UNIVERSIDAD AUTÓNOMA DE ZACATECAS

"Francisco García Salinas"

Implementación de ingeniería social para la detección de vulnerabilidades en los sistemas de información utilizados en la Universidad Autónoma de Zacatecas, Centro Educativo Rotary y la Coordinación de la Secretaría de Seguridad Pública, basados en metodologías de pentesting.

Pedro Morales González

MAESTRÍA EN INGENIERÍA Y TECNOLOGÍA APLICADA.

Asesores de tesis:

M.I.A. Santiago Villagrana Barraza.
M.I.A. H Carlos Castañeda Ramírez.
Dr. Sodel Vázquez Reyes.

Zacatecas, Zac., julio del 2020

Resumen: En la actualidad el cibercrimen es un riesgo para las organizaciones no importando el giro que esta tenga, los sistemas informáticos con los que cuentan son atacados, esto con múltiples fines, debido al aumento del uso de la tecnología y de la poca importancia que se le da a la seguridad al implementarla tienden a comprometer sus procesos y en el peor de los casos la información que estas poseen. Cualquier dispositivo conectado a una red local y con salida a internet es blanco y ventana a diversas amenazas, poniendo en riesgo la integridad de la información que existiese en el lugar donde se realice la conexión.

Actuar ante un incidente pudiera ser más costoso que capacitar al personal, ya sea con buenas prácticas en la seguridad informática, tener políticas sobre esto. O simplemente saber que acciones tomar para prevenir un ataque, las pruebas de penetración son parte fundamental en la detección de las vulnerabilidades potenciales; Vulnerabilidades que, aprovechadas por los atacantes, pueden tomar decisiones importantes sobre la organización, sin preocuparse por los daños que este puede causar.

Este trabajo revisa ,compara diferentes metodologías e implementa la que por los requerimientos se mejor se adapta, a su vez se habla de herramientas utilizadas actualmente para la detección de vulnerabilidades llámese software o hardware; Con el fin de detectar las principales fallas a los servicios que brindan la Universidad Autónoma de Zacatecas, Centro Educativo Rotary y La Secretaría de Seguridad Pública, obteniendo como resultado diversas vulnerabilidades empezando por el recurso humano, el equipo implementado y hasta en alguno de los casos los sistemas de información que pretenden brindar un servicio al publico, brindando la oportunidad de extraer información critica para la operación de las organizaciones mencionadas.

Palabras clave: Seguridad, Virus, Infraestructura, Vulnerabilidades, Ataques, Metodologías, Herramientas, Detección de vulnerabilidades.

ÍNDICE DE TESIS

Índice de Ilustración

Índice de gráficas

Dedicatorias

Este trabajo está dedicado a todas las personas que confiaron y proporcionaron las herramientas necesarias para la elaboración de este proyecto, directores, encargados de programas, secretarios, etc. Personas que sin saber fueron partes de ello.

En especial a toda mi familia, a mis padres, por su gran ejemplo y valioso apoyo desde el inicio de mis estudios, gracias a ustedes ahora culmino una meta más. Maestros cuyo conocimiento se me impartió para darle el mejor de los usos para un bien.

A mi hijo por todas las veces que este proyecto le quito el tiempo que él requería, de igual forma a mi pareja que por su insistencia todas esas ideas y micro trabajos realizados, hoy es posible tenerlos escritos.

1. CAPÍTULO I. INTRODUCCIÓN

1.1. Introducción

La presente tesis está orientada a la implementación de metodologías de pruebas de penetración (pentesting) una vez aplicado un cuestionario realizado a partir de las investigaciones de la Asociación Nacional de Universidades e Instituciones de Educación Superior mediante ingeniería social, metodologías, y cuestionarios que previamente fueron rediseñados para ser adaptados a las necesidades y realidad en la cual estaba realizando, con la finalidad de detectar los sistemas, tipos de información y vulnerabilidades que estos poseen.

Esta tesis consta de siete capítulos:

Capítulo I.- Plasma el contexto actual de la seguridad informática. Se mencionan los tipos de ataques que los cibercriminales realizan y su clasificación, al igual, se presenta la problemática de las organizaciones ante estos. En este capítulo también se define la formulación del problema, los objetivos de la investigación, la justificación e hipótesis.

Capítulo II.- Presenta los antecedentes de está investigación, lo que es la gestión de riesgos, políticas existentes que sirvieron de guía y referencia para la elaboración de ésta; También un resumen de las distintas metodologías de pentesting, necesarias para un mejor entendimiento de esta investigación.

Capítulo III.- Expone cada una de las organizaciones a las que se realizó el pentesting, lo extensas que estas pueden llegar a ser, y el porque de las áreas a evaluar.

Capítulo IV.- Describe la metodología de trabajo utilizando las bases del Penetration Testing Execution Estándar, para la gestión de las fases a seguir en el desarrollo del pentesting.

Capítulo 5.- Desarrolla las 7 fases de la prueba de penetracion a la Universidad Autónoma de Zacatecas en el edificio donde se encuentra el Sistema Institucional de Información Administrativa y Financiera (SIIAF), en el Centro educativo Rotary directamente a los servicios web y área administrativa y en el edificio donde actualmente se encuentra la Coordinación de la Secretaria de Seguridad Pública.

Capítulo 6.- Interpreta las graficas con los resultados de la encuesta que se aplico en la aplicación de ingeniería social.

Capítulo 7.- Realiza la conclusión de los resultados y la validación de la hipótesis, de igual forma se analiza al empleado sobre el conocimiento que se tiene ante los temas de seguridad de la información basados en la encuesta realizada.

1.2. Presentación

El uso de la tecnología ofrece una gran variedad de ventajas en múltiples áreas y sectores, ejemplos de esto existen muchos, por mencionar algunos el sector automotriz donde podemos ver vehículos con computadoras de viaje, múltiples sensores cuya función es alertar al conductor de alguna anomalía en coche o sus alrededores, algunos otros cuentan con una tecnología más compleja que le permite mayor independencia al manejar. En el sector médico observamos dispositivos que alertan y/o apoyan a los doctores en la predicción de algunas enfermedades, en las organizaciones proveen una gran oportunidad para incrementar la productividad, actualmente muchos empleados traen al trabajo sus teléfonos inteligentes, tabletas y laptops en los que instalan software para su apoyo, por último en el sector educacional, al igual que en el organizacional provee un sin fin de beneficios a los docentes y alumnos, ya que brinda un plus al dar acceso a una gran variedad de información y recursos para la educación .

Esto viene aunado con un tema que para muchos pasaban desapercibido y se le daba poca importancia, pero debido a diversos a taques se le ha puesto en la mira de muchas organizaciones por lo crítico que puede llegar a ser; Entiéndase al hablar de ciberseguridad a la “Protección de activos de información, mediante el tratamiento de las amenazas que ponen

en riesgo la información que se procesa, se almacena y se transporta mediante los sistemas de información que se encuentran interconectados" (ISACA,2013).

Por lo tanto, la seguridad de la información es el estado de "seguridad" de la información en la que se mantiene baja o tolerable la posibilidad de robo, manipulación y destrucción de la información y servicios.

La seguridad de la información debe cuidar cuatro puntos importantes:

- **Confidencialidad.** Garantía que la información se accesible solo a quien tiene la autorización de acceder a ella.
- **Integridad.** La confiabilidad del dato o recurso en términos de prevenir el cambio incorrecto o no autorizado.
- **Viabilidad.** Garantía de que el sistema responsable del almacenamiento o llevar el proceso de la información sea accesible cuando se requiere por el usuario.
- **Autentificación** Autentificar que la información sea genuina.

Según (Certiffed Ethical Hacker,2016) el nivel de seguridad de cualquier sistema se puede definir por la fortaleza de estos tres componentes:

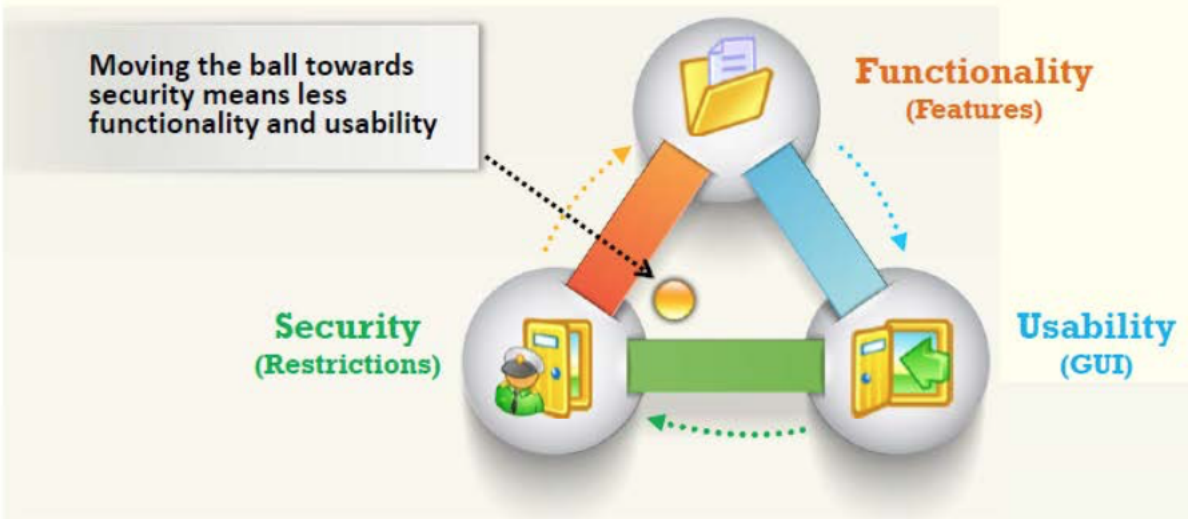


Ilustración 1.-Componentes para medir el nivel de seguridad.

En los últimos años hemos visto diferentes tipos de ataques cibernéticos, con múltiples fines, en los que podríamos destacar dos:

Ciberterrorismo: “Es aquel ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos” (Urueña, 2015)

Ciberdelincuencia: Delito informático cuya acción ilegal se da por vías informáticas, este tiene un alcance mayor, donde se incluyen delitos como fraude, robo, chantaje, falsificación, etc.

Existen muchas formas y métodos para estar “seguros”, pero esta simple palabra llega a ser algo abstracto hasta en el área de las TICS, ya que realmente nunca estaremos total mente protegidos, pero si podremos disminuir los riesgos a los que estamos expuestos.

Ataques cibernéticos a organizaciones

Existen gran variedad de ataques y muchos de estos se llegan a complementar para tener un mayor grado de impacto, es importante conocer al menos los más frecuentes, los que implican menor complejidad y no implican grandes recursos por ejemplo el Ataque de DDoS (Distributed denial of Service) que al traducir es un ataque distribuido denegación de servicio; lo que hace es atacar al servidor desde muchas computadoras para que deje de funcionar e interrumpir el servicio. Por otro lado, existe código malicioso de los que podríamos destacar los virus, troyanos, worms, etc. cuya intención es multifactorial, y con el único objetivo de ejecutar procesos en el sistema sin que el usuario se percate de ello.

Con el uso de herramientas informáticas y la falta o mala capacitación a los empleados en temas de seguridad de la información dan auge una práctica conocida como Phising, este método es muy utilizado en la web, comúnmente enviado por correo electrónico, la cual contiene un link a una página falsa en donde debemos tener cuidado debido a que podemos ingresar datos personales, cuentas de banco, passwords, etc. que pueden ser usadas de forma incorrecta o sin la autorización requerida ya sea para el robo de credenciales o robo de información digitalizada.

El 4 de julio (Policía de Ciberdelincuencia, 2016) lanza la alerta preventiva contra la delincuencia No. 42. Debido a que a muchas empresas sufrían un ataque que restringe el acceso a nuestros archivos o en casos muy extremos se nos impide el acceso a nuestro dispositivo telefónicos móviles sean Android o IOS (Policía de Ciberdelincuencia, 2016), ¿qué quiere decir eso? Pues bueno, se puede decir que es un secuestro de información, que de la misma forma que en la vida real, se nos pide un pago para poder rescatar los datos o el acceso al dispositivo, este ataque recibe el nombre de Ransomware.

Ataques cibernéticos a organizaciones.

Frente al avance de las TICS combinadas con la expansión de Internet, se ha creado el denominado Ciberespacio. En este lugar se incluyen muchas organizaciones sean instituciones educativas públicas y privadas, servicios gubernamentales incluyendo los hospitales, las policías y el ejército, bancos, etc.

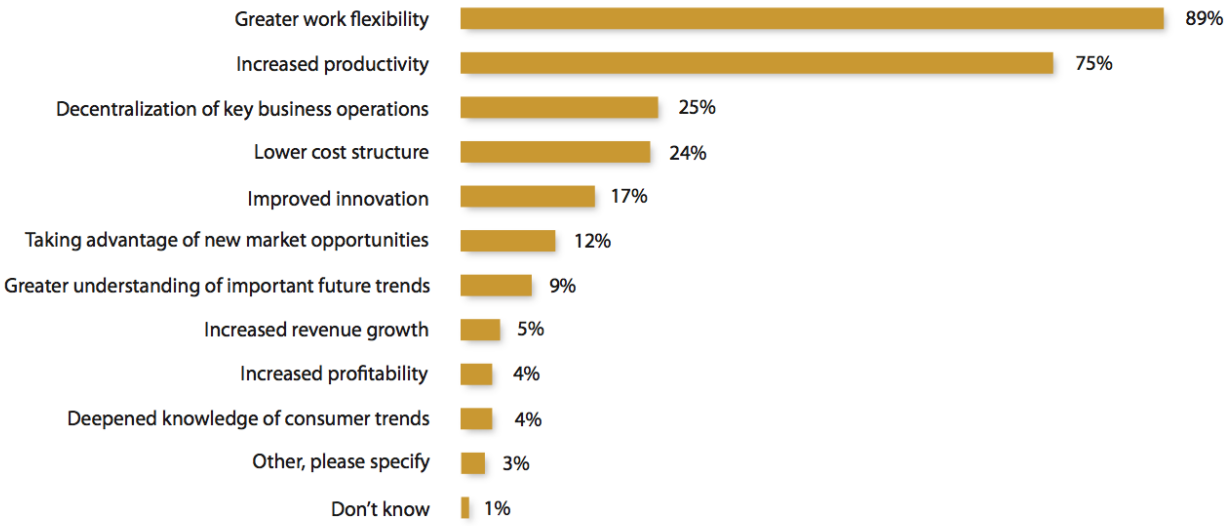


Ilustración 2.-Beneficios asociados a la ciber movilidad. (Hamilton, 2011)

Es importante hablar del ciberespacio y la ciber movilidad debido a que existen tres tipos de penetración a una empresa normalmente conocidos como:

- Black-Box: Este tipo de penetración no se conoce información sobre la infraestructura del blanco y no se tiene acceso a él, todo se maneja de forma externa.
- Grey-Box: se tiene un acceso y conocimiento limitado de la infraestructura que se necesita probar.
- White-Box: se conoce en su totalidad al igual que se tiene acceso total a la infraestructura a probar.

En un reciente estudio de Cisco, el 95% de todos los que participaron en el estudio indicaron que se les permite como empleados utilizar sus propios dispositivos en el trabajo. Además, el número de dispositivos que llega a utilizar un trabajador a lo largo de la jornada de trabajo está aumentando a más de tres dispositivos por empleado y la empresa puede ahorrar de $300 a más de 1,000 dólares por empleado.

El recurso humano es una de las principales debilidades en cuestión de seguridad de las empresas, ya que muchas veces estos no cuentan con la capacitación adecuada para un ataque a sus dispositivos por lo que facilita al hacker poder pasar de una fase de black-box a grey-box de una manera más fácil y rápida.

La llamada BYOD (Bring Your Own Device) y Shadow IT se refieren a la tendencia en la cual los empleados tienen la posibilidad de llevar y utilizar sus propios dispositivos móviles para acceder a los recursos de la compañía, para incrementar la productividad y eficiencia, generando grandes beneficios económicos. Desde smartphones privados, memorias USB, impresoras privadas, etc. Todos los recursos tecnológicos que se encuentra fuera de su propiedad o control.

Ilustración 3.-Porcentaje de empresas que creen que aumentará el BYOD

La cantidad de dispositivos en los seis países (Estados Unidos, Reino Unido, Alemania, India, China y Brasil) crecerá el 105 por ciento, de 198 millones a 405 millones, entre 2013 y 2016. (Loucks, Medcalf, Buckalew, & Faria, 2013)

Con dicha implementación se han creado nuevos flancos de vulnerabilidad poniendo en jaque a los departamentos de TI. Esto porque el funcionamiento de los servicios podría ser alterado por ejemplo si un empleado pierde o le es robado su Smartphone, la mayoría de las empresas no cuenta con una protección adecuada o mínimamente con un Mobile Device Managment los cuales son programas que permiten llevar a cabo de manera remota la instalación de aplicaciones, la sincronización de archivos o el rastreo de dispositivos y en el caso de ser necesario se puede realizar la eliminación remota de datos. Ya que la persona que lo encuentre puede tener acceso a información privada de la compañía y comprometer la información de la empresa para posteriormente darles un mal uso, llámese cuestiones políticas, crimen organizado, un grupo terroristas o simplemente empleados descontentos que sustraen información por despecho, según un reciente estudio, en el 2016 el 60% de los ataques perpetrados en empresas se llevaron a cabo desde dentro.(Mediacenter Panda, 2016)

Empleando las herramientas tecnológicas hoy libremente disponibles, se podrían saturar las comunicaciones o apoderarse de los servidores que controlan dichos servicios, paralizando por ejemplo transacciones financieras y las operaciones bancarias.

Ilustración 4.-Marcas reconocidas con Mobile Device Management

Grandes empresas como Sony, EBay, Evernote, etc. han sufrido importantes ataques en sus bases de datos en los últimos años. Dejando la información de todos sus usuarios a manos de los denominados “hackers”, ya sea como anteriormente se mencionó con fines políticos o con la intención de robar información y dinero.

En julio del 2015 una página de citas llamada Ashley Madison encargada como lo dice su nombre hacer citas con personas ya casadas, sufrió un ataque en el que la empresa perdió 151 millones de dólares debido a que los usuarios expuestos la demandaran. (KARL THOMAS, 2015)

En mayo del 2014 eBay pidió a los usuarios de PayPal, la página web de pagos online de su propiedad, que cambiaran sus contraseñas de acceso. Según la portavoz de eBay

“los hackers copiaron una base de datos de usuarios que contenía esas contraseñas, así como direcciones de correo electrónico, fechas de nacimiento, direcciones de correo y otra información personal, pero no los datos financieros como números de tarjetas de crédito.” (Miller, 2014).

En este caso todas estas organizaciones perdieron información confidencial, ya que tenía la información de sus clientes, de sus decisiones, de sus cuentas, etc. Poniendo está en manos de cibercriminales que pudieran hacer pública de una forma no autorizada y esto puede suponer graves consecuencias, ya que se perderá credibilidad de los clientes, se perderán posibles negocios, se puede enfrentar a demandas e incluso puede causar la quiebra de la organización.

El crecimiento en el uso de la información ha llevado a que los temas relacionados con su seguridad cobren importancia dentro de las organizaciones. Lo más complicado al momento de incorporar un modelo de ciberseguridad es que, generalmente, no están enfocados en los objetivos del negocio y sus intereses.

Protección ante los ciberataques en las empresas

La información, los procesos, servidores y la red, son acticos de importancia, por lo que se tienen que proteger de manera adecuada ante las amenazas comunes que se conocen, para evitar la disponibilidad, integridad y confidencialidad.

Con una política de seguridad adecuada, los riesgos se reducen. El problema es que muchas empresas no están preparadas, como se deriva de la encuesta de IBSG Cisco, donde se recoge que sólo la mitad de las grandes empresas y el 41% de las compañías medianas cuentan con una política vigente en relación con el acceso a la red corporativa por parte de dispositivos ajenos a la empresa.

Entre políticas de las empresas comúnmente requeridas, un empleado debe estar de acuerdo en permitir que el departamento de TI de la empresa instale, actualice y controle bajo cierto tipo de software de seguridad el dispositivo del empleado, incluyendo la capacidad de borrar por completo si el empleado deja la empresa voluntariamente o no.

Ataques cibernéticos a universidades.

Las TIC´s se han convertido en una herramienta insustituible y de indiscutible valor para las universidades, ya que permite acceder a un sin fin de información. Permitiendo a los alumnos la posibilidad de disponer de información reciente, interacción y colaboración entre

ellos, y un desarrollo de nuevas competencias. (Canós, Ramón y Albaladejo, 2008) Mencionan algunas de las ventajas que se pueden apreciar gracias al implemento de las TIC´s:

- Acceso de los estudiantes a un abanico ilimitado de recursos educativos.
- Acceso rápido a una gran cantidad de información en tiempo real.
- Obtención rápida de resultados.
- Gran flexibilidad en los tiempos y espacios dedicados al aprendizaje.
- Adopción de métodos pedagógicos más innovadores, más interactivos y adaptados para diferentes tipos de estudiantes.
- Mayor interacción entre estudiantes y profesores a través de las videoconferencias, el correo electrónico e Internet.
- Colaboración mayor entre estudiantes, favoreciendo la aparición de grupos de trabajo y de discusión.

Hasta hace algunos años, las universidades solían estar tecnológicamente mejor equipadas que la mayoría de los estudiantes. Por ejemplo, muchos estudiantes no tenían una computadora en su casa, pero podían utilizar las del centro de cómputo. Sin embargo, los avances en la tecnología han permitido que exista mayor competitividad y demanda entre las empresas que desarrollan dispositivos móviles y esto hace que más usuarios puedan acceder a dicha tecnologías, ya que al haber competencia bajan los costos, por lo que ahora es común que los estudiantes dispongan de tecnología más avanzada, productiva y eficaz que la que dispone la universidad.

Pero al igual que en las empresas, la tecnología se vuelve un arma de doble filo y sufren de ciberataques, en las que información de docentes y alumnos quedan comprometidos. Sean proyectos, patentes, teléfonos, correos, etc. toda esta información debería estar protegida bajo un modelo adecuado de ciberseguridad.

Según (SDPnoticias, 2013) Las universidades dedicadas a la investigación en Estados Unidos son sujetas de un creciente número de ataques cibernéticos, principalmente de China, y algunos de ellos han sido exitosos en robar información.

En Alemania en abril de 2016 tres universidades confirmaron tener un ataque desde el interior de la red, su objetivo fueron las impresoras, en las que se imprimieron panfletos antisemitas y racistas.

Rijkhoek porta voz de una de las universidades afectadas menciona que los empleados denunciaron los hechos al centro de procesamiento de datos de la universidad, al departamento jurídico y al de prensa. La institución académica contó alrededor de 190 impresiones, algunas procedentes de impresoras que fueron accionadas a distancia más de una vez. (El Intransigente, 2016).

Cabe aclarar que los incidentes de seguridad no solo hacen referencia a los ataques ya anteriormente mencionados, ya que también se deben de contemplar todas aquellas que puedan afectar la disponibilidad, factores como inundaciones, terremotos, incendios, etc.) al igual que siempre está el factor humano.

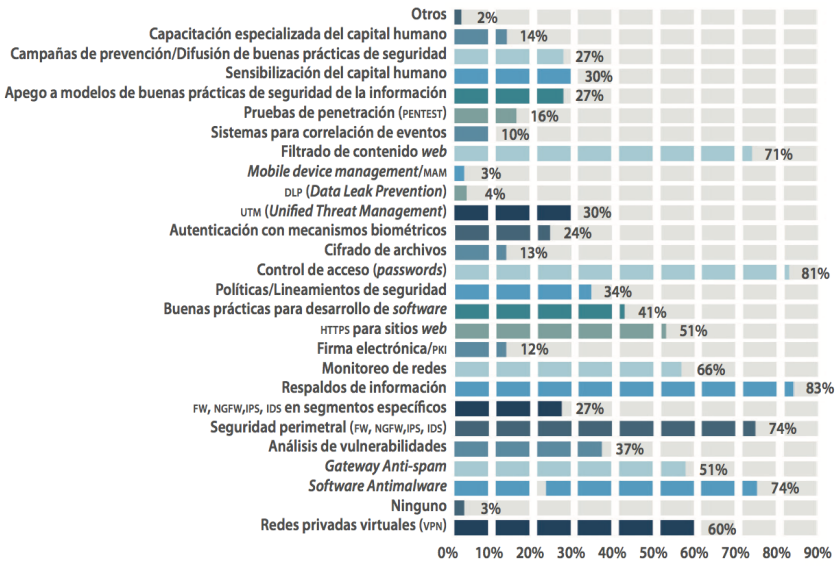


Ilustración 5.-Herramientas de seguridad informática más utilizadas en las IES según (ANUIES, 2016)

1.3. Planteamiento del problema

> Según cálculos (Policía Federal, 2016), el cibercrimen al mundo le puede llegar a costar hasta US$575.000 millones al año.

En el segundo congreso latinoamericano de ciberseguridad realizado en octubre de 2016 se habló que durante la administración actual se atendieron más de 120 mil incidentes cibernéticos y se desactivaron 10,745 sitios web falsos evitando robo de identidad y pérdidas económicas.

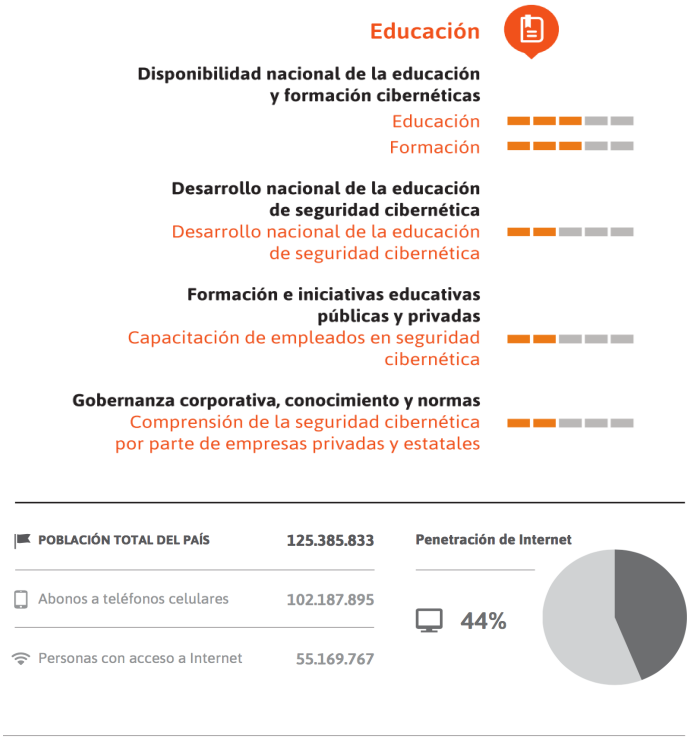


Ilustración 6.-Perfil de México en educación de cibernética. (La, 2016)

El 12 abril de 2016 la Policía de Ciberdelincuencia Preventiva de la Secretaría de Seguridad Pública de la Ciudad de México, lanza una alerta gracias al incremento de denuncias a nivel nacional por ataque de tipo RANSOMWARE a teléfonos móviles, en el que se pide un pago para poder liberar los dispositivos móviles afectados.

Tener en cuenta las vulnerabilidades de la seguridad es punto crucial para poder tomar medidas ante alguna situación de riesgo, al igual que hacer auditorias de seguridad informática permitirán identificar el nivel de exposición a nivel de seguridad. En la investigación de la ANUIES en el 2016 menciona que solo el 47% de las instituciones que participaron en la encuesta cuenta con auditorias.

Existen varias metodologías para el control de los recursos de una empresa, para este tema uno de los más usados es la gestión de riesgos, ya que nos permite valorar el impacto de este y lo que generaría en la organización, el objetivo de esta metodología es identificar los activos tanto de tecnologías de la información como las de información y al igual que las auditorias poder identificar las vulnerabilidades que más puedan llegar a impactar.

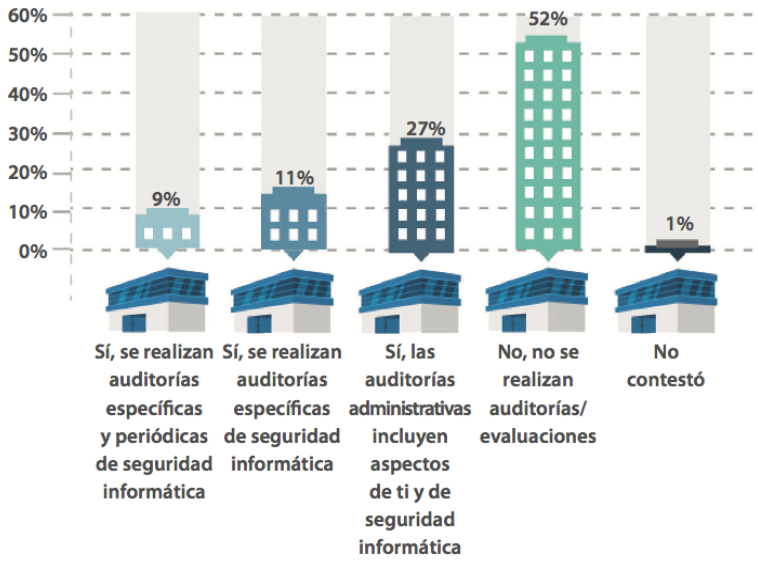


Ilustración 7.-Instituciones que cuentan con auditorias.

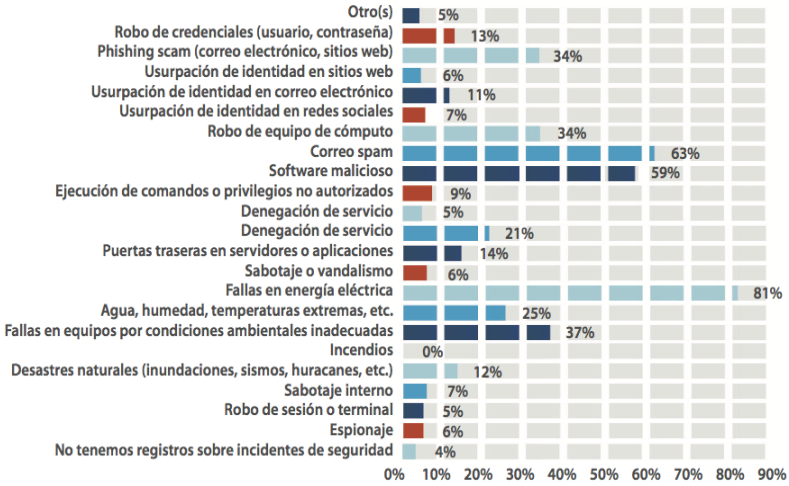


Ilustración 8.-Incidentes con mayor frecuencia según la ANUIES en las IES.

El 5 de julio del 2010 entra en vigor la ley federal de protección de datos personales en posesión de particulares.

El cual en el capítulo uno habla de los principios a los que la organización en este caso la universidad debe tener al poseer información personal de los docentes y alumnos, este capítulo contiene del articulo 16 al 30 de los cuales podemos rescatar

Artículo 23 y 24. Hablan de las responsabilidades que tiene que adoptar, establecer y documentar; de igual forma las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, como los procedimientos para la conservación, a fin de que no se altere la veracidad de éstos y en algún caso el bloqueo o eliminación de ellos.

Esta misma ley en su capítulo dos contiene doce artículos que mencionan los deberes que conlleva almacenar y manejar los datos. seis de ellos se cubren teniendo un sistema de gestión de seguridad de la información que como se menciona en esta ley artículo 34

"Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la presente Ley y las demás disposiciones que le resulten aplicables en la materia."

Artículo 31 y 32. Hablan de que no importa el sistema en el que se encuentren los datos, el responsable debe tener medidas de seguridad para brindar protección a los datos personales, al igual que garantizar su confidencialidad, integridad, disponibilidad y por último se mencionan las medidas de seguridad para ocho de los puntos a tomar en cuenta en el artículo 32.

Artículo 33 y 34. Hablan de que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar una serie de actividades interrelacionadas. Y que las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.

Artículo 35 y 36. Hablan de manera general en que el responsable deber elaborar un documento para la seguridad de la información con siete puntos indispensables, de igual forma de los cuatro eventos en los que se debe actualizar la documentación cuando lleguen a ocurrir.

Por todo lo anteriormente mencionado entiéndase al humano como el eslabón mas débil de toda organización ya que cada día se conecta más a la red y según datos este no esta informado, capacitado y mucho menos preparado para el riesgo que esto conlleva, riesgos que puede llegar de forma personal al perder su información o al usarse sin su consentimiento o en el peor de los casos de forma legal violando alguno de los artículos mencionados.

1.4. Justificación

En el 2016 la ANUIES (Asociación nacional de universidades e instituciones de educación superior) en su estudio" El estado actual de las tecnologías de la información y las

comunicaciones en las instituciones de educación superior en México", analizó a 140 instituciones de educación superior, de las cuales 115 eran públicas y 25 privadas, 45% de estas eran instituciones, 9% centros y 4% colegios.

Los resultados fueron bastante interesantes y esperados, de los puntos a resaltar son los de las auditorias en temas de seguridad informática, ya que estas permiten la revisión de implementación de la infraestructura de seguridad de la información. Donde solo el 47% de las instituciones cuentan con una auditoria pero solo el 9% de estas cuentan con una auditoria específica y periódica en el área de seguridad informática.

Por lo anteriormente mencionado es importante en primera instancia tener algo a que auditar sea especifico a la seguridad o no. Para ello se es necesario realizar un pentesntin que permita ubicar a la organización bajo un nivel de riesgo, sea por vulnerabilidades que se tienen en los sistemas de información implementados, en la falta de capacitación de empleados o malas practicas de seguridad informática. Posterior mente pensar en soluciones como lo es la implementación de un sistema gestión de seguridad de la información (SGSI), ya que la información de estudiantes o docentes investigadores pueden llegar a sufrir algún tipo de ataque en el que pueda llegarse a usarse de forma no autorizada. Al igual que brinda con los siguientes beneficios según (ANUIES, 2016):

- Una mejora continua en la gestión de la seguridad.
- Una garantía de continuidad y disponibilidad de los servicios.
- Reducción de los costos vinculados a los incidentes.
- El incremento de los niveles de confianza de los usuarios.
- La mejora de imagen institucional.

De lo contrario la universidad, el centro educativo o la coordinación podrían quedar expuestas a demandas que las hagan tener pérdidas económicas o de desprestigio.

1.5. Objetivos

Objetivo general

Detectar vulnerabilidades implementando pentesting en las áreas detectadas como críticas para los servicios que proporcionan la Universidad Autónoma de Zacatecas, Centro Educativo Rotary y la Coordinación de la Secretaria de Seguridad Pública, utilizando ingeniería social.

Objetivos específicos

1. Establecer las interacciones de Pre-compromiso.
2. Obtención inteligente de información.
3. Realizar ingeniería social para poder realizar el pentest de forma específica.
4. Modelado de la amenaza.
5. Análisis de Vulnerabilidad.
6. Explotación.
7. Explotación Post.
8. Reporte.

1.6. Hipótesis

Más del 60% de los empleados tiene un bajo conocimiento en temas de seguridad de la información, lo cual permitirá que más del 50% de ellos aun siendo conscientes del nivel de importancia en la información que maneja cediendo el acceso a sus ordenadores, esto mediante la aplicación de ingeniería social, permitiendo obtener información critica de su área y la necesaria para un ataque específico a su sistema.

2. CAPÍTULO II. MARCO TEÓRICO

Las universidades al igual que las organizaciones, son blancos de ataques, sea por su gran capacidad de cómputo que tienen o por la información que llegan a contener, por lo que han optado por utilizar metodologías para la protección de su información, entiéndase con metodología a las etapas en las que se estructuran los procesos de diseño, implementación y operación de un SGSI, apoyados por modelos ya definidos:

- ISO/IEC 27000
- Open Web Application Security Project (OWASP).
- Open Source Security Testing Methodology Manual (OSSTMM).
- Information System Security Assessment Framework (ISSAF).

Con estas metodologías ya definidas minuciosamente por expertos a lo largo de mucho tiempo ayudan al establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora, al igual que incluyen buenas prácticas en los temas de SGSI.

Universidades como la UNIVERISDAD DE INDIANAPOLIS o HARVARD cuentan con políticas para la protección de su información, en el caso de la primera universidad mencionada se basa en el ISO/IEC 27000 en las que se incluyen políticas como, por ejemplo:

- Reporte de incidentes.
- Seguridad para hardware y software.
- Información de seguridad y programa de privacidad.
- Herramientas para privacidad y seguridad.

Según datos del estudio de la (ANUIES,2016) el 25% de las 140 universidades cuentan con políticas alineadas a los objetivos institucionales, el 9% cuenta con políticas, pero no alineadas y el 24% tienen políticas, pero no incluyen objetivos.

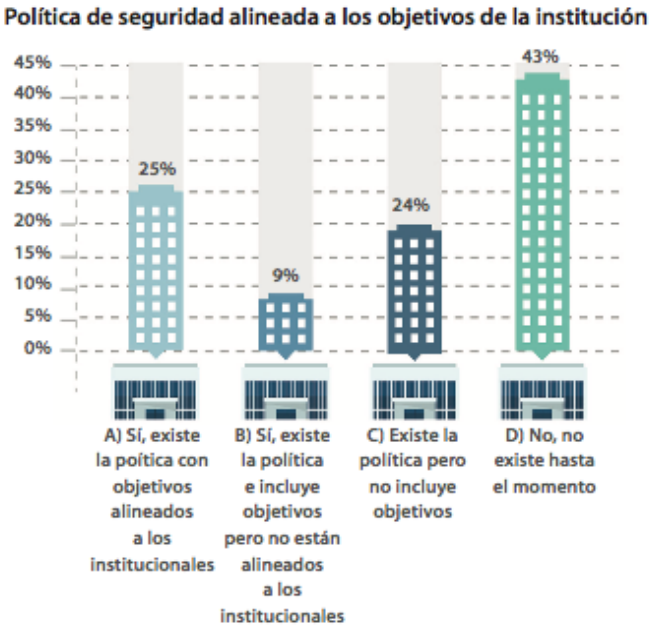


Ilustración 9.- 4 de cada 10 IES encuestadas no tienen políticas de seguridad informática.

2.1. Gestión de riesgos.

Entendamos como riesgo a la contingencia o proximidad de daños sociales, ambientales y económicos dentro de la universidad, las cuales se miden por el tiempo de respuesta, la frecuencia con la se presenta y el impacto que causa.

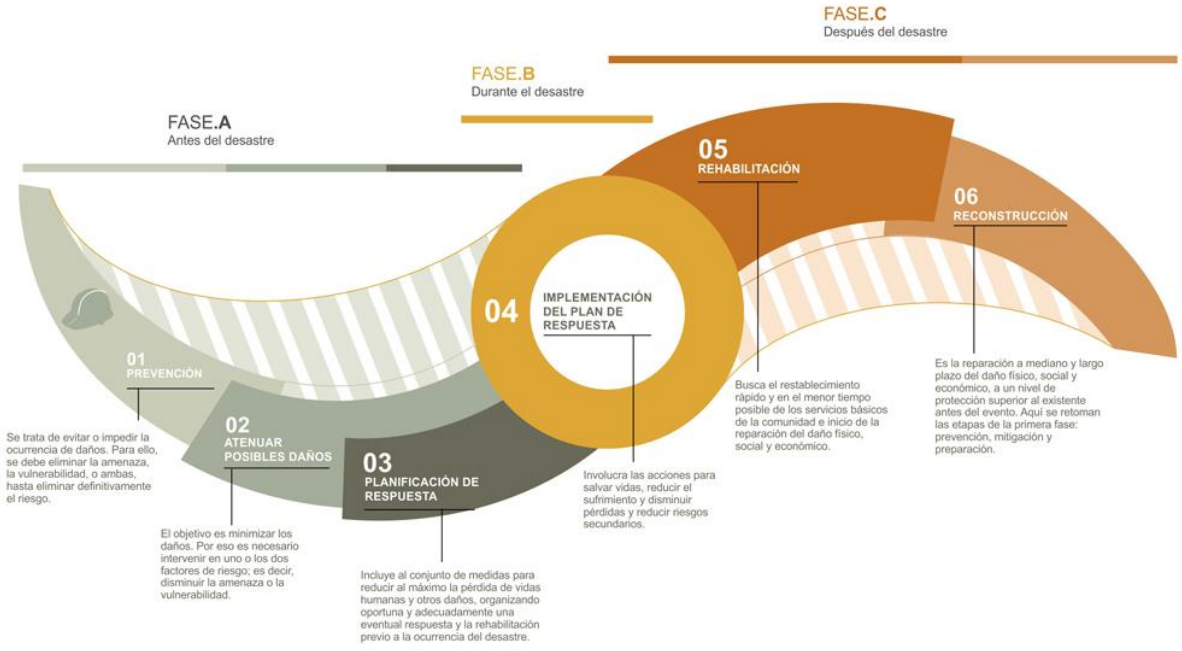


Ilustración 10.-Fases de la administración de riesgos.

Todas las prioridades de seguridad deben ser capaces de ser asignadas a las prioridades del negocio. Este es el primer paso hacia el establecimiento de la relevancia de cada iniciativa de seguridad y muestra a la administración de negocios cómo la seguridad apoya la misión. (Morana et al., 2013)

Con esta lógica lo primero que tenemos que hacer es priorizar e identificar las áreas que necesitan atención, considerando el costo beneficio del impacto que llegaría a tener en caso

de que esta se atacada cuidando la misión u objetivos de la organización, una buena gestión de riesgos permite identificar, medir y administrar los riesgos para los activos ya identificados de la organización, permitiendo actuar de manera oportuna, minimizando los daños causados ante algún evento, ya que como se observa en la ilustración de fases de la administración de riesgo(figura 9) se toman medidas antes del desastre, durante y después de ello, cada una de estas fases con puntos a realizar para no impedir la continuidad de los procesos de la organización.

Las amenazas de manera general se clasifican de la siguiente forma:

Naturales: no interviene el factor humano, por ejemplo, terremotos, inundaciones, tormentas, entre otros.

Humanas: procesos que puede intervenir el humano por ejemplo incendios, explosiones, acciones maliciosas, entre otros.

Según (Morales Alejandro, 2016) los riesgos podemos clasificarlos de acuerdo a los criterios aplicables a cada situación.

Dentro de los riesgos que menciona están los que afectan de manera directa a la organización y pueden ser controlables, ejemplo de algunos de ellos son:

Riesgos físicos: incluyen las lesiones o muerte de personas y todas las formas de pérdida o daño de propiedades. En las que los dos tipos de amenaza pueden ser causantes de este riesgo.

Riesgos de responsabilidad: Los riesgos de responsabilidad pueden provenir de reclamaciones de los empleados, de los clientes o proveedores y del público en general.

Riesgos de interrupción de negocios: en este parte es importante haber detectado el costo beneficio de los activos de la organización para minimizar este riesgo y entre más meticulosos seamos al analizar las amenazas tanto naturales como humanas, menor será el impacto que se tenga.

Riesgos de administración: Una administración deficiente puede tener un efecto catastrófico en las organizaciones, aunque su costo muchas veces permanezca oculto hasta que los resultados de una pobre administración se hacen evidentes en los resultados generales de la organización.

2.2. Métricas para la seguridad de la información

Las métricas nos sirven para medir y/o comparar las acciones que se realizan ante exposición a los riesgos a los que se esta la organización, en este caso la universidad, ofreciendo información puede ser utilizada para hacer planes y mejoramientos, ya que no solo se trata de tener software o hardware adecuado y actualizado, sino que también se ocupa una serie de reglamentos y políticas que solventen la gestión de los activos minimizando los riesgos contra estos.

> *Las métricas como medio para mitigar las vulnerabilidades y el tiempo para parchar son útiles si la organización cuenta con procesos maduros y altamente optimizados, pero eso no se aplica al 95% de las organizaciones de hoy en día* (Caroline Wong, 2015)

Tener en cuenta los siguientes puntos para poder tener una buena métrica

- objetivas y tangibles
- valores discretos
- medidas absolutas y concretas

No se administra lo que no se puede medir, por lo tanto, no se mejora lo que no se puede administrar

2.3. Definición de auditoria.

La auditoría son normas, técnicas y conjunto de buenas prácticas dedicadas a la evaluación y aseguramiento de activos relacionados con los sistemas de información con el fin de evaluar la eficacia y eficiencia del uso de los recursos informáticos, actualmente la información que se maneja se consideran como activos de igual o mayor importancia que los humanos o materiales, de igual forma la auditoria nos sirve para conocer si se está brindando el soporte adecuado con objetivos y metas del lugar en cuestión.

Objetivos de una auditoria.

- Optimizar la relación costo-beneficio de los sistemas diseñados e implementados para el procesamiento de datos.
- Incrementar la satisfacción de los usuarios de los SI.
- Asegurar la integridad, viabilidad y confidencialidad de la información mediante las recomendaciones de seguridad y control.
- Brindar seguridad a los activos.
- Minimizar riesgos.
- Continuidad de negocio.
- Capacitación y educación sobre el control de los SI.

Justificación de una auditoria.

- Evitar decisiones incorrectas, por lo que reduce el costo económico y tiempo.
- Control del uso de las Tics.
- Evita consecuencias subyacentes con la pérdida de datos críticos o sensibles, evitando demandas, desprestigio y/o posibles fraudes.
- Se contabiliza y valoran los activos TICS.

con todo esto surgen preguntas como ¿cuál es la mejor? ¿cuál se adapta mejor en una organización? ¿cuál se debe elegir? Lo cierto es que una prueba o metodología es perfecta y menos en un ambiente que está en constante actualización.

2.4. Metodologías para pruebas de penetración.

Para poder evaluar la seguridad de un aplicación, sistema u organización se utiliza un método denominado pen test(prueba de penetración) la cual como lo menciona (Meucci & Muller, 2014) es un arte el cual ayuda a detectar las vulnerabilidades en el diseño de un sistema u operatividad en una organización la cual comprometa la información "crítica" que este posea, este método consiste en simular ataques controlados por el pentester para poder tener acceso a la información y así poder manipularla o robarla.

Los ataques se aprovechan normalmente de las vulnerabilidades conocidas ya sean nuevas o aun no resueltas, existen paginas donde podemos estar al día con las vulnerabilidades que se van encontrando, aprovechando la falta de parche o la mala configuración de los responsables.

Las metodologías a explicar son cuatro de las más conocidas, completas, y complejas ya que su nivel de desglose es extenso y se requiere un medio-alto conocimiento en el área. Las cuales se pueden adaptar según los requerimientos de la organización.

ISO/IEC 27000

según (iso2700.es, n.d.): la familia de los ISO27000 son un conjunto de estándares desarrollados o en fase de desarrollo, que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

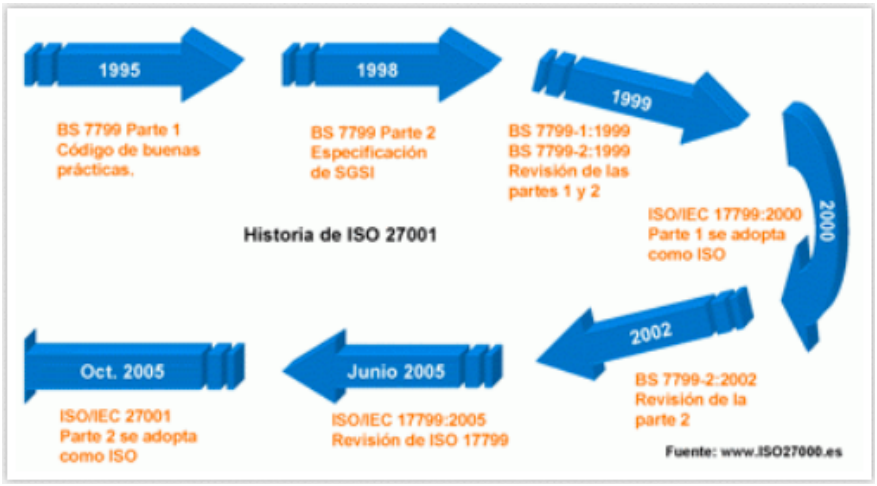


Ilustración 11.-Historia del ISO27001.

ISO/IEC 27000: Norma que proporciona una visión general de la familia 27000 la cual se compone de 35 normas, en la que indica el uso para cada una de ellas, alcance y propósito. Aporta las bases de por qué es importante la implantación de un SGSI.

ISO/IEC 27001: Norma principal de la serie que contiene los requisitos del SGSI con la que los auditores externos certifican a las organizaciones. Cuyo origen es la BS 7799-2:2002.

ISO/IEC 27002: Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No certificable. Actualmente, la última edición en el 2013 fue actualizada a un total de 14 Dominios, 35 Objetivos de Control y 114 Controles.

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la segur. de la información.
6.1.2 Segregación de tareas.
6.1.3 Contacto con las autoridades.
6.1.4 Contacto con grupos de interés especial.
6.1.5 Seguridad de la información en la gestión de proyectos.
6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.
6.2.2 Teletrabajo.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes.
7.1.2 Términos y condiciones de contratación.
7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en segur. de la informac.
7.2.3 Proceso disciplinario.
7.3 Cese o cambio de puesto de trabajo.
7.3.1 Cese o cambio de puesto de trabajo.
8. GESTIÓN DE ACTIVOS.
8.1 Responsabilidad sobre los activos.
8.1.1 Inventario de activos.
8.1.2 Propiedad de los activos.
8.1.3 Uso aceptable de los activos.
8.1.4 Devolución de activos.
8.2 Clasificación de la información.
8.2.1 Directrices de clasificación.
8.2.2 Etiquetado y manipulado de la información.
8.2.3 Manipulación de activos.
8.3 Manejo de los soportes de almacenamiento.
8.3.1 Gestión de soportes extraíbles.
8.3.2 Eliminación de soportes.
8.3.3 Soportes físicos en tránsito.
9. CONTROL DE ACCESOS.
9.1 Requisitos de negocio para el control de accesos.
9.1.1 Política de control de accesos.
9.1.2 Control de acceso a las redes y servicios asociados.
9.2 Gestión de acceso de usuario.
9.2.1 Gestión de altas/bajas en el registro de usuarios.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.
9.2.3 Gestión de los derechos de acceso con privilegios especiales.
9.2.4 Gestión de información confidencial de autenticación de usuarios.
9.2.5 Revisión de los derechos de acceso de los usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso
9.3 Responsabilidades del usuario.
9.3.1 Uso de información confidencial para la autenticación.
9.4 Control de acceso a sistemas y aplicaciones.
9.4.1 Restricción del acceso a la información.
9.4.2 Procedimientos seguros de inicio de sesión.
9.4.3 Gestión de contraseñas de usuario.
9.4.4 Uso de herramientas de administración de sistemas.
9.4.5 Control de acceso al código fuente de los programas.
10. CIFRADO.
10.1 Controles criptográficos.
10.1.1 Política de uso de los controles criptográficos.
10.1.2 Gestión de claves.
11. SEGURIDAD FÍSICA Y AMBIENTAL.
11.1 Áreas seguras.
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.
11.1.6 Áreas de acceso público, carga y descarga.
11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Instalaciones de suministro.
11.2.3 Seguridad del cableado.
11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de activos fuera de las dependencias de la empresa.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.
12. SEGURIDAD EN LA OPERATIVA.
12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades.
12.1.4 Separación de entornos de desarrollo, prueba y producción.
12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.
12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.
12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad.
12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema.
12.4.4 Sincronización de relojes.
12.5 Control del software en explotación.
12.5.1 Instalación del software en sistemas en producción.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Gestión de las vulnerabilidades técnicas.
12.6.2 Restricciones en la instalación de software.
12.7 Consideraciones de las auditorías de los sistemas de información.
12.7.1 Controles de auditoría de los sistemas de información.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.
13.1 Gestión de la seguridad en las redes.
13.1.1 Controles de red.
13.1.2 Mecanismos de seguridad asociados a servicios en red.
13.1.3 Segregación de redes.
13.2 Intercambio de información con partes externas.
13.2.1 Políticas y procedimientos de intercambio de información.
13.2.2 Acuerdos de intercambio.
13.2.3 Mensajería electrónica.
13.2.4 Acuerdos de confidencialidad y secreto.
ISO27002.es PATRONICADO POR:
GES CONSULTOR
GOBIERNO T.I. - RIESGO - CUMPLIMIENTO
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
14.1 Requisitos de seguridad de los sistemas de información.
14.1.1 Análisis y especificación de los requisitos de seguridad.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
14.1.3 Protección de las transacciones por redes telemáticas.
14.2 Seguridad en los procesos de desarrollo y soporte.
14.2.1 Política de desarrollo seguro de software.
14.2.2 Procedimientos de control de cambios en los sistemas.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
14.2.4 Restricciones a los cambios en los paquetes de software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.
14.2.6 Seguridad en entornos de desarrollo.
14.2.7 Externalización del desarrollo de software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
14.2.9 Pruebas de aceptación.
14.3 Datos de prueba.
14.3.1 Protección de los datos utilizados en pruebas.
15. RELACIONES CON SUMINISTRADORES.
15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
15.1.3 Cadena de suministro en teonologías de la información y comunicaciones.
15.2 Gestión de la prestación del servicio por suministradores.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.
16.1.2 Notificación de los eventos de seguridad de la información.
16.1.3 Notificación de puntos débiles de la seguridad.
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
16.1.5 Respuesta a los incidentes de seguridad.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.
16.1.7 Recopilación de evidencias.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
17.1 Continuidad de la seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información.
17.1.2 Implantación de la continuidad de la seguridad de la información.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
17.2 Redundancias.
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.
18. CUMPLIMIENTO.
18.1 Cumplimiento de los requisitos legales y contractuales.
18.1.1 Identificación de la legislación aplicable.
18.1.2 Derechos de propiedad intelectual (DPI).
18.1.3 Protección de los registros de la organización.
18.1.4 Protección de datos y privacidad de la información personal.
18.1.5 Regulación de los controles criptográficos.
18.2 Revisiones de la seguridad de la información.
18.2.1 Revisión independiente de la seguridad de la información.
18.2.2 Cumplimiento de las políticas y normas de seguridad.
18.2.3 Comprobación del cumplimiento.

ISO27000

Iso27000.es: Documento sólo para uso didáctico. La norma oficial debe adquirirse en las entidades autorizadas para su venta. Octubre-2013

Ilustración 12.-Estructura del ISO27002

Las ISO/IEC 27003-7009 son guías no certificables en su mayoría que se centra en los aspectos críticos necesarios para el diseño, desarrollo e implementación con éxito de un SGSI al igual que se nos indican las métricas para determinar la eficacia de este, proporcionan directrices para su aplicación satisfactoria para posteriormente acreditarse.

Del ISO/IEC TR 27008-2780032 son guías que definen los requisitos para la implementación de un SGSI en cualquier campo, área de aplicación o sector industrial, por ejemplo, telecomunicaciones, gobierno, sector financiero, etc. dentro de estos ISO tenemos el 27016 y el 27018 que nos ayudan a la valoración y buenas prácticas respecto a la seguridad de la información.

ISO/IEC 27032-27040 son norma y guías que establecen una descripción general de seguridad cibernética, gestión de incidentes, redacción digital y la seguridad en los medios

de almacenamiento al igual de proporcionar directrices para actividades relacionadas con la información almacenada en teléfonos, tarjetas memoria, cámaras, redes, etc.

Por último, se encuentran los **ISO/IEC 27041 al 27799** las cuales son guías para la garantizar la idoneidad y adecuación de los métodos de investigación, desarrollan principios y procesos para la recopilación de evidencia con directrices para el análisis e interpretación de la misma.

Open Web Application Security Project (OWASP)

Esta guía fue liberada en el 2014. Cuyo origen fue en el 2003. Esta metodología se enfoca a las aplicaciones web en determinadas circunstancias. El cual reúne varias técnicas de prueba y las explica. Basada en un enfoque de caja negra donde el tester no sabe nada o muy poca información sobre la aplicación a probar.

- Diciembre 2004 "The OWASP Testing Guide", versión 1.0
- Julio 14,2004 "OWASP Web Application Penetration Checklist", versión 1.1
- Diciembre 25, 2006 "OWASP Testing Guide", versión 2.0
- 15th septiembre, 2008 "OWASP Testing Guide", versión 3.0
- 2014"OWASP Testing Guide", versión 4.0

Esta guía se compone de 12 dominios y 111 objetivos.

1. Introducción y objetivos (12).
2. Pruebas de gestión de la configuración y la implementación (8).
3. Pruebas de gestión de identidad (5).
4. Pruebas de autentificación (10).
5. Prueba de autorización (4).
6. Prueba de administración de sesión (8).
7. Prueba de validación de salidas (27).
8. Prueba de manejo de errores (2).
9. Pruebas de criptografía débil (3).
10. Prueba lógica de negocio (9).
11. Prueba de cliente (12).
12. Reporte.

Esta sección se compone por cuatro apéndices con sus respectivos objetivos.

12.1.- Apéndice A: Herramientas de prueba (1).

12.2.- Apéndice B: Lectura sugerida (3).

12.3.- Apéndice C: Vectores (1).

12.4.- Apéndice D: Inyección codificada (2).

PTES (Penetration Testing Execution Standard)

Es una Guía que se basa en la experiencia de analistas y expertos en seguridad, siendo este un estándar para procesos normalmente implementados. Este se divide en doce dominios de los cuales el séptimo es el de reporte, de ahí en adelante son anexos. No mencionara más información ya que en el desarrollo se abarcan todos sus dominios.

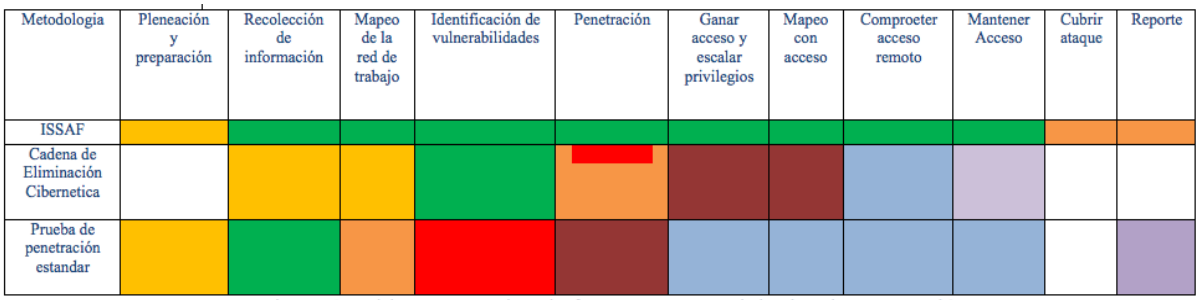


Ilustración 13.- Tabla comparativa entre metodologías de penetración.

3. CAPÍTULO III. ORGANIZACIONES A EVALUAR

3.1 Universidad Autónoma de Zacatecas

La Universidad Autónoma de Zacatecas (UAZ) es la máxima casa de estudios desde hace muchos años en el estado de Zacatecas. Actualmente está conformado por veintidós áreas académicas, que a su vez se conforman por diferentes unidades.

Tabla 1.-Unidades Académicas nivel superior

Unidad académica	**Carreras**
Agronomía	Licenciatura en desarrollo regional sustentable. Ingeniero agrónomo.
Antropología	Licenciatura en humanidades antropología.
Artes	Licenciatura en artes. Licenciatura en canto. Licenciatura en música. Licenciatura en música con especialización en instrumentos.
Ciencias biológicas	Licenciatura biología.
Ciencias de la tierra	Ingeniero geólogo. Ingeniero minero metalurgista. Licenciatura en ciencias ambientales.
Ciencias químicas	Ingeniero químico. Química en alimentos. Químico farmacéutico-biólogo.
Contaduría y administración	Licenciatura en contaduría.

Cultura	Licenciatura en lenguas extranjeras.
Derecho	Licenciado en derecho.
Economía	Licenciado en economía.
Enfermería	Licenciado en enfermería. Licenciado en nutrición.
Filosofía	Licenciatura en filosofía.
Física	Licenciatura en física.
Historia	Licenciatura en turismo. Licenciatura en historia.
Ingeniería Eléctrica	Ingeniería en electrónica industrial. Ingeniería en computación. Ingeniería en diseño industrial. Ingeniería en robótica y mecatrónica. Ingeniero electricista. Ingeniería en software.
Ingeniería I	Ingeniero civil. Ingeniero mecánico. Ingeniero topógrafo e hidrógrafo.
Letras	Licenciatura en letras.
Matemáticas	Licenciatura en matemáticas.
Medicina Humana	Médico general.
Medicina veterinaria y zootecnia	Médico veterinario zootecnista.
Odontología	Médico cirujano dentista
Psicología	Licenciatura en psicología.

Como se observa en la Tabla 1 está institución es compleja por lo que se decide realizar en primera instancia un diagnóstico de seguridad a los servicios administrados por el SIIAF ya que este desarrolla diferentes sistemas de impacto para la universidad, uno de ellos es el portal donde los docentes pueden consultar su información laboral, más los sistemas internos, de igual manera son los responsables del manteamiento al equipo de cómputo concentrados en el edificio de rectoría, edificio que se encuentra dentro del campus siglo XXI

3.2 CENTRO EDUCATIVO ROTARY

Este centro educativo contaba en el 2018 con un matricula de 906 estudiantes con ingresos fiscales de 19,580,525.82 de pesos mexicanos según datos obtenidos.

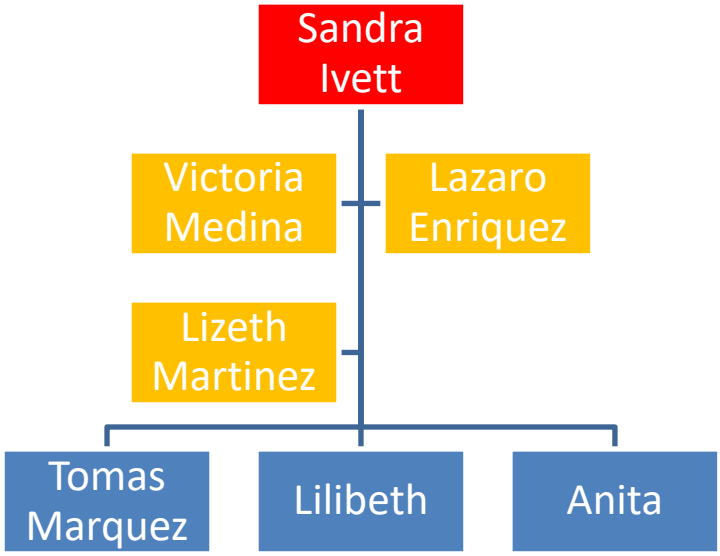


Ilustración 14.-Organigrama del Centro Educativo Rotary 2018

Encabezando el organigrama se encuentra la directora general, siguiendo de los coordinadores y por ultimo los administrativos, cuenta con nivel de prescolar 2º a 3º con grupos del A hasta el D, nivel de primaria de 1º hasta 6º, secundaria 1º hasta 3º y bachillerato. Además de contar con clubes como música, arte, innovación y actividades físicas por la tarde. Alrededor de 2000 personas incluyendo alumnos, docentes, directores, encargados, etc. La prueba se realiza en el área administrativa y en los servicios web existentes para el docente

como para padres de familia, cabe destacar que estos no son desarrollados por el área de informática de esta unidad, la cual esta compuesta por un coordinador y los docentes de las materias de computación de todos los niveles.

3.3 SECRETARÍA DE SEGURIDAD PÚBLICA.

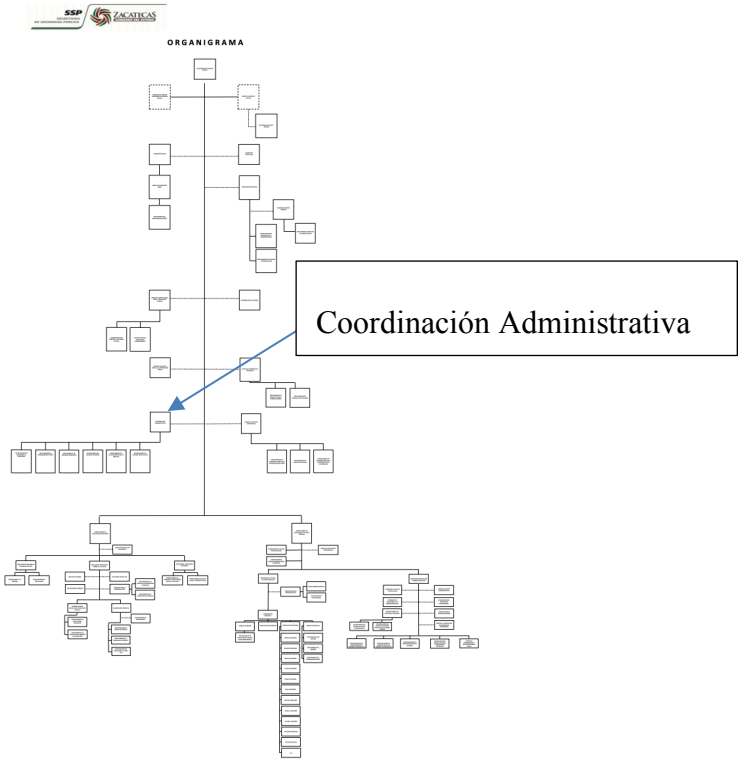


Ilustración 15.-Organigrama de la Secretaría de Seguridad Pública

La Coordinación de Seguridad Pública esta compuesta por 4 diferentes secretarias de las cuales se tienen la subsecretaria de vinculación ciudadana y la subsecretaria de inteligencia y política criminal que se dividen en múltiples coordinaciones, direcciones, departamentos y unidades las cuales administran información del personal, personas, recursos, etc. Por la complejidad de esta secretaría y el tiempo que se llevaría la prueba se enfoca a una sola coordinación.

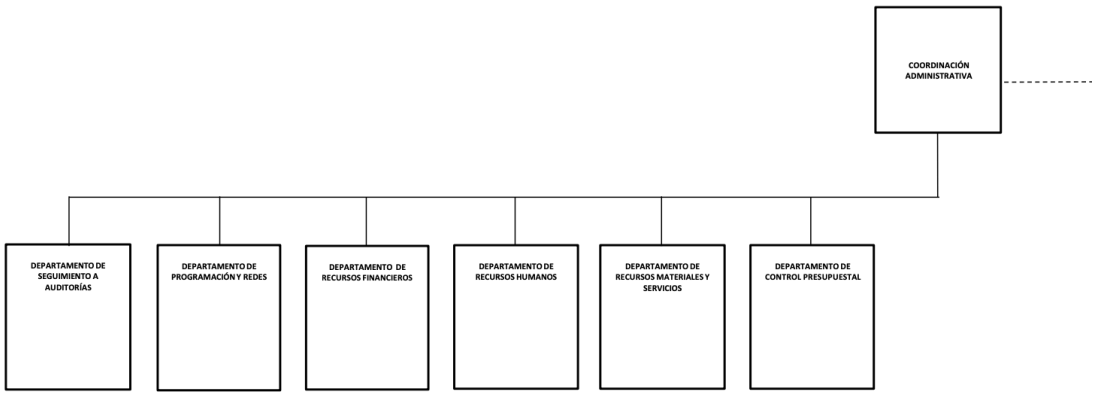


Ilustración 16.-Organigrama de la Coordinación administrativa de la SSP

Compuesta internamente por seis áreas consideradas criticas, ya que estas son encargadas de administrar los diferentes recursos llámese humano, material o económico, de igual forma son responsables de las redes internas y externas con la policía vial, policía estatal preventiva, Centros de Readaptación y Reinserción Social (CERERESO) por mencionar algunas unidades que la componen y el desarrollo de los sistemas informáticos que se implementan internamente como el de control vehicular, correspondencia, etc.

4. CAPÍTULO IV. METODOLOGIA DE INVESTIGACIÓN

Basado en 7 fases las cuales contienen sub fases que se irán desarrollando

1. Interacciones de Pre-compromiso.
2. Obtención inteligente de información.
3. Modelado de la amenaza.
4. Análisis de Vulnerabilidad.
5. Explotación.
6. Explotación Post.
7. Reporte.

Una fase importante en el proceso de cualquier pentest es el levantamiento de requerimientos; a través de él, se permite entender mejor el problema, organizando y estructurando la información que se ha recabado, la recopilación de información se llevó a cabo mediante el uso de cuestionarios, en el que se pueden identificar las necesidades de cada organización, los objetivos, alcances, limitaciones y posibles vulnerabilidades.

Como se menciona este ya existen metodologías para realizar pruebas de penetración, no obstante en algunas organizaciones se complica el poder llevarlas a cabo, sea por falta de recurso humano, económico o la capacitación de los empleados en el tema, por lo tanto para esta investigación se implementa un cuestionario compuesto de 10 preguntas para poder obtener información que ayude a realizar un pentest de acuerdo a los requerimientos de la organización, este cuestionario está basado en un apartado de la investigación "Estado actual de las Tecnologías de la información y las Comunicaciones en las instituciones de Educación superior en México" por parte del ANUIES en el 2018 este permite crea las condiciones necesarias o adecuar las existentes; Mostrando de igual forma datos cuantitativos que permitan aclarar las necesidades y vulnerabilidades que sean de utilidad en la investigación.

Pudiéndose aislar tanto el área de las organizaciones como las subáreas a evaluar, para el uso de las herramientas se elabora laboratorios virtuales, sin dañar el equipo real y permitiendo modificase bajo las circunstancias que se vayan encontrando en el desarrollo de esta.

5. DESARROLLO DE LA METODOLOGIA Y PRUEBA DE PENETRACIÓN

5.1. Interacciones de Pre-compromiso.

5.1.1. Información general.

El SIIAF se encuentra ubicado en el edificio de rectoría dentro del campus siglo XXI por lo que se nos pide en primera instancia se realice un ataque tipo black box en el cual no se conoce información de ningún tipo de este edificio, el escaneo de la red se hace desde fuera de este para ir identificando las ip disponibles dentro de la red, se implementa ingeniería social para obtener todo tipo de información sea departamentos existentes, número de trabajadores, maquinas activas, etc. toda información que sea relevante y pueda servir para acceder a la información que comprometa el funcionamiento de los departamentos, de no poder recabar información por ingeniería social y escaneo se nos ira proporcionando información hasta tener lo requerido para realizar un ataque interno.

De la misma manera por parte del Centro Educativo Rotary y la Secretaría de Seguridad Publica de gobierno se cuenta con el apoyo interno del encargado de sistemas para poder ir corroborando la información que se obtenga, así mismo ir omitiendo las áreas que este considera “no importantes”.

Se implementa un laboratorio de practica en que se utilizan los siguientes SO:

- Kali Linux.
- Windows XP, Windows Vista, Windows Seven y Windows 8.

Estos por ser los sistemas operativos usados en las organizaciones, con estas máquinas virtualizadas se tiene un entorno controlado, donde se pondrán implementar las herramientas de hacking sin poner en riesgo los sistemas implementados por el objetivo.

5.1.2. Introducción al alcance.

El alcance de este proyecto como ya se mencionó específicamente se centra a los principales servicios administrados por los encargados de sistemas: páginas web, servidores y sistemas de cómputo dentro del edificio de estas áreas.

La limitación del alcance es sin duda lo más importantes de una prueba de penetración, para este caso las limitaciones fueron claras ya que todo se centraba en un edifico. Como en todo proyecto el factor cliente es uno de los más difíciles de confrontar, debido a que talvez no dimensiona la magnitud del trabajo o simplemente lo que pide es imposible realizar bajo los términos que el pide.

Entendiendo que la prueba no solo se centra una aplicación sino en una prueba donde el cliente proporciona una amplia gama de direcciones IP para probar con el objetivo de encontrar vulnerabilidades en alguna de ellas.

5.1.3. Métricas para la estimación del tiempo.

Se tiene un tiempo límite de dos años para la presentación de los reportes debido a que es un tema para obtener el grado de Maestro.

5.1.4. Reunión.

En la reunión de alcance se llegó al acuerdo de no elaborar ningún tipo de contrato de confidencialidad por parte de la UAZ. Para las otras organizaciones se llega al acuerdo de mostrar ciertas capturas de pantalla, en las que no se exponga ningún tipo de información que las vincule. Otro de los objetivos de la discusión es el tema de lo que se pone a prueba y las reglas que se tienen que seguir. Esto con el fin de confundir lo que se quiere probar, los horarios en los que se puede trabajar sin dañar o interrumpir algún sistema que comprometa la continuidad. Ya que en algunos de ellos cuentan con dispositivos que monitorean la red y este al detectar tráfico irregular bloquea la red.

Los encargados de estas áreas afirman estar protegidos de manera aceptable pero que no se cuenta con un documento escrito que valide la seguridad con la que se cuenta. Las IP no se proporcionaron en esta reunión ya que como se mencionó se hará en primera instancia como black box.

5.1.5. Soporte adicional.

Se tiene el apoyo del departamento de sistemas de cada área y de los asesores especializados en el tema como soporte, con el fin de mantenernos dentro del alcance de trabajo y cuidar la información que se obtiene ya que ellos podrán evaluar el nivel de la información que se obtiene.

5.1.6. Cuestionarios.

Para tener un claro alcance de trabajo y tener un tiempo estimado adecuado usaremos las preguntas que se ponen como ejemplo en esta metodología ya que se adaptan al entorno de trabajo, la prueba se divide en

- Área de trabajo.
- Aplicaciones web
- Áreas inalámbricas de trabajo
- Penetración física
- Ingeniería social

Cada una de ellas se relacionan para obtener una prueba exitosa done el resultado puede ser encontrar vulnerabilidades o encontrarnos con una seguridad aceptable.

5.1.7. Preguntas generales.

5.1.7.1. Prueba de Penetración en Red.

¿Cuándo y a qué hora se podrán realizar las pruebas de penetración?

¿Cuántas IP se van a probar externas como internas?

¿Existen dispositivos (cortafuegos, proxys) que puedan impactar en los resultados?

En caso de poder acceder a los sistemas ¿Cómo debemos actuar?

5.1.7.2. Prueba de Penetración de Aplicaciones Web.

¿Cuántas aplicaciones serán evaluadas y qué tipo de prueba en específico?

¿Cuántos inicios de sesión se evaluarán y qué tipo de prueba en específico?

5.1.7.3. Prueba de penetración de red inalámbrica.

¿Cuántas redes componen la red de la universidad?

¿A cuáles redes se les aplicará mapeo?

¿El edificio cuenta con la misma red de trabajo que la universidad?

5.1.7.4. Prueba de Penetración Física.

¿En qué orden se tienen que analizar los departamentos?

¿Las unidades cuentan con un administrador para la seguridad de la información?

¿Existe algún personal que proteja las áreas de los servidores?

5.1.7.5. Ingeniería Social.

¿Existe una lista de correos y teléfonos en particular a la que el cliente quiera aplicar ingeniería social?

¿Podremos usar ingeniería social para obtener información y acceder a lugares físicos no autorizados?

¿Cuántas personas serán el blanco?

5.1.7.6. Preguntas para los gerentes de unidades de negocio.

¿Qué datos no se pueden exponer, corromper o eliminar?

¿Existen procesos para la continuidad y recuperación de negocio?

5.1.7.7. Preguntas para administradores de sistemas.

¿Cuáles son las aplicaciones y servidores más importantes?

¿Estos son propensos a interrupciones o bloqueos?

¿Existen backups de los sistemas?

¿Cuánto es el tiempo de respuesta para recuperarse a una interrupción?

¿Existen softwares para monitoreo de la red?

5.1.8. Especificar fechas de inicio y finalización.

Universidad Autónoma de zacatecas.

Fecha de inicio octubre 2017

Fecha de fin enero 2018

Centro Educativo Rotary.

Fecha de inicio agosto 2018

Fecha de fin enero 2019

Secretaría de Seguridad Pública.

Fecha de inicio febrero 2019

Fecha de fin junio 2019

5.1.9. Especificar rangos de IP y dominios.

Universidad Autónoma de zacatecas

Para la prueba de servicios web se utilizó las ip

Tabla 2.-Direcciones ip UAZ

NOMBRE DE DNS	IP
SIIAF.UAZ.EDU.MX	148.217.18.36

WWW.ESCOLAR.UAZ.EDU.MX	148.217.18.9

Centro Educativo Rotary

Tabla 3.-Direcciones ip Centro educativo

NOMBRE DE DNS	IP
	51.79.113.90

Secretaría de Seguridad Pública.

El rango de Ips son privadas, en las que se corren varios servidores, servicios de impresión e igualmente empleada para los trabajadores.

Tabla 4.-Direcciones IP secretaría

NOMBRE DE DNS	IP
SERVIDOR REDES	10.12.63.23
SERVIDOR WEB	10.12.63.6
SERVIDOR VMWARE	10.12.63.10

5.1.9.1. Validar rangos.

Universidad Autónoma de Zacatecas

Después de la obtención, se confirma que la ip publica en la que se trabajara es la 148.217.18.36

Centro Educativo Rotary.

51.79.113.90

Secretaría de Seguridad Pública.

dedicándose únicamente al segmento 10.12.63.1/24

5.1.10. Trato con terceros.

Universidad Autónoma de Zacatecas.

N/A (Almacena localmente los servicios web)

Centro Educativo Rotary.

Desarrollador externo José Luis Carrillo Guerrero quien aparece como contacto registrado a la ip.

Secretaría de Seguridad Pública.

N/A (Almacena localmente los servicios web)

5.1.10.1. Servicios en la nube.

Universidad Autónoma de Zacatecas.

Axel, S.A.B de C.V

Centro Educativo Rotary.

Domain Name: centenarioderotary.edu.mx

Created On: 2008-12-15
Expiration Date: 2019-12-14

Last Updated On: 2018-12-15
Registrar: Akky (Una división de NIC México)
URL: http://www.akky.mx
Whois TCP URI: whois.akky.mx
Whois Web URL: http://www.akky.mx/jsf/whois/whois.jsf

Secretaría de Seguridad Pública.

N/A

5.1.10.2. ISP.

Universidad Autónoma de Zacatecas.

Axel, S.A.B de C.V

Centro Educativo Rotary.

Teléfonos de México, S.A.B. de C.V.

Secretaría de Seguridad Pública.

Teléfonos de México, S.A.B. de C.V.

5.1.10.3. Managed Security Service Providers (MSSPs).

Universidad Autónoma de Zacatecas.

Cortafuegos (Firewall) perimetral marca Fortigate.

Centro Educativo Rotary.

N/A.

Secretaría de Seguridad Pública.

Cortafuegos (Firewall) perimetral marca Fortigate.

Las soluciones que ofrece este cortafuego Fortigate son:

- Firewall
- Filtrado de contenido
- VPN
- Antivirus
- Antispam
- Detección y prevención de intrusos y gestor de tráfico
- Balanceo de carga
- Alertas por e-mail

Siempre y cuando se mantenga bajo licencia de lo contrario las funciones quedan limitadas

5.1.10.4. Países donde se alojan los servidores.

Universidad Autónoma de Zacatecas.

Al contar con el servicio de almacenamiento en nube este sistema no está centralizado.

Centro Educativo Rotary.

Al contar con el servicio de almacenamiento en nube este sistema no está centralizado.

Secretaría de gobierno.

Mayor parte de los servidores se encuentran en el edificio de la Secretaría de Seguridad Pública.

5.1.11. Definición de pretextos aceptables de ingeniería social.

Evaluación del conocimiento sobre el tema de seguridad de la información en el personal de la organización

5.1.12. Pruebas de DoS.

Los ataques de negación de servicio para la Universidad Autónoma de Zacatecas, así como para el Centro Educativo Rotary fueron controlados por la organización con la que tienen contrato el alojamiento del servidor, para el caso de la Secretaría de Seguridad Publica la implementación y administración correcta del Fortigate mitigo dicho ataque.

5.1.13. Metas.

5.1.13.1. Primaria

Detectar las vulnerabilidades de los sistemas que se implementan

5.1.13.2. Secundaria

Solucionar las vulnerabilidades

5.1.13.3. Análisis de Negocio

Conocer el impacto negativo y el alcance que llego a tener para los usuarios

5.1.14. Información de contacto para emergencias

5.1.14.1. Proceso de notificación de incidentes

Se realiza el reporte de la incidencia.

Según la importancia se agenda una cita con el encargado.

Se verifica que la vulnerabilidad se ha corregido.

5.1.14.2. Definición de Incidentes

Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información.

5.1.14.3. Frecuencia del informe de estado

Según la importancia de la vulnerabilidad se puede llamar en el instante que esta es detectada, de no ser así se agenda para una posterior revisión en el encargado de los sistemas.

5.2. Obtención inteligente de información.

5.2.1. Físico.

5.2.1.1. Localización.

Ilustración 17.-Campus siglo XXI edificio donde se implementa el pentest en la Universidad.

Ilustración 18.-Edificio del Centro Educativo Centenario de Rotary donde se implementa el pentest.

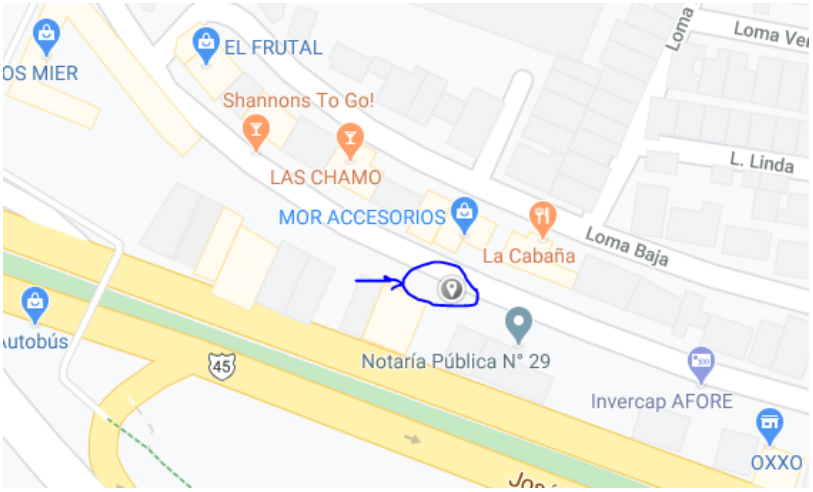


Ilustración 19.-Ubicación del edificio de la Secretaría de Seguridad Pública donde se implementa el pentest.

5.3. Modelo de la amenaza.

Como primera parte se elabora una "encuesta" digital y un script, estos se desarrollan para Windows ya que es el sistema operativo que se utiliza en los departamentos a evaluar.

La función del script es crear una cuenta de usuario administrador con contraseña preestablecida, obtener la IP de la computadora y sustraer archivos (Excel, Word, PDF e imágenes) de forma paralela al tiempo que el empleado contesta un cuestionario. En promedio, la encuesta se completa en 6 minutos, tiempo suficiente para extraer 1 GB de información aproximadamente. Se obtienen archivos como nóminas, usuarios dentro de sus sistemas, proveedores, estados financieros, topologías de red, manuales, contrataciones externas, etc.

El fin de la encuesta es analizar, reducir y personalizar el ataque ya que esta nos arroja información importante como puesto que desempeña, el nivel que este le da a su información, sistema operativo y la existencia de algún software anti malware, si bien existe software que permite la detección de vulnerabilidades de forma automatizada, normalmente arrojando falsos positivos, por lo tanto, se descarta la opción de estos, para lo que la segunda pregunta

permite reducir las vulnerabilidades hacia el sistema operativo con la que trabaja el empleado.

Una vez analizada la información cada encargado de departamento indica que sistemas desean probar, y es aquí donde entra en la aplicación de metodología del pentest con todas sus fases anteriormente mencionadas.

5.4. Post Explotación y resultados.

Universidad Autónoma de zacatecas

Los archivos extraídos de las máquinas de los 24 empleados a los que se le implemento ingeniería social permiten corroborar información obtenida por otros medios, de igual manera, otros permitían conocer sub áreas ampliando más el panorama que se tenía del edificio y los sistemas que se implementan. Con esto pues podemos afirmar que la hipótesis planteada es correcta, ya que el bajo conocimiento sobre seguridad para su información permitió que de 11 de los 24 trabajadores se obtuvieran 500 archivos de Word; 3773 imágenes personales y de trabajo, siendo estas computadoras de uso laboral; 1353 archivos PDF y presentaciones de PowerPoint; por último 397 archivos de Excel. De los 13 trabajadores faltantes la información no fue procesada en su totalidad por el área o puesto que desempeñaba.

Centro Educativo Rotary

Por una mala configuración del servicio web que ofrecen a los padres de familia se obtiene el acceso de forma “administrador” al sistema.

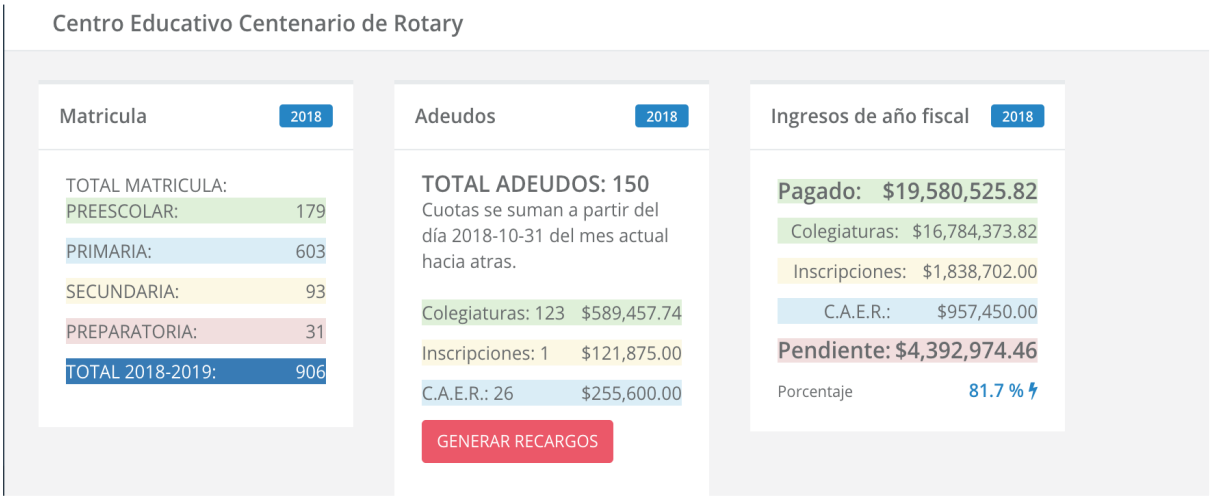


Ilustración 20.-Información financiera

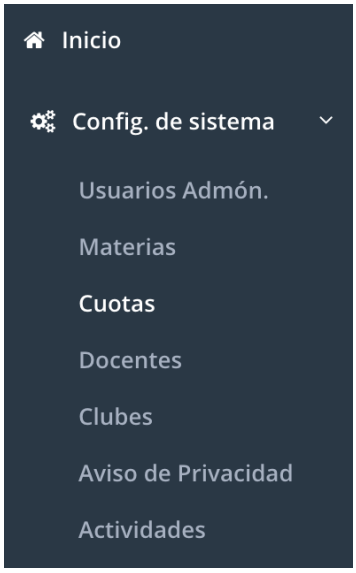


Ilustración 21.-Acceso a información

Información de 36 docentes en los que se incluye su nómina, nombre, dirección, correos, teléfonos, a falta de limpieza de información en la base datos existe el registro el más de tres mil padres de familia en las que se expone lo anterior más el nombre de su hijo, números telefónicos del trabajo y las cuotas que pagan.

Secretaría de gobierno

Por medio de un escaneo dentro de la red se identifican en promedio 94 equipos conectados, 10 de los cuales son impresoras que tenían configuración por defecto lo que permite conocer libreta de direcciones del personal asociado a esta, de igual forma permite realizar ciberterrorismo como el antes mencionado en Alemania en abril de 2016 a las tres universidades.

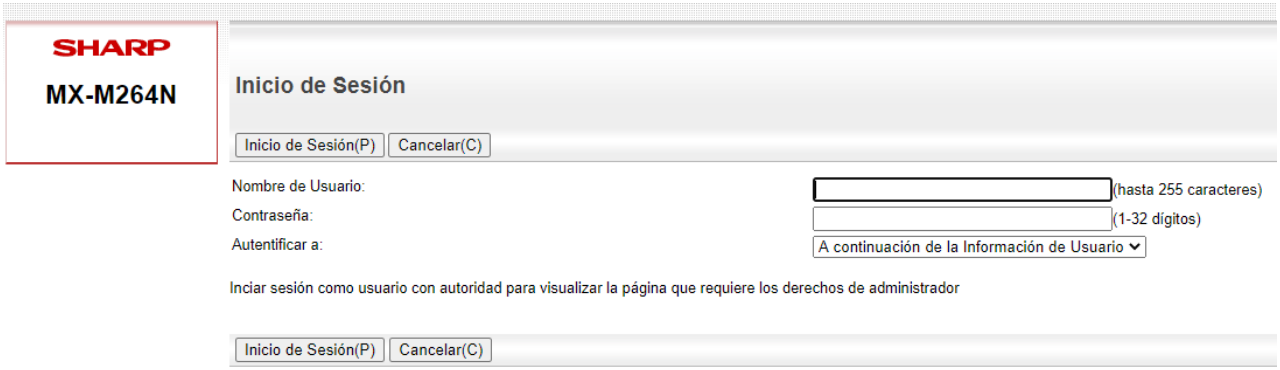


Ilustración 22.- Mala configuración con usuario y contraseña por defecto.

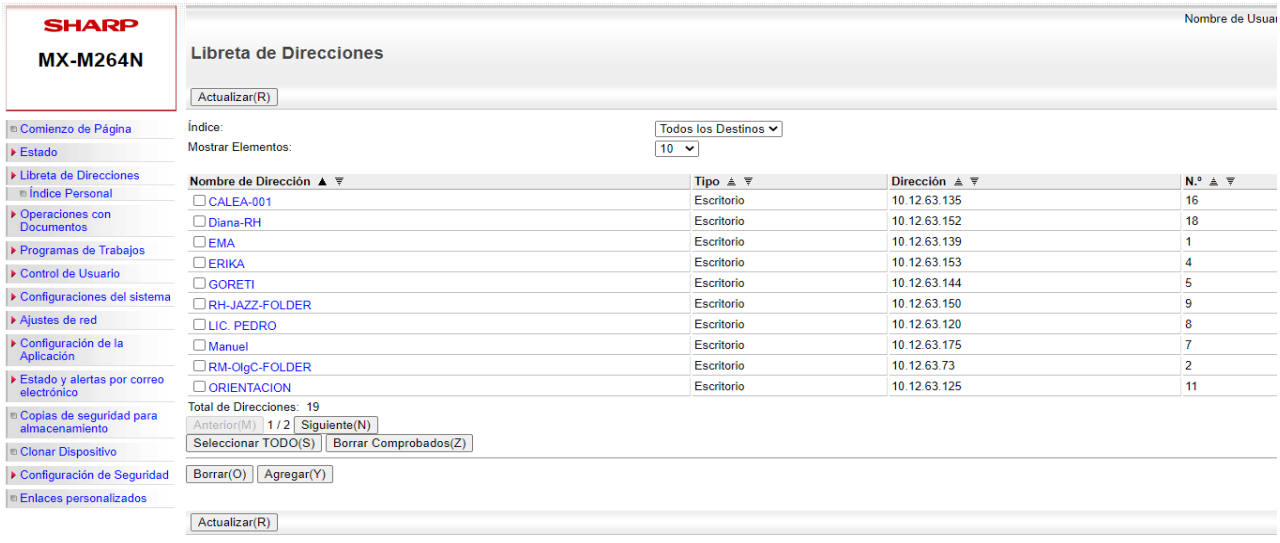


Ilustración 23.- Datos obtenidos de la multifuncional Sharp mx-m2644n

5.5. Reporte

Las Vulnerabilidades y exposiciones comunes por sus siglas en ingles CVE, Es una base de datos de vulnerabilidades, la cual brinda información sobre el manejo, impacto y complejidad de estas, Para los casos de La Universidad Autónoma de Zacatecas no existe un CVE para la ingeniería social, de igual forma para la Secretaría de Seguridad Pública por la mala configuración de los dispositivos por lo que se pasa a la realización de una junta con los encargados para la demostración de dicha vulnerabilidad y considerar el impacto que esta tiene.

Centro Educativo Rotary.

Vulnerabilidad: **CVE-2019-1010259**

Puntuación CVSS: 7.5

Impacto confidencial: Existe una divulgación informativa considerable

Impacto en la integridad: La modificación de algunos archivos o información del sistema es posible, pero el atacante no tiene control sobre lo que se puede modificar, o el alcance de lo que puede afectar el atacante es limitado.

Impacto de disponibilidad: Hay un rendimiento reducido o interrupciones en la disponibilidad de recursos.

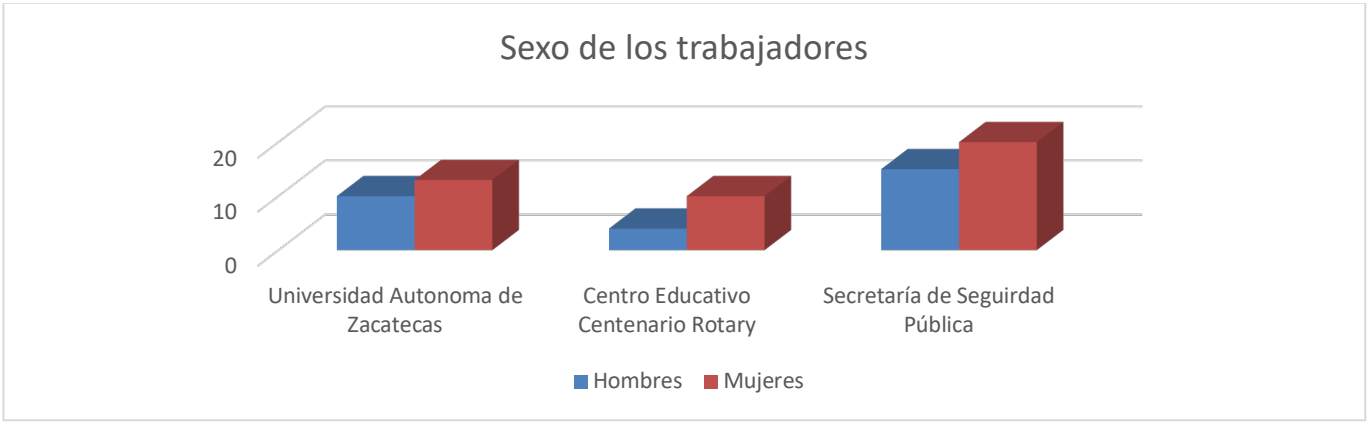
Complejidad de acceso: No existen condiciones de acceso especializadas o circunstancias atenuantes. Se requiere muy poco conocimiento o habilidad para explotar.

Autentificación: No se requiere autenticación para aprovechar la vulnerabilidad.

Tipo de vulnerabilidad: SQL Injection

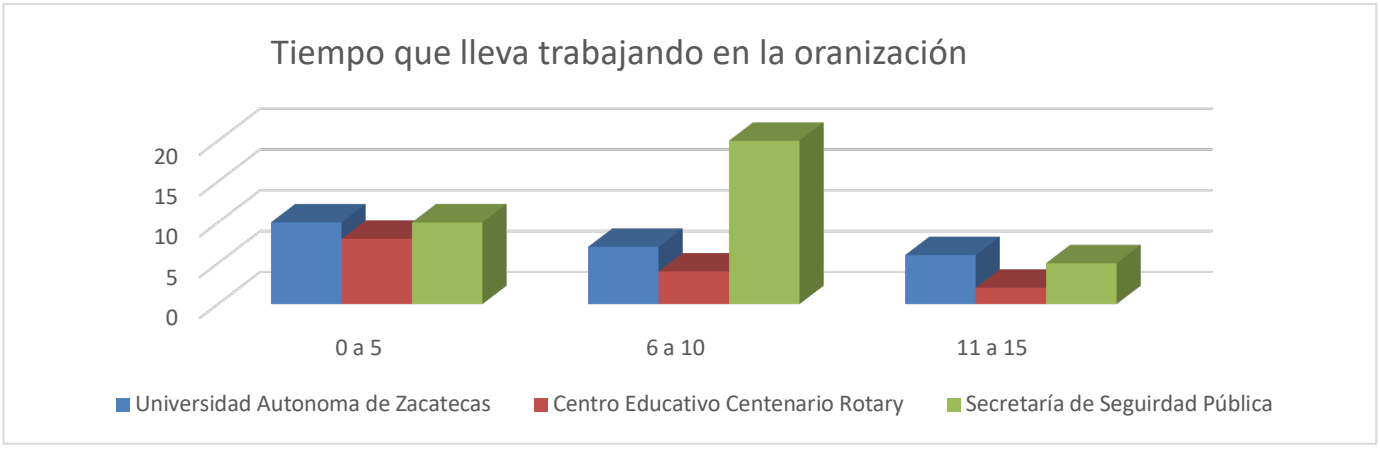
6. RESULTADOS DE LAS ENCUESTAS.

6.1. Análisis descriptivo



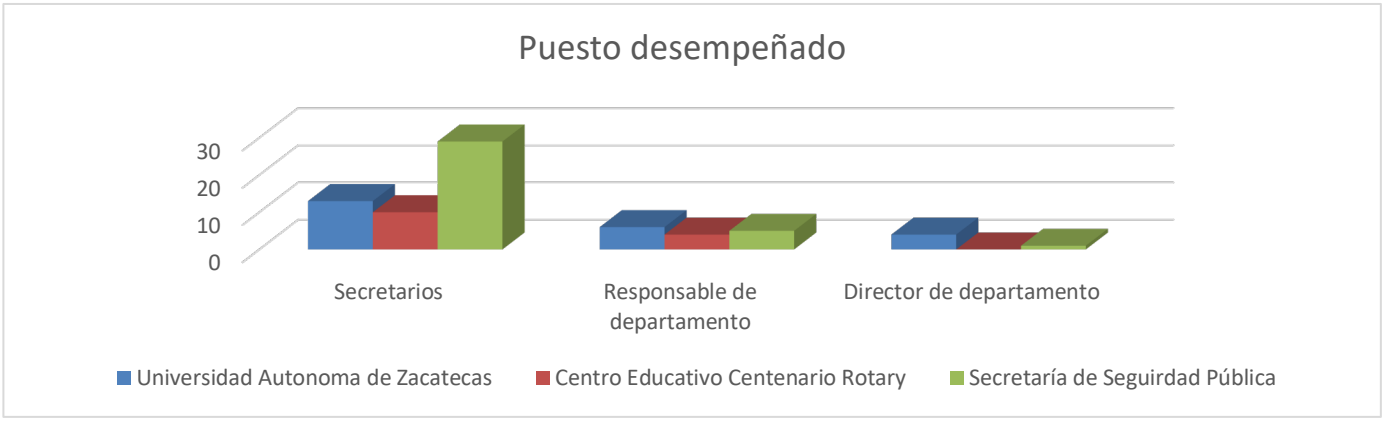
Gráfica 1.- Seleccione su sexo.

En la gráfica 1 se observa que la mayoría de las personas a las que se aplicó el cuestionario son mujeres.



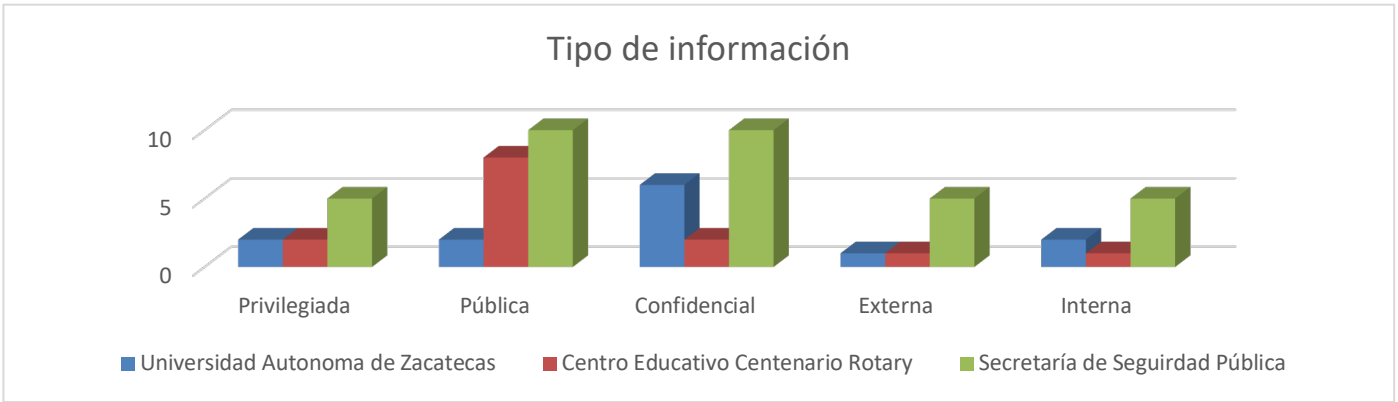
Gráfica 2.- Tiempo que lleva trabajando en la universidad

En la gráfica 2 se observa que la mayoría de las personas a las que se aplicó el cuestionario tienen menos de 5 años trabajando dentro de su organización.



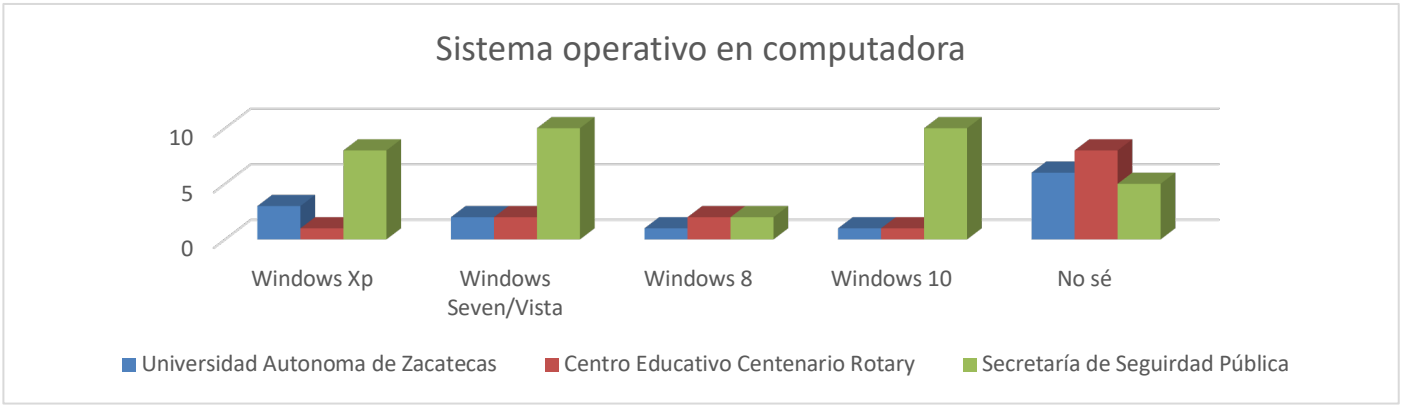
Gráfica 3.- ¿Qué puesto desempeña dentro del departamento actual?

En la gráfica 3 se observa que en la mayoría de las personas que se aplicó el cuestionario tienen puesto de secretarios.



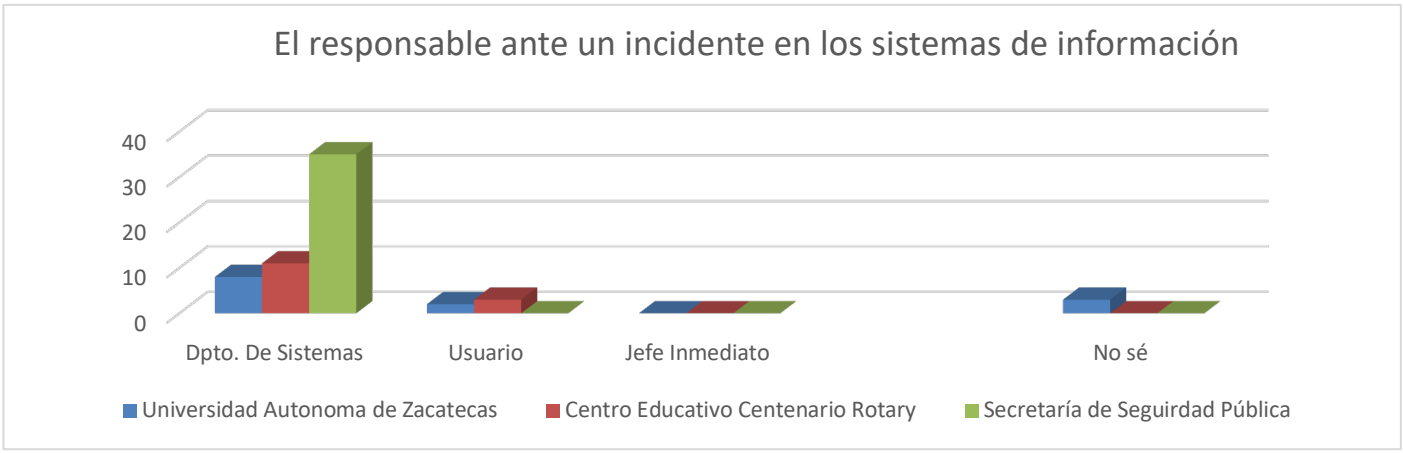
Gráfica 4.- ¿Qué tipo de información maneja?

En la gráfica 4 se observa que en la mayoría de las personas que se aplicó el cuestionario maneja información pública.



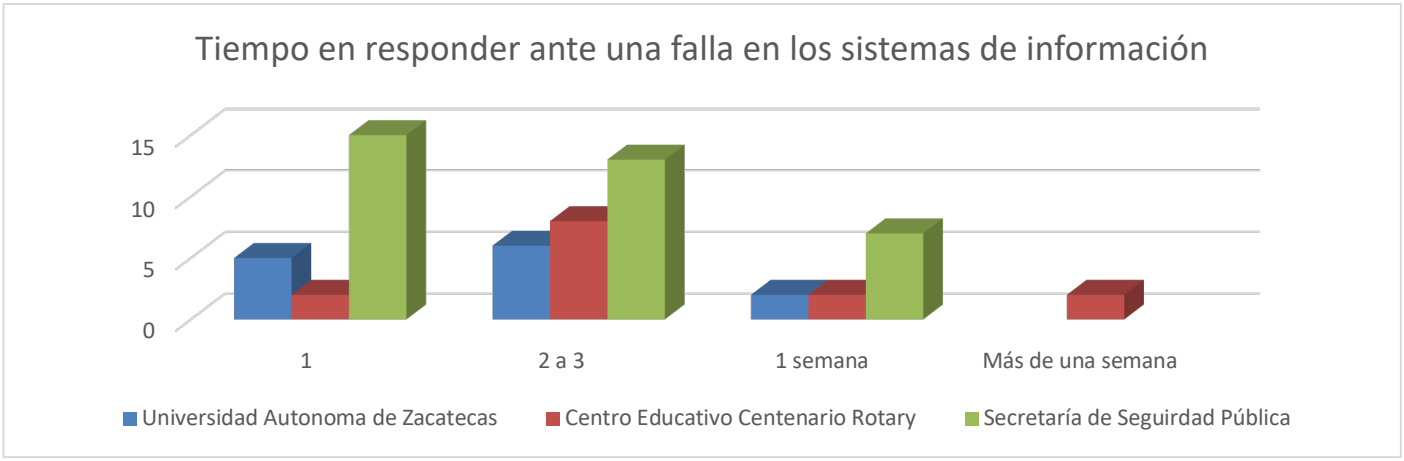
Gráfica 5.- ¿Cuál es el sistema operativo que tiene su computadora?

En la gráfica 5 se observa que la mayoría de las personas a las que se aplicó el cuestionario desconocen el sistema operativo que manejan.



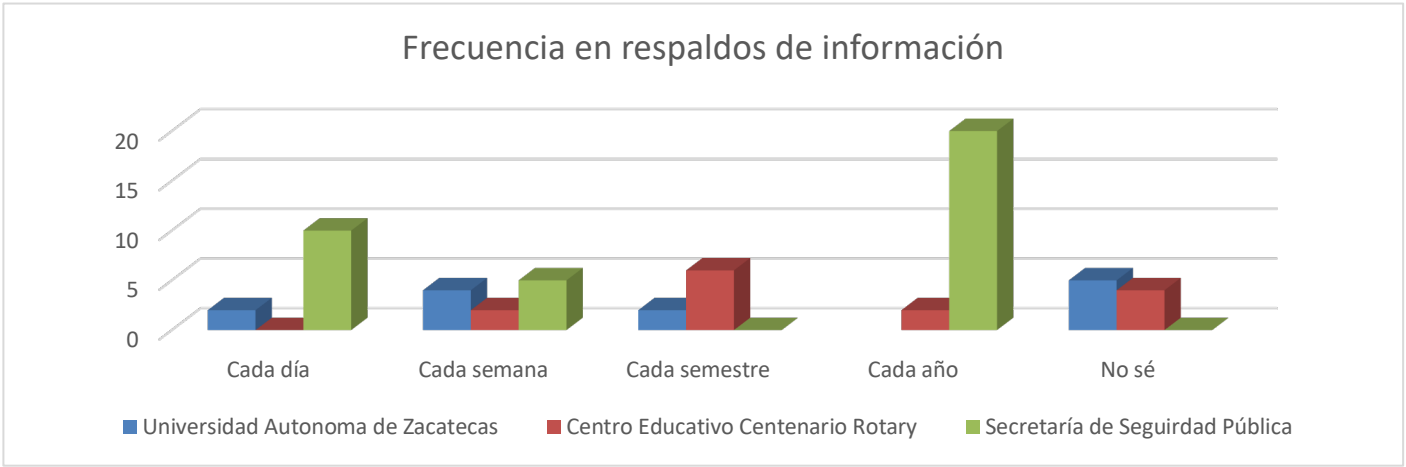
Gráfica 6.- ¿Quién es el responsable ante un incidente en los sistemas de información?

En la gráfica 6 se observa que la mayoría de las personas a las se aplicó el cuestionario identifica al departamento de sistemas como responsable ante un incidente.



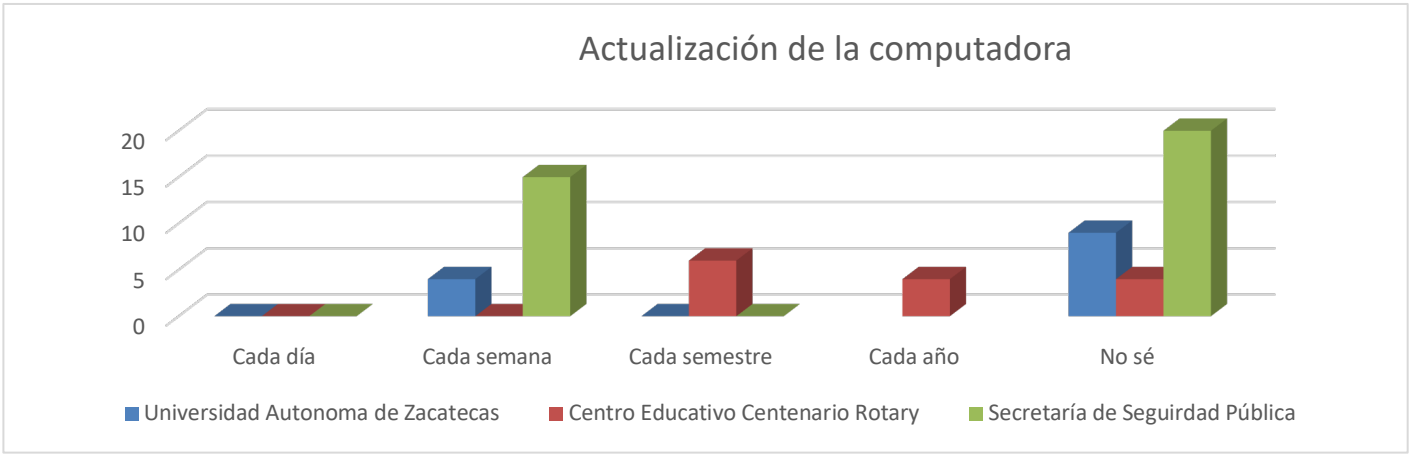
Gráfica 7.- ¿Cuánto tardan en responder ante una falla en los sistemas de información?

En la gráfica 7 se observa que la mayoría de las personas a las que se aplicó el cuestionario reconoce que su falla será resuelta entre 2 a 3 días.



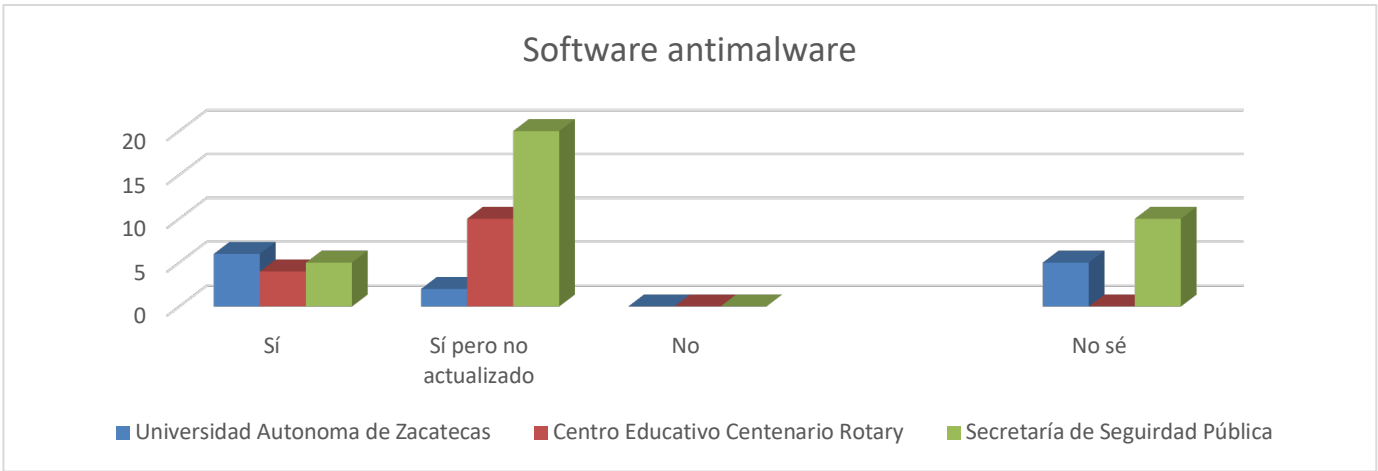
Gráfica 8.- ¿Se realizan respaldos de información? ¿con qué frecuencia?

En la gráfica 8 se observa que la mayoría de las personas a las que se aplicó el cuestionario hace respaldo cada semana.



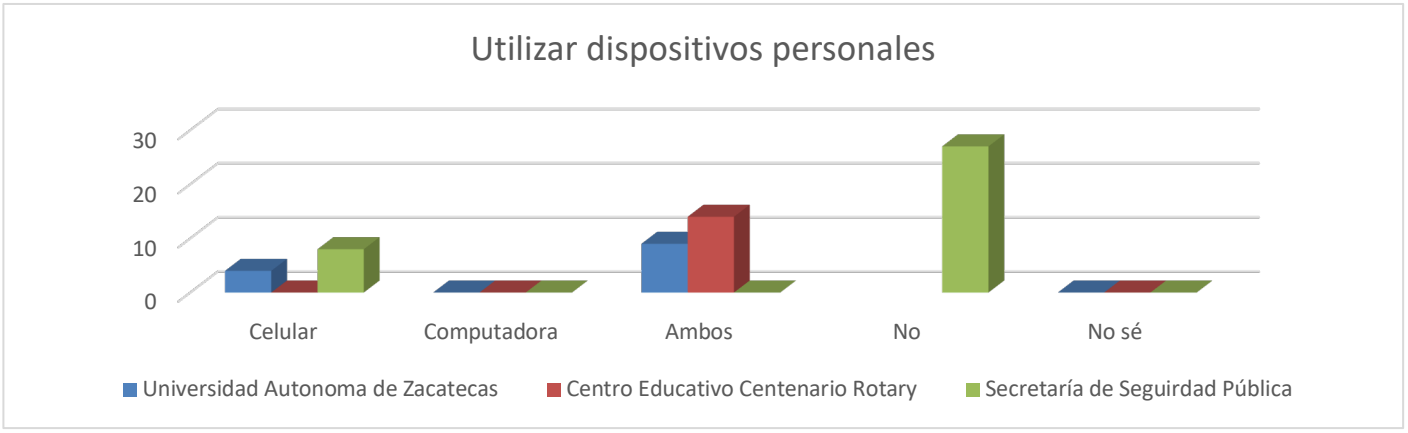
Gráfica 9.- ¿Qué tan seguido se actualiza la computadora que utiliza?

En la gráfica 9 se observa que la mayoría de las personas a las que se aplicó el cuestionario desconoce si tiene su sistema operativo actualizado.



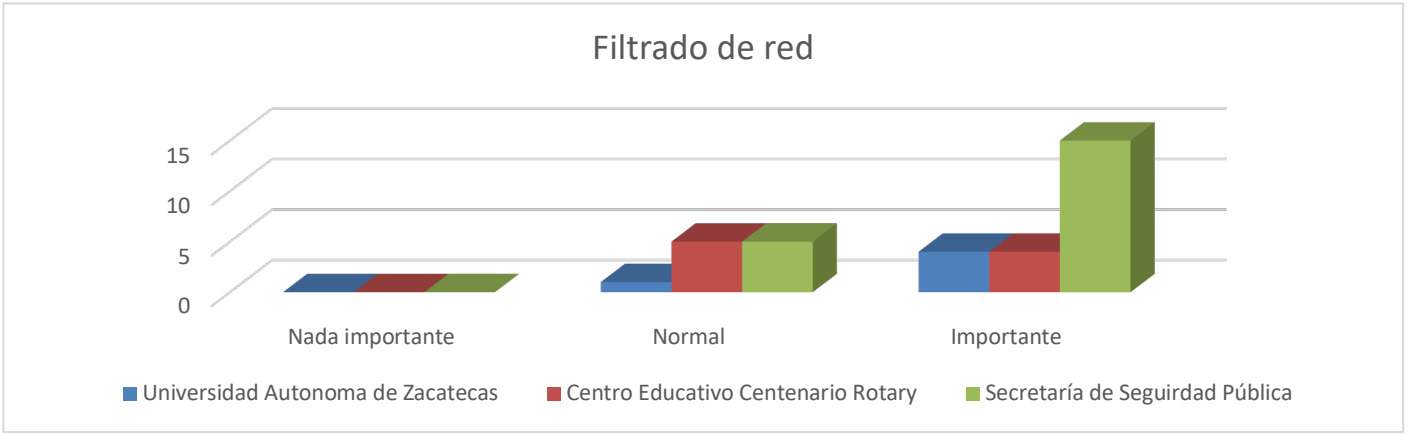
Gráfica 10.- ¿Cuentan con software antimalware?

En la gráfica 10 se observa que la mayoría de las personas a las que se aplicó el cuestionario cuenta con un software anti virus pero desactualizado.



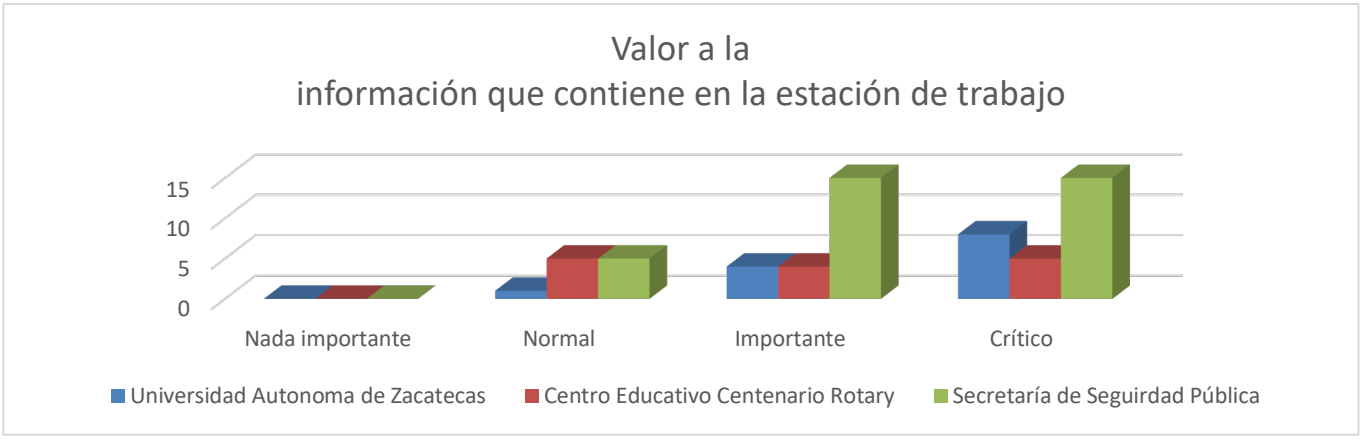
Gráfica 11.- ¿Se les permite usar sus dispositivos personales en la red de trabajo?

En la gráfica 11 se observa que la mayoría de las personas que se aplicó el cuestionario puede utilizar celulares y computadoras personales en la red de trabajo.



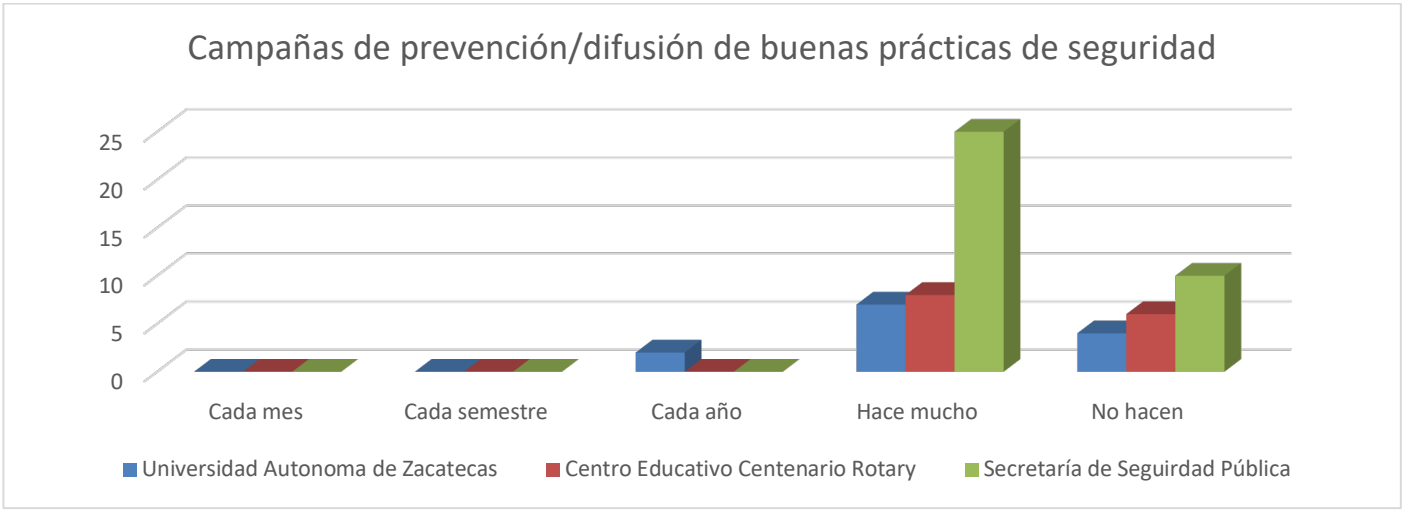
Gráfica 12.- ¿Cuenta con filtrado de red (YouTube, Facebook, WhatsApp)?

En la gráfica 12 se observa que la mayoría de las personas a la que se aplicó el cuestionario cuenta con un filtrado dentro de la red.



Gráfica 13.- Del uno al diez tomando como diez el valor más crítico, ¿qué valor le daría a la información que contiene en su estación de trabajo?

En la gráfica 13 se observa que la mayoría de las personas que se aplicó el cuestionario considera que maneja información crítica para su organización.



Gráfica 14.- ¿Se han realizado campañas de prevención/difusión de buenas prácticas de seguridad? ¿con qué frecuencia?

En la gráfica 14 se observa que en la mayoría de las personas a las que se aplicó el cuestionario mencionan que hace mucho tiempo que no se le ha brindado algún tipo de campaña de prevención o difusión de buenas prácticas de seguridad.

7. Conclusiones

Con la realización de esta investigación se explicaron las funciones y las características de la ciberseguridad. Se explicó por qué el uso de la ingeniería social como apoyo a las pruebas de penetración, ya que normalmente no se tiene el recuso económico y humano para la realización de este; En ella se explica por qué la identidad, datos personales, trabajos, etc. en línea son vulnerables a los delincuentes cibernéticos. Esto con el fin de crear una

mentalidad de prevención desde los altos mandos, hasta los rangos más inferiores, ya que los ataques en la seguridad de la información pueden darse desde cualquier nivel organizacional, se ofrecen sugerencias sobre cómo puede proteger la vulnerabilidad afectada y en los casos que fueron críticos se corrigieron.

Se es necesario iniciar con la implementación de un programa dedicado a la seguridad de la información que permita evaluar los riesgos y establecer los mecanismos de control necesarios, normalmente existen equipos de TI, pero tienen que andar haciendo múltiples trabajos que impiden el trabajo de prevención y mitigación, entrando hasta la fase de recuperación, ya cuando todo ha pasado; Ya que se analizaron los datos de la organización: cuáles son, dónde están y por qué deben protegerse. Se explicó quiénes son los atacantes cibernéticos y lo que quieren. Los profesionales de la ciberseguridad deben tener las mismas habilidades que los atacantes cibernéticos, se debe trabajar dentro de los parámetros de la ley local, nacional e internacional basándose en las anteriormente mencionadas y las que vayan surgiendo y sobre todo deben usar sus habilidades con ética. Al igual que una inversión en diferentes estrategias no solo de software y hardware, porque los empleados son los que administran y usan estas herramientas y al no estar capacitados ponen en riesgo la información de la organización así como se muestra en los resultados de las encuestas, gran parte de ellos no tienen capacitación por parte de la organización en temas de seguridad, de igual forma desconocen si están protegidos aun consientes del valor de su información.

8. Referencias

ANUIES. (2016). *Estado actual de las Tecnologías de la Información y las Comunicaciones en las Instituciones de Educación Superior en México* (Primera Ed).

Caroline Wong. (2015). 4 métricas de seguridad que salvarán su empresa - Revista ITNow. Retrieved May 18, 2017, from https://revistaitnow.com/4-metricas-seguridad-importan/

El Intransigene. (2016). Qué flash: ciberataques racistas a impresoras de universidades alemanas - El Intransigente. Retrieved November 1, 2016, from http://www.elintransigente.com/mundo/internacionales/2016/4/21/flash-ciberataques-racistas-impresoras-universidades-alemanas-379416.html

Hamilton, B. A. (2011). Cybersecurity in the Age of Mobility :

iso2700.es. (n.d.). ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información. Retrieved April 22, 2017, from http://www.iso27000.es/iso27000.html

KARL THOMAS. (2015). Caso Ashley Madison: la cronología de los hechos. Retrieved October 24, 2016, from http://www.welivesecurity.com/la-es/2015/08/31/caso-ashley-madison-cronologia/

La, O. D. E. (2016). Ciberseguridad, 193.

Loucks, J., Medcalf, R., Buckalew, L., & Faria, F. (2013). El impacto financiero de BYOD Diez principales consideraciones globales del estudio de Cisco IBSG Horizons. Retrieved from http://www.cisco.com/c/dam/en_us/about/ac79/docs/re/byod/BYOD-Economics_Top-10-Insights_ES-XL.pdf

Mediacenter Panda. (2016). Insiders, el mejor disfraz para robar información. Retrieved

November 23, 2016, from http://www.pandasecurity.com/spain/mediacenter/noticias/ataques-insiders/

Meucci, M., & Muller, A. (2014). 4.0 Testing Guide. Retrieved from https://www.owasp.org/images/1/19/OTGv4.pdf

Morales Alejandro. (2016). ¿Qué es la Administración de Riesgos? Retrieved May 21, 2017, from https://www.auditool.org/blog/control-interno/700-administracion-de-riesgos-conceptos-fundamentales-parte-1

Morana, M., Gondrom, T., Keary, E., Lewis, A., Tan, S., & Watson, C. (2013). Application Security Guide For CISOs. Retrieved from https://www.owasp.org/images/d/d6/Owasp-ciso-guide.pdf

Policía de Ciberdelincuencia. Alerta preventiva contra la ciberdelincuencia No.39 (2016). Retrieved from http://data.ssp.cdmx.gob.mx/documentos/ciberdelincuencia/ciberalertas/39_alerta.pdf

Policía de Ciberdelincuencia. ALERTA PREVENTIVA CONTRA LA CIBERDELINCUENCIA No. 42 (2016). Retrieved from http://data.ssp.cdmx.gob.mx/documentos/ciberdelincuencia/ciberalertas/42_Alerta.pdf

Policía Federal. (2016). Policía Científica Federal participa en 2° Congreso Latinoamericano de Ciberseguridad | Policía Federal | Gobierno | gob.mx. Retrieved October 26, 2016, from https://www.gob.mx/policiafederal/prensa/policia-cientifica-federal-participa-en-2-congreso-latinoamericano-de-ciberseguridad

SDPnoticias. (2013). Sufren universidades de EU creciente número de ciberataques, especialmente de China: NYT | SDP Noticias. Retrieved November 1, 2016, from http://www.sdpnoticias.com/internacional/2013/07/17/sufren-universidades-de-eu-creciente-numero-de-ciberataques-especialmente-de-china-nyt

Urueña, F. J., & Documento De Opinión, C. (2015). CIBERATAQUES, LA MAYOR AMENAZA ACTUAL.