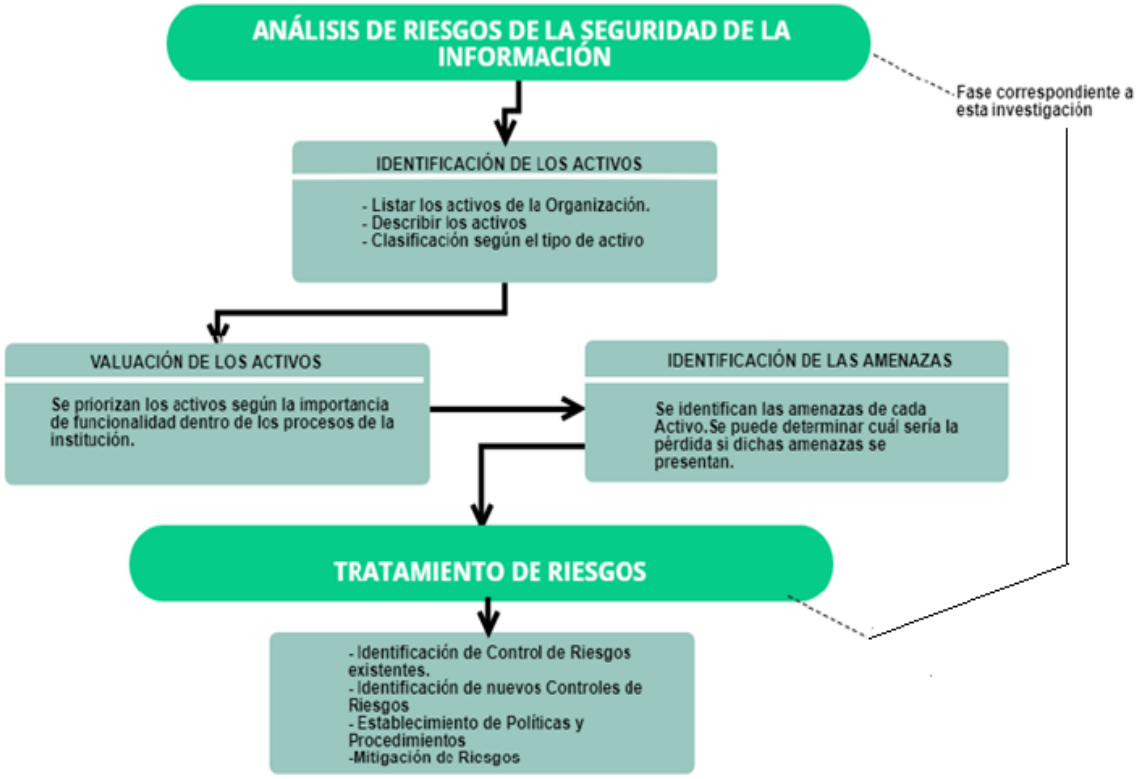


Ilustración 14. Proceso General de un Análisis de Riesgos de la Seguridad de la Información

Este proceso de análisis de riesgos está basado en identificar las amenazas que pueden ocurrir en determinado tiempo, espacio, y, sobre todo, activo de información de una institución, y que, por ende, puede afectar de manera directa o indirecta el funcionamiento esencial de ésta. Dentro De este proceso, se pueden utilizar herramientas muy interesantes, como lo es la matriz de riesgo. Una matriz de riesgo, tal como dice Erb (2011), sirve para analizar y determinar los riesgos en el manejo de los datos e información de una institución. La Matriz, puede dar una mirada aproximada y generalizada de los riesgos y amenazas de cada uno de los activos de información de la institución, y a través de ésta, se pueden tomar diferentes medidas pertinentes que tienen que ver con la mitigación de dichos riesgos.

El INCIBE, reafirmando lo anteriormente descrito, dimensiona que el análisis de riesgos permite valorar el coste de los posibles incidentes de seguridad que afecten

a la información y priorizar las medidas que se tomen para evitarlos. Este análisis de riesgos será necesario si se tratan datos de carácter personal pues es esencial para determinar las medidas técnicas y organizativas necesarias para proteger la privacidad. Así mismo, De Freitas (2010), afirma que con el análisis del riesgo se pretende identificar y calcular los riesgos basados en la identificación de los activos, en el cálculo de las amenazas y sus vulnerabilidades. Y es que, según la Academia Latinoamericana de Seguridad Informática, las amenazas son constantes y pueden ocurrir en cualquier momento. Esta relación de frecuencia-tiempo, se basa en el concepto de riesgo, lo cual representa la probabilidad de que una amenaza se concrete por medio de una vulnerabilidad o punto débil. Esta misma Academia sugiere una clasificación interesante, afirmando que estas mismas se podrán dividir en tres grandes grupos:

1. **Amenazas naturales:** condiciones de la naturaleza y la intemperie que podrán causar daños a los activos, tales como fuego, inundación, terremotos,
2. **Intencionales:** son amenazas deliberadas, fraudes, vandalismo, sabotajes, espionaje, invasiones y ataques, robos y hurtos de información, entre otras.
3. **Involuntarias**: son amenazas resultantes de acciones inconscientes de usuarios, por virus electrónicos, muchas veces causadas por la falta de conocimiento en el uso de los activos, tales como errores y accidentes.

Todas estas amenazas, se van detectando según sean las necesidades geográficas, físicas y organizacionales de la misma propia institución. Otra visión interesante respecto a la clasificación de la amenaza es la que nos da Flores Hines (2010), en donde podemos dimensionar las amenazas y riesgos de la siguiente manera:

Factores de riesgo por sucesos físicos: Aquí se pueden categorizar todos aquellos problemas relacionados con los problemas con el flujo de corriente, daños causados por temblores, daños por inundaciones, daños causados por el polvo, riesgos de cableado, entre otros.

Factores de riesgo relacionados con el manejo de la información por parte del personal: Son todos aquellos factores que están directamente relacionados con el

factor humano, y que, por ende, se pueden mitigar con la implementación de diversas normas.

Factores de riesgo por criminalidad común y crimen político: Son todos aquellos riesgos y amenazas que tienen que ver con el factor delincuencial, en donde entran, sin duda alguna, los delitos cibernéticos.

Existen diferentes maneras de relacionar los valores asignados a los activos de información y aquellos asignados a las vulnerabilidades y amenazas para así obtener mediciones de riesgo. La organización debe decidir qué método va a usar para hacer el cálculo del riesgo; sin embargo, todas las metodologías propuestas por diversos expertos y autores, como ya se había mencionado, están basados en las Normas ISO/IEC 27001, normas que marcan la pauta para poder gestionar adecuadamente entornos de Seguridad de la Información en cualquier institución, y que, por ende, nos marca la pauta para poder también implementar políticas de seguridad respecto a ese contexto. En este sentido, también cada una de las instituciones y encargados que ocupan algún puesto estratégico, deberá decidir cuáles son los riesgos y amenazas que puedan poner en jaque las funcionalidades esenciales de la institución en donde se hará el análisis de riesgos; es aquí donde yace la complejidad: cada empresa tiene sus necesidades y características muy particulares, aunque habrá riesgos aparecerán en cualquiera de éstas.

2.2.6. Políticas de Seguridad de la Información

Las políticas son una serie de instrucciones documentadas que indican la forma en que se llevan a cabo determinados procesos dentro de una organización, también describen cómo se debe tratar un determinado problema o situación. Este documento está dirigido principalmente al personal interno de la organización, aunque hay casos en que también personas externas quedan sujetas al alcance de las políticas. Así pues, tal como afirma Altamirano Yupanqui & Bayona Oré (2017), las organizaciones públicas o privadas, implementan políticas de seguridad informáticas con el fin de proteger su información. En esta lógica, los mismos autores, describen muy eficazmente procesos relacionados con la seguridad de la información, partiendo de la idea esencial de que el considerar que la protección de

la seguridad de la información, a través de sus políticas, se llevaría a cabo solo a través de una perspectiva tecnológica, tendría un enfoque incompleto, pues los estudios que se han realizado a la fecha, demuestran que es necesario tener una visión amplia a través de un enfoque interdisciplinario, donde el principal factor, el humano, juega un papel fundamental. En este tenor, tal como se ha venido afirmando en la presente investigación, para proteger los datos de toda organización o institución se tiene que apostar más allá de los aspectos tecnológicos, es decir, se tiene que apostar por la implementación de reglas y planes de concientización para atacar la problemática desde la génesis que lo ocasiona: las malas prácticas de seguridad de la información.

La complejidad de la Seguridad de la información, yace en que el uso de las tecnologías está dado por el factor humano, y, tal como se mencionó con anterioridad, esto va estar sujeto al comportamiento de este mismo en las organizaciones. En este sentido, la propuesta de Altamirano Yupanqui & Bayona Oré (2017), respecto a las teorías que explican el cumplimiento de las Políticas de seguridad, mismas que se exponen a continuación.

2.2.6.1. Teoría del Comportamiento Planificado (TPB)

Esta teoría, según los autores antes mencionados, postula que el comportamiento individual está influenciado por la actitud, las normas subjetivas y el control de comportamiento percibido. La actitud se define como los sentimientos positivos o negativos del individuo hacia la participación en un comportamiento especificado. Las normas subjetivas describen la percepción de un individuo de lo que las personas importantes para ellos piensan acerca de un comportamiento dado. El control cognitivo percibido se define como las creencias del individuo con respecto a la eficacia y los recursos necesarios para facilitar un comportamiento. En este tenor, la investigación realizada por Moreno Zamudio et al. (2018), pone de manifiesto la importancia a conocer la Teoría del Comportamiento Planificado, y la relación evidente que hay entre el comportamiento de las organizaciones y la percepción que hay para poder llevar a cabo algo eficientemente.

2.2.6.2. Teoría de Protección de motivación (TPB)

Según Altamirano Yupanqui & Bayona Oré (2017), esta Teoría sostiene proporcionar claridad conceptual para la comprensión de las apelaciones al miedo.). Desde la perspectiva de estos autores, la PMT propone que la intención de proteger a uno mismo depende de cuatro factores: (1) la percepción de la gravedad de la amenaza de un evento (por ejemplo, un ataque al corazón), (2) la probabilidad percibida de la aparición, o vulnerabilidad (en este ejemplo, la vulnerabilidad percibida del individuo al escuchar un ataque), (3) la eficacia de la conducta preventiva recomendada (la percepción de la eficacia de respuesta), y (4) la percepción de auto-eficacia (es decir, el nivel de confianza en la propia capacidad para llevar a cabo el comportamiento preventivo recomendado).

2.2.6.3. Teoría del Enlace Social

Según Lozares, López Roldán, Miquel Verd, Martí, & Luis Molin (2011), el vínculo social es un recurso de los individuos y colectivos; precisamente es lo que da pie y forma a las posiciones o estatus sociales diferenciados de los individuos y colectivos en la estructura de la red; en esta lógica, en esa red se empiezan a conformar situaciones de relaciones y donde se crean enlaces sociales. Este componente, según estos autores, es un sustantivo que está constituido por recursos de cualquier naturaleza apropiados o en vista a su apropiación por individuos o colectivos que participan en las interacciones o relaciones. Así mismo, Altamirano Yupanqui & Bayona Oré (2017), afirman que la Teoría del Enlace Social, describe las vinculaciones o vínculos sociales que las personas tienen con su grupo. La teoría postula que cuando las personas se basan en tales vínculos, su deseo de entrar en comportamientos antisociales o anti-establecimiento se reduce.

2.2.6.4. Teoría de la Acción Razonada

Esta teoría, de manera muy genérica, está vinculada con otros conceptos y teorías que tienen que ver con la actitud. Así pues, según Bejarano Macías & Alarcón López (2007), la teoría de Acciona razonada menciona que la intención del

comportamiento de una persona es predecible por su actitud a este y por cómo piensa que otras personas verán aquel comportamiento. Por otro lado, Altamirano Yupanqui & Bayona Oré (2017), exponente que ésta sugiere que cuanto más fuerte sea la intención de involucrarse en un comportamiento, mayor será la probabilidad de que se lleve a cabo el comportamiento. En el contexto del cumplimiento de las políticas de seguridad de la información, la actitud de un empleado hacia el cumplimiento de estas políticas combinadas con las normas sociales llevará al empleado a la intención de cumplir con las políticas de seguridad, lo que sugiere el poder cumplir dichas políticas implementadas.

2.2.6.5. La Ingeniería Social

Moreno Zamudio, Tarango Rodríguez y Correa Venegas (2017), retoman una definición que Borghello (2009) aborda, misma que hace referencia a que la Ingeniería Social es una acción o conducta social destinada a conseguir información de las personas cercanas a un sistema. Es el arte de conseguir de un tercero aquellos datos de interés para el atacante por medio de habilidades sociales. Estas prácticas están relacionadas con la comunicación entre seres humanos. Así pues, tal como afirma Altamirano Yupanqui & Bayona Oré (2017), las técnicas de ingeniería social realizadas por hackers educados, explotan tres elementos principales, a saber: 1) factores humanos, 2) aspectos organizativos y 3) controles tecnológicos. En esta lógica, las medidas organizativas sólidas, por ejemplo, políticas y procedimientos, deben estar en su lugar para poner todo en perspectiva.

2.2.6.6. La Teoría Social Cognitiva

Por último, Altamirano Yupanqui & Bayona Oré (2017), ponen de manifiesto que la teoría social cognitiva también es un factor importante para el seguimiento de las Políticas implementadas, afirmando que ésta es una premisa relevante para explicar el comportamiento humano. SCT permite que se estudie la interacción simultánea y dinámica entre factores sociales y personales; todo esto partiendo desde dos elementos esenciales: en primera instancia, el ***Locus Control***, que hace alusión al

grado en que un individuo cree que él o ella tiene la capacidad de controlar los eventos que directa o indirectamente los afectan. En segunda instancia, la ***auto-eficacia***, que se refiere a la creencia de los individuos en sus propias competencias y capacidades.

Todas estas teorías marcan la pauta para considerar que el implementar o crear una Política de Seguridad tiene una complejidad humana y tecnológica, pero que es necesario saber las problemáticas que se tienen que mitigar a través de un análisis objetivo y concreto, para así, poder otorgar un panorama claro y contundente y poder predecir si las Políticas de Seguridad de la Información que se han creado e implementado se pueden seguir adecuadamente; aquí se hace alusión a lo que ya ha abordado en esta investigación: el factor humano sigue siendo el eslabón más vulnerable para poder establecer contextos de Seguridad de la Información en cualquier institución.

CAPÍTULO III: METODOLOGÍA

3.1. Tipo de Investigación

En esta investigación de enfoque cuantitativo se pueden observar tres principales tipos, mismos que hacen alusión a lo que se explica a continuación:

Tipo de investigación de campo: Esta investigación se apoya en la información recabada. Esta información se obtuvo mediante observaciones dentro del área administrativa de la Unidad Académica de Psicología, y a través de reuniones y entrevistas con los directos y coordinadores de esta misma área.

Tipo de investigación descriptiva: Esta investigación describe las actividades que se llevan a cabo en los procesos manejados en el objeto de estudio, permitiendo conocer en forma sistemática las vulnerabilidades o riesgos que se presentan en los mismos.

Tipo de investigación explicativa: Esta investigación intenta establecer los aspectos que causan el objeto de la investigación, plantea una valoración de

hipótesis que ayude a comprender los fenómenos que se están suscitando dentro de la población en la que se desarrolla la investigación.

3.2. Nivel de Investigación

Nivel Descriptivo: Se describen los hechos tal y como se han observado dentro de la Institución, específicamente en espacios donde se tenga contacto con la Tecnología y aquellas prácticas que se siguen específicamente en el personal administrativo de la Unidad Académica de Psicología de la Universidad Autónoma de Zacatecas.

Nivel Aplicativo: Se plantea resolver problemas o intervenir en la historia natural del fenómeno que se presenta. Enmarca a la innovación técnica, como la científica. Se apunta a evaluar el éxito de la intervención en cuanto a: proceso, resultados e impacto. Para ello se identificaron los indicadores adecuados; en este caso, aquellos procesos y/o indicadores que puedan ayudar a crear políticas de seguridad de la información a través del análisis de riesgos realizado.

3.3. Diseño de la Investigación

El Diseño de esta investigación es no experimental, ya que se observan los fenómenos tal y como ocurren naturalmente, sin intervenir en el desarrollo de dicho proceso, partiendo de que el mismo objeto de estudio no se puede modificar deliberadamente. También el diseño de la presente investigación hace referencia a lo transversal, ya que recopila datos en el momento del estudio del análisis de riesgos que aquí se presenta.

3.4. Población y Muestra

3.4.1.1. Universo

En la recaudación de la información esencial para a esta investigación dentro de la Unidad Académica de Psicología, se tomó en cuenta al *Coordinador Administrativo* de dicha Unidad. A partir de aquí, se incluyeron, para el análisis de riesgos, todos los activos de la información del área administrativa de la institución; tales como todos los procesos esenciales de esta área, recursos financieros, recursos físicos,

recursos tecnológicos en general y todos los integrantes que constituye el recurso humano que está contacto directo con dichos recursos dentro de la Unidad Académica de Psicología de la Universidad Autónoma de Zacatecas.

.

3.4.1.2. Muestra

Para el estudio y análisis de datos, se utilizó una muestra de tipo no probabilística. En esta lógica, se realizó un muestreo por conveniencia donde los criterios para la selección dentro de la población fueron los siguientes:

- Coordinador administrativo que posee un amplio conocimiento del proceso de actividades que juega cada uno de los administrativos de la Unidad Académica de Psicología, así como de los activos de la información más relevantes para esta investigación.

3.5. Instrumentos de Recolección de datos.

Los instrumentos para la recolección de datos dentro de esta investigación son los siguientes:

- Escala para Tasación de activos de la información.
- Escala de Probabilidad de ocurrencia de amenazas en activos de la información de la institución.
- Matriz de evaluación de Riesgos de Seguridad de la Información.

3.6. Plan de Procesamiento de la Información

Una vez definida la población se tuvieron que elegir las actividades relacionadas a los objetivos de la Investigación, abordados en los siguientes puntos:

3.6.1. Plan para el Análisis de Riesgos

1. Realizar una búsqueda teórica respecto a los conceptos que en esta investigación se utilizan.
2. Definir la Métricas que se evaluarán dentro de la Unidad.
3. Determinar cuáles estándares podrán adaptarse al Modelo propuesto.

4. Identificación de los activos de información: listar los activos de la organización, describir los activos, clasificar los activos.
5. Tasación de los activos de información, en donde se priorizan los activos según la importancia de funcionalidad dentro de los procesos de las instituciones.
6. Identificación de las amenazas a través del instrumento definido.
7. Obtención de la matriz de amenazas/riesgos de los activos de información.

3.6.2. Plan para la Creación de Políticas de Seguridad de la Información basado en el Análisis de Riesgos.

Siguiendo la metodología que propone Duque Méndez (s.f.), el plan en cuanto a la creación de Políticas que lleva la presente investigación corresponde a los siguientes pasos:

1. **Mercadeo del Proyecto**, en donde es necesario usar diferentes estrategias para involucrar a la alta gerencia en el proyecto y facilitar el trabajo de concientización, apoyándose en casos de fallos de seguridad ocurridos en negocios similares y los efectos generados.
2. **Inventario y calificación**, en donde es necesario hacer un juicioso inventario de recursos informáticos (hardware, software y liveware), y de los servicios ofrecidos, donde se determine la importancia para la organización y el grado de criticidad de cada uno.
3. **Determinar los objetivos**, en donde se establece la orientación a proteger la organización contra amenazas que atentan contra los pilares de la Seguridad de la Información.
4. **Análisis de Riegos y Amenazas**, descrito con anterioridad.
5. **Documentación e investigación,** de estándares y Políticas de Seguridad existentes para poder establecer una base estructural y una Guía de las posibles prácticas que se puedan incorporar en la propuesta resultante de la presente Tesis.

CAPÍTULO IV: RESULTADOS

4.1. Identificación y Clasificación de los activos de Información

Los activos de información que se obtuvieron se adecuaron a las necesidades específicas del objeto de estudio, considerando aquellos procesos y recursos de cualquier índole que ayude a preservar la funcionalidad principal de las áreas administrativas. Esto se obtuvo con base a la documentación de los activos de información que se tienen en la Unidad Académica de Psicología, se obtuvo como resultado la clasificación de los activos, tomando en cuenta procesos, activos físicos, trabajadores y departamentos. Esta clasificación se elaboró de acuerdo a las funcionalidades esenciales de esta Unidad y Universidad, considerando que estas características se pueden observar en la mayoría de las Universidades, y que, cada activo constituye un rol importante para el buen funcionamiento de la organización. Dicho proceso se muestra en la tabla 17, con su correspondiente descripción.

Tabla 17. Identificación y Clasificación de los Activos de la Información para realizar el análisis de riesgos dentro de la Unidad Académica de Psicología de la Universidad Autónoma de Zacatecas.

Clasificación de Activo	Descripción	ACTIVO
DATOS Y PROCESOS INSTITUCIONALES	Son todos aquellos procesos que se llevan a cabo dentro de la institución para poder dar funcionalidad correcta y efectiva a los objetivos académicos y organizacionales de la Universidad y Unidad Académica. Así mismo, en esta	Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc. Finanzas
		Servicios bancarios
		Directorio de Contactos
		Productos institucionales (Investigaciones, Folletos, Fotos, etc.)

	categorización se encuentran activos que tienen que ver con la información sensible e importante que maneja la institución, así como todos los medios que impliquen el manejo de ésta, como correos, servicios bancarios, Documentos, etc. Estos activos, como ya se mencionó con anterioridad, ponen de manifiesto todos aquellos procesos que hacen que la organización funcione, y los activos que lo constituyen son de diferente índole.	Correo electrónico
		Bases de datos internos
		Página Web interna (Intranet)
		Página Web externa
		Respaldos
		Infraestructura (Planes, Documentación, etc.)
		Informática (Planes, Documentación, etc.)
		Base de datos de Contraseñas
		Navegación en Internet
		Chat
		Llamadas telefónicas internas
		Llamadas telefónicas externas
SISTEMAS INSTITUCIONALES	Son todos aquellos activos o bienes materiales físicos, destinados a brindar servicios a la Universidad, tales como internet, alojamiento de plataformas/sistemas y lo que tenga que ver con administración y envío de datos. Se refiere también a los sistemas o programas que	Equipos de la red cableada (router, switch,etc.)
		Equipos de la red inalámbrica (router, punto de acceso, etc.)
		Servidores
		Computadoras
		Portátiles
		Software de administración (contabilidad, manejo de personal, etc.)
		Software de Servicio Social, Congresos, etc.

	optimizan/automatizan las tareas dentro de la Institución. Están algunos de éstos, relacionados con las funciones del Hardware que le corresponde.	Software de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)
		Impresoras
		Memorias portátiles
		Celulares
		Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)
		Vehículos
PERSONAL ADMINISTRATIVO	Encargadas también de gestionar información dentro de la Institución. Así mismo, son quienes usan otros activos, tales como Hardware y Software, consolidando así los procesos y datos institucionales, a través de diversos sistemas.	Consejo de Unidad
		Dirección / Coordinación
		Administración
		Personal técnico
		Recepción
		Piloto / conductor
		Informática / Soporte técnico interno
		Soporte técnico externo
		Servicio de limpieza

4.2. Tasación de los Activos de la Información del Área Administrativa de la Unidad Académica de Psicología de la UAZ.

Una vez que se identificaron los activos de la Unidad Académica de Psicología, se procedió a asignar un valor en cuestiones de importancia en cuanto a su confidencialidad, integridad y disponibilidad. A este proceso se le titula ***tasación***, el cual debe ser realizado por los propietarios de los activos; en este caso, el

Coordinador Administrativo de la Unidad Académica de Psicología, quien tiene la responsabilidad de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos del objeto de estudio (De Freitas, 2009).

Para la tasación de los activos se utilizó una escala de Likert, donde el valor 1 significa “nada importante”, 2: “Poco importante” ,3: “Mediadamente importante”, 4: “Altamente importante” y 5: “Demasiado importante”. Dicha escala, giró en torno a la siguiente pregunta: *¿Qué importancia tiene el activo para la organización, área, departamento o dirección?* (De Freitas, 2010); esta pregunta en cuanto a confidencialidad, disponibilidad e integridad de cada uno de los activos. En la tabla 18, se puede observar la asignación de valores de los activos empezando por su confidencialidad, disponibilidad e integridad. El Total se obtiene de la suma de los puntos asignados al activo dividido entre 3 (De Freitas, 2010) y hace referencia a la última columna de la tasación. Este proceso de tasación, ayudó a priorizar los activos que son más esenciales dentro de la organización, teniendo como promedio los valores de 4 y 5, lo que nos indica que todos los activos seleccionados para realizar el análisis de riesgos requieren tener los 3 pilares de seguridad de la información, y que la importancia de conservarlos seguros es sumamente relevante para el buen funcionamiento de los procesos de la Unidad Académica de Psicología; como ya se había mencionado con anterioridad, a este proceso se le llamó *tasación de los activos.*

Tabla 18. Tasación de los Activos de la Información dentro del Área Administrativa de la Unidad Académica de Psicología de la Universidad Autónoma de Zacatecas

Clasificación de Activo	**ACTIVO**	**TASACIÓN**			
		Confidencialidad	**Integridad**	**Disponibilidad**	**TOTAL**
DATOS Y PROCESOS INSTITUCIONALES	Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.	5	5	5	**5**
	Finanzas	5	5	5	**5**

	Servicios bancarios	5	5	5	**5**
	Directorio de Contactos	3	3	4	**4**
	Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	4	4	4	**4**
	Correo electrónico	3	4	4	**4**
	Bases de datos internos	4	4	4	**4**
	Página Web interna (Intranet)	4	4	4	**4**
	Página Web externa	4	4	4	**4**
	Respaldos	5	5	4	**5**
	Infraestructura (Planes, Documentación, etc.)	5	5	5	**5**
	Informática (Planes, Documentación, etc.)	4	4	4	**4**
	Base de datos de Contraseñas	4	4	4	**4**
	Navegación en Internet	4	4	4	**4**
	Chat	3	3	3	**3**
	Llamadas telefónicas internas	4	4	4	**4**
	Llamadas telefónicas externas	4	4	4	**4**
SISTEMAS INSTITUCIONALES	Equipos de la red cableada (router, switch,etc.)	5	5	5	**5**
	Equipos de la red inalámbrica (router, punto de acceso, etc.)	5	5	5	**5**
	Servidores	5	5	5	**5**
	Computadoras	5	5	5	**5**

	Portátiles	4	4	4	**4**
	Software de administración (contabilidad, manejo de personal, etc.)	5	5	5	**5**
	Software de Servicio Social, Congresos, etc.	4	4	4	**4**
	Software de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	4	4	4	**4**
	Impresoras	4	4	4	**4**
	Memorias portátiles	4	4	4	**4**
	Celulares	3	3	3	**3**
	Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	4	4	4	**4**
	Vehículos	4	4	4	**4**
PERSONAL ADMINISTRATIVO	Consejo de Unidad	4	4	4	**4**
	Dirección / Coordinación	5	5	5	**5**
	Administración	5	5	5	**5**
	Personal técnico	5	5	5	**5**
	Recepción	5	5	5	**5**
	Piloto / conductor	4	4	4	**4**
	Informática / Soporte técnico interno	4	4	4	**4**
	Soporte técnico externo	4	4	4	**4**
	Servicio de limpieza	4	4	4	**4**

4.3. Identificación de las Amenazas de los Activos de la Información y su probabilidad de ocurrencia dentro de la Unidad Académica de Psicología de la Universidad Autónoma de Zacatecas.

Ya que se tiene la tasación de los activos, es necesario identificar las amenazas que tiene cada uno de éstos. Además, fue también necesario calcular su probabilidad de ocurrencia a través de una escala Likert respondiendo la siguiente pregunta: *¿Cuál es la probabilidad de que ocurra dicha amenaza en los activos de información del Área Administrativa de la Unidad Académica de Psicología?*, además, dicha pregunta se puede complementar con las siguientes: *¿Cuál es el interés o la atracción por parte de individuos externos, de atacar la institución?, ¿El activo es vulnerable ante esa amenaza?, ¿Cuántas veces ha sucedido ese hecho?*, según sea la amenaza del activo evaluado.

Dicha(s) pregunta(s) se realizaron al Coordinador Administrativo de la Unidad Académica de psicología, quien es el encargado de todos los activos y procesos administrativos de dicha institución. Las respuestas que aquí se seleccionaron mediante la escala Likert se explican de la siguiente manera: Si el coordinador respondió con el valor 1: ”Nula Posibilidad” significa que no existen condiciones para que suceda un ataque, daño o perdida de ese activo, 2: “Poco probable” significa que pudiera que se dé un ataque, daño o perdida al activo, pero es una posibilidad lejana., 3: “Medianamente Probable” significa que hay posibilidades de que se dé un ataque, daño o pérdida del activo, y hay condiciones para que suceda. y 4: “Altamente probable” significa que la posibilidad de que se dé un ataque, daño o pérdida del activo es inevitable, no existen condiciones para protegerlo, y pudiera que se haya dado ya.

Así pues, la columna de *“Ocurrencia promedio por activo (OPA)”* se obtuvo de la suma de los puntajes obtenidos y se divide entre el número de amenazas que se identificaron para cada activo. Otro dato importante que se obtuvo, es el que se muestra en la columna de “*Magnitud de Daño”*, misma que es un análisis perceptivo respecto a qué *impacto tendría su institución si ese activo se pierde, se daña o es hackeado;* esta pregunta, al igual que la anterior, se responde a través de escalas Likert, utilizando las siguientes respuestas: 1: “Nulo Impacto” que significa que no

afecta las funciones, ya que no causa relevancia la pérdida o daño de ese active, 2: “Poco Impacto” que significa que las funciones se ven afectadas, sin embargo, la institución se recuperará pronto, 3: “Mediano impacto” que significa que la institución no podría seguir funcionando, pero habría otras alternativas costosas y 4: “Alto impacto” que significa que es imposible que la institución funcione si se daña, pierde o hackea ese activo.

En este sentido, en la Tabla 19 podemos observar, en primera instancia, que la *Magnitud de Daño* de la Mayoría de los Activos de Información oscilan entre Mediano y Alto impacto, lo que significa que si cualquiera de estos activos que están marcados con esos valores se pierde o se daña podrían inhabilitar por completo las funcionalidades esenciales de la Unidad Académica de Psicología. Sin embargo, sí hay activos que a nivel perceptual tienen menor valor de *Magnitud de Daño*, oscilando entre 1 y 2; como en el caso de los activos de información alusivos a impresoras o personal técnico externo, en donde si alguno de estos activos sufre alguno de las amenazas que se muestra en el instrumento las funciones se verán afectadas, pero la institución se recuperará pronto. Claro está, que para ninguna empresa o institución es viable que exista ese nivel de Magnitud de Daño y hay que buscar erradicarlo, o en su defecto, disminuirlo.

En cuanto a la *Probabilidad de Ocurrencia de la Amenaza*, podemos observar que ésta, en su mayoría, oscila entre los valores 2 y 4 de cada activo; en donde el valor de 3 es el que predomina. Así pues, por ejemplo, en la categoría de amenazas que tienen que ver *con la criminalidad común y motivación Política* y en la categorización de activos de *Datos y Procesos Institucionales*, podemos observar que el activo de *Finanzas* en específico tiene **alta posibilidad de que haya *acceso no autorizado*** ya que el coordinador administrativo respondió ese apartado con el valor de 4; esta misma interpretación se hace en cada categoría de activos y en cada categoría amenazas, haciéndolo en cada activo de la información.

Por último, utilizando el cálculo que se describió con anterioridad, se observa que la *Ocurrencia Promedio de Amenaza por Activo*, oscila en los valores de 2 y 3, lo que significa que la mayoría de los activos tiene un promedio medianamente alto respecto a dicha ocurrencia. Por ejemplo, volviendo al activo de *Finanzas*, se

observa que se asignó el valor de 3 en la columna de la *Ocurrencia Promedio*, lo que significa que, en promedio, tiene una alta probabilidad de que ocurran riesgos que se describen en esta investigación, sin importar cual sea; esta misma interpretación se realiza igual en cada uno de los activos, haciendo el cálculo correspondiente de promedio. Así pues, el tener una idea de este promedio por activo, nos da un acercamiento respecto a en qué activos se debe tener mayor cuidado; sin embargo, es a través de la Matriz de Riesgos o Matriz threats-Vulnerabilities-Assets (TVA) en donde se muestra exactamente el panorama de los riesgos y amenazas en los que debe centrar la mitigación a través de la incorporación de Políticas de Seguridad de la Información para cada categoría de activo respecto a las posibles amenazas que se han identificado con anterioridad.

Tabla 19. Identificación de amenazas de los activos de información y la probabilidad de ocurrencia dentro del Área Administrativa de la Unidad Académica de Psicología de la UAZ.

		PROBABILIDAD DE OCURRENCIA DE LA AMENAZA																														
	MD	Criminalidad común y motivación política										Sucesos físicos							Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales														
	MAGNITUD DE DAÑO	Acceso no autorizado	Persecución (Civil, fiscal o penal)	Orden de secuestro/Detención	Ataque físico o electrónico	Daños por vandalismo	Fraude/Estafa	Extorsión	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Virus / Ejecución no autorizado de programas	Violación a derechos de autor	Incendio	Inundación / deslave	Sismo	Falta de ventilación	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro	Falta de capacitación sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de software 'pirateado	Falta de conocimiento de software nuevo	Perdida de datos	Infección de sistemas a través de USB	Tener Unidades portables con información sensible	Compartir contraseñas o permisos a terceros	Extravío de equipo, (USBS, lap, compu)	Sobrepasar autoridades	Falta restricciones del personal	Falta de mantenimiento físico	Falta de actualización de software	Fallas en permisos de usuarios (acceso a archivos)	Accesos no autorizados a Sistemas	Falta de normas y reglas claras	Ausencia de documentación	OCURRENCIA PROMEDIO POR ACTIVO (OPA)
Documentos institucionales (Proyect	4	4	[redacted]	3	3	[redacted]	4	3	[redacted]	3	3	2	1	[redacted]	2	[redacted]	2	[redacted]	3	[redacted]	3	3	[redacted]	3	[redacted]	3	3	3	**3**

os, Planes, Evaluaciones, Informes, etc.																																					
Finanzas	4	4			3	3	4	3	4	3			3	3	2				3	4	3		2	2	3		2	3		3	3	3	2	2	3	3	3
Servicios bancarios	4	4			3	4	3	3	4	3	2				3		3	3	3	3	3		3	3	4		3	4		3	2	2	3	3	3	3	3
Directorio de Contactos	2	3			3	3			3	2			3	3	3									3				3		2			3		3	3	2
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	1	4			3	2			3	2	3	3	2	3	3					3	3			2	3			3		2	3		3		2	3	3
Correo electrónico	3	3			3	2		3	3	2	2				2			3	3		3			3	3		2			2	3	3	3	2	2	3	2
Bases de datos internos	4	3			3	2			3	3	3				2		3	3	2	2	3		3	3	2	2		3		2	2	3	3	2	2	2	2
Página Web interna (Int	3	2			3	3		2	3	2	2	2			3		2	3	2		2	3	2	3	3		3			2	2	3	2	3	2	3	2

ran et)																																				
Página Web externa	2	3			2	3		4	3	4	3	3			2			3	3			3	2	3	3		2			2	3	3	3	3	3	2	3
Respaldos	4	4			2	3			3	2	3		3	3	3		2	3	2		3		2	2	3	3	3	2		3	2	3	2	2	3	2	2
Infraestructura (Planes, Documentación, etc.)	3	3			3	2			3	3		2	3	3	2			4			4		3	3	2			2		3	3		3		3	2	3
Informática (Planes, Documentación, etc.)	3	3			3	3			2	4	3	4	3	2	3	2		3	3	4	4		2	2	3			3		3	2	2	3	3	2	2	3
Base de datos de Contraseñas	4	2			3	2			2	3	3	2	2	3	3	2	2	2	2	3	3		3	3	2	2	2	3		2	3	3	2	2	3	3	3
Navegación en Internet	2	3			2	3	2	3	3	3	3	2			3			4			2		3	3	2		2			3		2	3	3	2	2	2
Chat	2	2			3	2	3	4	2	3	3				3			4	3		2		2		2		2			3		2	3	2	3	3	2
Llamadas telefónicas internas	2	2			3	2	3	2	3	3	2				2			3			2						3			2			2	3	3	3	2

Llamadas telefónicas externas	**2**	3			2	3	4	4	3	2	2				2			3			2						3			2			3	2	3	1	**2**
Equipos de la red cableada (router, switch,etc.)	**4**	3			2	3			3	3	3		4	3	2	3	3	2	4	3	3		2	2	3		3	3		2	3	3	3	2	2	3	**3**
Equipos de la red inalámbrica (router, punto de acceso, etc.)	**4**	4			3	3			2	3	3		3	3	2	3	2	2	3	3	2		3	3	2		4	4		2	2	3	2	1	2	3	**3**
Servidores	**3**	3			2	3			2	3	1		4	3	2	3	2	2	3	2	3		2	3	3		3	2		3	3	3	2	3	1	3	**3**
Computadoras	**4**	3			2	3		3	2	2	3		2	3	1	2	3	2	3	2	3	3	3	2	3		2	1		3	2	1	3	2	3	3	**2**
Portátiles	**4**	3			3	2		3	3	2	3		2	3	2	3	2	3	1	2	3	2	3	3	3		2	3		1	2	2	3	4	3	3	**2**
Software de administración (contabilidad, manejo de	4	2			3	3			2	3	3	3	3	2	2	3	3	2	2	3	3	2	3	2			2	3		3	2	3	3	3	2	2	**2**

personal, etc.)																																						
Software de Servicio Social, Congresos, etc.	4	2		3	2	3		3	2	3	2			2	3	2	3	3	3	3	2	2	3		3	2		2	2	3	3	3	2	3	**3**
Software de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	3	3		2	3	2	2	3	3	3	2			3	2	3	2	3	2	3	2	3	2	2	3		2	2		3	2	3	3	3	2	2	**2**
Impresoras	2	3		2	3	3		2	2	3		2	3	2	3	2	3		3	3		2	2		2	2		3	3	3	2	2	2	3	**2**
Memorias portátiles	2	3		2	2			3	2	2		2	3	2		3	3			3			2	2	4		3	3	2	3	2	3	3	3	**2**
Celulares	2	3		2	3	2	3	2	2	2		3	3	3		3			3	3	3	3	2	4		3	3		3	2	3	2	3	2	3	**3**
Edificio (Oficinas, Recepción, Sala de espera, Sala de	2	4		3	3			3	3			2	3	3	2	3			3	2	2		3			3		3	2	3	3	3	2	2	**3**

reunión, Bodega, etc.)																																				
Vehículos	2	3			4	3			3	2		3	2	3	3	2		2	3							3		2	3		2		3	2	3
Consejo de Unidad	3	3	4	3	3	2	3	2	3	3								3	2	3	2	2	3	3	2	2	3	3		2	3	3	3	2	3
Dirección / Coordinación	4	3	4	3	2	3	2	3	2	2								2	3	2	3	2	3	2	3	3	3	3		2	3	2	2	3	3
Administración	4	4	4	3	3	2	3	4	3	3								3	2	3	2	3	3	3	2	3	3	2		3	2	3	3	3	3
Personal técnico	3	4	3	3	4	3	2	3	3	3								3	2	3	2	3	2	3	3	1	3	3		3	2	3	2	2	2
Recepción	3	3	3	2	2	3	3	2	3	2								2	3	2	3	2	3	3	3	2	3	3		2	2	2	3	3	2
Piloto / conductor	2	3	3	2	3	2	3	2	2	2								3	2	3	3	3	3	2	3	1	3	2		3	3	2	2	1	2
Informática / Soporte técnico interno	3	3	4	3	2	2	3	2	3	3								3	2	3	2	3	2	3	3	3	3	2		3	2	2	2	2	2
Soporte técnico externo	1	3	3	3	3	2	2	3	2	3								3	3	3	3	3	2	3	2	2	3	2		3	3	2	1	3	2
Servicio de limpieza	1	3	3	3	3	3	2	2	3	2								2	2	2	3		3	3	2	2	2	3		3	3	2	2	1	2

4.4. Identificación de Riesgos de los Activos de Información de la Unidad Académica de Psicología: Matriz TVA (Threats-Vulnerabilities-Assets) de los activos de información dentro de la Unidad Académica de Psicología.

La matriz de Análisis de Riesgos o Matriz TVA que aquí se muestra, es el resultado de todo el proceso que se siguió con anterioridad para poder comprobar los riesgos o amenazas de los activos que se han identificado, tasado y evaluado. Ésta, a final de cuentas, representa una forma para determinar los riesgos en el manejo de los datos e información del Área Administrativa de la Unidad Académica de Psicología de la UAZ. Así pues, en esta matriz se localizan y visualizan los recursos de esta institución educativa que están en mayor peligro de sufrir un daño por algún impacto negativo, para posteriormente tener la capacidad de tomar las decisiones y medidas adecuadas para la superación de las vulnerabilidades y la reducción de las amenazas; en este caso, poner en marcha la génesis de esta investigación, misma que hace alusión a la creación de Políticas de Seguridad para mitigar dichos riesgos. Así pues, La Matriz que se muestra en la Ilustración 16, se basa en el método de Análisis de Riesgo usando la siguiente fórmula:

Riesgo = Probabilidad de Amenaza x Magnitud de Daño

Esa fórmula, se aplica para cada valor que se le dio a cada amenaza y activo de información y que fuere respondido a través del Instrumento aquí planteado, tales respuestas se visualizan en la Tabla 19, la cual ya fue analizada y explicada con anterioridad. En este tenor el Riesgo que resulta del producto de la multiplicación Probabilidad de Amenaza por Magnitud de Daño, está agrupado en tres rangos, y para su mejor visualización, se aplica diferentes colores.

- Bajo Riesgo = 1 – 6 (**verde**)
- Medio Riesgo = 7 – 10 (**amarillo**)
- Alto Riesgo = 11 – 16 (**rojo**)

Cabe aclarar, que aquellos espacios que están en negro, sugieren que no hay una relación directa entre el activo seleccionado y la amenaza seleccionada, por lo tanto,

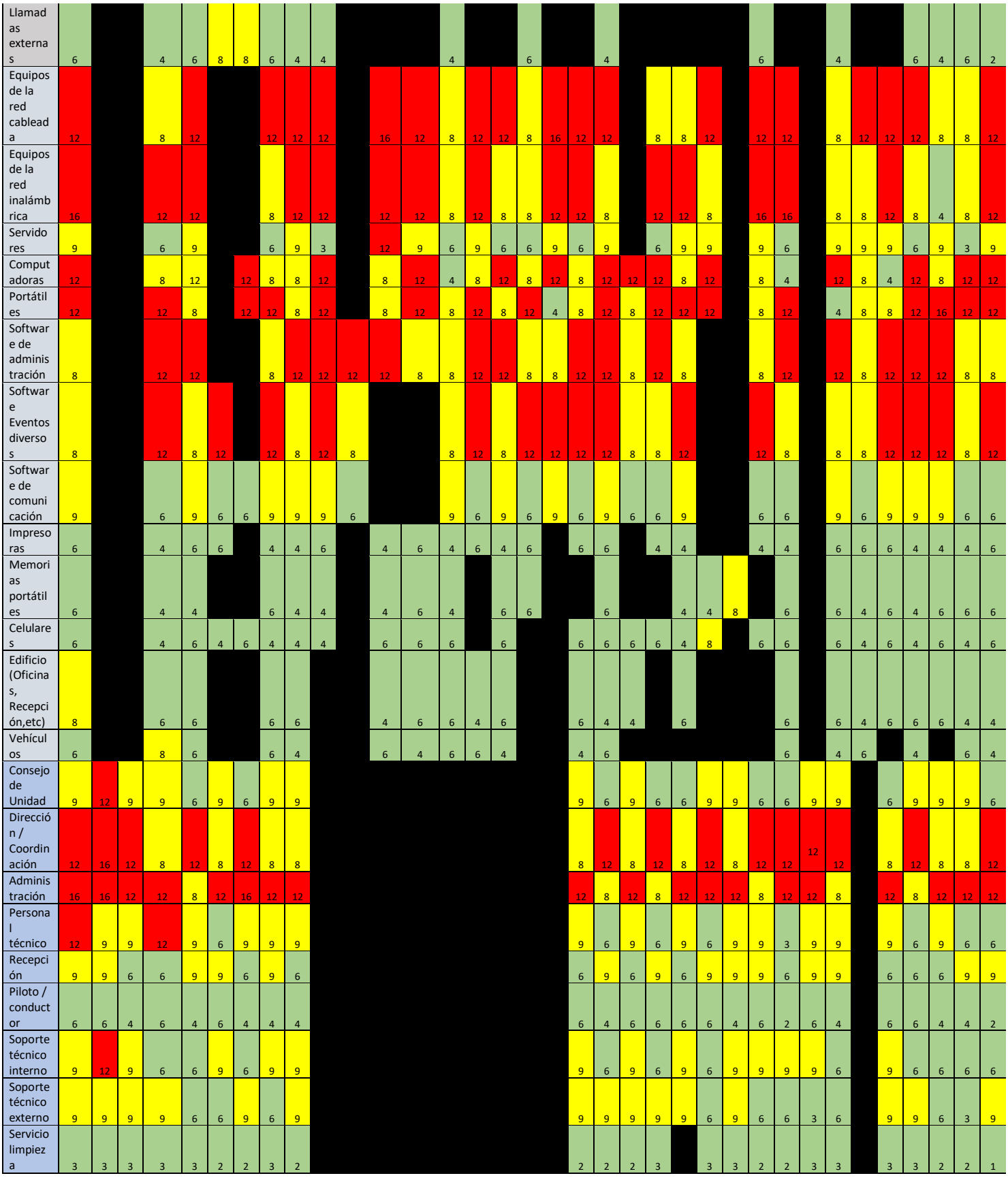
no se toma en cuenta para su análisis, y, por ende, no se toma en cuenta. Sin embargo, las demás que están con algún color verde, amarillo o rojo, se empiezan a considerar como factores de riesgo, determinando su nivel según sea el caso. Así pues, dependiendo de los valores de la Probabilidad de Amenaza y la Magnitud de Daño, la Matriz calcula el producto de ambos variables y visualiza el grado de riesgo, a través de la aplicación de la fórmula descrita con anterioridad. La Matriz, tal como se muestra en la Ilustración 16, está dividida en 3 categorías de Probabilidad de Amenazas y en 3 categorías de activos de información. Las amenazas, hacen alusión a las categorías de ***criminalidad y motivación política***; que contiene amenazas de Acceso no autorizada, Persecución (Civil, fiscal o penal), Orden de secuestro/Detención, Ataque físico o electrónico, Daños por vandalismo, Fraude/Estafa, Extorsión, Robo / Hurto (físico) Robo/Hurto de información electrónica, Virus / Ejecución no autorizado de programas y Violación a derechos de autor, ***Sucesos físicos***; Incendio, Inundación / deslave, Sismo, Falta de ventilación, Sobrecarga eléctrica, Falla de corriente (apagones) y Falla de sistema / Daño disco durdo y la categoría ***Negligencia de usuarios y decisiones institucionales***; que contiene amenazas de Falta de capacitación sobre riesgos, Mal manejo de sistemas y herramientas, Utilización de software 'pirateado, Falta de conocimiento de software nuevo, Perdida de datos Infección de sistemas a través de USB , Tener USB con información sensible, Compartir contraseñas o permisos a terceros, Extravío de equipo, (USBS, laptop, computadoras), Sobrepasar autoridades, Falta restricciones del personal, Falta de mantenimiento físico, Falta de actualización de software, Fallas en permisos de usuarios (acceso a archivos), Accesos no autorizados a Sistemas, Falta de normas y reglas clara y Ausencia de documentación. Del lado izquierdo de la matriz, se cuenta con las categorías de Activos de información, mismas que hacen alusión a **Datos y Procesos institucionales**; donde se analizan activos de información como Documentos institucionales, Finanzas, Servicios bancarios, Directorio de Contactos, Productos institucionales, Correo electrónico, Bases de datos internos(Intranet), Página Web externa, Respaldos, Infraestructura, Informática, Base de datos de Contraseñas, Navegación en Internet, Chat, Llamadas internas, Llamadas externas, ***Sistemas***

Institucionales; donde se analizan activos de información como Equipos de la red cableada, Equipos de la red inalámbrica, Servidores, Computadoras, Portátiles ,Software de administración, Software Eventos diversos, Software de comunicación, Impresoras, Memorias portátiles, Celulares, Edificio (Oficinas, Recepción, etc.) y Vehículos, ***y Personal Administrativo;*** que se compone de los activos de información de Consejo de Unidad, Dirección / Coordinación, Administración, Personal técnico, Recepción, Piloto / conductor, Soporte técnico interno, Soporte técnico externo y Servicio de limpieza.

Dicho lo anterior y haciendo alusión a parte de la metodología que plantea Erb (2011), dependiendo del color de cada celda, podemos sacar conclusiones no solo sobre el nivel de riesgo que corre cada elemento de información de sufrir un daño significativo, causado por una amenaza, sino también sobre las medidas de protección necesarias, medidas en donde entran la creación de Políticas que pueden mejorar en la mitigación de dichos riesgos. En esta lógica, poniendo como ejemplo nuevamente el activo de información de *finanzas*, podemos observar que tiene un alto riesgo en la amenaza de acceso no autorizado, de ataque físico o electrónico, daños por vandalismo, fraude, extorsión robo físico o electrónico, virus, violación de derecho de autor, incendio, inundación, falla de sistema, falta de capacitación, mal manejo de sistema, Infección de sistema a través de USB, extravió de computadoras o USB, falta de restricción en el personal, falta de mantenimiento físico, falta de normas y reglas claras y ausencia de documentación; todos estos riesgos altos se pueden visualizar ya que éstos salieron en un rango de valores de 11-16, y por ende, están marcados con rojo. Sin embargo, en ese mismo activo se observa que hay 6 amenazas con valores con rangos de 7-10, lo que significa que el riesgo de que ese activa sufra esas amenazas es mediana, y eso se puede observar con claridad ya que está en color amarillo. Esta interpretación es necesario realizarla por cada activo y cada amenaza para poder implementar adecuadamente la mitigación de riesgo. Sin duda alguna, esta matriz TVA brindó un panorama muy amplio para poder detectar los riesgos a los que con mayor posibilidad están expuestos los activos de información de esta institución.

Ilustración 15. Matriz TVA (Threats-Vulnerabilities-Assets) del Área Administrativa de la Unidad Académica de Psicología UAZ

	Criminalidad común y motivación política											Sucesos físicos							Negligencia de usuarios/as y decisiones institucionales																
	Acceso no autorizado	Persecución (Civil, fiscal o penal)	Orden de secuestro/Detención	Ataque físico o electrónico	Daños por vandalismo	Fraude/Estafa	Extorsión	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Virus / Ejecución no autorizado de programas	Violación a derechos de autor	Incendio	Inundación / deslave	Sismo	Falta de ventilación	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro	Falta de capacitación sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de software 'pirateado	Falta de conocimiento de software nuevo	Perdida de datos	Infección de sistemas a través de USB	Tener USB con información sensible	Compartir contraseñas o permisos a terceros	Extravío de equipo, (USBS, lap, compu)	Sobrepasar autoridades	Falta restricciones del personal	Falta de mantenimiento físico	Falta de actualización de software	Fallas en permisos de usuarios (acceso a	Accesos no autorizados a Sistemas	Falta de normas y reglas claras	Ausencia de documentación
Documentos institucionales	16			12	12			16	12		12	12	8	4						8			8				12		12	12		12		12	12
Finanzas	16			12	12	16	12	16	12			12	12	8			12	16	12		8	8	12			8	12		12	12	12	8	8	12	12
Servicios bancarios	16			12	16	12	12	16	12	8				12		12	12	12	12	12		12	12	16		12	16		12	8	8	12	12	12	12
Directorio de Contactos	6			6	6			6	4			6	6	6									6				6		4			6		6	6
Productos institucionales	4			3	2			3	2	3	3	2	3	3					3	3			2	3			3		2	3		3		2	3
Correo electrónico	9			9	6		9	9	6	6				6			9	9		9			9	9		6			6	9	9	9	6	6	9
Bases de datos internos	12			12	8			12	12	12				8		12	12	8	8	12		12	12	8	8		12		8	8	12	12	8	8	8
(Intranet)	6			9	9		6	9	6	6	6			9		6	9	6		6	9	6	9	9		9			6	6	9	6	9	6	9
Página Web externa	6			4	6		8	6	8	6	6			4			6	6			6	4	6	6		4			4	6	6	6	6	6	4
Respaldos	16			8	12			12	8	12		12	12	12		8	12	8		12		8	8	12	12	12	8		12	8	12	8	8	12	8
Infraestructura	9			9	6			9	9		6	9	9	6			12			12		9	9	6			6		12	12		12		12	6
Informática	9			9	9			6	12	9	12	9	6	9	6		9	9	12	12		6	6	9			9		9	6	6	9	9	6	6
Base de datos de Contraseñas	8			12	8			8	12	12	8	8	12	12	8	8	8	8	12	12		12	12	8	8	8	12		8	12	12	8	8	12	12
Navegación en Internet	6			4	6	4	6	6	6	6	4			6			8			4		6	6	4		4			6		4	6	6	4	4
Chat	4			6	4	6	8	4	6	6				6			8	6		4		4		4		4			6		4	6	4	6	6
Llamadas internas	4			6	6	6	4	6	6	4				4			6			4						6			4			4	6	6	6


Llamadas externas 6 4 6 8 8 6 4 4 4 6 4 6 4 6 4 6 4 6 2
Equipos de la red cableada 12 8 12 12 12 12 16 12 8 12 12 8 16 12 12 8 8 12 12 12 8 12 12 12 8 8 12
Equipos de la red inalámbrica 16 12 12 8 12 12 12 12 8 12 8 8 12 12 8 12 12 8 16 16 8 8 12 8 4 8 12
Servidores 9 6 9 6 9 3 12 9 6 9 6 6 9 6 9 6 9 9 9 9 6 9 9 9 6 9 3 9
Computadoras 12 8 12 12 8 8 12 8 12 4 8 12 8 12 8 12 12 12 8 12 8 4 12 8 4 12 8 12 12
Portátiles 12 12 8 12 12 8 12 8 12 8 12 8 12 8 12 4 8 12 8 12 12 12 8 12 4 8 8 12 16 12 12
Software de administración 8 12 12 8 12 12 12 12 8 8 12 12 8 8 12 12 8 12 8 8 12 12 12 8 12 12 12 8 8
Software Eventos diversos 8 12 8 12 12 8 12 8 8 12 8 12 12 12 12 12 8 8 12 12 8 8 8 12 12 12 8 12
Software de comunicación 9 6 9 6 6 9 9 9 6 9 6 9 6 9 6 9 6 6 9 6 6 9 6 9 9 9 6 6
Impresoras 6 4 6 6 4 4 6 4 6 4 6 4 6 6 6 4 4 4 4 6 6 6 4 4 4 6
Memorias portátiles 6 4 4 6 4 4 4 6 4 6 6 6 6 6 4 4 8 6 6 4 6 4 6 6 6
Celulares 6 4 6 4 6 4 4 4 6 6 6 6 6 6 6 6 4 8 6 6 6 4 6 4 6 4 6
Edificio (Oficinas, Recepción,etc) 8 6 6 6 6 4 6 6 4 6 6 4 6 6 4 4 6 6 6 4 6 6 6 4 4
Vehículos 6 8 6 6 4 6 4 6 6 4 4 6 6 6 4 6
Consejo de Unidad 9 12 9 9 6 9 6 9 9 9 6 9 6 6 9 9 6 6 9 9 6 9 9 9 6
Dirección / Coordinación 12 16 12 8 12 8 12 8 8 8 12 8 12 8 12 8 12 12 12 12 8 12 8 8 12
Administración 16 16 12 12 8 12 16 12 12 12 8 12 8 12 12 12 8 12 12 8 12 8 12 12 12
Personal técnico 12 9 9 12 9 6 9 9 9 9 6 9 6 9 6 9 6 9 3 9 9 9 6 9 6 6
Recepción 9 9 6 6 9 9 6 9 6 6 9 6 9 6 9 9 9 6 9 9 6 6 6 9 9
Piloto / conductor 6 6 4 6 4 6 4 4 4 6 4 6 6 6 6 4 6 2 6 4 6 6 4 4 2
Soporte técnico interno 9 12 9 6 6 9 6 9 9 9 6 9 6 9 6 9 9 9 9 6 9 6 6 6 6
Soporte técnico externo 9 9 9 9 6 6 9 6 9 9 9 9 9 9 6 9 6 6 3 6 9 9 6 3 9
Servicio limpieza 3 3 3 3 3 2 2 3 2 2 2 3 3 3 3 2 2 3 3 3 3 2 2 1

4.5. Análisis de Riesgo Promedio

Una vez sustentados los hallazgos respecto a los riesgos de los activos de información, se pudo obtener el Análisis de Riesgo promedio, en donde se observa una visión general de los 35 riesgos planteados en esta investigación respecto a los 39 activos tasados y valorados dentro del Área Administrativa de la Unidad Académica de Psicología. En este sentido, se obtuvo el promedio de dichos riesgos, haciendo la sumatoria total de las valoraciones de riesgo de todos los activos y este resultado se dividió por la sumatoria total de cada categoría de riesgo dentro de cada categoría de activos. Así pues, se sigue la siguiente fórmula para cada una de las categorías de activos de la información respecto a cada una de las categorías de las amenazas:

Riesgo Promedio = ∑ *(Total de las Amenazas por Categoría de Activos respecto a la categoría de Amenazas / Total de las Amenazas de toda la matriz) * 100*

El total de las Amenazas de toda la matriz se obtuvo de la suma de los 35 activos de información identificados en cada uno de los 35 riesgos utilizados en esta matriz, y al final sólo se hizo la suma de esos totales, obteniendo como resultado final la cantidad de 7,496; dicho valor será una constante. El total de las amenazas por categoría de activos respecto a la categoría de amenazas, se obtiene de sumar los valores de cada categoría de activos en cada uno de los 35 riesgos; en este caso hay 3 categorías, cada una con numero de activos de información diferentes, pero se consideran siempre los mismos riesgos. En este sentido, las operaciones que se realizaron fueron las siguientes, tomando en cuenta que la matriz que se explicó con anterioridad es de 3 (Categoría de los activos de información) x 3 (Categoría de las amenazas), dando como resultado 9 operaciones para la construcción de una nueva matriz, que representará el Riesgo Promedio:

Riesgo Promedio de los Datos y Procesos Institucionales con respecto a Riesgos de Criminalidad Común y Motivaciones Políticas:

Riesgo Promedio = (987 / 7496) * 100 = **13.17%**

Riesgo Promedio de los Datos y Procesos Institucionales con respecto a Riesgos de Sucesos de Origen Físico:

Riesgo Promedio = (518 / 7496) * 100 = **6.91%**

Riesgo Promedio de los Datos y Procesos Institucionales con respecto a Riesgos de Negligencia de usuarios/as y decisiones institucionales:

Riesgo Promedio = (1522 / 7496) * 100 = **20.30%**

Riesgo Promedio de Sistemas y Procesos Institucionales con respecto a Riesgos de Criminalidad Común y Motivaciones Políticas:

Riesgo Promedio = (719 / 7496) * 100 = **9.59%**

Riesgo Promedio de Sistemas y Procesos Institucionales con respecto a Riesgos de Sucesos de Origen Físico:

Riesgo Promedio = (636 / 7496) * 100 = **8.48%**

Riesgo Promedio de Sistemas y Procesos Institucionales con respecto a Riesgos de Negligencia de usuarios/as y decisiones institucionales:

Riesgo Promedio = (1406 / 7496) * 100 = **18.76%**

Riesgo Promedio del Personal Administrativo con respecto a Riesgos de Criminalidad Común y Motivaciones Políticas:

Riesgo Promedio = (658 / 7496) * 100 = **8.78%**

Riesgo Promedio del Personal Administrativo con respecto a Riesgos de Sucesos de Origen Físico:

Riesgo Promedio = (0 / 7496) * 100 = **0%**

Riesgo Promedio del Personal Administrativo con respecto a Riesgos de Negligencia de usuarios/as y decisiones institucionales:

Riesgo Promedio = (1050 / 7496) * 100 = **14.01%**

Por último, para sacar los totales del eje horizontal y vertical, sólo es fue necesario sumar los resultados, dando como resultado 100%, tanto en el eje horizontal, como en el eje vertical. Estos resultados se muestran en la Tabla 20, en donde cada valor está representado también con un color. Estos colores matriciales tienen una explicación respecto a la ponderación que se le otorgó a cada riesgo, mismos que hacen alusión a lo siguiente:

- Del 0% al 5%: Promedio inexistente de riesgo, el cual se representa con el color **gris**.
- Del 6% al 10%: Promedio Bajo de existencia de riesgo, el cual se representa con el color **Verde**.
- Del 11% al 15%: Promedio Medio de existencia de riesgo, el cual se representa con el color **Amarillo**.
- Del 16% al 20%: Promedio Alto de existencia de riesgo, el cual se representa con el color **Rojo**.

Tabla 20. Análisis de Riesgo Promedio de los Activos de Información de la Unidad Académica de Psicología UAZ

		Probabilidad de Amenaza			
		Criminalidad y Político	Sucesos de Origen Físico	Negligencia y Institucional	TOTAL
	Datos y Procesos Institucionales	13.17%	6.91%	20.30%	40.38%
Magnitud de Daño	Sistemas e Infraestructura Institucional	9.59%	8.48%	18.76%	36.83%
	Personal Administrativo	8.78%	0.0	14.01%	22.79%
	TOTAL	31.54%	15.39%	53.07%	100.00%

En este tenor, en la Tabla 20, se observa que, en general, hay un 13.17% de riesgo de que los *Datos y Procesos Institucionales* sufran algún ataque de *Criminalidad y Político*, lo que indica un nivel medio de riesgo para la institución. Así mismo, en esa

misma categoría o clasificación, se observa que respecto a que haya riesgos o amenazas relacionados con *sucesos de origen físico* hay un 6.19%, lo que indica que el riesgo es muy bajo, pero podrían aparecer en algún momento de la vida institución. Dentro de esa misma categoría también se observa el porcentaje relacionado con los riesgos de *Negligencia de usuarios y decisiones institucionales,* es de 20.30%, lo que indica que hay un riesgo alto de que sucedan este tipo de eventos, lo que sugiere que es donde hay que poner más atención respecto a esta categoría. Dentro de la categoría de activos relacionada con los *Sistemas e Infraestructura Institucional* observamos que, respecto a las amenazas relacionadas con la *Criminalidad y Motivación Política,* existe en promedio 9.59% de probabilidad que ocurran hechos de esta índole, lo que indica que es una probabilidad baja, aunque el riesgo ahí está latente. Dentro de esa misma categoría se observa que hay un 8.48% de que ocurran sucesos de origen físico en esa categoría de activos, lo que sugiere que el riesgo es bajo. Así mismo, dentro de la misma categoría en cuestión, se observa un porcentaje de 18.76% de que ocurran eventos relacionados a *Negligencia de usuarios y decisiones institucionales,* lo que indica un riesgo alto, dando la noción de que hay que poner atención en esa relación matricial. En cuanto a la categoría de *Personal Administrativo*, se observa que existe en promedio de 8.78% en relación a la amenaza de *Criminalidad y Motivación Política*, lo que indica que hay un riesgo bajo de ocurrencia. En esta misma categoría, en relación con la categoría de amenazas relacionadas con *sucesos de origen físico*, se observa que hay un 0%, lo que indica que el riesgo es inexistente, ya que, según lo que se analizó y respondió estas amenazas no ocurrirían en esta categoría de activos. Así mismo, dentro de esta misma categoría de activos, se observa que existe un 14.05% de probabilidad promedio de que ocurran eventos relacionados con la *Negligencia de usuarios y decisiones institucionales,* lo que indica que el riesgo es medio, y habría que ponerle atención.

Si bien se analizó cada una de la relación matricial entre las categorías de los activos de información y las categorías de amenazas entre cada una de éstas, es menester la explicación relacionada con los totales de cada una de éstas. En primera instancia, en los ejes verticales de la matriz, se observan los totales 40.38% en la

categoría de *Datos y Procesos Institucionales*, un 36.83% en la categoría de *Sistemas e Infraestructura Institucional* y un 22.79% en la categoría de *Personal Administrativo*, expuesto lo anterior, se pone de manifiesto que la categoría de *Personal de Personal Administrativo* tiene menor probabilidad promedio de riesgos, a comparación de la categoría de *Sistema e Infraestructura institucional* que tiene bajo promedio de riesgos y de la categoría de *Datos y Procesos Institucionales* que tiene un alto promedio de riesgos; así pues, con base a los resultados del análisis vertical de esta matriz, se observa que los activos de *Datos y procesos institucionales* son los a los que más atención hay que ponerles en cuestión de seguridad, y se tendrán que implementar inmediata y urgentemente políticas para mitigar los riesgos relacionados a esta categoría de activos, además de todo lo que involucre ese proceso. Así mismo, observamos en ese mismo eje que, dentro de la categoría de activos *de Sistemas e Infraestructura Institucional*, hay un riesgo medio, lo que indica también la necesidad de implementar con urgencia políticas que resguarden dichos activos, aunque esta necesidad yace en menor gravedad. Por último, en este mismo eje, se observa que la magnitud de riesgo es más baja en los activos correspondientes al *Personal Administrativos*, sin embargo, esto no significa que no se tengan que poner atención, ya que el riesgo sí existe, pero en menor grado; en esta lógica sólo hay que implementar medidas para evitar más riesgos y empezar a mitigar los posibles existentes. En el caso del otro eje de la matriz, correspondiente al horizontal, se puede observar que las amenazas relacionadas con la *Criminalidad y motivación Política*, se observa que existe un 31.54% de que éstos ocurran en cualquiera de las categorías de los activos de información, este porcentaje sugiere que hay un riesgo medio promedio, por lo tanto, hay que poner atención relevante en su mitigación y tratamiento. En cuanto a las amenazas relacionadas con los *Sucesos de origen físico,* se observa un riesgo promedio de ocurrencia bajo contando con el 15.39%, lo que sugiere que no debe haber una preocupación relevante en la ocurrencia de estas amenazas, pero hay que seguir medidas genéricas para evitarlas. Por último, situándonos en el mismo eje horizontal, encontramos la categoría de amenazas y riesgos en los cuales se tiene que poner mayor atención y énfasis para mitigarlos, misma que hace alusión

a aquellos que tienen que ver con la *Negligencia de usuarios y decisiones institucionales*, contando con 53.07%, indicando así que hay que centrar esfuerzos para mitigar este tipo de riesgos y evitarlos lo más antes posible.

Esta matriz otorgó un panorama más general de las políticas de seguridad de la información que la institución educativa requiere; a partir de esta misma matriz, se puede partir por priorizar los activos que se protegerán y los riesgos que se mitigarán, haciendo uso también de la matriz TVA que ya expuso con anterioridad para poder lograr una serie de medidas un poco más eficientes y útiles la protección de los activos de información del Área Administrativa de la Unidad Académica de Psicología de la Universidad Autónoma de Zacatecas. Así pues, el proceso que se siguió para crear la Políticas de Seguridad yace en el análisis de los porcentajes de cada una de las categorías, para posteriormente atender los "focos rojos" que se muestran en la Matriz TVA, tomando como punto de partida Políticas de Seguridad implementadas en otras empresas, pero adaptándolas a las necesidades particulares de la Unidad Académica de Psicologías obtenidas a través de este complejo proceso de Análisis de Riesgos de los activos de información de dicha institución.

4.6. Reducción de Riesgos: Propuesta de Políticas de Seguridad de la Información para la Unidad Académica de Psicología de la Universidad Autónoma de Zacatecas.

Siguiendo la metodología ya antes evocada de la ISO/IEC 27001, la que propone Erb (2009), De Freitas (2010) y otras instancias expertas en seguridad de la información, el último paso de una gestión y control adecuado de riesgos de la seguridad de la información, es precisamente la reducción de éstos. Una vez realizado el análisis de riesgos en los activos de información, fue sumamente importante tomar las acciones necesarias para contrarrestar dichas vulnerabilidades. Hay específicamente 3 formas y categorización de reducción de riesgos: medidas físicas/técnicas, personales y organizativas, sin embargo, la que compete en la presente investigación y constituye el punto neurálgico de ésta, hace alusión a las ***medidas organizativas***, específicamente en la creación o

implementación de normas, o políticas que el personal administrativo tiene que seguir para poder disminuir diversas vulnerabilidades.

El resultado final de un arduo trabajo de investigación basado en un Análisis de Riesgos de los activos de la información se resume en un documento en el cual se definen un conjunto de políticas y buenas prácticas de Seguridad de la información específicas para cada categoría que le compete proteger de los activos y amenazas identificadas dentro de la Unidad Académica de Psicología. Además del arduo proceso que conlleva un análisis de riesgos de los activos de la información, y tal como se menciona en la metodología de la presente investigación, se tuvieron que consultar algunas Políticas existentes para poder formar un criterio de estructura y recuperar algunas prácticas que puedan servir; en este tenor, se pudieron consultar las *Políticas Generales de Seguridad de la Información* del Banco Nacional de Obras y Servicios Públicos (2018), el *Manual de Políticas de Seguridad de la Información* de la Escuela Nacional de Ingeniería Julio Gavito (2018), el *Manual de Políticas de Seguridad y Privacidad de la Información* del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) del Gobierno de Colombia (2019) y otras recomendaciones de buenas prácticas y estándares que ayudaron para poder culminar las Políticas aquí propuestas. Así pues, en el documento se cubren los siguientes puntos de seguridad de la información:

- Organización de seguridad de la Información
- Gestión de los Activos de la Información
- Seguridad de los Datos y Procesos Institucionales
- Seguridad de Sistemas e Infraestructura Institucionales
- Seguridad del Personal Administrativo y del Recurso Humano
- Control de Acceso.
- Seguridad Física y Ambiental
- Gestión de incidentes de seguridad de la información
- Cumplimiento

Dentro de estos puntos importantes de Seguridad de la Información, se encuentran medidas relacionadas a políticas y buenas prácticas para cada uno de los activos que en la presente investigación se identificaron, recordando que se tomaron en

cuenta 39 activos de la información y 35 vulnerabilidades y amenazas en total. Así pues, se tiene que, en la ***Organización de seguridad de la Información***, se abordan acciones relacionadas con la organización Interna, dispositivos Móviles y Teletrabajo, roles y responsabilidades. Dentro del punto de ***Gestión de los Activos de Información*** se atienden acciones alusivas a la responsabilidad de los Activos de Información, clasificación de la Información, protección y Manejo de la Información, protección de Datos y manejo de Medios de Almacenamiento. Dentro de las ***Políticas de Seguridad para los Datos y Procesos Institucionales***, se encuentran las Políticas y Prácticas de Seguridad de las operaciones, Políticas y Prácticas de Seguridad para la Protección contra códigos maliciosos, Políticas y Prácticas de Seguridad de los Documentos Institucionales, Políticas y Prácticas de Seguridad de las Finanzas, Políticas y Prácticas de Seguridad de los procesos bancarios, Políticas y Prácticas de Seguridad en el uso de Correos Electrónicos, Políticas y Prácticas de Seguridad en el uso de Base de Datos internos, Políticas y Prácticas de Seguridad en el uso y configuración de Intranet, Políticas y Prácticas de Seguridad de Respaldos de la información, Políticas y Prácticas de Seguridad en procesos informáticos, Políticas y Prácticas de Seguridad en el uso y configuración de Contraseñas y Políticas y Prácticas de Seguridad en Página web de la Institución. Dentro de las ***Políticas de Seguridad en Sistemas e Infraestructura Institucionales***, se abordan las Políticas y Prácticas de Seguridad en la configuración y uso de Equipos de Red Cableada, Políticas y Prácticas de Seguridad en la configuración y uso de Equipos de Red inalámbrica, Políticas y Prácticas de Seguridad en la configuración y uso de Computadoras, Políticas y Prácticas de Seguridad en la configuración y uso de Portátiles, Políticas y Prácticas de Seguridad en el uso y configuración de sistemas administrativos (Tauro, siaaf, etc.) y Políticas y Prácticas de Seguridad en el uso y configuración de sistemas para eventos, servicio social, etc. Por último, pero no menos importante que los otros lineamientos, dentro de las ***Políticas de Seguridad del Personal Administrativo y del Recurso Humano***, están los puntos que abordan las Políticas y Buenas Prácticas en Direcciones y Coordinaciones, Políticas y Buenas Prácticas en procesos administrativos, y Políticas y Buenas Prácticas en procesos de Recepción;

todas estas consideran también el seguimiento de las demás Políticas, ya que, tal como se abordó en este trabajo, el ser humano es el principal eslabón de la Seguridad de la Información.

Dentro de cada uno de estos puntos de Seguridad de la Información, se desglosan una serie de Políticas y Buenas prácticas para proteger los activos que tengan que ver con cada uno de estos puntos y categorías, velando siempre por el resguardo de la confidencialidad, disponibilidad e integridad de todos los elementos esenciales de la Institución. En cada Política y Buena práctica se tratan de atender todos los riesgos predominantes en la matriz TVA de cada activo y categoría de activo, ofreciendo así una solución objetiva para poder mitigar y prevenir los posibles riesgos. Es importante señalar que la propuesta que aquí se plantea a través de las Políticas, también puede servirle a Docentes, alumnos y visitantes de la Unidad Académica de Psicología, aunque va orientado específicamente a los trabajadores Administrativos de la dicha Unidad. Dicho documento se puede ver completo en el **Anexo 11** de esta investigación.

CAPÍTULO V: DISCUSIÓN

En la presente investigación se utilizó un recorrido teórico y práctico de diferentes metodologías, investigaciones y resultados respecto al Análisis de Riesgos de los Activos de Información y la Creación de Políticas se Seguridad de la Información, tomando en cuenta todo lo que esto implica. Si bien, todas las investigaciones y propuestas que aquí se revisaron siguen un estándar basado en ISO/IEC 27001 en sus diferentes versiones, a partir de éstas se pudieron adaptar varios procesos significativamente sin perder la visión de los estándares y metodologías que ya están bien convenidas y establecidas. De Freitas (2009) y De Freitas (2010), utiliza una metodología bastante completa, en la cual expone la mayoría de los procesos que en esta tesis se detalla. Sin embargo, los activos de información que detalla en su investigación quedan cortos para el objeto de estudio que aquí se detalla; para contrarrestar esta limitante, se tuvo que hacer uso de la técnica de Rolling-Play, entrevista y búsqueda de información en los inventaros para poder recopilar toda la

información pertinente de la Unidad Académica de Psicología en cuanto a los activos de información se refiere. Este mismo autor maneja con claridad todos los términos y procesos que se deben seguir en una Gestión de Riesgos en general, sin embargo, por practicidad se pudieron optimizar algunos procesos en esta tesis, tales como los de tasación, el cálculo de la Magnitud de Daño y la simplificación de las preguntas de Escala Likert a una Encuesta que pudiera contestar el Coordinador Administrativo de esta Unidad, facilitando así la aplicación y cálculo de Riesgo. Otra investigación fundamental que sirvió para el desarrollo de esta tesis, fue el de la Metodología de Markus Erb (2009), en donde detalla adecuada y entendiblemente todo el proceso que se debe realizar para mitigar riesgos a través de un análisis de riesgos. La propuesta de Matriz que él realiza es en verdad muy basta, sin embargo, para fines prácticos, en una Universidad con las características de la propia Autonomía, se tienen que simplificar algunos procesos. Si bien, el mismo Erb propone herramientas en donde se automaticen los cálculos de riesgos, es más efectivo hacer algunos ajustes a esa matriz, y, sobre todo, a la matriz del riesgo promedio; todo ese proceso que está muy completo y basto sirvió para proponer la matriz de calor (TVA) y matriz de riesgo promedio que aquí se aborda. Sin duda alguna, las demás investigaciones también sustentaron el análisis y la propuesta teórica que aquí se plantea, ya que, a través del estado de la cuestión, se pudo corroborar que los riesgos y amenazas que existen a nivel global, también pueden existir en los objetos de estudio que se definan en cada investigación. Todas estas investigaciones en conjunto brindaron un panorama conceptual y estratégico más amplio, adoptando algunas técnicas y posturas, pero cambiando otras más para que surgiera una propuesta y perspectiva innovadora a través del producto final que emana de esta tesis. En cuanto al proceso de Creación de las Políticas de Seguridad en específico, se puede observar que las propuestas que tienen el Banco Nacional de Obras y Servicios Públicos (2018), la Escuela Nacional de Ingeniería Julio Gavito (2018) y Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) del Gobierno de Colombia (2019), son sumamente bastos, y éstos están apegados a versiones alusivas al ISO/IEC 27001; sin embargo, aunque tienen una estructura muy completa y bien establecida, en la

propuesta que aquí se plantea se especifican acciones concretas para cada uno de los activos de información, incorporando hábitos de mitigación de dichos riesgos. A diferencia de los Manuales y Políticas de las instituciones antes señaladas, las Políticas que emanan de esta Tesis va orientada a atender acciones con directrices más establecidas acorde al proceso que se siguió del análisis de riesgos aquí elaborado. En esta lógica, el producto aquí presentado tiene una visión más completa y específica relacionado a lo que aquí se buscó analizar, incorporando estructuras más integrales y con panoramas más amplios.

Si bien, la metodología que se aborda en la presente investigación cumple con los requisitos genéricos de un análisis de riesgos y creación de políticas a partir de éstos, es menester realizar mejoras para optimizar procesos, estrategias e inclusive resultados; se tiene que apostar por tener más certeza en las aplicaciones de las escalas aquí utilizadas e inclusive combinar un análisis meramente perceptivo con un análisis ya más pragmático y técnico. Sin embargo, la implementación de la metodología que aquí se siguió ayudó para comprobar la hipótesis aquí planteada. Efectivamente, el realizar un análisis de riesgos de los activos de la información, aunque es un proceso sumamente complejo, ayudó en su totalidad a crear la políticas de seguridad de la información que aquí se proponen; esta confirmación de hipótesis yace en el hecho de que el conocer los puntos más vulnerables en cuanto a riesgos y amenazas ya definidas en cada activo de información de una empresa o institución, brinda un panorama más objetivo y efectivo para establecer estrategias más específicas y orientadas a cada una de las problemáticas detectadas, en esta lógica, se comprueba contundentemente la hipótesis en mención.

CONCLUSIONES

El objetivo fundamental de esta tesis era abordar diversas estrategias, tanto teóricas, como conceptuales, alusivas a la implementación de Análisis de Riesgos

de los activos de información para que, a partir de este mismo, se propongan medidas objetivas para mitigar cualquier riesgo relacionado con la Seguridad de la Información siempre y cuando se hayan sido identificado.

En esta lógica, la aportación principal de esta tesis consistió en el diseño y creación de Políticas de Seguridad de la Información dirigido al Personal Administrativo de la Unidad Académica de Psicología de la Benemérita Universidad Autónoma de Zacatecas. Este proceso de creación no fue nada sencillo, ya que, como se pudo observar a lo largo de este trabajo, la seguridad de la información depende de muchos factores que debemos tomar en cuenta, entre los que destaca la incorporación de normas claras institucionales de una forma objetiva y estando seguros de que los riesgos que se quieren atacar en verdad existan desde una lógica perceptiva o inclusive técnica. Uno de los hallazgos primordiales que se resaltan en este trabajo fue el de identificar los principales riesgos y amenazas que ocurren dentro de la Unidad Académica de Psicología, mismas que se pudieron acentuar a través de un proceso de Rolling-Play, entrevistas y análisis de estándares que dan un panorama genérico respecto a este tema. Los resultados obtenidos a través de un proceso de identificación, tasación y valuación de riesgos, fueron los siguientes:

Existe un 13.17% de riesgo de que los *Datos y Procesos Institucionales* sufran algún ataque de *Criminalidad y Político*, lo que indica un nivel medio de riesgo para la institución. Así mismo, en esa misma categoría o clasificación, se observa que respecto a que haya riesgos o amenazas relacionados con *sucesos de origen físico* hay un 6.19%, lo que indica que el riesgo es muy bajo, pero podrían aparecer en algún momento de la vida institución. Dentro de esa misma categoría también se observa el porcentaje relacionado con los riesgos de *Negligencia de usuarios y decisiones institucionales,* es de 20.30%, lo que indica que hay un riesgo alto de que sucedan este tipo de eventos, lo que sugiere que es donde hay que poner más atención respecto a esta categoría. Dentro de la categoría de activos relacionada con los *Sistemas e Infraestructura Institucional* observamos que, respecto a las amenazas relacionadas con la *Criminalidad y Motivación Política,* existe en promedio 9.59% de probabilidad que ocurran hechos de esta índole, lo que indica

que es una probabilidad baja, aunque el riesgo ahí está latente. Dentro de esa misma categoría se observa que hay un 8.48% de que ocurran sucesos de origen físico en esa categoría de activos, lo que sugiere que el riesgo es bajo. Así mismo, dentro de la misma categoría en cuestión, se observa un porcentaje de 18.76% de que ocurran eventos relacionados a *Negligencia de usuarios y decisiones institucionales,* lo que indica un riesgo alto, dando la noción de que hay que poner atención en esa relación matricial. En cuanto a la categoría de *Personal Administrativo*, se observa que existe en promedio de 8.78% en relación a la amenaza de *Criminalidad y Motivación Política*, lo que indica que hay un riesgo bajo de ocurrencia. En esta misma categoría, en relación con la categoría de amenazas relacionadas con *sucesos de origen físico*, se observa que hay un 0%, lo que indica que el riesgo es inexistente, ya que, según lo que se analizó y respondió estas amenazas no ocurrirían en esta categoría de activos. Así mismo, dentro de esta misma categoría de activos, se observa que existe un 14.05% de probabilidad promedio de que ocurran eventos relacionados con la *Negligencia de usuarios y decisiones institucionales,* lo que indica que el riesgo es medio, y habría que ponerle atención.

A partir de saber los porcentajes de riesgos que yacen en cada una de las categorías tanto de activos como de amenazas de cada uno de estos activos, se pudo tomar una decisión para llevar a cabo, la creación de políticas de seguridad de la información en los puntos más vulnerables que se detallaron en esta investigación. El producto final, que yace en este documento, toma las siguientes medidas, abordando en cada una de estas, prácticas y políticas para cada uno de los activos que en esta tesis se proponen:

- Organización de seguridad de la Información
- Gestión de los Activos de la Información
- Seguridad de los Datos y Procesos Institucionales
- Seguridad de Sistemas e Infraestructura Institucionales
- Seguridad del Personal Administrativo y del Recurso Humano
- Control de Acceso.

- Seguridad Física y Ambiental
- Gestión de incidentes de seguridad de la información
- Cumplimiento

Sin duda alguna, el proceso que se siguió fue complicado, sin embargo, los resultados fueron los que se esperaron, y, en general, se pudieron responder las preguntas de investigación para poder confirmar la hipótesis que aquí se plantea.

RECOMENDACIONES

Dentro de este arduo trabajo de investigación se adecuaron algunas metodologías y acciones implementadas para el Análisis de Riegos de los Activos de Información, específicamente, dentro de la Unidad Académica de Psicología de la Universidad Autónoma de Zacatecas. Dentro de esta institución, la mayoría de la Unidades Académicas comparten muchas características en común, lo que abre la posibilidad de replicar la investigación que aquí se propone dentro de otras Unidades Académicas de la UAZ y así poder comparar su efectividad con respecto a los análisis y las Políticas que surgen de éste en cada Unidad Académica. Así mismo, esta investigación puede, inclusive, ir más allá; con la posibilidad de implementar las acciones y metodologías aquí propuestas en otras Universidades Públicas del País, adaptándolas y mejorándolas para poderlas estandarizar dentro de este contexto educativo.

Otra mejora importante que se puede realizar en la metodología que aquí se expone, es revaluar los riesgos y activos de información que se tomaron en cuenta para poder realizar el análisis de riesgos, considerando ahora, no solo el punto de vista perceptual del encargado de dichos activos, sino ahora ir más allá de ese análisis, en donde se pueden ir incluyendo otras metodologías de auditoría como el PenTesting o cualquier otro, lo que ayudará a tener un panorama más amplio de los riesgos a nivel físico, de red y de sistemas de información en general. A través de esta leve mejora metodológica, se pueden incluir más lineamientos técnicos dentro

de las Políticas de Seguridad de la información, y se podría ampliar también una perspectiva más objetiva en cuanto a los riesgos que se puedan incorporar o excluir en la matriz TVA o de calor que ayuda a explicar las contingencias, vulnerabilidades o riesgos en los que se encuentran las herramientas tecnológicas, humanas y de procesos de la institución que será el objeto de estudio.

REFERENCIAS

Academia Latinoamericana de Seguridad Informática. Introducción a la Seguridad de la Información. ALSI. Recuperado de http://www.elmayorportaldegerencia.com/Documentos/TICs/[PD]%20Documentos%20-%20Seguridad%20informatica%20introduccion.pdf

Altamirano Yupanqui, J.R. & Bayona Oré, S. (2017). Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, (25), 112-134.

ANUIES. (2016). Estado Actual de las Tecnologías de la Información y la Comunicación en las Instituciones de Educación Superior de México, Estudio 2016. ANUIES-TIC. ANUIES-TIC.

ANUIES. (2019). Estado Actual de las Tecnologías de la Información y la Comunicación en las Instituciones de Educación Superior de México, Estudio 2019. ANUIES-TIC. ANUIES-TIC.

Bejarano Macías, A. R., & Alarcón López, F. E. (2007). *Teoría de la Acción Razonada: Evaluación de las actitudes, norma subjetiva e intención de compra en la industria de supermercados de la ciudad de Guayaquil* (Ingeniero). Escuela Superior Politécnica el Litoral.

Banco Nacional de Obras y Servicios Públicos. (2018). Políticas Generales de la Información. Ciudad de México, México.: BanObras. Recuperado de https://transparencia.banobras.gob.mx/wp-content/uploads/2018/07/Pol%C3%ADticas-Generales-de-Seguridad-de-la-Informaci%C3%B3n.pdf

Bello, A. (2019). "México no avanza a la velocidad necesaria en ciberseguridad". Expansión. Recuperado de https://expansion.mx/empresas/2019/10/25/mexico-no-avanza-a-la-velocidad-necesaria-en-ciberseguridad

Borghello, C. F. (2012). Seguridad Informática: Sus Implicancias e Implementación. Universidad Tecnológica Nacional.

Cavalcanti, G. A. D. (2012). Sistema para el Análisis y Gestión de Riesgos.Universidad Ricardo Palma, Facultad de Ingeniería, Escuela Profesional de Ingeniería Informática. Lima, Perú.

Cano Pita, G. (2018). Las TICs en las empresas: evolución de la tecnología y cambio estructural en las organizaciones. Domino De Las Ciencias, (2477-8818).

Chávez, G. (2013). México paga costos millonarios a causa del 'malware', según un reporte. Expansión. Recuperado de https://expansion.mx/tecnologia/2013/10/14/mexico-paga-costos-millonarios-a-causa-del-malware-segun-un-reporte

Chávez, G. (2014). México, 'en pañales' en ciberseguridad. Expansión. Recuperado de https://expansion.mx/tecnologia/2014/05/13/mexico-lejos-del-promedio-en-seguridad

CHIAVENATO, I. (2009). Comportamiento organizacional: La dinámica del éxito en las organizaciones (2.ª ed., p. 5-40). MCGrawHill. MCGrawHill.

CISCO. (2019). Correo electrónico: haga clic con precaución. Cómo protegerse contra la

suplantación de identidad, el fraude y otras estafas (pp. 5–22). CISCO. Recuperado de https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/email-security-spa-final-version.pdf

Committee on National Security Systems. (2010). National Information Assurance (IA):Glossary. 4009: CNSS. 4009: CNSS.

Coordinación de Infraestructura de la Universidad Autónoma de Zacatecas. (2017). *Informe de activos fijos de la U.A. de Psicología Plantel Zacatecas*. Zacatecas, México: UAZ. Zacatecas, México: UAZ.

De Freitas, V. (2010). Propuesta de metodología de gestión de seguridad de las TIC's para el sector universitario venezolano. Espacios, (31). Recuperado de https://www.revistaespacios.com/a10v31n01/10310152.html

De Freitas, V. (2009). Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. Enl@ce: Revista Venezolana de Información, Tecnología y Conocimiento, 6 (1), 43-55
De Freitas, V. (2010). Propuesta de metodología de gestión de seguridad de las TIC's para el sector universitario venezolano. Espacios, (31). Recuperado de https://www.revistaespacios.com/a10v31n01/10310152.html

De Haas Matamoros, M. (2019). #ColumnaInvitada | Regulación de la ciberseguridad, un tema urgente. Expansión. Recuperado de https://politica.expansion.mx/voces/2020/02/27/regulacion-de-la-ciberseguridad-tema-urgente

DELL, T. (2011). Son incalculables los riesgos de seguridad originados por amenazas internas. Recuperado 6 de abril de 2020, de DELL TECHNOLOGIES website: https://corporate.delltechnologies.com/es-ar/newsroom/announcements/2007/12/12232007.htm

Düque Méndez, N. D. (s.f.). *DISEÑO EIMPLEMENTACIÓN DE UNA POLÍTICA DE SEGURIDAD*. Recuperado de http://bdigital.unal.edu.co/58108/1/dise%C3%B1oeimplementaciondeunapoliticadeseguridad.pdf

Erb, M. (2010). Análisis de Riesgo. Recuperado 10 de abril de 2020, de Gestión de Riesgo en la Seguridad Informática website: https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

Erb, M. (2011). Matriz para el Análisis de Riesgo. Recuperado 10 de abril de 2020, de Gestión de Riesgo en la Seguridad Informática website: https://protejete.wordpress.com/gdr_principal/matriz_riesgo/

Flores Hine, C. (2010). ¡Pongámonos las Pilas! Reflexiones y acciones concretas para asegurar la información en nuestras organizaciones sociales (2.ª ed., pp. 32–42). Creative Communs. Creative Communs.

Escuela Colombiana de Ingeniería Julio Gavito. (2018). Manual de Políticas - Seguridad y Privacidad de la Información. Bogotá Colombia: ECIJG. Recuperado de https://www.escuelaing.edu.co/escuela/importantDoc/Manual-politica-seguridad-dela-Informacion.pdf

FORBES, S. (2018). Las universidades, tercer destino de ciberataques en RD. FORBES MÉXICO. Recuperado de https://www.forbes.com.mx/las-universidades-terOcer-destino-de-ciberataques-en-rd/

FUNIBER, F. U. I. (2020). Las universidades no se libran de los ciberataques. Recuperado 7 de abril de 2020, de FUNIBLOGS website: https://blogs.funiber.org/tecnologias-informacion/2019/10/23/funiber-universidades-ciberataques

Gandaria, M. (2019). Instalarán laboratorios de ciberseguridad para vigilar red pública de internet. El Sol De Zacatecas. Recuperado de

https://www.elsoldezacatecas.com.mx/mexico/justicia/instalaran-laboratorios-de-ciberseguridad-para-vigilar-red-publica-de-internet-deep-web-policia-federal-operativo-semana-santa-2019-3311691.html

González Tabares, E. (2018). . Esta norma hereda muchos conceptos de la serie de normas ISO 9000 y subraya la seguridad entendida como proces (Maestro). Universidad Nacional ABierta y a Distancia - UNAD, Medellín.

Instituto Nacional de Ciberseguridad (INCIBE). PROTECCIÓN DE LA INFORMACIÓN. Ministerio de Asuntos Económicos y Transformación Digital de España. Recuperado de https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf#page=32&zoom=100,0,0

ISO/IEC:27001. (2013). Estándar Internacional ISO/IEC 27001. ISO/IEC. ISO/IEC.

Laboratorio de Redes y Seguridad de la UNAM (2014). Esquemas de Seguridad Informática. Ciudad de México, México: Seguridad Informática.

Recuperado el 15 de septiembre de 2017 de: http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/AnalisisRiesgos.php

Ledesma Cristina, L. A. y P. M. (2014). Ingeniería social – El hackeo al ser humano. Un enfoque holístico | Magazcitum. Retrieved from http://www.magazcitum.com.mx/?p=2747B

Lozares, C., López Roldán, P., Miquel Verd, J., Martí, J., & Luis Molin, J. (2011). Cohesión, Vinculación e Integración sociales en el marco del Capital Social. *REDES- Revista Hispana Para El análisis De Redes Sociales* , (20).

Lubeck, L. (2019). Recuperado 7 de abril de 2020, de welivesecurity by ESET website: https://www.welivesecurity.com/la-es/2019/07/17/amenazas-informaticas-mas-impacto-trimestre-abril-junio-2019/

Malvido, G. (2010). La policía detecta ataques informáticos desde servidores de la Universidad todos los meses. Recuperado 10 de abril de 2020, de La Opinión A Coruña website: https://www.laopinioncoruna.es/coruna/2010/04/11/policia-detecta-ataques-informaticos-servidores-universidad-meses/374203.html

Mantilla Guerra, A. R. (2018). Gestión de seguridad de la información con la norma ISO 27001:2013. Espacios, (18 Vol 39). Recuperado de https://www.revistaespacios.com/a18v39n18/a18v39n18p05.pdf

Mendoza, J. C., Jalpilla, J. R., Ramírez M. E., M., Olguín R. H,. (2016). UNA METODOLOGÍA DE ANÁLISIS Y EVALUACIÓN DE RIESGOS EN TECNOLOGÍAS DE INFORMACIÓN (Tesis de Pregado). Universidad Nacional Autónoma de México, Ciudad Universitaria, México, Cuidad de México.

Mendiola Zuriarrain, J. (2016). Dropbox reconoce el 'hackeo' de 60 millones de cuentas: cómo saber si la tuya está afectada. El País. Recuperado de https://elpais.com/tecnologia/2016/08/31/actualidad/1472642567_500051.html

Medina Iriarte, J. (2006). ESTANDARES PARA LA SEGURIDAD DE INFORMACIÓN CON TECNOLOGIAS DE INFORMACIÓN (Maestría). UNIVERSIDAD DE CHILE

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2019). Manual de Políticas de Seguridad y Privacidad de la Información. Colombia: Gobierno de Colombia. Recuperado de https://www.mintic.gov.co/portal/604/articles-1516_manual_seguridad_informacion_20190501.pdf

Moreno Zamudio, T. de J., Tarango Rodríguez, J. A., & Correa Venegas, J. M. (2020). LA INGENIERÍA SOCIAL: UN FENÓMENO LATENTE EN SOCIEDADES CARENTES DE CONCIENTIZACIÓN SOBRE EL USO DEL INTERNET Y LAS TECNOLOGÍAS DE

LA INFORMACIÓN. En *La Humanidad frente a los desafíos del capitalismo decadente* (1.ª ed.). Zacatecas, México: Taberna Libraria. Zacatecas, México: Taberna Libraria.

Moreno Zamudio, T. de J., Villagrana Barraza, S., Castañeda Ramírez, C. H., Ortiz Esquivel, D. I., Ortiz Romero , V. M., & Olvera Olvera, C. A. (2018). PERCEPCIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN TRABAJADORES ADMINISTRATIVOS DE LOS PROGRAMAS DE PSICOLOGÍA E INGENIERÍA EN COMPUTACIÓN DE LA UNIVERSIDAD AUTÓNOMA DE ZACATECAS. *Compendio Investigativo De Academia Journals Celaya 2018*, (978-1-939982-42-1).

Nimnicht, M. (2019). Encuesta de McAfee descubre que estudiantes universitarios ponen en peligro la información personal. Recuperado 7 de abril de 2020, de McAfee website: https://www.mcafee.com/enterprise/en-gb/about/newsroom/press-releases/press-release.html?news_id=20190813005021

PandaSecurity, N. (2014). eBay pide cambiar las contraseñas tras un posible ataque de seguridad. Recuperado 7 de abril de 2020, de PandaSecurity Media Center website: https://www.pandasecurity.com/spain/mediacenter/noticias/ebay-ataque-seguridad-cambia-contrasenas/

PandaSecurity, P. (2014). Los ataques de seguridad más importantes de 2014 – 2ª parte. Recuperado 7 de abril de 2020, de PandaSecurity Media Center website: https://www.pandasecurity.com/spain/mediacenter/seguridad/otros-ataques-informaticos-2014/

Restrepo Rivas, L. G. (2005). Las Tecnologías de la Información y las Comunicaciones en la Empresa. Medellín Colombia. Recuperado de http://luisguillermo.com/TIC.pdf

Rivera Ledesma, E. M. (s.f). Estándares para la seguridad de la información. (1.ª ed.). SENA. Recuperado de https://es.slideshare.net/domaty/estandares-de-seguridad-108713992

Obando Jaramillo, V. (2015). Universidades, víctimas de “hackers”. El Espectador. Recuperado de https://www.elespectador.com/noticias/judicial/universidades-victimas-de-hackers-articulo-560884

VARGAS MELGAREJO, L. M. (1994). Sobre el concepto de percepción. *Alteridades [en línea]*, (0188-7017). Recuperado de http://www.redalyc.org/articulo.oa?id=74711353004

Vega Velasco, Walter. (2008). POLITICAS Y SEGURIDAD DE LA INFORMACION. Fides et Ratio - Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia, 2(2), 63-69. Recuperado en 05 de abril de 2020, de http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008&lng=es&tlng=es.

Vieites, A. G. (2015). DIRECTRICES PARA LA DEFINICION E IMPLANTACION DE POLITICAS DE SEGURIDAD. Caixanova: Escuela de Negocios Caixanova.

UAZ. (2018). NUMERALIAS UAZ. Recuperado 7 de abril de 2020, de Numeralia UAZ 2016-2018 website: http://numeralia.uaz.edu.mx/

UAZ (s.f.). Organigrama de la Unidad Académica de Psicología UAZ. Recuperado 25 de abril de 2020, de Página Oficial de la Unidad Académica de Psicología website: http://psicologia.uaz.edu.mx/organigrama

APÉNDICES

Anexo 1. BREVE ESCALA PARA TASACIÓN Y PROBABILIDAD DE OCURRENCIA DE AMENAZAS EN ACTIVOS DE LA INFORMACIÓN DE UNIVERSIDADES PÚBLICAS (RESPONDIDO).

BREVE ESCALA PARA TASACIÓN Y PROBABILIDAD DE OCURRENCIA DE AMENAZAS EN ACTIVOS DE LA INFORMACIÓN DE UNIVERSIDADES PÚBLICAS

Universidad: Universidad Autónoma de Zacatecas

Unidad Académica o Facultad: Unidad Académica de Psicología

Puesto organizacional del encargado de los Activos de Información o de quien responde este instrumento: Coordinador Administrativo

El siguiente instrumento busca medir, en primera instancia, la prioridad que usted considera en cuanto confidencialidad, disponibilidad e integridad de los activos de información que usted tiene en su institución educativa. Posteriormente, se medirán la probabilidad de ocurrencia de las amenazas que aquí se le muestran. En ambas situaciones, se utiliza una escala de Likert, con la finalidad de que usted otorgue el valor correspondiente según su experiencia laboral. Le las instrucciones en cada escala.

ESCALA PARA TASACIÓN DE ACTIVOS

La siguiente escala presenta una clasificación de sus activos de información. Tendrá que llenar cada uno de estos activos contestando las siguientes preguntas:

Para el recuadro "Confidencialidad": ¿Qué importancia tiene para usted que el activo de información tenga la capacidad de confidencialidad dentro la organización, área, departamento o dirección?

Para el recuadro "Disponibilidad": ¿Qué importancia tiene para usted que el activo de información tenga la capacidad de Disponibilidad dentro de la organización, área, departamento o dirección?

Para el recuadro "Integridad": ¿Qué importancia tiene para usted que el activo de información tenga la capacidad de Integridad dentro de la organización, área, departamento o dirección?

Responder con los siguientes valores:

1: Nada importante

2: Poco importante

3: Mediadamente importante

4: Altamente importante

5: Demasiado importante

Ejemplo para el primer activo de información:

¿Qué importancia tiene para usted que los **Documentos institucionales (¿Proyectos, Planes, Evaluaciones, Informes, etc.** tengan la capacidad de **confidencialidad** dentro la organización, área, departamento o dirección**?**

Si para usted es demasiado importante que este activo tenga la capacidad de confidencialidad dentro de su institución tendrá que poner el valor de 5 en el recuadro de Confidencialidad. Y así para cada uno de los recuadros y activos. Se hace la misma pregunta (Sólo cambiando Confidencialidad, integridad o disponibilidad) para cada reactivo. El recuadro de "Total", dejarlo vacío.

Definiciones de cada dimensión de la Seguridad de la Información

Si usted no conoce qué significa confidencialidad, disponibilidad o integridad de la información, aquí se describen brevemente cada una de estas dimensiones:

Confidencialidad: Implica que la información es accesible únicamente por el personal autorizado. Se hace referencia a que la información solo debe ponerse en conocimiento de las personas, entidades o sistemas autorizados para su acceso. Un claro ejemplo de información que requieren confidencialidad son aquellos sistemas o accesos que necesitan alguna contraseña,

Integridad: Mantener la información sin alteraciones, y, por ende, mantener su valor original de cualquier índole. En esta lógica, cualquiera que tenga acceso a esta información, debe tener la certeza de que al consultarla contendrá los valores originales y que no ha sido alterada de alguna forma que pueda vulnerar la funcionalidad institucional.

Disponibilidad: Permite que la información pueda estar disponible cuando sea necesaria. Hace alusión al acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Clasificación de Activo	**ACTIVO**	**TASACIÓN**			
		Confidencialidad	**Integridad**	**Disponibilidad**	**TOTAL**
DATOS Y PROCESOS INSTITUCIONALES	Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.	5	5	5	
	Finanzas				
	Servicios bancarios	5	5	5	
	Directorio de Contactos	3	3	4	

	Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	4	4	4	
	Correo electrónico	3	4	4	
	Bases de datos internos	4	4	4	
	Página Web interna (Intranet)	4	4	4	
	Página Web externa	4	4	4	
	Respaldos	5	5	4	
	Infraestructura (Planes, Documentación, etc.)	5	5	5	
	Informática (Planes, Documentación, etc.)	4	4	4	
	Base de datos de Contraseñas	4	4	4	
	Navegación en Internet	4	4	4	
	Chat	3	3	3	
	Llamadas telefónicas internas	4	4	4	
	Llamadas telefónicas externas	4	4	4	
SISTEMAS INSTITUCIONALES	Equipos de la red cableada (router, switch,etc.)	5	5	5	
	Equipos de la red inalámbrica (router, punto de acceso, etc.)	5	5	5	
	Servidores	5	5	5	
	Computadoras	5	5	5	
	Portátiles	4	4	4	

	Software de administración (contabilidad, manejo de personal, etc.)	5	5	5	
	Software de Servicio Social, Congresos, etc.	4	4	4	
	Software de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	4	4	4	
	Impresoras	4	4	4	
	Memorias portátiles	4	4	4	
	Celulares	3	3	3	
	Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	4	4	4	
	Vehículos	4	4	4	
PERSONAL ADMINISTRATIVO	Consejo de Unidad	4	4	4	
	Dirección / Coordinación	5	5	5	
	Administración	5	5	5	
	Personal técnico	5	5	5	
	Recepción	5	5	5	
	Piloto / conductor	4	4	4	
	Informática / Soporte técnico interno	4	4	4	
	Soporte técnico externo	4	4	4	
	Servicio de limpieza	4	4	4	

Por favor, continúe a la siguiente página para llenar la *Escala relacionada a la Probabilidad de Ocurrencia de Amenas en los Activos de Información de su institución*

ESCALA DE PROBABILIDAD DE AMENAZA POR CADA ACTIVO DE INFORMACIÓN DE LA INSTITUCIÓN

A continuación, se presentan un instrumento que permite valorar la Probabilidad de amenaza que podrían tener sus activos de información. Se observa entonces, del lado izquierdo de la tabla, todos los activos relacionados con los Datos Institucionales, los Sistemas institucionales y el Personal Administrativo. Así mismo, del lado derecho se encuentran todas las posibles amenazas que podría tener ese mismo activo. También verá una columna titulada "Magnitud de Daño", que significa la relevancia que tiene si alguno de esos activos fuera dañado, hackeado o perdido.
Para determinar la ***probabilidad de amenaza***, apóyese de la siguiente pregunta principal:

¿Cuál es la probabilidad de que ocurra dicha amenaza en los activos de información de su institución educativa?

También podría usted considerar otro tipo de preguntas según sea el activo de información que esté evaluando, pero jamás perdiendo de vista la pregunta principal: ¿Cuál es el interés o la atracción por parte de individuos externos, de atacar la institución? ¿El activo es vulnerable ante esa amenaza?, ¿Cuántas veces ha sucedido ese hecho?
Para responder, anote en cada uno de los recuadros el número correspondiente a la respuesta que usted vea más conveniente de la siguiente tabla:

No.	Respuesta	Descripción
1	Nula posibilidad	No existen condiciones para que suceda un ataque, daño o perdida de ese activo
2	Poco probable	Pudiera que se dé un ataque, daño o perdida al activo, pero es una posibilidad lejana.
3	Medianamente probable	Hay posibilidades de que se dé un ataque, daño o pérdida del activo, y hay condiciones para que suceda.
4	Altamente probable	La posibilidad de que se dé un ataque, daño o pérdida del activo es inevitable, no existen condiciones para protegerlo, y pudiera que se haya dado ya.

Ahora bien, para determinar la ***Magnitud de Daño***, apóyese en la siguiente pregunta y posibles respuestas:

¿Qué impacto tendría su institución si ese activo se pierde, se daña o es hackeado?

No	Respuesta	Descripción
1	Nulo impacto	No afecta las funciones, ya que no causa relevancia la pérdida o daño de ese activo
2	Poco impacto	Las funciones se ven afectadas, sin embargo, la institución se recuperará pronto
3	Mediano Impacto	La institución no podría seguir funcionando, pero habría otras alternativas costosas.
4	Alto impacto	Imposible que la institución funcione si se daña, pierde o hackea ese activo.

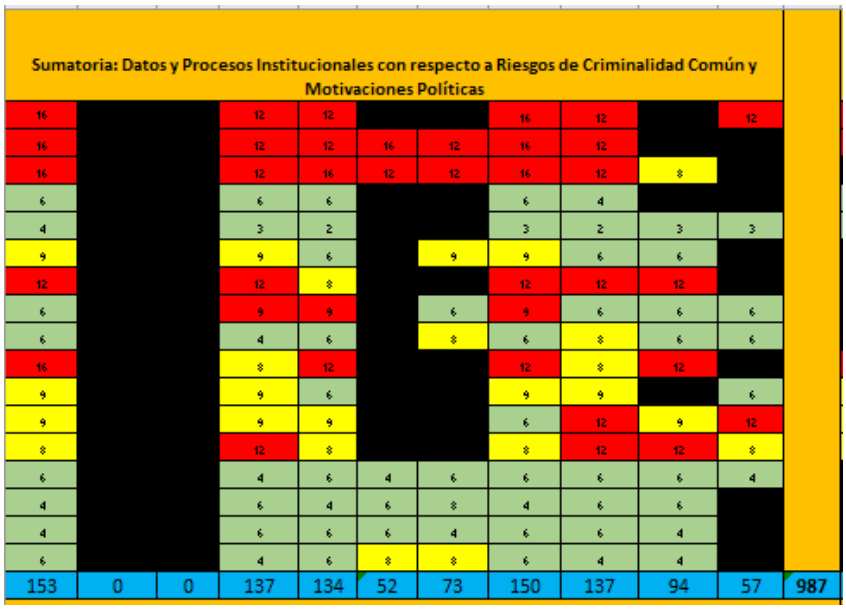
		PROBABILIDAD DE OCURRENCIA DE LA AMENAZA																																
	MD	Criminalidad común y motivación política											Sucesos físicos							Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales																
MAGNITUD DE DAÑO		Acceso no autorizado	Persecución (Civil, fiscal o penal)	Orden de secuestro/Detención	Ataque físico o electrónico	Daños por vandalismo	Fraude/Estafa	Extorsión	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Virus / Ejecución no autorizado de programas	Violación a derechos de autor	Incendio	Inundación / deslave	Sismo	Falta de ventilación	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro	Falta de capacitación sobre riesgos	Mal maneio de sistemas y herramientas	Utilización de software 'pirateado	Falta de conocimiento de software nuevo	Perdida de datos	Infección de sistemas a través de USB	Tener Unidades portables con información	Compartir contraseñas o permisos a terceros	Extravío de equipo, (USBS, lap, compu)	Sobrepasar autoridades	Falta restricciones del personal	Falta de mantenimiento físico	Falta de actualización de software	Fallas en permisos de usuarios (acceso a	Accesos no autorizados a Sistemas	Falta de normas y reglas claras	Ausencia de documentación	**OCURRENCIA PROMEDIO POR ACTIVO**
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.		4			3	3			4	3		3	3	2	1					2				2				3		3	3		3		3	3	
Finanzas		4			3	3	4	3	4	3			3	3	2				3	4	3		2	2	3		2	3		3	3	3	2	2	3	3	
Servicios bancarios		4			3	4	3	3	4	3	2				3		3	3	3	3	3		3	3	4		3	4		3	2	2	3	3	3	3	
Directorio de Contactos		3			3	3			3	2			3	3	3									3				3		2			3		3	3	
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)		4			3	2			3	2	3	3	2	3	3					3	3			2	3			3		2	3		3		2	3	
Correo electrónico		3			3	2		3	3	2	2				2			3	3		3			3	3		2			2	3	3	3	2	2	3	
Bases de datos internos		3			3	2			3	3	3				2		3	3	2	2	3		3	3	2	2		3		2	2	3	3	2	2	2	

Página Web interna (Intranet)		2			3	3		2	3	2	2	2			3		2	3	2		2	3	2	3	3		3			2	2	3	2	3	2	3		
Página Web externa		3			2	3		4	3	4	3	3			2			3	3			3	2	3	3		2			2	3	3	3	3	3	2		
Respaldos		4			2	3			3	2	3		3	3	3		2	3	2		3		2	2	3	3	3	2		3	2	3	2	2	3	2		
Infraestructura (Planes, Documentación, etc.)		3			3	2			3	3		2	3	3	2			4			4		3	3	2			2		3	3		3		3	2		
Informática (Planes, Documentación, etc.)		3			3	3			2	4	3	4	3	2	3	2		3	3	4	4		2	2	3			3		3	2	2	3	3	2	2		
Base de datos de Contraseñas		2			3	2			2	3	3	2	2	3	3	2	2	2	2	3	3		3	3	2	2	2	3		2	3	3	2	2	3	3		
Navegación en Internet		3			2	3	2	3	3	3	3	2			3			4			2		3	3	2		2			3		2	3	3	2	2		
Chat		2			3	2	3	4	2	3	3				3			4	3		2		2		2		2			3		2	3	2	3	3		
Llamadas telefónicas internas		2			3	2	3	2	3	3	2				2			3			2						3			2			2	3	3	3		
Llamadas telefónicas externas		3			2	3	4	4	3	2	2				2			3			2						3			2			3	2	3	1		
Equipos de la red cableada (router, switch,etc.)		3			2	3			3	3	3		4	3	2	3	3	2	4	3	3		2	2	3		3	3		2	3	3	3	2	2	3		
Equipos de la red inalámbrica (router, punto de acceso, etc.)		4			3	3			2	3	3		3	3	2	3	2	2	3	3	2		3	3	2		4	4		2	2	3	2	1	2	3		
Servidores		3			2	3			2	3	1		4	3	2	3	2	2	3	2	3		2	3	3		3	2		3	3	3	2	3	1	3		
Computadoras		3			2	3		3	2	2	3		2	3	1	2	3	2	3	2	3	3	3	2	3		2	1		3	2	1	3	2	3	3		

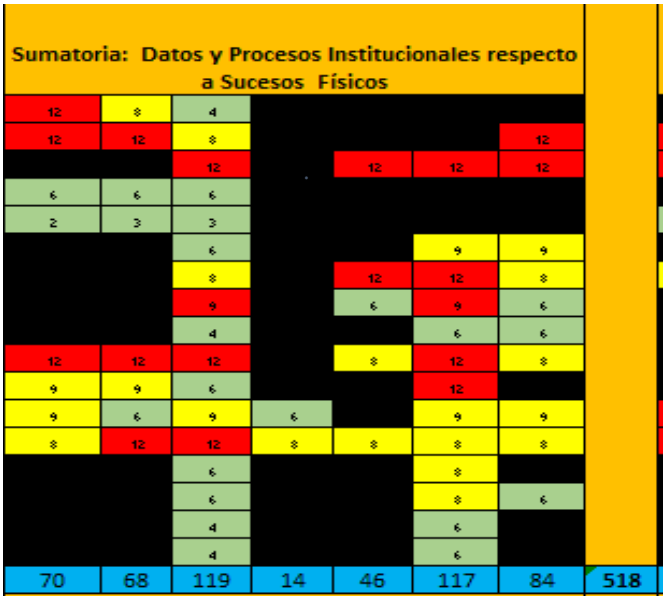
Portátiles		3			3	2		3	3	2	3		2	3	2	3	2	3	1	2	3	2	3	3	3		2	3		1	2	2	3	4	3	3	
Software de administración (contabilidad, manejo de personal, etc.)		2			3	3			2	3	3	3	3	2	2	3	3	2	2	3	3	2	3	2			2	3		3	2	3	3	3	2	2	
Software de Servicio Social, Congresos, etc.		2			3	2	3		3	2	3	2			2	3	2	3	3	3	3	2	2	3			3	2		2	2	3	3	3	2	3	
Software de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)		3			2	3	2	2	3	3	3	2			3	2	3	2	3	2	3	2	2	3			2	2		3	2	3	3	3	2	2	
Impresoras		3			2	3	3		2	2	3		2	3	2	3	2	3		3	3		2	2			2	2		3	3	3	2	2	2	3	
Memorias portátiles		3			2	2			3	2	2		2	3	2		3	3			3			2	2	4		3		3	2	3	2	3	3	3	
Celulares		3			2	3	2	3	2	2	2		3	3	3		3			3	3	3	3	2	4		3	3		3	2	3	2	3	2	3	
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)		4			3	3			3	3			2	3	3	2	3			3	2	2		3				3		3	2	3	3	3	2	2	
Vehículos		3			4	3			3	2			3	2	3	3	2			2	3							3		2	3		2		3	2	
Consejo de Unidad		3	4	3	3	2	3	2	3	3										3	2	3	2	2	3	3	2	2		3		2	3	3	3	2	
Dirección / Coordinación		3	4	3	2	3	2	3	2	2										2	3	2	3	2	3	2	3	3		3		2	3	2	2	3	
Administración		4	4	3	3	2	3	4	3	3										3	2	3	2	3	3	3	2	3		2		3	2	3	3	3	
Personal técnico		4	3	3	4	3	2	3	3	3										3	2	3	2	3	2	3	3	1		3		3	2	3	2	2	
Recepción		3	3	2	2	3	3	2	3	2										2	3	2	3	2	3	3	3	2		3		2	2	2	3	3	

Piloto / conductor		3	3	2	3	2	3	2	2	2		3	2	3	3	3	3	2	3	1		2		3	3	2	2	1	
Informática / Soporte técnico interno		3	4	3	2	2	3	2	3	3		3	2	3	2	3	2	3	3	3		2		3	2	2	2	2	
Soporte técnico externo		3	3	3	3	2	2	3	2	3		3	3	3	3	3	2	3	2	2		2		3	3	2	1	3	
Servicio de limpieza		3	3	3	3	3	2	2	3	2		2	2	2	3		3	3	2	2		3		3	3	2	2	1	

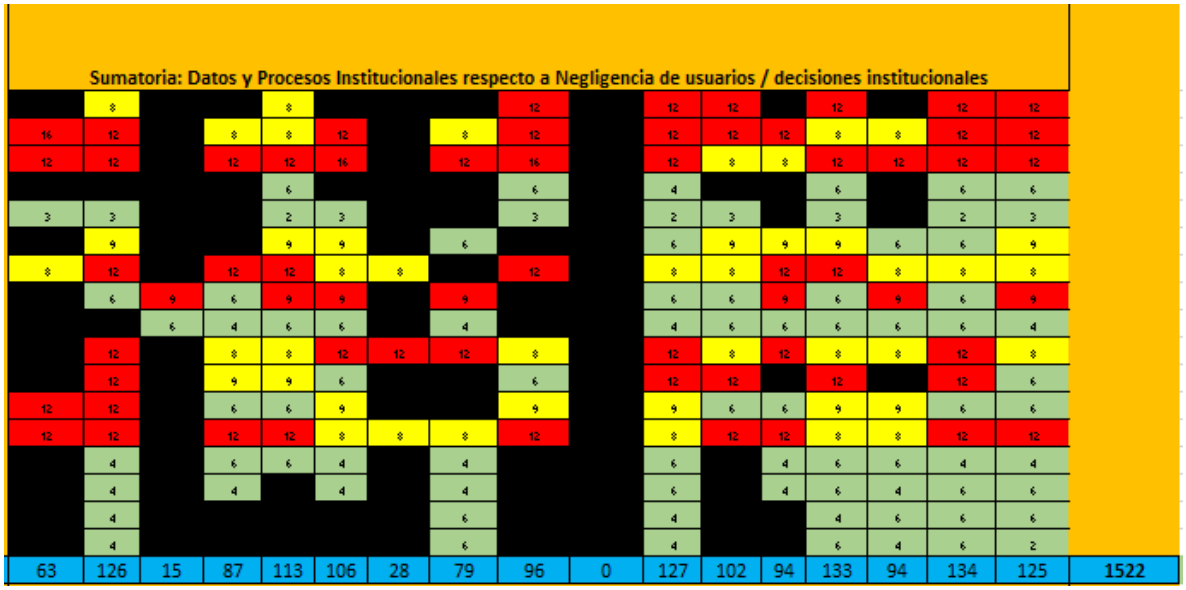
Anexo 2. Sumatoria y Promedio de los Datos y Procesos Institucionales respecto a los Riesgos de Criminalidad Común y Motivaciones Políticas dentro de la Unidad Académica de Psicología de la UAZ.



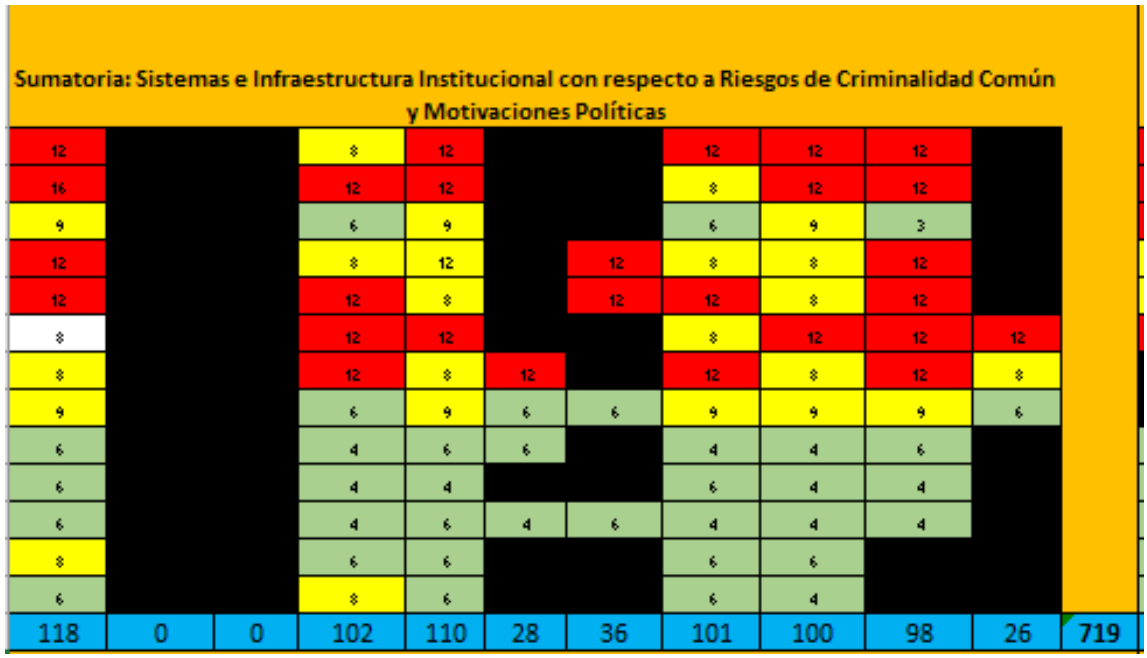
Anexo 3. Sumatoria y promedio de los Datos y Procesos Institucionales respecto a Sucesos Físicos dentro de la Unidad Académica de Psicología de la UAZ.



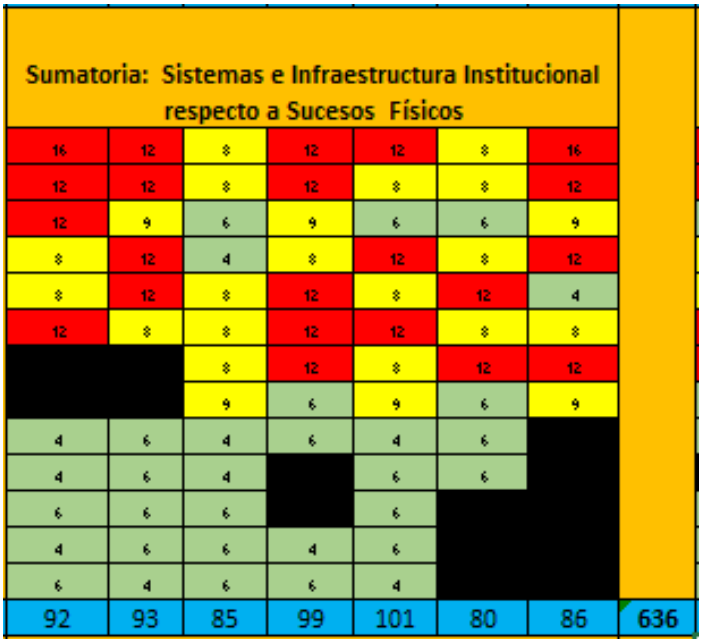
Anexo 4. Sumatoria y promedio de los Datos y Procesos Institucionales respecto a Negligencia de usuarios / decisiones institucionales dentro de la Unidad Académica de Psicología de la UAZ.



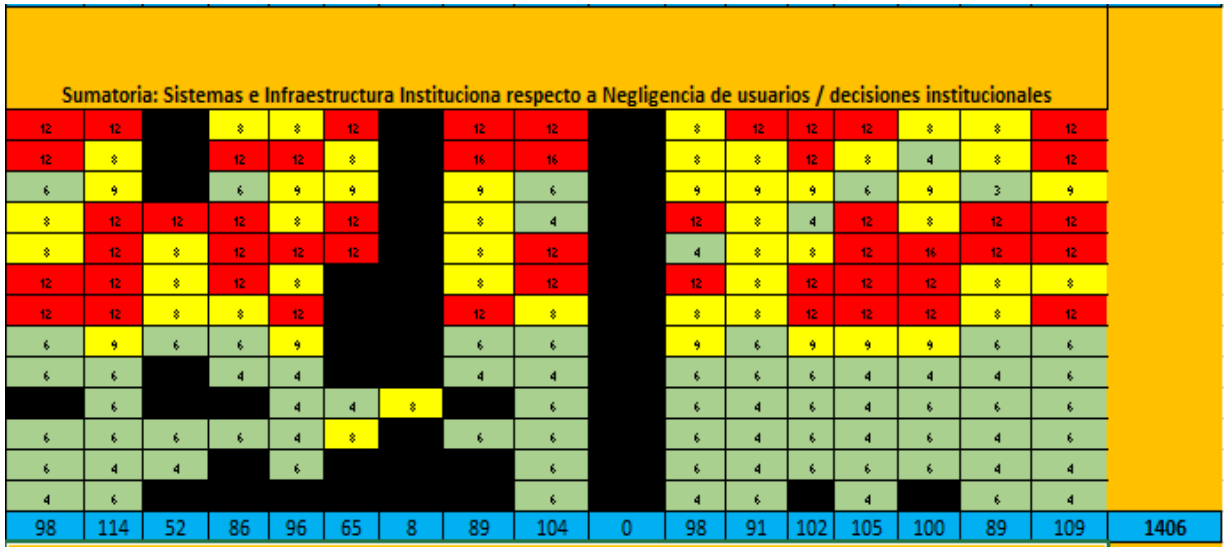
Anexo 5. Sumatoria y promedio de los Sistemas e Infraestructura Institucional con respecto a Riesgos de Criminalidad Común y Motivaciones Políticas dentro de la Unidad Académica de Psicología de la UAZ.



Anexo 6. Sumatoria y promedio de los Sistemas e Infraestructura Institucional respecto a Sucesos Físicos dentro de la Unidad Académica de Psicología de la UAZ.



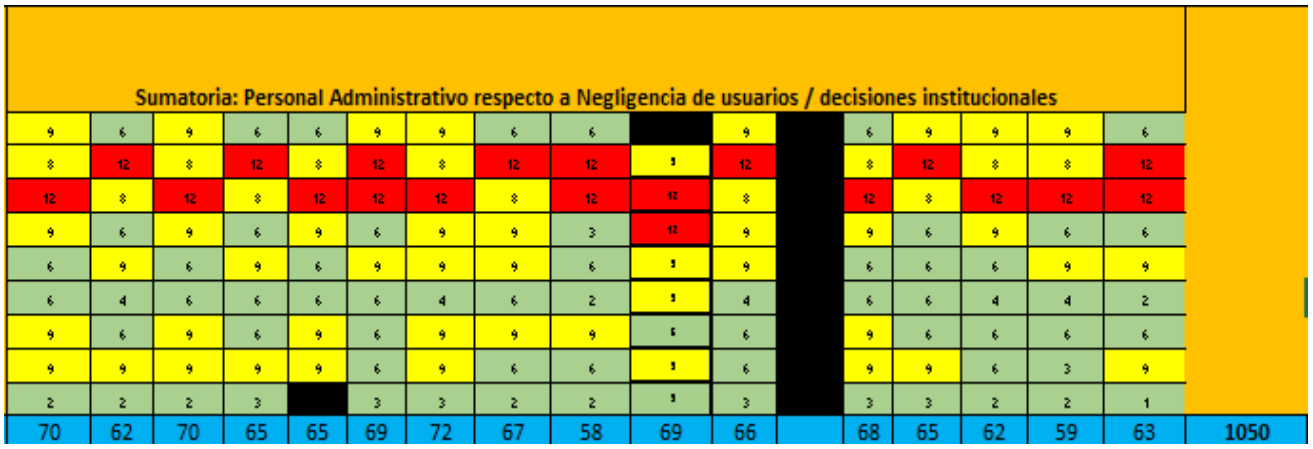
Anexo 7. Sumatoria y promedio de los Sistemas e Infraestructura Instituciona respecto a Negligencia de usuarios / decisiones institucionales dentro de la Unidad Académica de Psicología de la UAZ.



Anexo 8. Sumatoria y Promedio del Personal Administrativo con respecto a Riesgos de Criminalidad Común y Motivaciones Políticas dentro de la Unidad Académica de Psicología de la UAZ.

9	12	9	9	6	9	6	9	9			
12	16	12	8	12	8	12	8	8			
16	16	12	12	8	12	16	12	12			
12	9	9	12	9	6	9	9	9			
9	9	6	6	9	9	6	9	6			
6	6	4	6	4	6	4	4	4			
9	12	9	6	6	9	6	9	9			
9	9	9	9	6	6	9	6	9			
3	3	3	3	3	2	2	3	2			
85	92	73	71	63	67	70	69	68	0	0	658

Anexo 9. Sumatoria y promedio Personal Administrativo respecto a Negligencia de usuarios / decisiones institucionales dentro de la Unidad Académica de Psicología de la UAZ.



9	6	9	6	6	9	9	6	6		9		6	9	9	9	6
8	12	8	12	8	12	8	12	12	8	12		8	12	8	8	12
12	8	12	8	12	12	12	8	12	12	8		12	8	12	12	12
9	6	9	6	9	6	9	9	3	12	9		9	6	9	6	6
6	9	6	9	6	9	9	9	6	8	9		6	6	6	9	9
6	4	6	6	6	6	4	6	2	8	4		6	6	4	4	2
9	6	9	6	9	6	9	9	9	6	6		9	6	6	6	6
9	9	9	9	9	6	9	6	6	8	6		9	9	6	3	9
2	2	2	3		3	3	2	2	8	3		3	3	2	2	1
70	62	70	65	65	69	72	67	58	69	66		68	65	62	59	63	1050

Anexo 10. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARAR PROTEGER ACTIVOS DE INFORMACIÓN DEL ÁREA ADMINISTRATIVA DE LA UNIDAD ACADÉMICA DE PSICOLOGÍA

PRESENTACIÓN

Rector de la Universidad Autónoma de Zacatecas
Dr. Antonio Guzmán Fernández

Secretario General de la Universidad Autónoma de Zacatecas
Dr. Rubén Ibarra Reyes

Director de la Unidad Académica de Psicología
Mtro. Hans Hiram Pacheco García

Responsable de Programa de la Unidad Académica de Psicología
Jesús Manuel Correa Vengas

Coordinador Administrativo de la Unidad Académica de Psicología.
Roberto Carlos Valadez Morúa.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Proyecto Académico e Institucional
Zacatecas, Zacatecas, México. Julio 2020.
Unidad Académica de Psicología de la Universidad Autónoma de Zacatecas.
Primera Edición, Versión 1.0. Versión de cambios internos: 1.5.

Elaborado por:
Ing. Tomás de Jesús Moreno Zamudio, Mtro. Santiago Villagrana, Mtro. Carlos Héctor Castañeda Ramírez.

** Estas políticas de Seguridad de la Información fueron creadas a partir de un **Análisis de Riesgos de los Activos** de esta institución. Además, se utilizaron como base de elaboración documentos ya existentes al respecto, basados en el estándar ISO/IEC27001. En esta lógica, se adaptaron las estrategias de buenas prácticas a las necesidades específicas de esta Unidad.*

CONTENIDO

GLOSARIO

Para poder entender adecuadamente los contenidos e indicaciones que se abordan en las presentes Políticas, es necesario contextualizar y comprender algunos conceptos básicos relacionados con la Seguridad de la Información, mismos que se explican a continuación:

Análisis de Riesgos: Proceso mediante el cual se pueden cuantificar los riesgos relacionados con la seguridad de la información y evaluar si este análisis es adecuado y tomar medidas para reducirlo (Como la implementación de Políticas de Seguridad).

Activos de la Información: Cualquier objeto o ente dentro de la organización que contiene información y que se debe proteger.

Seguridad de la Información: Proceso por el cual se buscar proteger la información de riesgos que puedan afectarla en sus diferentes formas y estados. Consta de 3 pilares fundamentales: Confidencialidad, Disponibilidad e Integridad de la información.

Confidencialidad: término que hace referencia a que la información solo debe ponerse en conocimiento de las personas, entidades o sistemas autorizados para su acceso.

Integridad: Mantener la información sin alteraciones, y, por ende, mantener su valor original de cualquier índole

Disponibilidad: Condición que permite que la información pueda estar disponible cuando sea necesaria

Gestión de la Seguridad de la Información: Proceso que implica la identificación de activos y los riesgos a los que están expuestos, el análisis de los riesgos identificados para cada activo, la selección e implantación de controles que reduzcan los riesgos y el seguimiento, medición y mejora de las medidas implementadas.

Medios removibles: Todo aquel activo que contenga información y que tenga la capacidad y/o caracterítica de moverse. Por ejemplo, las memorias USB, Cd´s, Diskettes, etc.

Entorno Virtual/Máquina Virtual: Software que permite emular el funcionamiento de un dispositivo electrónico dentro de otro dispositivo electrónico. Se puede emular, por ejemplo, un Sistema Operativo dentro de otro Sistema Operativo.

Malware: Cualquier software o código malicioso que puede llegar a dañar gravemente a un sistema operativo y/o compromete los datos que se manejan en éste.

Anti Malware: Cuaqluier software o código que combate de manera contundente el funcionamiento de un Malware.

Protocolo HTTPS: (HyperText Transfer Protocol Secure, Protocolo de transferencia de hipertexto) es un protocolo de comunicación de Internet que protege la integridad y la confidencialidad de los datos de los usuarios entre sus dispositivos y el sitio web.

Protocolo HSTS: (HTTP Strict Transport Security) es un mecanismo de seguridad diseñado para asegurar las conexiones HTTPS contra ataques de secuestros de sesión.

Extensión de Navegador: Cualquier fuunción adicional que se puede añadir fácilmente a los navegadores web.

Factor de doble autenticidad: Medida de seguridad extra que frecuentemente requiere de un código obtenido a partir de una aplicación, o un mensaje SMS, además de una contraseña para acceder al servicio de logueo (Correo electrónico, páginas web, sistema, etc).

Bluesnarfing: Acceso no autorizado a información de un dispositivo móvil por medio de una conexión Bluetooth de los dispositivos de los usuarios.

Phishing: Delito que consiste en engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de créditos o cualquier otro tipo de información valiosa por el usuario.

Proceso de anonimización: Proceso que consiste en crear una versión similar, manteniendo la misma estructura que la original, pero alterando los datos sensibles para que permanezcan protegidos, visualizando siempre que se debe conservar el formato.

Firewall: Dispositivo o sistema que permite tomar la decisión de qué tráfico de red se autoriza pasar y cuál se considera peligroso. Básicamente, permite filtrar lo que es bueno, o de confianza, de lo que no lo es.

Proxy: Herramienta tecnológica que establce un punto intermedio entre un dispositivo conectado a Internet y el servidor que está accediendor.

Datos POST: Datos que se pasan a través de un formulario par posteriormente ser procesado por una serie de códigos. Este proceso puede ser almacenamiento o manipulación de esa misma información.

Instrucciones SQL: Conjunto de instrucciones que consta de identificadores, parámetros, variables, nombres, tipos de datos y palabras reservadas de un lenguaje llamado SQL. Este lenguaje sirve para establecer comunicación a una Base de Datos en específico.

Protocolo AES encrypt: Método de encriptación que se usa con el fin de cifrar datos y de protegerlos contra cualquier acceso ilícito.

Dirección MAC: (Siglas en inglés de Media Access Control), un identificador único e irreemplazable para cualquier dispositivo de red. Analogamente es como una CURP o un RFC pero implementado en dispositivos.

Filtrado de dirección MAC: Serie de instrucciones al router para que permita conectarse a los dispositivos cuyo MAC aparezca en un listado definido. Es decir, restringe el acceso a toda dirección MAC que no esté registrada en esa lista.

VLANS: Del inglés Virtual LAN (Red de área local y virtual), es un método que permite crear redes que lógicamente son independientes, aunque estas se encuentren dentro de una misma red física. Es básicamente crear módulos de red independientes dentro de la misma red.

Acceso VOIP: Voz sobre Protocolo de Internet, es un método con el que se pueden hacer llamadas de voz a través de la red.

Criptografía de Red: Son diversas técnicas de cifrado utilizadas para poder proteger los datos de una red.

Encriptación WPA: Sistema para proteger las redes inalámbricas (Wi-Fi), muchas de las veces viene incorporado en los dispositivos que brindan el servicio de internet.

Técnicas Antiforense: metodologías para comprometer la disponibilidad de la evidencia a través de la manipulación de material de información destruyendo, ocultando, eliminando y/o falsificando la evidencia. En resumen, es el borrado por completo de toda información para que ya no pueda ser recuperada jamás.

Ataques DDOS: Tipo de ataque que aprovecha los límites de capacidad específicos que se aplican a cualquier recurso de red, tal como la infraestructura que habilita el sitio web de la empresa. A través de este tipo de ataque se envian diferentes solicitudes saturando así los

servicios. Una consecuencia de este tipo de ataques, puede ser, por ejemplo, el no tener acceso a una Página web o sistema en línea.

Inyección SQL: Ataque contra un sitio o aplicación web en el que se añade código de lenguaje SQL en formulario web con el objetivo de acceder a la base de datos y modificar los datos sin autorización.

Ofuscamiento de Código: Es una técnica de seguridad que hace alusión a ocultar el código original en cualquier sistema desarrollado, incluyendo aplicaciones web, aplicaciones de escritorio o cualquier plataforma virtual que pudiera ser desarrollada.

1. INTRODUCCIÓN

En el presente documento se definen un conjunto de políticas y buenas prácticas de seguridad de la información que tienen como objetivo primordial proteger a cada una de las categorías y clasificaciones de los activos de información de la Unidad Académica de Psicología ante las diferentes amenazas y vulnerabilidades identificadas a través de la implementación de un Análisis de Riesgos de la Seguridad de la Información en dicha Unidad. En esta lógica, las Políticas aquí propuestas, se abordan los siguiente puntos y dimensiones esenciales de los procesos de seguridad de la información dentro de esta institución:

- Organización de seguridad de la Información: Se indican las responsabilidades generales para poder gestionar adecuadamente los procesos relacionados con la protección de los activos de información y los datos que se manejan dentro de la Unidad Académica de psicología, así como el uso adecuado de dispositivos móviles y Teletrabajo.
- Gestión de los Activos de la Información: Se establecen lineamientos y directrices generales respecto a la responsabilidad de los activos de la información, así como el manejo y adecuado de la información dentro de la institución. Los puntos que se abordan en esta sección estarán sustentados por todas las secciones consecuentes, considerando cada una de las prácticas que se define para cada uno de los activos que se presentan en estas Políticas.
- **Seguridad de los Datos y Procesos Institucionales:** Se abordan un conjunto de lineamientos y buenas prácticas para proteger y salvaguardar todos los activos de la

información y datos relacionados e inmiscuidos en los procesos institucionales (Procesos como inscripción, finanzas, investigación, entre otros).

- **Seguridad de Sistemas e Infraestructura Institucionales:** Se abordan un conjunto de lineamientos y buenas prácticas para proteger y salvaguardar todos los activos de la información relacionados e inmiscuidos en los Sistemas e Infraestructura institucional (Sistemas como contabilidad -Tauro-, páginas web, dispositivos, entre otros).
- **Seguridad del Personal Administrativo y del Recurso Humano:** Se abordan un conjunto de lineamientos y buenas prácticas para proteger y salvaguardar los activos de información relacionados con el recurso humano del área administrativa de la Unidad Académica de Psicología, tales como miembros del Consejo de Unidad, directores, trabajadores, etc.
- Control de Acceso: Se abordan lineamientos y recomendaciones respecto al alcance de los activos de la información y la posibilidad de accesos a la misma infraestructura de la institución, así como a otros servicios como el internet, dispositivos, información, etc.
  Seguridad Física y Ambiental: Se establecen lineamientos generales para conservar adecuadamente todos los activos de información que tengan que ver con la infraestructura de ésta misma. Se abordan aspectos como uso adecuado de cajones, archiveros, entre otras. Asimismo, se hacen recomendaciones de registros de entradas y salidas, así como prácticas para poder darle seguimiento a los estados de los activos de la información.
- Gestión de incidentes de seguridad de la información: Se abordan una serie de lineamientos que explica cómo mitigar los riesgos y vulnerabilidades que se presentan dentro de la Unidad Académica de Psicología respecto a la Seguridad de la Información.
- Cumplimiento: Se establecen puntos que resaltan la importancia y la relevancia de cumplir con todos los lineamentos que aquí se establecen, con la finalidad de preservar en todo momento los pilares esenciales de la Seguridad de la Información.

Estos puntos se sustentan a partir de diferentes investigaciones documentales que utilizan estándares generales, además de los activos identificados y tasados en el Análisis de Riesgos realizado dentro de la Unidad Académica de Psicología. Dentro de cada uno de estos puntos de Seguridad de la Información, se desglosan una serie de Políticas y Buenas prácticas para proteger los activos que tengan que ver con cada uno de estos puntos y categorías, velando

siempre por el resguardo de la confidencialidad, disponibilidad e integridad de todos los elementos esenciales de la Institución. Este documento también puede servirle a docentes, alumnos y visitantes de la Unidad Académica de Psicología, aunque va orientado específicamente a los trabajadores Administrativos de dicha Unidad, incluyendo funcionarios y directores. La actualización y seguimiento de estas Políticas estará a cargo de algún Equipo o Comité orientado a establecer medidas para mitigar riesgos de Seguridad de la Información, o en su defecto, a los encargados de las situaciones tecnológicas subyacentes de la Coordinación Administrativa de esta Unidad.

OBJETIVOS

Establecer los lineamientos para la adecuada gestión de la seguridad de la información dentro del Área Administrativa de la Unidad Académica de Psicología de la Universidad Autónoma de Zacatecas, todo esto sustentado desde un Análisis de Riesgos de los Activos de Información implementado en la misma Unidad, en donde se obtuvo la identificación y valoración de los riesgos asociados a los activos de información que la conforman. Todos estos lineamientos siempre se tendrán que realizar velando por la protección de confidencialidad, integridad, disponibilidad, privacidad, continuidad, autenticidad y no repudio y por el cumplimiento de la normatividad general vigente aplicable dentro de esta institución.

ALCANCE

Los lineamientos contenidos en el presente documento se aplican a consideración de todos los miembros del área administrativa de la Unidad Académica de Psicología de la Universidad Autónoma de Zacatecas, en donde se incluyen todos los procesos y activos de información que la conforman. Algunas medidas también se deberán seguir por cualquier miembro de la comunidad Universitaria, como estudiantes, docentes y los mismos trabajadores. Todos estos lineamientos están fundamentados respecto a la clasificación de activos de información elaborada en el Análisis de Riesgos implementado dentro de la

Unidad, por lo que es de suma importancia estar monitoreando dichos riesgos a lo largo de la evolución de esta institución.

3. ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN

3.1. Organización Interna

Todos los activos de información deberán estar bajo la responsabilidad del Coordinador Administrativo - o de aquellos que tengan dicha facultad - para evitar conflicto y reducir oportunidades de modificación (intencional o no) no autorizada o mal uso de los activos de información de la Unidad Académica de Psicología.

La Unidad Académica de Psicología debe definir roles y responsabilidades que consideren actividades de administración, operación y gestión de la seguridad de la información, con la finalidad de poder controlar riesgos y conservar seguridad de la información en sus diversos ejes, departamentos, procesos y funciones.

La Coordinación Administrativa, en conjunto con los Departamentos especializados que subyacen de ésta, debe identificar a las autoridades pertinentes con quienes pueda acudir en el caso de que un incidente de seguridad la información suceda, tales como la Policía Federal, o expertos en los temas dentro de la misma institución educativa. Esta misma Coordinación debe mantener contacto y capacitación con entes especializados en el ámbito de la seguridad de la información que aporten a la gestión de los riesgos de seguridad identificados en la Unidad Académica de Psicología.

Todos los proyectos que tengan origen en la Unidad Académica de Psicología, deben tener una noción mínima de Seguridad de la Información para poder evitar problemáticas futuras con cualquiera de las amenazas o riesgos que existan respecto a la privacidad y seguridad de la información.

3.2. Dispositivos Móviles y Teletrabajo

Se deben estableces y actualizar constantemente protocolos que brinden a los departamentos, coordinaciones y áreas de la Administración de la Unidad Académica de Psicología, la orientación con respecto a la autorización, configuración y uso de los dispositivos móviles dentro de la Unidad. Con base a estos protocolos, se debe tener una actualización constante de los dispositivos móviles, con la finalidad de disminuir los riesgos de hackeo, robo de información o explotación de vulnerabilidades que pongan en riesgos los activos de la Unidad

Académica. Así mismo se deben instalar antivirus y anti-Malware en todo dispositivo móvil que se utilice dentro de la institución.

Se debe disponer de un mecanismo de conexión segura que garantice que las herramientas de teletrabajo autorizadas por la Unidad Académica de Psicología se conecten de forma segura y se protegen los activos de información en uso, considerando el resguardo de los procesos, personal administrativo y sistemas que se usan en esta Unidad.

Si se utilizan herramientas de comunicación para impartición de clases, tales como Zoom, Meet, Jitsi, entre otras, se debe contar con las actualizaciones más recientes, esto con la finalidad de no comprometer ningún dato personal de los usuarios, estudiantes y docentes. Asimismo, se recomienda la implementación de Plataformas Educativas Virtuales desarrolladas para tal fin para la impartición de clases virtuales.

3. 3. Roles y Responsabilidades

Dentro de la Unidad Académica de Psicología, específicamente para la adecuada organización y gestión de la Seguridad de la Información, se definen los siguientes roles y responsabilidades:

Encargado/a: Son las/los responsables de resguardar la información de su área, controlando que se cumplan los requerimientos de la seguridad de acuerdo con las medidas implementadas por el Gestor de la Seguridad de la Información. Algunos de estos responsables pueden ser los Directivos, Responsables de Programa y/o Administrativos/funcionarios de la Unidad Académica de Psicología

Gestor/a de la Seguridad de la Información: Son las/los responsables de implementar las medidas y controles necesarios para salvaguardar y proteger los activos de información de acuerdo con la categorización y clasificación establecida en el Análisis de Riesgos. Estas personas pueden ser las/los especialistas en temas de Seguridad de la Información y protección de datos dentro de la Unidad Académica de Psicología – Inclusive podrían ser las propuestas iniciales para la creación de un Comité orientado a esta Gestión -.

Usuario/a: Son las/los responsables de hacer buen uso del activo de la información de la Unidad Académica de Psicología. Es todo aquel personal administrativo que tenga relación directa con los recursos institucionales.

4. GESTIÓN DE LOS ACTIVOS DE INFORMACIÓN

4.1. Responsabilidad de los Activos de Información

Se debe diseñar una metodología para la identificación, clasificación, valoración y buen uso de los activos de información. Esta acción puede ser fundamentada con el proceso de investigación de donde nacen estas Políticas. Así mismo, se recomienda tener un equipo humano orientado a solucionar cualquier problema o contingencia relacionado con la seguridad de la información de los activos de esta institución, considerando, para futuras actualizaciones de estas políticas, la creación de algún *Comité de Seguridad de la Información dentro de la Unidad Académica de Psicología.*

Todos los activos de información de la Unidad Académica de Psicología, deben estar en constante acción de inventariado, y posteriormente clasificados de acuerdo a requerimientos y necesidades de la metodología de identificación, clasificación, valoración y buen uso que siga la misma Universidad, o en su defecto, la misma Unidad Académica en específico.

Es necesario identificar los ciberactivos (activos de seguridad digital). Estos ciberactivos son aquellos que contienen, trasmiten o procesan información de los servicios esenciales de la Unidad Académica de Psicología.

Los activos de información de la Unidad Académica de Psicología deben ser utilizados por toda la comunidad universitaria de acuerdo con las políticas contenidas en el presente documento y según la normatividad vigente de la Universidad, apegándose a la las Leyes externas que existan respecto al manejo de información y protección de datos.

Los Docentes y Administrativos deben utilizar los recursos tecnológicos de la Unidad Académica de Psicología con el único objetivo de llevar a cabo las labores asignadas al cargo; por ende, no deben ser utilizados para fines ajenos a este, tanto de índole personal como de otra índole. Lo mismo aplica para los estudiantes de esta Unidad Académica.

El área de cómputo en específico, debe establecer un inventario respecto a los sistemas de información y hardware que se encuentran permitidos en los lugares de trabajo de la institución para el desarrollo de las actividades laborales, así como verificar periódicamente que el software y hardware instalado en dichos lugares de trabajo funciones adecuadamente

en las computadoras o equipos móviles; aquí se incluyen bloqueos y accesos denegados a sitios que no son pertinentes para la institución, así como el uso adecuado de licenciamiento.

4.2. Clasificación de la Información.

Todas las Prácticas que se abordan en estas Políticas deben apegarse a la propuesta de clasificación que aquí se muestra. La clasificación idónea de la información para la Unidad Académica de Psicología será la siguiente:

- **Reservada:** Toda información de interés para la institución en general. Ésta es creada por la misma Unidad Académica de Psicología y es la que hace el funcionamiento de los procesos optima y eficazmente.
- **Confidencial**: Toda información que no puede divulgarse sin el consentimiento expreso de su encargado/a. Puede ser información creada por la Unidad, o información que tiene la Unidad en resguardo o protección. En general, son datos sensibles y privados.
- **Pública**: toda la información generada, obtenida, adquirida, transformada o en posesión de otros usuarios o sujetos, es accesible a cualquier persona. Se rige por la Ley de Transparencia u otras Leyes alusivas al acceso de información de índole Pública.

Se debe diseñar una guía para la clasificación de la información física y digital sobre información pública y protección de datos personales, de acuerdo a las leyes que existen sobre la protección de datos o los protocolos que existan dentro de la Universidad.

El Área Administrativa debe cumplir con los requerimientos de uso, manipulación y conservación de los medios tecnológicos para almacenamiento de información, con el fin de mantener la disponibilidad, confidencialidad e integridad de la información.

Cada encargado del activo de información debe velar el cumplimiento de su clasificación de acuerdo con lo establecido en las clasificaciones de activos de información que más se adecue a las necesidades propias de la Unidad Académica. Esta clasificación se puede visualizar al inicio de este apartado. Este mismo cumplimiento y uso de los activos y su clasificación se debe informar debida y constantemente a todos los usuarios de dichos activos dentro de la Unidad Académica de Psicología.

Es de suma importancia recoger de las impresoras, escáneres, y fotocopiadoras inmediatamente los documentos confidenciales para evitar su divulgación no autorizada. Así mismo, es de suma importancia que se verifiquen todos los elementos relacionados a estos

dispositivos que estén cercanos, con la misma intención de verificar que no se hayan quedado ningún tipo de documento.

Los Docentes y Administrativos deben asegurar que los documentos y medios de almacenamiento que contengan información sensible, no queden de forma desprotegida en al momento de ausentarse de su puesto de trabajo. Así mismo deben proteger la información física de la Unidad Académica de Psicología, utilizando medios de resguardo de los que dispongan, como archiveros y herramientas bajo llave.

4.3. Protección y Manejo de la Información

Es necesario llevar acabo prácticas que garanticen el correcto manejo de la información y la protección de los datos institucionales.

En cuestión de Protección de Manejo de la información, se recomienda que todo activo de información tasado según su clasificación, cuente con un control de acceso, donde se establezca qué personas son las autorizadas para el manejo de la información en el activo de acuerdo a los roles ya establecidos en estas Políticas.

El Personal Administrativo de esta Unidad está obligado a no revelar a terceras personas la información que conozcan por el ejercicio de sus funciones, por lo que están obligados a mantenerla confidencial y privada para evitar su divulgación, apegándose a leyes que evoquen este hábito; este cumplimiento debe ser de leyes o Políticas de la propia Universidad o Leyes o Políticas publicadas en los diarios nacionales.

4.4. Protección de Datos

Es menester que todas las áreas deban considerar el mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o mal uso, acceso o tratamiento no autorizado, así como cuidar su confidencialidad, integridad y disponibilidad, pilares que son esenciales para la Seguridad de la Información en general. Lo anterior servirá para poder estar cumpliendo los lineamientos de la LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS, y todas aquellas Leyes que garanticen la protección de datos.

4.5. Manejo de Medios de Almacenamiento

Se debe definir un procedimiento para el uso de medios removibles a través de la generación de una guía de usuario para administrar el control de dichos medios.

Todo medio extraíble o removible, tales como USB, Discos Duros externos o CD, deberá ser escaneado mediante algún software anti Malware utilizado dentro de la Unidad Académica de Psicología. Este procedimiento se debe realizar cada vez que se conecte a un equipo de la Unidad Académica. Así mismo, se debe tener configurado en el software Anti Malware el bloqueo de la reproducción automática de archivos ejecutables, todo esto con la finalidad de evitar ejecutar archivos o programas que roben la información automáticamente.

Se recomienda tener un entorno virtual (Máquinas Virtuales dentro de los dispositivos) para abrir archivos de un medio extraíble, esto para evitar robo de información sensible que contenga el activo de información de la Unidad Académica de Psicología. Esta acción se debe realizar en Laptops, Computadoras, celulares institucionales, impresoras, etc.

Cada usuario debe tomar las medidas para la protección de la información que se encuentra en medios extraíbles, para evitar acceso físico y lógico no autorizado, daños, pérdida de información o extravío del mismo.

La movilidad de los medios de almacenamiento debe contar con las condiciones apropiadas para salvaguardar la integridad, confidencialidad y disponibilidad de la información de la Unidad Académica de Psicología.

Toda información deberá ser eliminada de los medios de almacenamiento de forma segura cuando ya no sea necesaria, utilizando procedimientos y herramientas de borrado seguro, garantizando que no queden rastros de ésta.

5. POLÍTICAS DE SEGURIDAD PARA LOS DATOS Y PROCESOS INSTITUCIONALES

5.1. Políticas y Prácticas de Seguridad de las operaciones

Es recomendable tener documentación de todo Sistema elaborado por la Institución, Universidad o proveedor externo. Además, es menester la actualización de los procedimientos relacionados con la operación y administración de los sistemas de información de la institución. Esto se puede dar mediante manuales, Project Charter, documentos de requerimientos, entre otros y mediante la asesoría del Gestor de Seguridad de la Información designado en la Unidad Académica de Psicología.

Se deben establecer procedimientos que permitan asegurar la gestión de cambios de emergencia a nivel de infraestructura, aplicaciones y servicios tecnológicos para que estos sean desarrollados bajo estándares de eficiencia, seguridad, calidad y permitan determinar las actividades y responsables en la gestión de cambios dentro de la Unidad Académica.

Se debe dar seguimiento continuamente al uso de los recursos tecnológicos con el fin de realizar los pertinentes cambios o actualizaciones. A partir de este seguimiento, se podrán analizar las futuras necesidades de capacidad y aseguramiento en el rendimiento del sistema específico para cada actividad.

Se debe estar en constante búsqueda de actualización de sistemas y herramientas tecnológicas, con el fin de asegurar el desempeño y capacidad de las plataformas tecnológicas que se requieran utilizar. Hay que considerar aspectos como el consumo de recursos de procesador, memorias, impresoras, el ancho de banda requerido, tráfico de redes, capacidades de almacenamiento, servidores contratados, tecnologías web, entre otras. Toda actualización es importante, ya que se disminuyen muchos riesgos de acceso no autorizado, infección de virus no conocidos, rendimiento muy bajo, entre otros riesgos que comprometen la efectividad y funcionamiento de los procesos institucionales a través de los sistemas utilizados.

5.2. Políticas y Prácticas de Seguridad para Protección contra códigos maliciosos

Es necesario instalar o contratar una solución antimalware o antivirus en todos los activos que sean utilizados por los trabajadores dentro de la institución. Se recomiendan herramientas de Software Libre que permiten el escaneo constante de todo tipo de código malicioso. Esto también debe aplicarse en el uso de los docentes, y alumnos, para evitar cualquier tipo de ataque dentro del Área administrativa.

Fomentar que ningún docente, administrativo, estudiante o tercero, descargue software desde sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas sin la debida autorización del departamento encargado de la cuestión informática, o del Gestor de Seguridad de la Información de los activos de información designado en la Unidad Académica de Psicología.

Se debe establecer una organización y/o lugar para que los docentes, administrativos y terceros que sospechen de alguna infección por virus notifiquen y proceda la revisión y eliminación del virus.

Todo mensaje sospechoso de procedencia desconocida debe ser inmediatamente reportado al departamento encargado de las cuestiones informáticas, tomando las medidas de control necesarias, evitando así cualquier tipo de robo de información o infección que ponga en riesgo los pilares de la Seguridad de la Información dentro de la Unidad Académica de Psicología.

Se deben establecer capacitaciones constantes para que todo personal administrativo, docente y estudiante pueda saber cómo actuar ante cualquier tipo de contingencia de infección informática a través de un malware.

5.3. Políticas y Prácticas de Seguridad de los Documentos Institucionales

Se debe tener bien establecido un control de accesos autorizados y no autorizados para todo tipo de Documento institucional, preservando así su integridad, confidencialidad y disponibilidad. Se puede hacer uso de herramientas de resguardo dentro y fuera de los cubículos establecidos. Este establecimiento de accesos estará regido por el organigrama institucional y los roles que se han asignado en el presente documento.

Se deben establecer constantemente respaldos de documentos importantes para la institución. Estos respaldos pueden ser digitales o físicos; Si se opta por un respaldo digital, hay que tener un control de riesgos respecto a la infección de códigos maliciosos. Si se opta por un respaldo físico se tienen que tomar en cuenta parámetros de acceso y consideraciones de riesgos de sucesos físicos, como incendios, inundaciones, entre otros.

Todos los documentos, ya sean digitales o físicos, deben estar en lugares en donde se imposibiliten riesgos de incendios, inundaciones, falta de ventilación, sobre carga eléctrica o

situaciones que les puedan causar un daño físico o lógico que deje inhabilitado su funcionamiento operacional.

Todo documento debe estar protegido ante robo, implementando mecanismos de protección digital e incorporando mecanismos de protección de resguardo bajo llave. Todo esto para evitar la pérdida total de la documentación, así como el mal uso de ésta.

Todo documento emitido por la Unidad Académica de Psicología, así como proyectos, investigaciones y propuestas académicas, deben estar debidamente verificados contra violación de derechos de autor.

Es de suma importancia tener capacitado al personal administrativo respecto al manejo de los documentos institucionales, para que estos sepan los alcances de funcionalidad y publicación de estos mismos. Además, es importante tener normas, manuales y reglas para el uso de la documentación sensible dentro de la Unidad Académica de Psicología; estas normas se deben implementar para cualquier tipo de proceso educativo dentro de esta institución.

Se tiene que dar seguimiento constante y revisión periódica de la existencia de los activos de información, esto con la finalidad de evitar pérdidas o robos de los documentos de mayor importancia, y saber la cantidad exacta de cada uno de éstos.

5.4. Políticas y Prácticas de Seguridad de las Finanzas

Es importante tener todas las consideraciones que están establecidas en la legislación vigente para la protección de información en el sector financiero y bancario, como la Ley de Privacidad de Datos Federales y su Reglamento, con la finalidad de salvaguardar la sana operación de los datos de los trabajadores, estudiantes, proveedores o usuarios.

En la lógica del conocimiento de las leyes para operaciones financieras se deben establecer protocolos de accesos a sistemas o procesos que tengan que ver con las finanzas de la Unidad Académica, asignando roles específicos para tal proceso.

Es necesario siempre contar con procedimientos para actuar en cuestiones de fraude o extorsión, para salvaguardar los procesos financieros de la Unidad Académica. Todo personal administrativo que se perciba como víctima de cualquier de estos delitos tiene que ser dirigido a instituciones capacitadas para brindar una asesoría legal y técnica respecto a ese incidente.

Toda persona que tenga acceso a los procesos financieros, debe tener la responsabilidad de operar adecuadamente los recursos que emanen de éste, estar siempre capacitado para realizar las transacciones necesarias, para utilizar el sistema adecuadamente, para saber actuar en caso de alguna infección de código malicioso, de no permitir entrada de memorias USB al activo de información en donde tenga datos sensibles y de seguir las normas establecidas para poder llevar a cabo de manera efectiva todo proceso financiero dentro y fuera de la Unidad Académica de Psicología.

5.5. Políticas y Prácticas de Seguridad de los procesos bancarios

Es necesario tener instalado un antivirus y un Anti Malware en todos los equipos y dispositivos móviles que acceda a las cuentas Bancarias de la Universidad o de la Unidad Académica de Psicología.

Toda persona que realice un pago, transacción o acceso bancario debe tener los permisos necesarios asignados a través de su rol institucional, para poder hacer uso de dichos servicios.

Es necesario establecer un protocolo de control de acceso bancario.

Se recomienda tener un gestor de contraseñas para que éstas se estén cambiando periódicamente, además de que utilizan un grado alto de complejidad.

Verificar en todo momento el nombre de la barra de direcciones (URL), para comprobar si es fiable la página o no. Siempre se debe tener precaución en la página donde se realizará algún movimiento bancario, garantizando su fiabilidad y autenticidad institucional.

Todo personal administrativo que esté facultado para llevar a cabo operaciones bancarias debe seguir al pie de la letra los siguientes pasos:

- Acceder a la banca en línea directamente del navegador y no a partir de enlaces o correos electrónicos.
- Verificar que la URL es HTTPS y que al lado (parte superior del navegador) aparezca un candado cerrado. Eso determinará la autenticidad del sitio web.
- Cambiar la contraseña de acceso de forma periódica. Además, ha de ser compleja, añadiendo diferentes caracteres, números y letras minúsculas/mayúsculas, en donde se recomienda el uso del "@".
- Tener siempre actualizado el navegador y el sistema operativo.
- Evitar llevar a cabo operaciones en dispositivos públicos y a través de redes públicas.

- Recordar que los bancos nunca solicitan información personal a través del correo ni el teléfono.
- Cerrar la sesión tras realizar las operaciones o al retirarse del dispositivo, aunque sea solo un momento.

Se recomienda usar siempre el factor de doble autenticidad, los servicios bancarios como Banorte, Bancomer y demás, utilizan factor de autenticidad a través del alta de Token Bancario y envío de SMS al momento de realizar algún movimiento. Todo el personal que haga uso de procesos bancarios deberá seguir esta recomendación.

No se debe acceder a ninguna cuenta financiera ni personal mediante una red pública y, a ser posible, cerrar la sesión cuando se haya terminado, aun estando en una red segura propia.

Se debe mantener siempre desconectado el Bluetooth en aquellos dispositivos que utilicen movimientos bancarios. Esto con la finalidad de evitar acciones maliciosas como el *bluesnarfing.*

Se recomienda hacer una verificación periódica de la cuenta bancaria desde una ubicación segura. En caso de notar alguna actividad sospechosa ha de notificarse al banco de inmediato. Es importante saber que existe un periodo de días máximo, diferente en cada banco, para reclamar cualquier cargo anómalo o robo de dinero. Todo personal que haga uso de un servicio bancario dentro de la institución debe seguir esta recomendación.

Se debe mantener en todo momento desactivado el inicio de sesión automático, ya que al almacenar los datos del inicio de sesión (usuario y contraseñas) en un navegador, no se sabe qué medidas de seguridad tiene implantadas y cómo de eficaces serán en el tiempo a medida que evolucionen las amenazas.

Es obligación mantener actualizado los equipos en donde se realizan movimientos bancarios. Para comprobar si es verdad que hay nuevas actualizaciones disponibles, basta con ir a Configuración y buscar actualizaciones en el dispositivo o actualizar el propio sistema operativo.

Si se van a realizar depósitos bancarios, es sumamente importante seguir las siguientes recomendaciones:

- No retirar altas sumas de dinero en efectivo.
- Prestar atención a las personas que tengan una actitud sospechosa, ya sea al acceder al banco, en el interior o al salir del mismo. En caso de observar algo anómalo, avisar

a los trabajadores de la entidad y a la policía si fuese necesario. En caso de robo o secuestro no hay que enfrentarse a los ladrones y hacer lo que pidan hasta que se marchen o llegue la policía.

- Al retirar el dinero en efectivo a través de la ventanilla, hacer el conteo directamente delante del empleado del banco para reducir la exposición e informarle si hay algún error.

En caso de querer deshacerse de documentos físico con algún proceso importante de la institución, hay que tener la debida eliminación de ésta, rompiendo por completo y dejando ilegible dicho documento, esto con la finalidad de evitar que los datos contenidos ahí sean usados con malas intenciones.

Es de suma importancia mantener capacitado siempre al personal administrativo que tenga facultad de realizar movimientos y procesos bancarios.

5.6. Políticas y Prácticas de Seguridad en el uso de Correos Electrónicos

Es de suma importancia tener a los trabajadores administrativos constantemente capacitados, especialmente aquellos que hagan uso de correos institucionales con la finalidad de evitar conductas de riesgo al utilizar su correo.

Los correos electrónicos que tengan fecha de 2 meses de antigüedad deben ser debidamente eliminados. Si el trabajador considera que esa información es relevante se puede hacer un respaldo en un disco duro externo, o en una base de datos.

Es de suma importancia crear una contraseña compleja, que nadie pueda adivinarla, pero teniendo en cuenta que es una clave que se utilizará muy a menudo y debe ser capaz de recordarla con facilidad. No compartir con nadie esta información, ni anotarla en hojas.

Está estrictamente prohibido iniciar sesión en el correo electrónico institucional desde dispositivos computacionales públicos, centros de acceso a Internet o cafeterías. Se debe asegurar el haber finalizado la sesión antes de abandonar el dispositivo. Sólo hay que usar los correos institucionales en redes que sepamos que son de suma confianza.

Todo personal de la Unidad Académica de Psicología debe tener cuidado con los correos electrónicos engañosos que hacen creer que deben restablecer la contraseña para obtener mayor seguridad. Si realmente se requiere cambiar la contraseña, habrá que dirigirse al sitio

web oficial del proveedor de correo electrónico y realizar allí la modificación, únicamente por ese medio.

El correo electrónico institucional sólo debe ser usado como herramienta de trabajo, el personal no debe comunicarse con él con amigos ni con familiares, ni para eventos personales.

Se recomienda en todo momento tener programas que impidan que archivos indeseables entren en contacto con la información más delicada de los correos. Estos programas ayudan a filtrar spam para asegurar la productividad del trabajador.

Es altamente recomendable utilizar la verificación en dos pasos que ofrecen algunos proveedores de servicios de correo electrónico. Google, a través de Gmail ofrece este servicio, a través de su página: https://www.google.com/intl/es-419/landing/2step/#tab=how-it-works. Esto ayudará a tener más protegida la cuenta y evitará accesos no autorizados a terceros.

Para evitar todo tipo de Phishing y fraude, es necesario seguir las siguientes recomendaciones:

- No responder nunca a un email sospechoso.
- Reenviar el email sospechoso al banco que usa la Unidad Académica, escribiendo la dirección real o llamar para verificar la autenticidad.
- No reenviar el correo a personas del entorno.
- No hacer clic en el enlace ni descargar el archivo adjunto.

5.7. Políticas y Prácticas de Seguridad en el uso de Base de Datos internos

Todo aquel Encargado/a de gestionar una base de datos de la institución, debe hacer un riguroso control de ingreso para que sepan quiénes, cuándo y desde dónde han ingresado. Esto impedirá que cualquier tercero pueda ingresar sin haber sido registrado previamente. En esta lógica, el trabajador que haga uso de una base de datos de la institución deberá limitar los tipos de procesos que estén autorizados con las bases de datos.

Es obligación del Encargado/a de gestionar la base de datos, realizar respaldos periódicamente, por lo menos dos veces al mes. Dichos respaldos, si están en discos extraíbles, debe estar fuera de todo peligro, como incendios, inundaciones, robo o clonación.

Estos respaldos deben estar resguardados bajo llave y con todas las medidas posibles de protección.

Es sumamente necesario tener un inventario de lo que se tiene en la base de datos para que no se quede ningún dato sensible o crítico por fuera al momento de hacer una copia de respaldo.

Se recomienda utilizar algoritmos robustos en los datos sensibles y críticos para cifrar la información. Esto con la finalidad de resguardar el contenido de los datos más importantes dentro de la Unidad Académica de Psicología.

Siempre que se estén realizando procesos de migración o iniciación de proyectos tecnológicos nuevos que requiera el uso de una base de datos existente, es obligación del encargado realizar el proceso de anonimización, mismo que consiste en crear una versión similar, manteniendo la misma estructura que la original, pero alterando los datos sensibles para que permanezcan protegidos, visualizando siempre que se debe conservar el formato.

Todos aquellos trabajadores y usuarios que estén vinculados con bases de datos de la institución, deben apegarse al monitoreo constante de esta misma, actualizando los procesos y optimizándolos para mitigar los riesgos de pérdida o robo de información.

Se recomienda limitar la cantidad de contenido que se almacena en las bases de datos, para disminuir la probabilidad de ser el objeto de ataque de los ciberdelincuentes.

5.8. Políticas y Prácticas de Seguridad en el uso y configuración de Intranet

Se deben establecer barreras o Firewalls, que son combinación de hardware y software que controla el tipo de servicios permitidos hacia o desde la Intranet. Estos Firewalls muchas de las veces son otorgadas por la misma Universidad, en este sentido, la recomendación es acatar la configuración que viene de la Coordinación de Informática y Telecomunicaciones de la Universidad Autónoma de Zacatecas. Aun así, si existiera el caso de tener una red aparte, hay que instalar los servicios necesarios de Firewall. Dependerá de los encargados del Departamento de informática o a fin de llevar a cabo dichas prácticas.

Se recomienda la utilización de servidores sustitutos permitiendo a los administradores de sistemas seguir la pista de todo el tráfico que entra y sale de una Intranet.

Se deben siempre configurar sistemas de contraseñas confiable y robustas. Las contraseñas deben cambiar frecuentemente, que no sean adivinadas fácilmente y tienen que ser elaboradas por personas autorizadas.

Se tiene que contar con conocimientos para el uso y configuración de un proxy. Esto con la finalidad de proteger los envíos que vienen de fuera y hacer los accesos a Internet más rápidos y que el canal de acceso a Internet se libere de forma significativa.

Es obligatorio el uso de software para examinar virus basado en el servidor. Hay muchas alternativas que se pueden hallar a nivel comercial o gratuito, siempre siguiendo la premisa que aquellos que son de acceso libre no tienen la misma potencia de protección, sin embargo, es mejor tener alguno de uso liberado a no tener ninguna protección ante algún virus o software malicioso dentro de la red interna.

5.9. Políticas y Prácticas de Seguridad en el uso de Respaldos de la información

Se debe y es sumamente necesario, definir y documentar un plan o procedimiento de copias de respaldo y restauración de la información de la Unidad Académica de Psicología, donde se establezca el esquema, de qué, cómo, quién, con qué periodicidad, tipo de respaldo y nivel de magnitud de daño se requiere conocer para realizar una copia de seguridad.

Se debe respaldar periódicamente toda la información (configuraciones, logs, documentos institucionales, bases de datos, etc.) que resida en los sistemas de la Unidad Académica de Psicología, considerando su grado de magnitud de daño. Este respaldo se debe hacer por lo menos dos veces al mes. Sin embargo, lo idóneo es que se haga semanalmente dicho respaldo.

Todo tipo de respaldo que se realice, debe estar debidamente asegurado y analizado, sabiendo que está libre de riesgo de pérdida, robo, incendio, inundación o cualquier otro factor que ponga en vulnerabilidad la información parcial o total de lo que se está respaldando.

Se debe evitar que los medios de respaldo utilizados para el almacenamiento de información se vuelvan obsoletos. En la medida de lo posible, debe utilizar tecnologías de punta que permitan reducir el espacio físico que ocupan estos medios.

La persona responsable de realizar el respaldo, debe garantizar que los respaldos no sean alterados.

La persona responsable de realizar el respaldo debe programar y documentar los actos de restauración de información, simulando situaciones de contingencia, bajo parámetros de tiempo establecidos.

Los respaldos realizados deben ser utilizados únicamente para fines académicos, y queda estrictamente prohibido transportar algún respaldo a ámbitos sociales, deportivos o de otra índole que no sea dentro de los lineamentos laborales.

5.10. Políticas y Prácticas de Seguridad en procesos informáticos

Todos los procesos relacionados con la adquisición, renta o desarrollo de software deben estar debidamente documentados, esto con la finalidad de conocer su funcionamiento y conocer las posibles modificaciones que se requieran en un futuro. Además, esto ayudará a que, en caso de que haya un cambio administrativo, se tenga todo documentado respecto al sistema, software o programa que se utiliza en cierto departamento.

Es obligatorio realizar monitoreo permanente del uso que dan los administrativos a los recursos de la plataforma tecnológica y los sistemas de información de la institución.

Es necesario establecer procedimientos para controlar la instalación, o en su defecto, desarrollo de software en los equipos informáticos, se cerciorará de contar con el soporte de los proveedores de dicho software. Además, se tiene que verificar constantemente que el Software tenga un funcionamiento óptimo.

Se debe contar con procedimientos para la validación del software que sea instalado o desarrollado. Asimismo, debe asegurarse que todo el software que se instale en los servidores y equipos de cómputo personal cuente con el licenciamiento vigente y original, suficiente para atender los requerimientos de la institución, apegados al presupuesto y recursos tecnológicos con los que cuente la Unidad.

Todo software instalado o desarrollado dentro de la Unidad Académica de Psicología, debe contar con un debido Manual de uso, además de ser auditado constantemente en cuestiones de actualización, mantenimiento y funcionamiento.

5.11. Políticas y Prácticas de Seguridad en el uso y configuración de Contraseñas

Se deben establecer políticas de gestión de claves/contraseñas: cómo se distribuyen, cómo se guardan, quién accede a los repositorios donde se almacenan o con qué periodicidad hay que cambiarlas.

En todo momento se tienen que activar mecanismos en los sistemas que garanticen que las contraseñas del persona o miembros de la institución se generen de forma robusta, y que obliguen a los usuarios al cumplimiento de una serie de requisitos, como por ejemplo los periodos de validez de las mismas, que no sea posible su reutilización, el formato que deberán seguir, si cabrá la posibilidad de modificación, etc.

Se debe evitar en todo momento el uso de las contraseñas que vienen por defecto en los sistemas y aplicaciones, ya que pueden ser fácilmente identificables. Esto aplica para todos los sistemas de la Universidad, como Tauro, control escolar, además de Módems y herramientas tecnológicas que se adquieran. Este cambio se le tiene que notificar al encargado del activo en cuestión o en su defecto al Directivo en turno.

Queda estrictamente prohibido compartir contraseñas para evitar perder el control sobre los accesos a los sistemas, servicios o aplicaciones. También no se permite escribir las contraseñas en papeles o post-it, ni enviarlas en correos electrónicos o cualquier otro sistema o servicio que permita la captura.

Para no tener escritas las contraseñas en papel, se requiere utilizar gestores de contraseña, mismas que son herramientas de gran utilidad cuando hay que manejar un número importante de contraseñas. Hay algunos gestores de contraseña muy recomendadas, como lo es LastPass.

Nunca se debe utilizar una misma contraseña para diferentes servicios, ni una misma contraseña para un uso personal y profesional.

Las contraseñas deben contener caracteres que lo hagan robusta, se recomienda el uso de @ o puntos, seguidos de combinaciones numéricas fuertes. Jamás poner datos personales en la contraseña, como nombres, apellidos, gustos, etc.

Las contraseñas institucionales deben ser cambiadas cada cierto periodo.

Si es posible, se recomienda en todo momento utilizar la autentificación de dos factores. En donde se defina otro factor para saber la identidad de la persona. Por ejemplo, ingresar con algún código que se envía al número telefónico, o algún otro factor. Esta recomendación se deberá implementar siempre y cuando se esté con las posibilidades.

5.12. Políticas y Prácticas de Seguridad en Página web de la Institución.

Desarrollo y Gestión web

Toda página web desarrollada o editada dentro de la Unidad Académica de Psicología debe considerar la autenticación de dos factores, de manera que, además de la contraseña, el usuario tenga que introducir algún otro código de autenticación. Además, también es importante dimensionar que en la contratación de cualquier servicio se incluya esta consideración.

Es necesario seguir los protocolos generales que tiene la Coordinación de Informática y Telecomunicación de la UAZ al momento de configurar el servidor. Además, es necesario configurarlo con herramientas HTTPS y HTTP Strict Transport Security (HSTS). Esto asegurará que las credenciales de inicio de sesión, cookies, datos POST e información de cabecera permanecen menos disponibles a los atacantes.

Es obligatorio generar copias de respaldo con frecuencia con la finalidad de estar preparado ante la eventualidad más indeseable para un desarrollador, como la infección de la página web y posterior pérdida de datos importantes de la Página Web de la institución. Para esto también es importante tener clones de Página Web, por si el servidor principal de la Universidad se cae, se tenga otra alternativa para los usuarios de la Página web.

Se debe establecer una política de perfiles para el acceso, escritura y modificación de directorios y archivos comunes, aplicando permisos lo más restrictivos posibles, tanto a las carpetas y ficheros como a los usuarios. Esto va a depender de los roles que se asignen.

Al introducir los elementos de programación en la página web, establecer validaciones en todos los campos de datos, y evitar usar instrucciones SQL en las que concatenen cadenas aportadas por los propios usuarios.

Se debe encriptar toda la información sensible, como inicios de sesión de usuario, contraseñas y, por supuesto, los datos bancarios y de carácter personal almacenada en la base de datos que se contrate o tenga. Se recomienda, como mínimo, protocolo AES encrypt.

Se debe disponer de algún servicio de seguridad que permita comprobar de forma periódica si la web de la Unidad Académica de Psicología tiene alguna vulnerabilidad o malware. En este sentido también se debe estar monitoreando constantemente la actualización de Software de servidores como Apache, Mysql, o las herramientas de desarrollo Web que se estén utilizando.

Navegación en Páginas Web

Se recomienda a los a estudiantes, docentes y administrativos no seguir enlaces de e-mail de remitentes desconocidos o de noticias de dudosa procedencia, verificar que la dirección URL de las páginas web sea la correcta y evitar rellenar formularios de páginas web desconocidas o formularios enviados por e-mail. Un mecanismo para saber si una página es confiable o no, es la herramienta WOT o Web De Confianza (Web Of Trust). Es una extensión para navegadores como Chrome o Firefox, que contiene una base de datos de puntos de confianza en confidencialidad, fiabilidad, privacidad y seguridad basada en la reputación de los usuarios que usan esta extensión.

Se recomienda no utilizar dispositivos públicos para ingresar a cuentas donde maneje información sensible, como cuentas bancarias, sistemas administrativos, etc. Tener cuidado en las compras por internet, y utilizar tarjetas virtuales. Así se evitaría el robo de información por diversos medios.

No ingresar información de ninguna índole en formularios dudosos, verificando así que el dominio y la utilización del protocolo HTTPS estén activas, esto con la finalidad de garantizar la confidencialidad de la información.

Nunca ejecutar archivos de dudosa procedencia. Si algún archivo se descarga al momento de navegar por alguna página web es necesario eliminarlo inmediatamente, para evitar cualquier tipo de robo o infección cibernética.

Hacer caso omiso de publicidad falsa que ofrezca recompensas o algún beneficio para usted; recuerde que la mayoría de las veces son estafas. Para evitar este tipo de anuncios se recomienda instalar herramientas como Ad Block Plus.

Siempre que se utilicen herramientas de teletrabajo a través de la navegación de internet, se debe tener siempre el cuidado de tener las herramientas de navegación actualizadas. Se recomienda usar Firefox o Google, aunque cada una de éstas se debe verificar que estén debidamente actualizada y debidamente configurado.

Siempre que se navegue dentro de la Unidad Académica de Psicología, se debe utilizar la opción de "navegación privada o segura" del navegador que se utilizando, con la finalidad de impedir que se almacenen datos personales dentro del navegador como el historial de páginas vistas, imágenes, nombres de usuario y contraseñas.

Queda estrictamente prohibido visitar sitios que comprometan los datos institucionales de la Unidad Académica de psicología, tales como sitios de adultos, sitios donde ofrezcan situaciones fraudulentas, sitios de falsas noticias, entre otras.

Todas las demás recomendaciones abordadas en este documento, se deben sujetar también a las conductas y prácticas que se realizan en cualquier navegación web.

6. POLÍTICAS DE SEGURIDAD PARA SISTEMAS E INFRAESTRUCTURAS INSTITUCIONALES

6.1. Políticas y Prácticas de Seguridad en la configuración y uso de Equipos de Red Cableada

El encargado de la red dentro de la Unidad Académica de Psicología, debe tener una clara y completa comprensión de la infraestructura de la red, como por ejemplo el modelo, la ubicación, las configuraciones básicas de los firewalls, ruteadores, switches, puertos y cableo de Ethernet y Access Points Inalámbricos.

El departamento encargado de la red dentro de la Unidad Académica, debe saber qué servidores, computadoras, impresoras y demás dispositivos están conectados a la red, dónde están conectados y si su conectividad pasa por la red corporativa. Una aplicación recomendada es Fing.

Es necesario estar en un constante monitoreo y mapeo a través de diversas auditorias, esto con la finalidad de encontrar alguna anomalía dentro de la red cableada y así poderlo solucionar adecuadamente.

Se debe tener actualizada toda la infraestructura de la red. En este sentido, se debe estar verificando constantemente que los cables y todos los elementos físicos que componen el buen funcionamiento de la red estén en perfectas condiciones.

Se debe tener en todo momento un filtrado de dirección MAC, proporcionando así un método de autenticación rápida y fácil o de un método de criptografía.

Implementar VLANs para separar el tipo de tráfico de la red (accesos en general, VoIP) y los tipos de usuarios (colaboradores, administración, invitados) por razones de seguridad.

Se recomienda realizar la criptografía de toda la red, con la finalidad de cifrar todo el tráfico de la red. Una opción es el OPsec.

6.2. Políticas y Prácticas de Seguridad en la configuración y uso de Equipos de Red inalámbrica

* Las recomendaciones que se exponen aquí se pueden hacer con servicios privados dentro de la Unidad Académica. Algunas recomendaciones o políticas ya vienen configuradas desde la Coordinación de Informática y Telecomunicaciones de la Universidad, sin embargo, puede considerar combinar algunas recomendaciones.

Todos los Access Point de la institución deben tener una contraseña diferente a la que se tiene por defecto.

Se debe utilizar encriptación WPA o WPA2. El protocolo WEP sólo provee una forma débil de autenticación y no encripta el tráfico en la red inalámbrica, por lo tanto, todos los Access Point o aparatos alusivos al acceso de red inalámbrico deben estar encriptados con WPA O WPA2.

Se recomienda, en la medida de las posibilidades, usar el filtrado por MAC, armando una lista con las MAC de los dispositivos que tienen permitido conectarse a la red, con lo que se rechazará todo equipo cuya MAC no se encuentre en la lista. Esto se puede hacer por áreas o departamentos; considerar dicha configuración.

Se recomienda, en las medidas de las posibilidades, ocultar SSID, mismo que es el nombre de la red. Esto para disminuir el riesgo de que gente que no sea de la institución conozca la rede y logre conectarse.

6.3. Políticas y Prácticas de Seguridad en la configuración y uso de Computadoras

Todas las computadoras de la institución deben tener correctamente instalado un Software Antivirus y/o un software Anti Malware.

Todas las computadoras que tienen Sistemas Operativo igual o menor a Windows 7 debe ser inmediatamente actualizado. Windows 7 ya no tiene soporte, por ende, hay más probabilidades de infección y ataques cibernéticos.

Queda prohibido la inserción de memorias USB en computadoras que contengan información sensible. Si es muy necesario usarla, hay que considerar utilizar una computadora con menos información o ejecutar esa USB dentro de una máquina virtual.

Se deben mantener todas las actualizaciones vigentes en la computadora de los empleados.

Cada computadora debe estar conectada a un regulador, con la finalidad de evitar sobrecargas eléctricas.

Todas las computadoras deben estar en lugares en donde no puedan sufrir ningún riesgo físico, como inundación, derrumbe e inclusive robo.

Todas las computadoras deben tener implementada una contraseña combinado con números, letras y signos. Olvidarse del famoso “1234”.

Se recomienda utilizar Antispyware en todas las computadoras, con la finalidad de detectar cualquier software malicioso.

El Departamento de informática, podrá configurar la computadora con la finalidad de que sólo sea utilizada con fines laborales, a nivel red, y a nivel interno (para instalación de programas, accesos a internet, etc.).

6.4. Políticas y Prácticas de Seguridad en la configuración y uso de Portátiles

Toda Laptop dentro de la institución debe estar resguardado en un lugar seguro, y si es posible, bajo llave cuando no se esté utilizando.

Toda laptop debe tener un sistema antivirus instalado y un sistema Anti Mal Ware.

La laptop sólo se podrá usar con fines laborales. Evitar, en la medida de las posibilidades, traer la laptop a eventos o lugares que no sea con fines académicos.

Toda laptop, en caso de ser vendida, tiene que utilizar un borrado de información segura, a través de un Software anti-forense o técnicas anti-forense. De ser posible, hay que conservar el dispositivo dentro de la institución y seguirle dando uso.

Todas las laptops que tienen Sistemas Operativo igual o menor a Windows 7 debe ser inmediatamente actualizado, por la misma razón que ya explicó con anterioridad en el apartado de uso y configuración de Computadoras.

Queda prohibida la inserción de memorias USB en laptops que contengan información sensible. Si es muy necesario usarla, hay que considerar utilizar una computadora con menos información o ejecutar esa USB dentro de una máquina virtual.

Toda laptop debe tener una contraseña configurada, misma que contenga números, dígitos y símbolos robustos.

Considere instalar alguna alerta en la laptop, con la finalidad de saber la ubicación en caso de ser robada.

Tomar en cuenta las Políticas implementadas para el uso y configuración de Computadoras.

6.5. Políticas y Prácticas de Seguridad en el uso y configuración de sistemas administrativos (Tauro, siaaf, etc.)

Se deben establecer roles muy específicos para el uso de cada uno de los sistemas.

En la medida de las posibilidades, se deben crear cuentas de usuario diferente para cada persona que lo use.

Se debe evitar en todo momento el uso de las contraseñas que vienen por defecto en los sistemas y aplicaciones, ya que pueden ser fácilmente identificables. Esto aplica para todos los sistemas de la Universidad, tales como Tauro, control escolar, además de Módems y herramientas tecnológicas que se adquieran. Este cambio se le tiene que notificar al encargado del activo en cuestión o en su defecto al Directivo en turno.

Toda la información confidencial que se suba a sistemas debe estar debidamente respaldada y asegurada.

Se debe tener muy claro la entidad o persona a la que hay que acudir en caso de que exista alguna falla, hackeo o pérdida de información en los diferentes sistemas utilizados.

Todos estos sistemas administrativos sólo deben estar instalados en computadoras o dispositivos autorizados por la Coordinación de Informática y Telecomunicaciones de la UAZ.

6.6. Políticas y Prácticas de Seguridad en el uso y configuración de sistemas para eventos, servicio social, etc.

En el caso de desarrollar sistemas dentro de la Unidad Académica, se debe considerar la protección ante ataques DDos, inyección SQL y si es posible, utilizar ofuscamiento del código utilizado.

Sede debe tener un protocolo mínimo de encriptación, en caso de aquellos datos que sean sensibles. Para el uso de base de datos se puede utilizar, como mínimo, el protocolo de encriptación AES ENCRYPT.

Todo software contratado o desarrollado dentro de la institución debe realizar constantes respaldos de la información que se tenga en los hostings o servidores para tal sistema.

Es necesario que cada uno de los sistemas contratados, instalados y usados dentro de la Unidad Académica de Psicología, cuenten con un Manual técnico y de configuración, tanto del lado de usuario como del lado de administrador.

Es conveniente hacer auditorias constantes al sistema, y cerciorarse de que la Seguridad que se utilizan en éstos sea la correcta.

En el caso de sistemas de Gestión, se deben asignar roles de uso para cada uno del personal, con la finalidad de evitar malas prácticas y pérdida de la información.

7. POLÍTICAS DE SEGURIDAD DEL PERSONAL ADMINISTRATIVO Y DEL RESCURSO HUMANO

El eslabón más importante para conservar la Seguridad de la Información dentro de cualquier institución se encuentra en el Factor Humano. Si bien, las medidas que se han ido abordando con anterioridad conllevan una serie de prácticas respecto a diversos activos, es importante también abordar todo lo que tenga que ver con el personal. En primera instancia, lo que se tiene que implementar en todo momento es la ***capacitación, concientización y culturización al personal que labora en esta institución***, estas acciones deben estar orientadas a temas de la Seguridad de la Información. Partiendo de esto, es bueno considerar las recomendaciones, buenas práctica y políticas que se exhiben a continuación.

7.1. Buenas Prácticas en Direcciones y Coordinaciones

La Dirección deberá requerir a trabajadores, docentes, estudiantes y usuarios de terceras partes, aplicar la seguridad en concordancia con las políticas y los procedimientos establecidos en este documento, incluyendo a integrantes del Consejo de Unidad, estudiantes, personal de limpieza, choferes y todo aquel personal que tenga relación con la institución.

Es necesario establecer la responsabilidad para asegurarse de que el abandono de la Unidad Académica de Psicología por parte de los trabajadores o terceras personas se controle, y así asegurar que se devuelva todo el equipamiento, o en su defecto, se elimine de forma completa todos los derechos de acceso, así como la información importante.

En caso de no existir, es necesario establecer un reglamento dentro del Consejo de Unidad, con la finalidad de tener bien claros los procesos internos que éstos siguen. En caso de su existencia, será responsabilidad de la Dirección hacer que se cumplan con debidos lineamientos.

Todas las responsabilidades de seguridad se deben definir antes de la contratación laboral mediante la descripción adecuada del trabajo y los términos y condiciones de empleo; si bien las definiciones se dan a nivel Universidad, se recomienda que dentro de la Unidad se establezcan los criterios para el cuidado de la Seguridad de la Información y protección de datos, aplicándolo en administradores, trabajadores, e inclusive, estudiantes.

La Dirección estará atenta en todo momento de estar capacitando a sus trabajadores, docentes y estudiantes en temas relacionados con la protección de datos, seguridad de la información y todos los temas necesarios para conservar la integridad, la disponibilidad y confidencialidad de los activos de la información, incluyendo, en este sentido, al factor humano.

Todos los activos que se encuentran dentro de dirección y departamentos afines, deben estar en constante resguardo; se recomienda no permitir ingresar memorias USB a los dispositivos con información sensible, hacer respaldos constantemente y seguir todas las medidas anteriormente descritas en este documento.

La Dirección y todo lo que subyaga de ésta, debe definir y establecer los procesos disciplinarios y el tratamiento que se le dará a los casos de incumplimiento al presente documento de políticas de seguridad de la información.

7.2. Buenas Prácticas en procesos administrativos

Los trabajadores y usuarios de terceras partes de los servicios de procesamiento de la información deben firmar un acuerdo sobre las funciones y las responsabilidades con relación a la seguridad de la Información, todo esto para que cada uno tenga bien claros y estructurados sus roles y alcances.

Se debe tener riguroso cuidado en los procesos de recolección, entrega y archivo de documentos que contengan información sensible. Tales procesos incluyen desde inscripción hasta el procesamiento de facturas a través de los diferentes sistemas.

No se otorgará ningún tipo de información confidencial, como calificaciones, datos personales, dirección, teléfono o correo a personas que no estén debidamente identificadas y que no formen parte del personal administrativo que tenga autorización y acceso a esa información.

Es de suma importancia tener los inventarios actualizados y listos para cualquier contingencia. Lo anterior se justifica en situaciones donde se presente que un trabajador se va, y así sería mucho más fácil verificar si el inventario de activos ha sido actualizado y si hace falta algún activo en esa actualización.

Se deben definir adecuadamente las funciones de cada una de las áreas, así como los procedimientos que relacionen a cada una de éstas, de modo que, para el usuario y para los trabajadores, sea más fácil conocer a cuál área se debe asistir y el proceso a seguir para realizar el trámite solicitado, o en su defecto, en caso de alguna contingencia relacionada a la Seguridad de la Información.

Dentro de los procesos administrativos, sea cual sea que fuese, se deben seguir todas las recomendaciones anteriormente descritas, de modo que, si se hace uso de cualquier activo de información se deben seguir sus medidas específicas y pertinentes.

Toda la comunidad universitaria que haga uso de la información de la institución, ya sean docentes, trabajadores o estudiantes de la Unidad Académica de Psicología, deben dar cumplimiento a lo indicado en el presente documento de políticas de seguridad de la información y asistir a las charlas y eventos que se convoquen para fomentar la cultura y concientización de la protección de datos y Seguridad de la Información.

7.3. Buenas Prácticas en procesos de Recepción.

Todo personal contratado externamente (conferencistas, profesores, profesores temporales, etc.), deben tener acceso a información, pero primero se debe firmar algún Acuerdo de Seguridad, antes de otorgar acceso a las instalaciones o a la plataforma tecnológica.

Todo personal que esté involucrado en procesos de recepción de documentos, incluyendo el ámbito de dirección, debe ser sumamente cuidadoso en el tratamiento y procesamiento de estos, siempre salvaguardando la integridad, confidencialidad y disponibilidad de los documentos.

Todo miembro universitario, ya sea docente, administrativo o estudiante debe de ser sumamente cuidadoso de no difundir información confidencial o personal que tenga relación con la institución académica o con cualquiera de los activos de información de esta misma. Estas acciones aplican a la difusión por escrito, verbal o digital.

8. CONTROL DE ACCESOS

A la medida de las posibilidades, se debe tener cierto control en el acceso a la institución, con la finalidad de tener un registro en caso de cualquier incidente. Por las condiciones del mismo edificio a veces esto es imposible, sin embargo, hacer algún esfuerzo para poder implementar esta política aporta al cuidado de los diferentes activos.

Se debe regular todo tipo de acceso a las áreas en donde se mantengan datos personales de docentes, estudiantes y trabajadores, la gente externa y que no labore en el área administrativa, no podrá ingresar a esta información sin la debida autorización expresa de los responsables o directores de dicha información y/o institución.

Los encargados de la red deben asegurar que las redes inalámbricas cuenten con mecanismos de autenticación que evite los accesos no autorizados.

Todo personal administrativo que haga uso de sistemas tecnológicos como lo son de control escolar, facturación, servicio social, entre otros, debe cambiar la contraseña inicial, después de que le fue asignada al sistema. Además, esa contraseña, debe seguir estándares de seguridad robustos.

Solo deben tener acceso a los activos de información los usuarios y personal autorizados, su usuario y contraseña asignados para tal efecto; en ningún caso deben acceder usando una cuenta diferente, y jamás debe facilitar esa información a terceros.

Todo miembro de la comunidad universitaria que haga uso de los recursos tecnológicos y los sistemas de información, debe realizar un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual se les ha permitido el acceso. Todo esto a través del seguimiento de este documento. La dirección y los encargados de los activos de información podrán reservarse el derecho de negarles el uso de cualquier recurso si no se respeta esta Política.

Todo aquel personal administrativo, docente o usuario de los recursos tecnológicos de la Unidad Académica de Psicología deberán apegarse a todos los lineamientos de este documento, conservando así la seguridad de los datos de todos y todas.

9. SEGURIDAD FÍSICA Y AMBIENTAL

Todas las puertas, cajones o espacios que contengan cualquier tipo de activo deben permanecer cerrado bajo llave si este no está siendo utilizado por alguno de los usuarios, encargados o trabajadores.

Se deben establecer mecanismos adecuados de vigilancia, a través de cámaras, rondines y colaboración entre todos los miembros de la comunidad. Respecto a la cámara, se le debe dar mantenimiento y corrección cada cierto tiempo.

Tanto en los centros de cómputo, como en lugares donde se tenga mayor acercamiento de activos de información tecnológicos, se debe implementar un protocolo de registro de entrada y salida, con la finalidad de tener un control más idóneo en los inventarios.

Los encargados de los centros de cómputo dentro de la Unidad Académica, deberán asegurarse que dentro, y cerca del lugar establecido, no se encuentren espacios inflamables y que se otorguen todas las medidas necesarias para prevenir riesgos de inundaciones, incendios, o derrumbes que afecten los activos de información que ahí se encuentren.

Ningún docente, administrativo o estudiantes deben abrir o destapar los equipos de cómputo la Unidad Académica de Psicología, así como ningún elemento que no le competa abrir o reparar. Solo el personal con las facultades asignadas podrá reparar, abrir o checar cualquier activo de información tecnológica de la Unidad.

Los docentes y administrativos de la Unidad Académica de psicología deben dejar su escritorio físico libre de información confidencial propia de la Unidad Académica de psicología, así mismo no debe dejar ningún documento que pueda comprometer cualquiera de los procesos de la institución. Esto aplica también en el escritorio de las computadoras; si la computadora es de uso comunitario, se debe tener la precaución de no dejar ningún documento en la computadora, para evitar cualquier tipo de riesgo como plagio o divulgación no autorizado.

Se deben tomar todas las medidas anteriormente descritas en este documento, en donde se consideran aspectos físicos como de cableado, eliminación de documentación, entre otros.

10. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Los encargados de gestionar las tecnologías, según sea el rol asignado por parte de la Coordinación Administrativa debe en todo momento notificar a las Coordinaciones y Departamentos pertinentes todos los incidentes detectados que puedan causar la pérdida de los pilares de la Seguridad de la Información y el funcionamiento de los activos de información dentro de la Unidad Académica de Psicología. Todos los incidentes y/o riesgos que se deben tomar en cuenta para hacer una notificación inmediata y establecer un plan para mitigarlos son aquellos relacionados con el Acceso no autorizado, Persecución (Civil, fiscal o penal), Orden de secuestro/Detención Ataque físico o electrónico, Daños por vandalismo, Fraude/Estafa, Extorsión, Robo / Hurto (físico), Robo / Hurto de información electrónica, Virus / Ejecución no autorizado de programas, Violación a derechos de autor, Incendio, Inundación / deslave, Sismo Falta de ventilación, Sobrecarga eléctrica, Falla de corriente (apagones), Falla de sistema / Daño disco duro, Falta de capacitación sobre riesgos, Mal manejo de sistemas y herramientas, Utilización de software "pirateado", Falta de conocimiento de software nuevo, Perdida de datos, Infección de sistemas a través de USB, Tener USB con información sensible, Compartir contraseñas o permisos a terceros, Extravío de equipo, (USBS, laptop, computadora), Sobrepasar autoridades, Falta restricciones del personal, Falta de mantenimiento físico Falta de actualización de software, Fallas en permisos de usuarios (acceso a archivos), Accesos no autorizados a Sistemas, Falta de normas y reglas claras y Ausencia de documentación.

Los miembros encargados de la gestión de recursos tecnológicos dentro de la Unidad Académica deben estar capacitados para poder tener una respuesta inmediata a los riesgos que le sea pertinente responder. En caso de que haya algún riesgo que no se pueda solucionar dentro de los alcances de los encargados, tendrán que saber a qué instancia acudir, ya sea dentro de la Universidad Autónoma de Zacatecas o alguna instancia externa especialista en resolver las amenazas antes mencionadas.

Los encargados de gestionar los recursos tecnológicos e incidentes dentro de la institución, deberán notificar las estrategias, lineamientos y acciones establecidos para gestionar adecuadamente los riesgos e incidentes de Seguridad de la Información.

Se deben llevar a cabo sesiones de análisis de los incidentes, y en su defecto, sesiones de auditorías (como pentesting u otras técnicas) para poder saber el estado de vulnerabilidad y criticidad de cada uno de los activos de información registrados en los Análisis de Riesgos de la Unidad Académica de Psicología.

Los docentes, administrativos y estudiantes deben ser responsables con el uso de cualquier activo de información, y en su caso, deberán reportar cualquier incidente relacionado con la seguridad de la información y los recursos tecnológicos de manera inmediata; no deberán tratar de reparar el daño o modificar cualquier condición del activo en ese momento.

En caso de que haya pérdida de información sensible, o divulgación de alguna de esta, los docentes, administrativos o usuarios en general deberán reportarlo de inmediatamente a las Direcciones o Coordinaciones Administrativas.

Los encargados de gestionar los recursos tecnológicos y los activos de información en general, deberán crear protocolos para ir recolectando evidencias sobre los riesgos, apoyándose de herramientas como Análisis de Riesgos, Matrices TVA o inclusive sistemas y estándares para registros de la Seguridad de la Información. Es importante recabar todos incidentes para poder ir creando un historial y empezar a trabajar en el nivel de magnitud de daño para la Unidad si se llegará a perder la confidencialidad, integridad y disponibilidad de alguno de los activos de información esenciales.

Se debe tener comunicación efectiva en todo momento con la Coordinación de Informática y Telecomunicaciones de la Universidad Autónoma de Zacatecas, con la finalidad de recibir orientación oportuna e inmediata en caso de una emergencia relacionada con los activos de información. También es importante recibir capacitación por parte de esta Coordinación y por otras entidades especializadas en temas de Gestión de riesgos.

11. CUMPLIMIENTO DE LAS POLÍTICAS

El cumplimiento de estos lineamientos, políticas y Buenas prácticas podrá evitar muchos de los riesgos descritos en el apartado de Gestión de Incidentes de este documento, por lo que, se vuelve esencialmente necesario el cumplimiento en su totalidad de lo que se indica aquí.

Todos los lineamientos que se abordan en este documento, deben estar sujetos y orientados a la Lineamientos para la Protección de Datos Personales en posesión, en este caso, de la Unidad Académica de Psicología. El cumplimiento de estos lineamientos ayudará a cumplir parcial o totalmente dicha Ley.

Se deben establecer mecanismos para fomentar el debido uso de Software, Licencias, Libros y artículos en el personal docente, administrativos y estudiantes de la Unidad Académica de Psicología, con la finalidad de respetar las leyes de derechos de autor y todo lo que subyaga de esta misma.

Los encargados de los activos, las direcciones y las Coordinaciones de la Unidad Académica de Psicología deben monitorear constantemente que se haga uso adecuado de este documento y que se apliquen la mayoría de los lineamientos para hacer respaldos, usar sistemas, configurar redes, controlar accesos y todas las acciones que se describen en este documento para poder conservar la información y los activos de información de una manera correcta y efectiva.

Se deben establecer mecanismos efectivos y avalados por el Consejo de Unidad, Directores y Coordinadores, para establecer sanciones en la falta de uso de este documento y de las repercusiones que pudiera haber si no se usa el mismo, en donde se deben integrar todo aquello que acontezca a la divulgación no autorizada de información, malas prácticas de Seguridad de la Información que pongan en riesgo la confidencialidad, disponibilidad e integridad de los datos y todo aquello que se genere a partir de una negligencia del factor humano en el uso de los activos de información.