República Dominicana
Universidad Autónoma de Santo Domingo
(UASD).
Recinto Santiago.
Facultad de Ciencias.
Escuela de Informática.

Nivel de Seguridad de las Redes Informáticas de la Fiscalía de Santiago en el Año 2017.

Monografía Para Optar por el Título de
Licenciado en Informática.

Presentado por:
Kelvin Rafael Núñez Marte
Enmanuel De Jesús Gavilán Cruz
Quirico Rafael Germán Martes

Asesor:
Sófocles Martínez Hernández.

Santiago de los Caballeros
Mayo, 2018.

Tabla de Contenido

Agradecimientos.

Primeramente agradezco infinitamente a Dios, quien todo lo puede y quien nunca nos desampara, porque en los momentos más difíciles cuando pensé que no podía seguir me dio la fuerza, valor, voluntad y paciencia para poder llegar hasta mi meta. Gracias Dios por iluminarme el camino correcto.

A mis padres porque siempre han hecho el mejor esfuerzo posible para que yo estudie y me enfoque en ser profesional y persona de bien donde quiera que esté. Gracias por enseñarme que no importa de dónde vengas y que todo sacrificio tiene un premio.

A mí querida esposa por motivarme siempre a seguir hacia delante, por darme ese gran apoyo de compañera para llegar a terminar mi carrera. Agradezco el tiempo que permitió para estudiar y prepararme y así servirle de ejemplo a nuestra querida hija.

A la profesora Ángela Jáquez por el gran apoyo al grupo de nuestro monográfico, por el trabajo incansable para con nosotros, por su dedicación y esfuerzo para ayudarnos a logar nuestro objetivo. Gracias profesora por su deseo de ayudar sin intención de recibir nada a cambio.

A mis compañeros de monografía Quirico Germán Martes y Enmanuel Gavilán, por darme la oportunidad de trabajar con ustedes y juntos concluir con un buen proyecto. Porque a pesar de las diferentes circunstancias que se nos presentaron logramos salir con éxito y de esa forma lograr nuestro sueño.

Kelvin Núñez Marte.

Agradezco primero a Dios por darme las fuerzas, sabiduría, inspiración y motivación para haber llegado hasta este momento tan importante de mi formación profesional y por permitir desarrollar y terminal con éxitos nuestra investigación.

A mis padres, Cayetano Gavilán y Antigua Cruz por darme la vida y el buen ejemplo.

A mis hermanos Niurka, Jordan y Jordana Gavilán por siempre darme motivación para continuar cada día y por ser parte importante en mi vida, quiero servirles de ejemplo.

A todos mis compañeros de monografía, en especial a Kelvin Núñez y Quirico Germán, por luchar juntos para alcanzar nuestra meta.

A nuestros asesores de monografía Gladys Núñez y Sófocles Martínez, por sus orientaciones y su apoyo incondicional para que lográramos nuestra meta.

A nuestra coordinadora de monografía Ángela Jáquez, por su apoyo absoluto en el transcurso del monográfico.

Y a todos los que de alguna u otra forma contribuyeron para que mis sueños se hicieran realidad.

Enmanuel Gavilán.

Primero agradezco a Dios por darme el valor para no rendirme, las fuerzas para continuar sin desfallecer, la sabiduría para saber cómo enfrentar cada reto, y así haber llegado hasta este momento muy importante de mi formación profesional.

A mi esposa, Aurelinda Celeste Díaz Rodríguez por darme apoyo y estar a mi lado como amiga y compañera.

A mi madre, Lucia Marte, por haberme engendrado y alentarme para que terminara mis estudios.

A mi hermano Fredy Nicolás por darme el apoyo económico que necesité en esos momentos oportunos.

A mi tía Ramonita por darme ese apoyo emocional y abecés económico que tanto necesite en ciertos momentos.

A nuestra coordinadora de monografía Ángela Jáquez, por su apoyo incondicional en el desarrollo de la monografía.

A todos mis compañeros de monografía, en especial a Enmanuel Gavilán y Kelvin Núñez, por permitirme ser parte de este equipo, para así juntos alcanzar esta meta.

A nuestros asesores de monografía Gladys Núñez y Sófocles Martínez, por sus orientaciones y su apoyo incondicional para que lográramos nuestra meta.

Quirico Rafael German Martes.

Dedicatorias.

A mis padres Percido Núñez y Nila Marte por su apoyo y bendiciones, por ser ejemplo a seguir y porque siempre han soñado con verme triunfar.

A mi esposa Milva López, porque cada día me expresa su amor y su apoyo incondicional, sabes que un logro mío también es tuyo.

A mi mejor regalo de Dios, mi hija Leslie por ser el motor que me empuja a seguir cada día y ser motivación para luchar incansablemente para que sea persona de bien.

A mi hermana Arisleyda porque siempre he querido ser para ti un ejemplo y motivo a seguir, porque de alguna forma u otra me has brindado el apoyo y la confianza para logar mi objetivo.

Kelvin Núñez Marte.

A mis padres, Cayetano Gavilán y Antigua Cruz por su amor, apoyo incondicional en todo momento y porque han sabido formarme con buenos hábitos y valores, los cuales me han permitido salir siempre adelante en los momentos más difíciles de mi vida.

A mis hermanos Niurka, Jordan y Jordana Gavilán por su apoyo y para que siempre tenga pendiente que a pesar de las adversidades, con Dios sobre toda las cosas, cuando se quiere se puede.

Enmanuel Gavilán.

A mi esposa Aurelinda Celeste Díaz Rodríguez y mi madrina Ramona Marte, por su apoyo, amor, respeto y buenos deseos en todos los momentos, los cuales me han llenado de ganas de salir siempre adelante en las situaciones difíciles de este trayecto para alcanzar esta meta.

A mi hermano Fredy Nicolás por su apoyo y para que nunca olvides que a pesar de los obstáculos que aparezcan en el camino, si ponemos a Dios como nuestro guía todo será posible.

Quirico Rafael German Martes.

INTRODUCCIÓN.

El mundo de la informática desde sus inicios ha venido creciendo muy rápidamente y al compás crecen las empresas e instituciones del estado. No importa el país que sea, no ha habido una gran empresa que pueda crecer sin el auxilio de la informática. Especialmente en la última década en que las empresas necesitan procesar gran cantidad de información y a gran velocidad.

En estos tiempos sería muy difícil para las empresas e instituciones el manejo actualizado de su gran cantidad de información, que gracias a la tecnología y al gran confort que le brinda la informática se hace mucho más fácil el procesamiento. Pero como todo en la vida nada es perfecto ese gran desarrollo que ha tenido también han crecido la necesidad de que las empresas prioricen la seguridad de sus datos y esto es parte de la informática.

A medida que las computadoras y las redes informáticas se incrementan en el mundo, también crece la necesidad de aumentar y fortalecer la seguridad de la misma, debido a lo vulnerable que están ante muchas amenazas de internet, ante todo este peligro es necesaria una buena gestión de la seguridad en las redes computacionales en toda organización; teniendo claro de que todavía no existe un procedimiento de seguridad en redes computacionales que nos garantice el cien por ciento de la seguridad.

En República Dominicana en los últimos tiempos es alarmante el número de empresas que han sido víctima de hackers. De todas empresas que han sido atacadas la mayoría corresponden a instrucciones del estado. Por esta razón decidimos seleccionar a

la Fiscalía de Santiago para verificar cual es el nivel de seguridad en que se encuentran sus redes informáticas en estos momentos.

La presente investigación es una monografía de grado y trata sobre el nivel de la seguridad de las redes informática de la Fiscalía de Santiago para evaluar y de ser necesario sugerir posibles mejoras en la seguridad de las plataformas, hardware y software que se utilizan en la misma.

En el primer capítulo se plantea y formula el problema, objetivos generales, objetivos específicos y las variables sobre el tema a investigar. En este capítulo es donde surgen las interrogantes que se le dan respuestas al final de la investigación.

En el segundo capítulo de esta investigación está el marco conceptual y el marco contextual, para que el lector pueda tener una idea más acabada sobre el tema que estamos trabajando. En este capítulo se desglosan todos los conceptos necesarios para el desarrollo de la investigación.

El tercer capítulo trata sobre la metodología utilizada, la cual nos proporciona el camino para llegar a desarrollar el proceso de la investigación, abarcando esto: tipo y diseño de estudio, métodos y técnicas para la recolección de datos, población y muestra.

En el cuarto capítulo se presenta el análisis de los resultados de los cuestionarios aplicados a los empleados de la Fiscalía de Santiago, así como también al encargado del departamento de tecnología de la información para satisfacer los objetivos específicos que surgieron en el inicio de la investigación.

En el quinto capítulo se describen las conclusiones y recomendaciones de la presente monografía en el que se intenta dar una solución al problema presentado. Se muestran las posibles soluciones a las debilidades encontradas durante la investigación.

CAPÍTULO 1. ASPECTOS GENERALES.

En este primer capítulo se plantea y formula el problema, objetivos generales, objetivos específicos y las variables que son los puntos que se describen a continuación.

Planteamiento y formulación del problema.

Efectuar un análisis de la seguridad de las redes informáticas de la Fiscalía de Santiago con el propósito de encontrar sus debilidades y fortalezas para proporcionar posibles mejoras ante el gran peligro de fuga de información que existe en la actualidad en términos informáticos. Este estudio se hace más imprescindible debido a que no existen informes de que tan protegida están las redes en esta importante institución que es dependencia de PGR (Procuraduría General de la República) desde la cual se administran algunas aéreas de las redes, el dominio que controla a los usuarios de los equipos y también la red privada virtual (VPN) para la conexión a internet. Esta parte de las redes son administradas por la Dirección de Tecnología de la Información de la Procuraduría. (DTI).

En la actualidad la Fiscalía de Santiago ha tenido un gran crecimiento y agregado a esto se ha venido creando muchas plataformas virtuales donde aceden muchos usuarios desde dentro de la institución y desde fuera de la misma, y por tanto se hace muy importante saber que tan protegida están sus redes informáticas internas y externamente. Todo esto debido a la gran vulnerabilidad que existe al navegar en internet y hacer uso del software y las plataformas informáticas.

Por el planteamiento de las situaciones anteriores se generan las siguientes

interrogantes:

1. ¿Cuál es el nivel de seguridad física y lógica de las redes informáticas de la Fiscalía de Santiago?

2. ¿En qué medida el software que se utiliza en la institución instala actualizaciones?

3. ¿Cuáles estándares de seguridad se pueden implementar para aumentar la seguridad de las redes informáticas de la Fiscalía?

4. ¿En qué medida los equipos informáticos realizan copias de seguridad en otros lugares fuera de los edificios donde opera la Fiscalía o en la nube?

Objetivos generales.

Analizar la situación de seguridad de las redes informáticas de la Fiscalía de Santiago para proporcionar posibles mejoras en la protección de los datos de la importante institución del Estado.

Objetivos específicos.

1. Determinar el nivel de seguridad física y lógica de redes informáticas de la Fiscalía de Santiago.

2. Comprobar las actualizaciones del software que se utiliza en la institución.

3. Determinar los estándares de seguridad que se pueden implementar para aumentar la seguridad de las redes informáticas de la Fiscalía.

4. Identificar si los equipos informáticos realizan copias de seguridad en otros lugares fuera

de los edificios donde opera la Fiscalía o en la nube.

Justificación e importancia.

Este trabajo de monografía que trata sobre el nivel de seguridad informática de La Fiscalía de Santiago se realiza en un momento muy determinante ya que en el pasado reciente no se tiene informe de que tan protegida están las redes en dicha institución. Además de eso en los últimos tiempos la Fiscalía ha crecido bastante en tamaño y por tanto en el área de redes informáticas, por lo que se hace justificable tener informes actualizados de su estructura de seguridad de la red en estos momentos.

Después de haber contactado al director de tecnologías de la información de la Fiscalía, el cual nos ha mostrado estar muy de acuerdo por la razón de que nuestro estudio le sería de gran importancia en la actualidad para ayudar a la toma de decisiones a lo relacionado con la seguridad del departamento de informática.

Además de lo expresado anteriormente entendemos es muy propicio estudiar el nivel de la seguridad informática en una institución como esta, porque es una de las más grande de la provincia de Santiago y porque también como es un primer estudio le serviría de base para otros estudios en el futuro.

Por ende, el desarrollo de la presente monografía (Nivel de Seguridad Informática de la Fiscalía de Santiago) se convierte en una necesidad de gran importancia la cual pretende indagar y poner en conocimiento del departamento de tecnología de la información y demás directivos las posibles soluciones en pro de elevar el nivel de seguridad informática de la organización.

Tabla 1

Matriz de variables.

Objetivo general: Analizar la situación de seguridad de las redes informáticas de la Fiscalía de Santiago para proporcionar posibles mejoras en la protección de los datos de la importante institución del estado.

Objetivos específicos	**Variables**	**Dimensiones**	**Indicadores**	**Fuentes**
Determinar el nivel de seguridad de la parte física y lógica de las redes informanticas de la Fiscalía de Santiago.	Nivel de seguridad física y lógica de las redes informáticas.	Divulgación de medidas de seguridad.	Políticas de seguridad que deben conocer los usuarios.	Cuestionarios. Observaciones.
Comprobar las actualizaciones del software que se utiliza en la institución.	Actualizaciones del software que se utilizan en la institución.	Gestión de activos.	Licencias.	Cuestionarios. Observaciones.
Determinar los estándares de seguridad que se pueden implementar para aumentar la seguridad de las redes informáticas de la Fiscalía.	Estándares de seguridad que se pueden implementar para aumentar la seguridad de las redes informáticas de la Fiscalía.	Operativa.	Departamento administrativo.	Cuestionarios. Observaciones.
Identificar sí los equipos informáticos realiza copias de seguridad en otros lugares fuera de los edificios donde opera la Fiscalía o en la nube.	Sí los equipos informáticos realizan copias de seguridad en otros lugares fuera de los edificios donde opera la Fiscalía o en la nube.	Operativa.	Políticas de seguridad.	Cuestionarios.

CAPÍTULO 2. MARCO TEÓRICO.

En este segundo capítulo de esta investigación se trata el marco conceptual y el marco contextual. En este capítulo es donde se desarrollan los conceptos sobre el tema de estudio.

Marco conceptual.

En el presente capítulo se desarrolla la conceptualización para adentrarse en el tema, donde se definen términos como la seguridad de las redes informáticas y las variables relacionadas al tema en cuestión.

La seguridad informática.

La seguridad informática, representa el conjunto de medios y técnicas implementados para asegurar la integridad y que no se difundan involuntariamente los datos que recorren el sistema de información, entendiendo como tal al conjunto de datos y de recursos (físicos, lógicos y humanos) que permiten almacenar y que circule la información que contiene. También representa la red de actores que intervienen sobre éste, que intercambian datos, acceden a ellos y los usan. (Marion, y otros, 2013).

La seguridad informática es aquella disciplina que tiene por objeto preservar la confidencialidad, y disponibilidad de la información; y que puede involucrar otras propiedades, como la autenticidad, la responsabilidad, el no repudio y la trazabilidad. (Jara & Pacheco, 2012)

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, destinados a conseguir un sistema de información

seguro y confiable. (Aguilera López, 2010)

Se puede definir la seguridad informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información. Comprometer su confidencialidad, disminuir el rendimiento de los equipos o bloquear el acceso de los usuarios autorizados al sistema. (Gomez Vieites, 2014, pág. 3)

Existen dos tipos de seguridad informática. Estas hacen referencia a los recursos a proteger, las cuales se describen a continuación:

Seguridad física de las redes informáticas.

La seguridad de las redes en lo que se refiere a la parte física no es más que toda la estructura física de la misma, incluyendo hardware, cableado, servidores, terminales etc. Los siguientes autores (Marion, y otros, 2013, pág. 235) afirman que "Todas las protecciones lógicas que se hayan implementado volverán superfluas si una persona con malas intenciones logra acceder físicamente a los servidores o si se produce una catástrofe natural en el centro de datos".

Seguridad física de los sistemas informáticos consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas para las amenazas a los recursos y la información confidencial. Más claramente, y particularizando para el caso de equipos Unix y sus centros de operación, por seguridad física, podemos entender todos aquellos mecanismos generalmente de prevención y detección destinados a proteger físicamente cualquier recurso del sistema; estos recursos son desde un simple teclado hasta una cinta de backups con toda la información que hay

en el sistema, pasando por la propia Unidad Central de procesamiento (CPU) de la máquina. (Huerta 2002 p.21)

La seguridad física cubre todo lo referido a los equipos informáticos: ordenadores de propósito general, servidores especializados y equipamiento de red. (Roca, 2013 p.15)

Las amenazas contra la seguridad física pueden ser: robos, fallos de suministros, incendios, inundaciones, sismos, señales de radar, actos vandálicos, en fin todo los daños que se le pueden provocar a las redes sin que se utilicen software. El espacio en el que se encuentre el hardware debe contar con diferentes restricciones de acceso a personas, en función del impacto que tendría sobre la zona el robo o el deterioro de los equipos y, sobre todo, de la información. Por esa razón, es obvio que el área o las habitaciones en las que se entren los servidores tendrán la máxima protección del conjunto de espacios en los que se concentre el hardware. (Aguilera López, 2010, pág. 31)

Debe existir un plan de contingencias ante amenazas a cualquiera de los activos del sistema de información que puedan poner en peligro la continuidad de un negocio. El plan de contingencias es un instrumento de gestión que contiene las medidas (tecnológicas, humanas y de organización) que garanticen la continuidad del negocio protegiendo el sistema de información de los peligros que lo amenazan o recuperándolo tras un impacto. (Aguilera López, 2010, pág. 23)

Son muy importantes los dispositivos físicos de protección, como pararrayos, detectores de humo y extintores, cortafuegos por hardware, alarmas contra intrusos, sistemas de alimentación ininterrumpida (para picos y cortes de corriente eléctrica) o

mecanismos de protección contra instalaciones. (Aguilera López, 2010, pág. 18)

En cuanto a las personas, acceso restringido a las instalaciones; por ejemplo, mediante vigilantes jurados o cualquier dispositivo que discrimine la entrada de personal a determinadas zonas. (Aguilera López, 2010, pág. 18)

Los equipos de los usuarios y estaciones de trabajo deben estar sometidos a las directrices establecidas en las Políticas de Seguridad de la organización. La organización podría implantar determinadas soluciones para facilitar el control de la conexión de dispositivos USB (como los pendrives) o firewall (IEEE 1394) en los equipos de los usuarios, así como el control del acceso a puertos de comunicaciones como los puertos serie, puertos paralelo o puertos de infrarrojos (IrDA). (Gomez Vieites, 2014, pág. 212)

También se podría limitar el uso de los puertos USB y de las unidades lectoras/grabadoras de CDs y DVDs, para evitar que se pudiera grabar información sensible o se pudiera introducir determinados contenidos dañinos en el equipo (virus, troyanos, gusanos o programas espía). (Gomez Vieites, 2014, pág. 212)

Seguridad lógica de las redes informáticas.

Hoy día, existen múltiples formas de atacar a una computadora personal o a una red de computadoras, ya sea por medio de Internet o mediante ataques directos. A la seguridad (o inseguridad) de este tipo se le llama seguridad lógica, término que hace alusión a la lógica matemática y a la logística que priva en cualquier computadora. (Baca 2016, p.153)

Las amenazas contra la seguridad lógica pueden ser: virus, troyanos, malware,

perdidas de datos, ataques a las aplicaciones de los servidores. Esta parte de la seguridad se refiere a todo lo que tiene que ver con la ejecución de un programa informático. La política de uso de las computadoras extiende la ley en lo que respeta a quien puede utilizar los sistemas de cómputos y como pueden ser utilizados. Gran parte de la información en esta política parece de simple sentido común, pero sí la organización no define una política de propiedad y uso de las computadoras, la organización queda es puesta a demandas legales por parte de los empleados. (Maiwald, 2005).

Un sistema debe ser capaz de verificar que un usuario identificado que accede a un sistema o que genera una determinada información es quien dice ser. Solo cuando un usuario o entidad ha sido autenticado, podrá tener autorización de acceso. Se puede exigir autenticación en la entidad de origen de la información, en la de destino o en ambas. (Aguilera López, 2010, pág. 17)

Si se consigue tener acceso a la instalación física de una red de área local inalámbrica (WLAN), éste es uno de los ataques más nocivos. Un Rogue AP es un punto de acceso que se conecta sin autorización a una red existente. Estos puntos de acceso no son gestionados por los administradores de la red y es posible que no se ajuste a las políticas de seguridad de la red. De esta forma se abre una puerta a todo tipo de ataques indeseados, puesto que permite a cualquiera con una terminal WLAN conectarse a la red, y vulnera todos los mecanismos que se basan en el cifrado de información entre extremos. (WEB, WEP2, WPA, etc.). (Pellejero, Andreu, & Lesta, 2006, pág. 37)

Las redes inalámbricas están popularizándose, y no es raro que los departamentos establezcan una red inalámbrica sin hacerlo del conocimiento del departamento

(Tecnología de la Información) TI. La política de seguridad debería definir las condiciones bajo la cual se permitirá operar una red inalámbrica y como tener autorización para tener una red de esta naturaleza. (Maiwald, 2005)

Conexión segura SSL/TTL.

El protocolo que habitualmente se utiliza para el cifrado en internet se llama SSL (Secure Socket Layer) o Protocolo de Capa de Conexión Segura. El protocolo HTTPS utiliza el cifrado basado en SSL/TTL. Una buena forma para saber si los datos que introducimos en una web viaja de forma segura, es observar en la barra de direcciones de nuestro navegador si aparece https:// lo que indicaría que es una web segura, o en su lugar parece http:// que significa que no cuenta con cifrado SSL. (Aguilera López, 2010, pág. 152)

Siempre que sea posible trabajaremos con cifrados, lo que es fácilmente configurable con la mayoría de navegadores actuales desde las Opciones de Internet o Preferencias. (Aguilera López, 2010, pág. 152)

Importancia de la seguridad informática.

Preservar la información y la integridad de un sistema informático es algo muy importante para una empresa u organización, por lo que en pérdidas económicas podría suponer, sin olvidarnos del peligro que podría alcanzar el acceso de un usuario al sistema no autorizado. (García & Pilar, 2011, pág.2).

Hoy en día la seguridad informática se ha convertido en una de las principales preocupaciones de las empresas. Por otro lado el uso de las tecnologías de la información y comunicaciones (TIC), es cada vez más extenso por lo que los activos a proteger y las

vulnerabilidades aumentan; y por otro lado los ciberataques son más frecuentes y complejos, llegando a tener consecuencias muy graves como la revelación de información entre otras, por lo que disponer de profesionales en seguridad TIC que puedan proteger los activos en la red se hace imprescindible en todas la empresas por pequeñas o grandes que estas sean. (Rodríguez, 2016)

Políticas de seguridad.

La política de seguridad recoge las directrices u objetivos de una organización con respecto a la seguridad de la información. Forma parte de su política general y, por tanto, ha de ser aprobada por la dirección. El objetivo principal de la redacción de una política de seguridad es la de concienciar a todo el personal de una organización, y en particular al involucrado directamente con el sistema de información, en la necesidad de conocer qué principios rigen la seguridad de la entidad y cuáles son las normas para conseguir los objetivos de seguridad planificados. Por tanto, la política de seguridad deberá redactarse de forma que pueda ser comprendida por todo el personal de una organización. (Aguilera López, 2010, pág. 21)

Se debe enseñar a los empleados porque la seguridad es importante para la organización. También deben ser capacitados en la identificación y la protección de la información confidencial. El entrenamiento de concientización de la seguridad proporcionada a los empleados la información necesaria en las áreas de política organizacional, selección de contraseña y prevención contra los ataques de ingeniería social. (Maiwald, 2005)

La política del uso del Internet define los usos apropiados de esta (como la

investigación relacionada con los negocios, las adquisiciones o las comunicaciones a través de correo electrónico). También puede definir los usos inapropiados (como visitas a sitios web no relacionados con el negocio, descargas de software protegido por derechos del autor, el comercio o intercambio de archivos de música o él envió de cadenas de correspondencia). (Maiwald, 2005)

Para poder implementar mejor algunas políticas de seguridad es importante que tos los usuarios tengan un perfil de usuario: El perfil de usuario es un conjunto a medida de opciones de configuración (fondo de escritorio, protector de pantalla, sonido, etc.) que fijan el funcionamiento y el aspecto del equipo para una cuenta de usuario determinada. Los perfiles de usuario permiten que se usen las preferencias fijadas en ellos al iniciar sesión. (Pérez Marqués, 2010, pág. 137)

Cada cuenta de usuario tiene asociado como un perfil que se crea cuando se crea la cuenta y que posteriormente puede modificarse; por lo tanto, para crear un perfil hay que crear previamente la cuenta a la que se va a asociar. Las propiedades que se asignen inicialmente a esa cuenta al crearla constituyen su perfil inicial. (Pérez Marqués, 2010, pág. 137)

Otra política de seguridad con respecto al empleado es establecer convenio de confidencialidad. Documento en el que las partes reflejan, de forma expresa, la protección jurídica de la información aportada en fase de actos preparatorios a la firma del contrato definitivo. Ello implica que cualquier uso fraudulento y doloso de la misma, además poder producir el desistimiento en el negocio por el afectado, dará lugar a la consiguiente indemnización por los daños y perjuicios causados. El convenio debe de

contener los datos referentes a la información protegida, su ámbito geográfico de aplicación y el plazo en el que se mantendrá en vigor. (Gómez Cáceres & Cárle, 2004)

Los administradores de red tienen que incrementar todo lo concerniente a la seguridad de sus sistemas, debido a que se expone la organización privada de sus datos así como la infraestructura de su red a los expertos de internet (internet Crackers). Para superar estos temores y proveer el nivel de protección requerida, la organización necesita seguir una política de seguridad para prevenir el acceso no autorizado de los usuarios a los recursos y protegerse contra la exportación privada de información. (Echeverria Peña, 2013)

Actualizaciones del software.

Las actualizaciones también denominadas parches, son una parte del software destinadas solucionar algún problema de otra aplicación, o bien actualizarla para incluir nuevas funcionalidades. De este modo permiten eliminar vulnerabilidades de seguridad, errores de funcionamiento o deficiencias, aunque en ocasiones producen otras, lo que se denomina regresión de software. (Gallego & Folgado, 20011)

Una vez instalado un sistema operativo es importante mantenerlo actualizado para corregir errores, mejorar la seguridad, añadir funcionalidades o mejorar las ya existentes. Una forma cómoda para mantener el sistema operativo actualizado son las actualizaciones automáticas, consiste en una herramienta que, una vez configurada, no es necesaria la intervención del usuario para realizar actualizaciones (Bellido Quintero, 2013)

La actualización del antivirus es tan importante, o más que la del sistema operativo,

si no contamos con una versión actualizada del archivo de definiciones de virus, el funcionamiento de la aplicación será pobre y no podrá detectar los últimos virus. Estos resultan ser lo más peligrosos, porque son aquellos contra los cuales el sistema tiene menos formas de defenderse. (Burgos, 2010)

Los antivirus detectan e impiden la entrada de virus y otro software malicioso. En el caso de infección tienen la capacidad de eliminarlos y de corregir los daños que ocasionan en el sistema, preventivo, detector y corrector. Protege la integridad de la información. (Aguilera López, 2010, pág. 17)

La instalación de aplicaciones sin control puede suponer un gasto en la empresa, porque el software instalado puede provocar un sistema inestable, por ejemplo, si un usuario instala un software y el sistema empieza a dar errores por causas relacionadas con la instalación. La empresa será la perjudicada ya que esto supondrá que se pare la realización de servicios y que el personal de sistemas tenga que diagnosticar y reparar el equipo. Estas operaciones requieren un gasto para las empresas. (Aranda Vera, 2014)

El uso de las computadoras proporcionadas por la organización también tendrá efectos en el software que estará cargado en los sistemas. Puede ser apropiado para la organización establecer que ningún software no autorizado puede ser cargado en los sistemas de cómputos. En dicho caso la deberá definir quién puede cargar el software autorizado y como obtener autorización para software. (Maiwald, 2005)

Estándares de seguridad de las redes informáticas.

Norma ISO: Esta norma específica los requisitos para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad informática con base en el

Círculo de Deming, consistente en planear, hacer, verificar y actuar, repitiendo el ciclo en forma indefinida hasta mejorar las condiciones iniciales, en este caso de seguridad informática. (Baca Urbina, 2016)

La norma ISO 27000 se refiere a los Sistemas de Gestión de la Seguridad de la Información, y como todas las ISO, es una norma internacional que permite el aseguramiento, la confidencialidad y la integridad de los datos y de la información, así como de los sistemas que la procesan, por medio de la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos. Por su parte, la norma ISO 27001 sugiere ante todo el conocimiento de la organización y su contexto, la comprensión de las necesidades y de las expectativas de las partes interesadas y la determinación del alcance del SGSI, antes de adoptar dicha norma. (Baca Urbina, 2016).

Como en toda la serie de normas ISO, en las citadas normas se hace patente la necesidad de que todos los empleados de la organización contribuyan al establecimiento de ésta, con el apoyo de la alta dirección, área que debe demostrar su liderazgo y compromiso mediante la elaboración de la política de seguridad que se aplicará, misma que debe conocer toda la organización. La norma enfatiza la importancia de la determinación de riesgos y oportunidades cuando se planifica un Sistema de Gestión de Seguridad de la Información, así como el establecimiento de objetivos de seguridad de la información y el modo de lograrlos. Dicho logro depende en gran parte de que la organización cuente con los recursos, las competencias, la conciencia, la comunicación y la información documentada pertinente en cada caso. La norma indica que para cumplir con los requisitos de seguridad de la información se debe planificar, implementar y controlar los procesos de la organización, así como hacer una valoración de los riesgos de

la seguridad de la información y un tratamiento de éstos. Asimismo, también establece la necesidad y la forma de llevar a cabo el seguimiento, la medición, el análisis, la evaluación, la auditoría interna y la revisión por la dirección del Sistema de Gestión de Seguridad de la Información, a fin de asegurar que funciona según lo planeado. (Baca Urbina, 2016)

La implantación de ISO/IEC 27001 en una organización es un proyecto que suele tener una duración entre 6 y 12 meses, dependiendo del grado de madurez en seguridad de la información y el alcance, entendiendo por alcance el ámbito de la organización que va a estar sometido al sistema de gestión de la seguridad de la Información (SGSI) elegido. El equipo de proyecto de implantación debe estar formado por representantes de todas las áreas de la organización que se vean afectadas por el SGSI liderado por la dirección y asesorado por consultores externos especializados en seguridad informática, por especialistas en aspectos legales de las nuevas tecnologías y de leyes de confidencialidad en la protección de datos y sistemas de gestión de seguridad de la información. (Baca Urbina, 2016)

Se puede obtener una certificación en SGSI mediante un proceso en el cual una entidad de certificación externa, independiente y acreditada audita el sistema, determinando su conformidad con ISO/IEC 27001, su grado de implantación real y su eficacia y, en caso positivo, emite el correspondiente certificado. Desde finales de 2005, las organizaciones ya pueden obtener la certificación ISO/IEC 27001 en su primera certificación con éxito o mediante su re-certificación trienal. (Baca Urbina, 2016)

Por su parte, ISO/IEC 27002: Guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información con 11

dominios, 39 objetivos de control y 133 controles. La ISO 27003 es una guía para la implementación de un SGSI. La ISO 27004: especifica las métricas y las técnicas de medida aplicables para determinarla eficiencia y eficacia de la implantación de un SGSI y de los controles relacionados. La ISO 27005 es una guía para la administración de riesgos en la seguridad informática. La ISO 27006 especifica los requisitos para acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad, y la ISO 27007 es una guía para presentarse ante una auditoría. La ISO 27000: consiste en una guía para la gestión del riesgo de la seguridad de la información y sirve, por tanto, de apoyo a la ISO 27001 y a la implantación de un sistema de gestión de seguridad de la información (SGSI). (Baca Urbina, 2016)

Copias de seguridad de los equipos informáticos.

Para garantizar la plena seguridad de los datos y de los ficheros de una organización no solos es necesario contemplar la protección de la confidencialidad, sino que también se hace imprescindible salvaguardar su integridad y disponibilidad. Para garantizar dos aspectos fundamentales de la seguridad es necesario que existan procedimientos de realización de copias de seguridad y de recuperación que, permiten recuperar y en su caso reconstruir los datos y ficheros dañados o eliminados. (Gomez Vieites, 2014)

Las copias de seguridad y sus duplicados deben almacenarse en ubicaciones seguras y fiables. La técnica más segura consiste en almacenar una copia en la misma ubicación de la compañía y un duplicado en una ubicación distinta. De este modo, en caso de que se pierdan los datos de nuestra empresa y unas de las copias de seguridad debido a una catástrofe o avería general en una situación geográfica se dispone de una copia en otro lugar del mundo. (Caballero & Clavero, 2016)

Ante una amenaza, se aplican medidas preventivas para evitar que se produzca un daño. Por ejemplo, crear y conservar en lugar seguro copias de seguridad de la información, instalar pararrayos o hacer simulacros de incendio. (Aguilera López, 2010, pág. 23)

Marco contextual.

A continuación una breve descripción histórica de la Fiscalía de Santiago y de su estura de redes informáticas, desde sus inicios hasta el año 2017.

Reseña histórica de la Fiscalía de Santiago.

La ciudad de Santiago de los caballeros es la segundad provincia más grande de la República Dominicana. A demás se encuentra el corazón del país lo que la hace una de las ciudades más importante y que en los últimos años ha tenido un gran desarrollo, entre lo que incluye las instituciones del Estado. Para ser más específico podemos mencionar la Fiscalía de Santiago y toda su estructura.

La Fiscalía de Santiago es una institución del estado dependencia de la Procuraduría General de la República dominicana, encargada de la defensa de la legalidad de los derechos de los ciudadanos. Esta institución está ubicada en la provincia de Santiago de los Caballeros, en la Avenida 27 de febrero, Ensanche Román, número 1.

Según cuentan algunos de los empleados con más tiempo en la Fiscalía para los años 1996 se encontraba ubicada en la Escuela Ercilia Pepín en el centro de la ciudad, lo que hoy en día es el recinto del Centro Universitario Regional Santiago de la Universidad Autónoma de Santo Domingo (UASD) Recinto Santiago. A partir de ahí fue trasladada al edificio del palacio de justicia donde están las actuales instalaciones. Edificio que es compartito con la Suprema Corte de Justicia (SCJ).

Para el año 2004 en lo relacionado al área de informática en la Fiscalía de Santiago las instalaciones de redes eran muy mínimas y el número de computadoras no pasada de diez. En estos años no contaba con conexión a internet. No fue sino a partir del año 2005 que se instaló la primera línea de internet, con el tipo de conexión frame relay que funcionaba a una velocidad de 256Kbps.

Con el paso de los años la estructura de la Fiscalía ha venido creciendo muy rápidamente, y con ella sus redes informáticas. Ya para el año 2010 contaba con una cantidad aproximada de 100 computadoras y con una línea dedicada con un ancho de banda para conexión a internet de un Mbps por segundo. Y para el año 2013 se implementó la conexión vía fibra óptica, que funcionaba a una velocidad de 10 Mbps lo que permitió un mejor funcionamiento para el proceso de compartir información en la red.

En la actualidad se está implementando el modo de conexión Línea de Abonado Digital Asimétrica (ADSL) aunque resulta menos estable que la fibra óptica esta resulta menos costosa, con varias líneas redundantes de diferentes proveedor de servicios de internet (ISP) con velocidad sobre los 20 Mbps cada una para tener una red más estable y en caso de fallo de alguna las demás entran en funcionamiento. Y en cantidad de computadoras aproximadamente unas 200 y estos números continúan creciendo constantemente. Además de eso utiliza telefonía IP como medio de comunicación interna y externa. Aparte de la estructura principal de la institución de esta también dependen otras pequeñas Fiscalías que no están conectadas a la red como son: Fiscalía de Navarrete, Licey, San José de las Matas, Tamboril, entre otras.

CAPÍTULO 3. METODOLOGÍA.

En el presente capítulo se desarrolla lo referente a la metodología a utilizada, la cual nos proporciona el camino para llegar a desarrollar el proceso de la investigación, abarcando esto: tipo y diseño de estudio, métodos y técnicas para la recolección de datos y población y muestra.

Tipo y diseño de estudio.

La investigación en esta monografía es de carácter exploratorio debido a que para recabar la información se hizo uso del diseño documental y de campo por lo que se han encontrado pocos elementos que faciliten la investigación porque no se tiene registro de que se haya estudiado anteriormente el tema de la Seguridad de la Redes Informáticas en la Fiscalía de Santiago.

Durante la investigación se hizo uso del diseño documental. En el proceso estudiamos diferentes puntos de vistas en lo que se refiere a los equipos que se utilizan en las redes informáticas de la Fiscalía de Santiago en lo que incluye computadoras, cableado, enrutadores, conmutadores, telefonía de voz sobre protocolo de internet o (VoIP) y servidores que se utilizan y todo lo que tiene que ver con las redes informáticas. Además de la forma en que trabajan los empleados y políticas de seguridad que se ejecutan.

Para la recolección de la información se acudió a diferentes fuentes que describiremos a continuación:

Fuentes primarias: Esta fue la misma estructura de la Fiscalía de Santiago la cual nos apersonamos por sus departamentos y el área de tecnología de la información para poder observar y verificar cómo funcionan las redes, e identificar cuáles son sus fortalezas y debilidades en estos momentos.

Fuentes secundarias: Las informaciones documentales fueron obtenidas de las visitas a diferentes bibliotecas de las universidades más importante en la provincia de Santiago de los Caballeros en las que se incluyen las Universidad Autónoma de Santo Domingo (UASD), Universidad Tecnológica de Santiago (UTESA), Pontificia Universidad Católica Madre y Maestra (PUCMM) y de libros encontrados en la web. En las visitas a esas bibliotecas se revisaron libros, tesis, monografías, proyectos de estudio, entre otros.

Este es un tipo de diseño de campo en el que fue necesaria la recopilación de los datos por medio de condiciones reales directamente. Para la recopilación de los mismos fue necesaria la utilización de entrevistas a los ejecutivos de la institución así también a los empleados que laboran en la institución.

Métodos y técnicas para la recolección de datos.

Para el desarrollo de esta monografía "Nivel de Seguridad Informática de la Fiscalía de Santiago en el Año 2017", se apoyó en el uso necesario del método inductivo y descriptivo que se trata a continuación:

En el método inductivo, se observó las redes, se describió la estructura y la situación actual del objeto de estudio. La utilización de este método fue muy importante porque con este se trató de manera detallada los aspectos referentes al funcionamiento de

la red actual, los equipos informáticos con que cuenta la institución, los softwares que se utilizan y las plataformas con que se dispone para el procesamiento de la información.

Para la aplicación del método descriptivo se visitaron las instalaciones de la institución, los departamentos y se observó de manera minuciosa la configuración de los equipos, tipo de conexión de las redes así como también los sistemas operativos que tienen las computadoras, las aplicaciones y los antivirus que tiene instalado, además sus actualizaciones. En la metodología se implementó este método debido a que el mismo permite describir los eventos y las situaciones al momento de realizar las observaciones y las encuestas.

En esta investigación se hizo necesaria la utilización de encuestas y observaciones como técnica de recolección de datos. Las encuestas y entrevista se elaboraron tomando en cuenta la estructura de los objetivos formulados en la monografía con una serie de preguntas dirigidas al el director de tecnología de la información de la Fiscalía de Santiago así como también a los empleados que laboran en la Fiscalía para tratar de obtener la informaciones necesarias para el análisis.

Es importante mencionar otra técnica muy interesante que fue utilizada que es la observación ya que nos permitió verificar toda la instalación de las redes, la ubicación de los equipos, versión de software que tienen, configuración, licencias, modelo de los equipos y la forma en que trabajan los empleados. También se identificó que tipos de conexión se utilizan para las conexiones de las redes de área local (LAN).

Para esta investigación fue indispensable la elaboración de preguntas cerradas que permitieron satisfacer los objetivos específicos y que permitieron obtener información que se desconocían, la cual fue de gran ayuda para nuestra investigación.

Población y muestra.

La población para esta investigación estuvo conformada por los 129 empleados de la Fiscalía de Santiago que utilizan computadoras. En el estudio se tomó en cuenta la estructura de red informática en la que se analizaron las computadoras, las actualizaciones del software, equipos de redes, sistemas operativos que se utilizan en la institución, copias de seguridad de los archivos, software y políticas de seguridad que se emplean, así como también el tipo de red LAN que se utiliza para conectar las computadoras.

Como es una muestra considerable se utilizó el método estadístico probabilístico para determinar la muestra que fue encuestada por los integrantes que componen la investigación.

Se utilizó como instrumento para la recolección de datos cuestionarios para determinar el nivel de seguridad de las redes informáticas de la Fiscalía. Un cuestionario dirigido a las personas que laboran en la Fiscalía y otro al encargado del departamento de tecnología de la información de dicha institución. Con la implementación de los cuestionarios antes mencionado y a través de las observaciones que se hicieron por medio de las visitas a la Fiscalía, se obtuvo información de todas las áreas a investigar los que permitió recolectar la información necesaria para la investigación.

A continuación se describe el método utilizado para determinar el tamaño de la muestra seleccionada para el estudio. Tomando como población para el estudio una cantidad de 129 empleados de la institución que utilizan computadoras.

$$n = \frac{Z^2 \text{ x } p \text{ x } q \text{ x } N}{e^2 \text{ x } (N-1) + Z^2 \text{ x } p \text{ x } q \text{ x } N}$$

N = Tamaño de la población = 129

Z = Nivel de confianza = 90%

e = Margen de error = 0.15

p = Probabilidad de éxito = 0.05

q = Probabilidad de fracaso = 0.05

n = Tamaño de la muestra = ?

$$n = \frac{1.645^2 \text{ x } 0.05 \text{ x } 0.05 \text{ x } 129}{0.15^2 \text{ x } (129-1) + 1.645^2 \text{ x } 0.05 \text{ x } 0.05} = 25$$

De una muestra de 129 personas que utilizan computadora para trabajar en la Fiscalía de Santiago con un nivel de confianza de un 90% y un margen de error de 15% además una probabilidad de éxito de un 5%, con este método estadístico para tomar el tamaño de la muestra obtuvimos un resultado que nos indica que debemos encuestar a 25 personas.

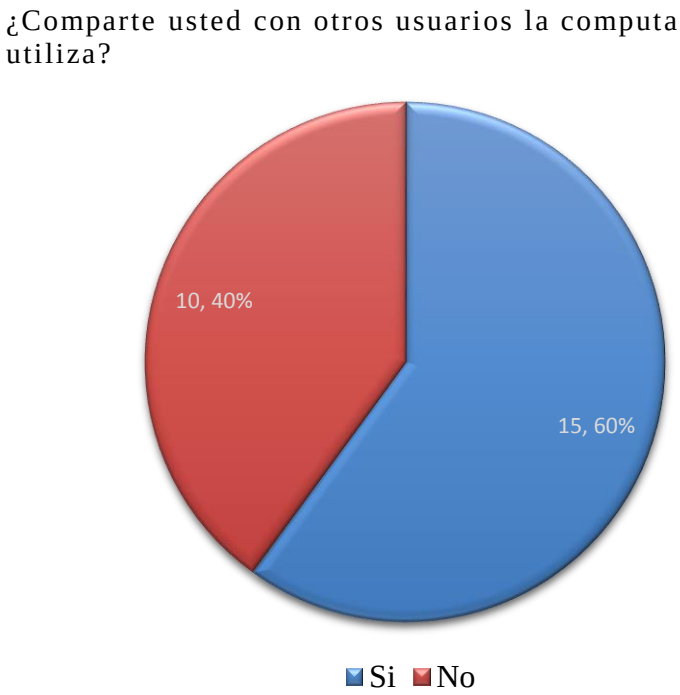
Para continuar con la investigación los datos se tabularon de forma manual, por conteo y luego se usó Microsoft Excel para representar los resultados en tablas lo cual permitió la creación de gráficos para la representación de los resultados, que permitan expresar de forma clara y confiable los resultados. Y para finalizar se realizó un análisis de los resultados obtenidos y se comparó con los supuestos teóricos que sustentan este estudio.

CAPÍTULO 4. PRESENTACIÓN Y ANÁLISIS DE LOS DATOS.

En este capítulo se presentan los resultados y el análisis de los cuestionarios aplicados a los empleados de la Fiscalía de Santiago, así como también al encargado del departamento de tecnología de la información para satisfacer los objetivos específicos que surgieron en el inicio de la investigación.

A continuación se muestran los gráficos que representan los resultados obtenidos de los cuestionarios que se emplearon en las encuestas realizadas a los empleados de la Fiscalía de Santiago. Para la tabulación de los datos se utilizó tablas que se encuentran en el apéndice C elaboradas en Microsoft Excel y de estas se generaron gráficas a fin de que se puedan identificar y analizar los resultados de manera más fácil.

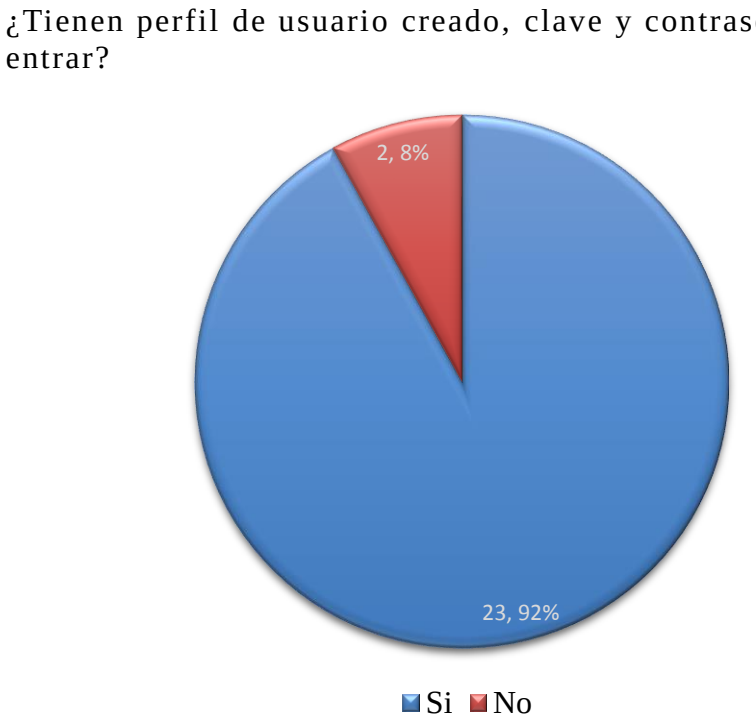
Presentación.
Gráfico 1



Fuente: Tabla 2 del apéndice c.

En el gráfico 1 que representa la pregunta realizada a los empleados de la Fiscalía, para saber sí comparten entre ellos las computadoras el 40% de la población contestaron que no y el 60% contestaron que sí la comparte.

Gráfico 2



Fuente: Tabla 3 del apéndice c.

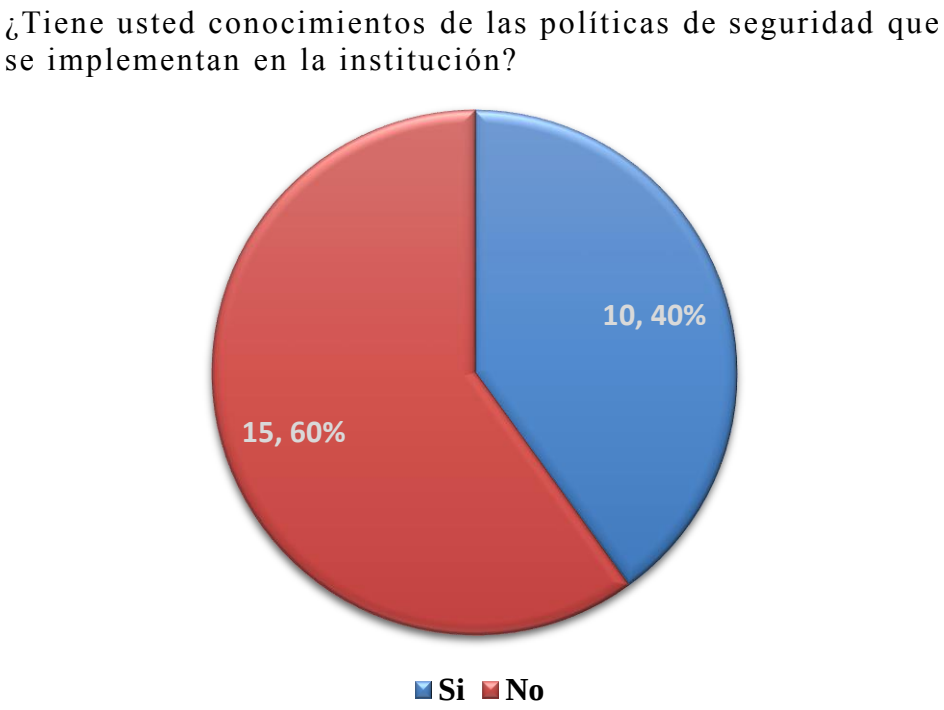
Los resultados porcentuales en la gráfica 2 muestran que el 92% de los encuestados tienen perfil de usuario creado para poder usar una computadora, mientras que el otro 8% aún no se le ha creado perfil de usuario.

Gráfico 3

Fuente: Tabla 4 del apéndice c.

Los resultados obtenidos en la gráfica 3 en cuanto a si la institución tiene políticas de seguridad para el uso de las computadoras, el 0% del encuestado contestó que no, 16% no sabe si la institución tiene políticas de seguridad y el 84% contestó que sí existen políticas de seguridad para el uso de las computadoras.

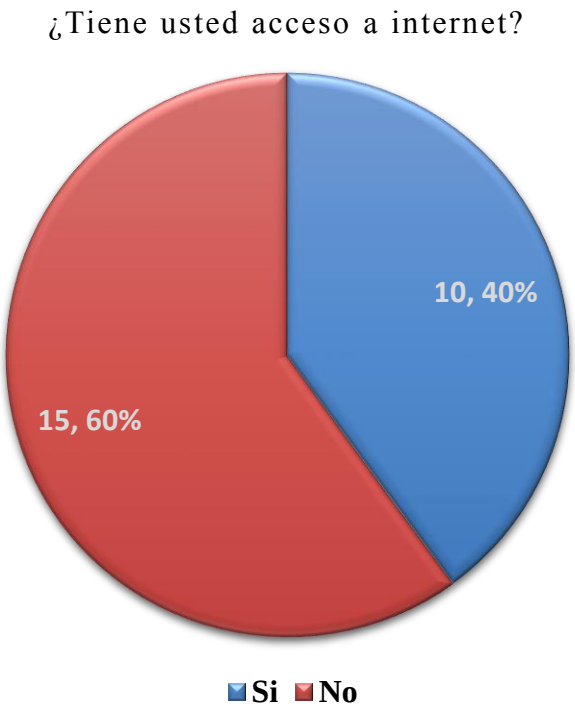
Gráfico 4



Fuente: Tabla 5 del apéndice c.

En el gráfico 4 que ilustra la respuesta de los encuestados acerca del conocimiento de las políticas de seguridad que se implementan en la Fiscalía el 40% contestó que no tiene conocimiento y el 60% contestó sí tiene conocimiento de las políticas de seguridad que se utilizan en la institución.

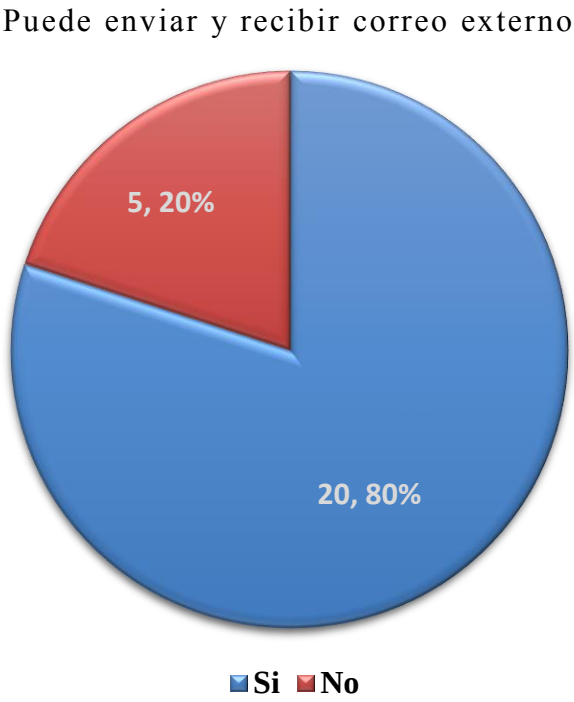
Gráfico 5



Fuente: Tabla 6 del apéndice c.

El gráfico 5 ilustra que de la muestra el 40% de los empleados no tiene acceso a internet mientras que el 60% sí puede navegar en internet.

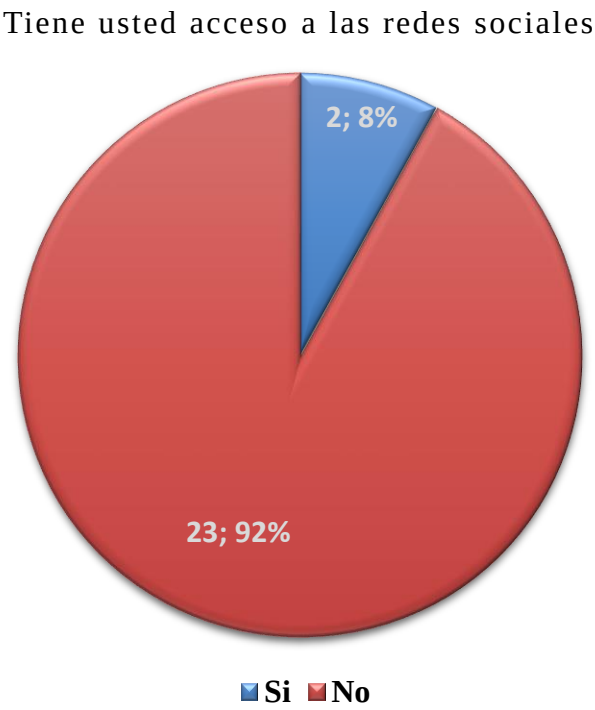
Gráfico 6



Fuente: Tabla 7 del apéndice c.

En el gráfico 6 se muestra el porcentaje de los usuarios que tienen acceso a enviar correos externos y cuáles no, lo que indica el que 80% tiene permitido enviar correos externos y el otro 20% no puede enviar correos hacia un correo fuera de la institución.

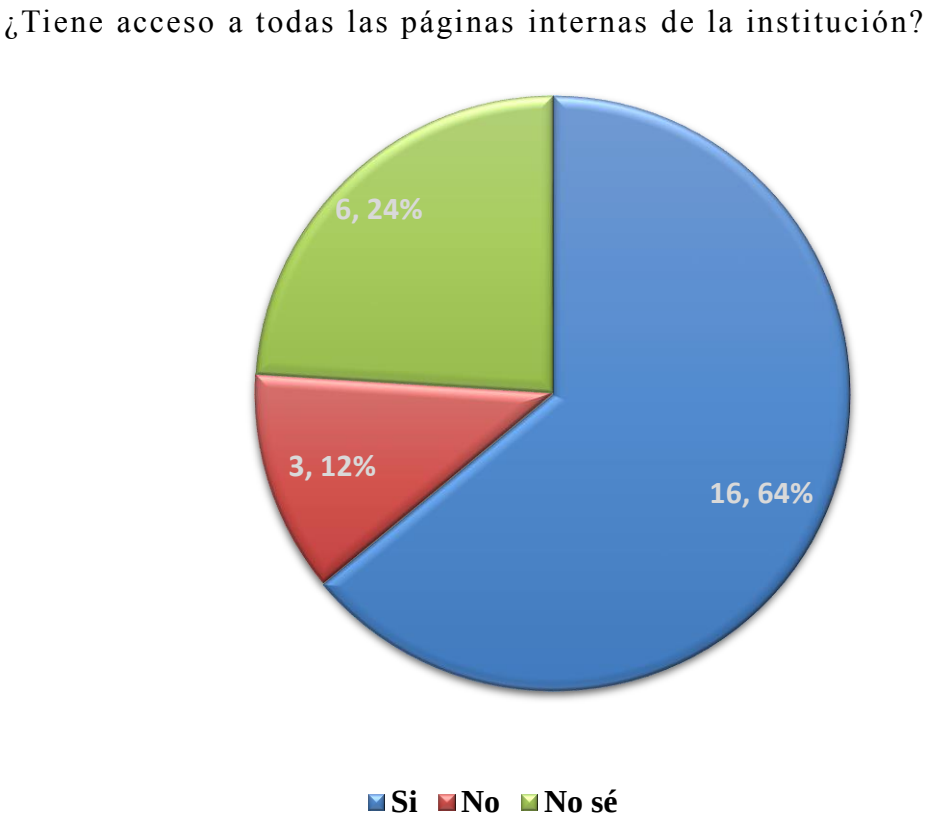
Gráfico 7



Fuente: Tabla 8 del apéndice c.

El gráfico 7 muestra el porcentaje de los empleados que tiene acceso a las redes sociales de los que solo un 8% puede acceder a ellas y 92% no tiene acceso.

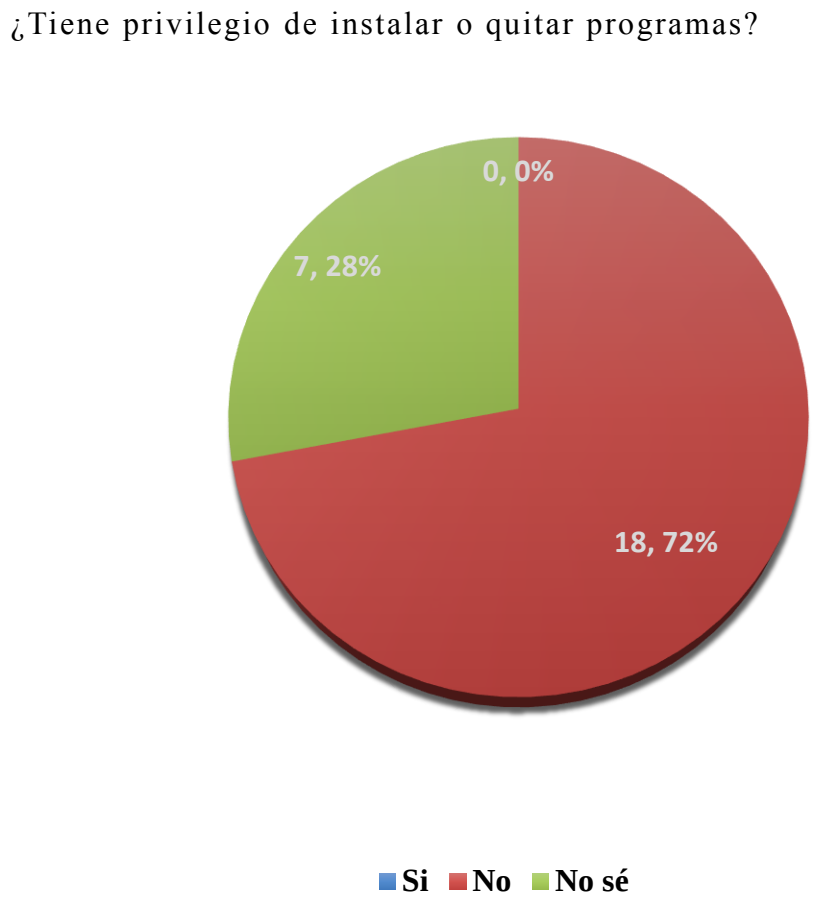
Gráfico 8



Fuente: Tabla 9 del apéndice c.

El gráfico 8 ilustra sobre los empleados que tiene acceso a todas las páginas web internas de la institución a lo que el 64% respondió que sí, el 12% entendió que no y el 24% no sabe si puede acceder.

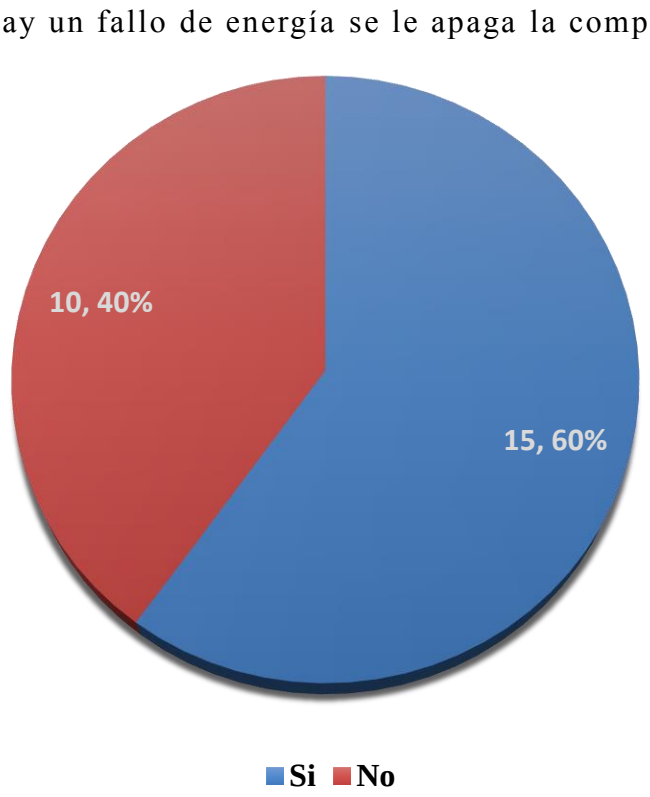
Gráfico 9



Fuente: Tabla 10 del apéndice c.

El gráfico 9 que muestra de manera porcentual lo respondido por los encuestados con respecto a sí tiene privilegio de instalar y quitar programas el 28% contestó no sé, el 72% contestó no y la respuesta sí un 0% de las veces.

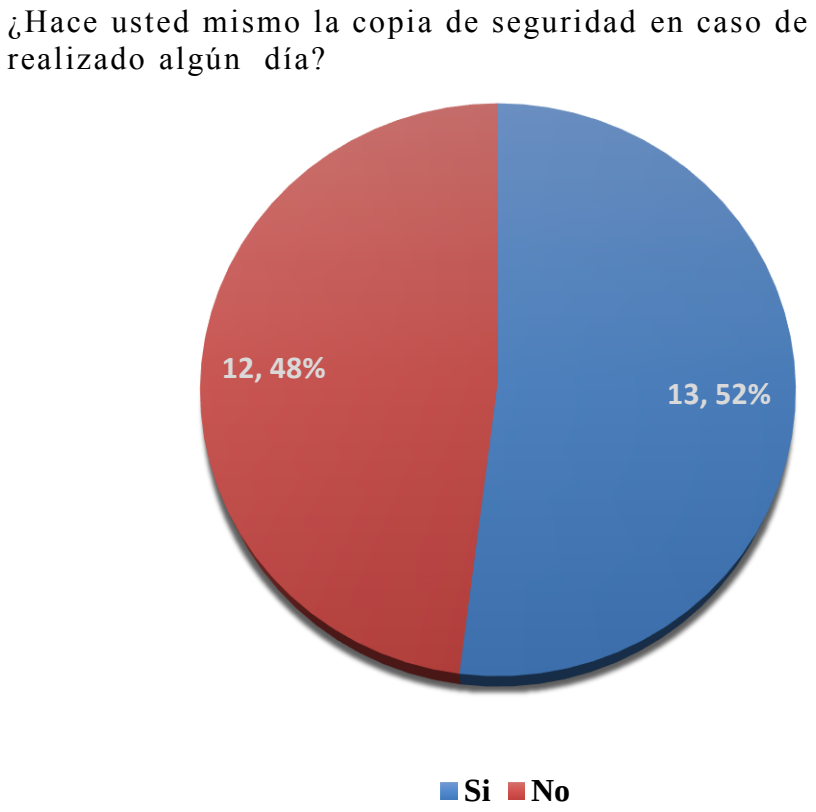
Gráfico 10



Fuente: Tabla 11 del apéndice c.

El gráfico 10 ilustra las respuestas de que cuando hay un fallo de energía un 60% de las computadoras se apagan y el otro 40% no se apagan.

Gráfico 11



Fuente: Tabla 12 del apéndice c.

El gráfico 11 muestra el porcentaje de respuesta con respecto a lo preguntado a los empleados para saber sí ellos realizan o han realizado copias de seguridad algún día a lo que el 52% contestó sí y el 48% contestó no.

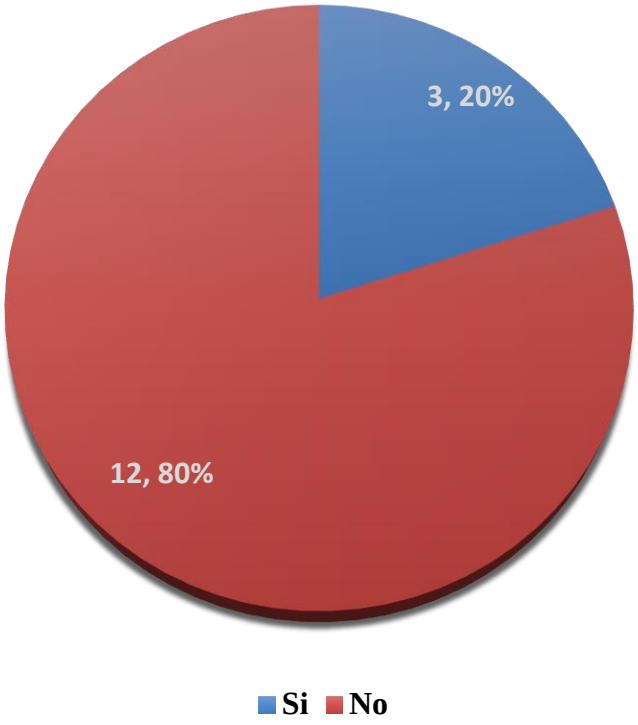
Gráfico 12

Fuente: Tabla 13 del apéndice c.

El gráfico 12 nos nuestra los resultados para identificar sí algunas vez los empleados han perdido información en las computadoras a los que un 32% contestaron que sí un 68% contestó que no ha perdido información.

Gráfico 13

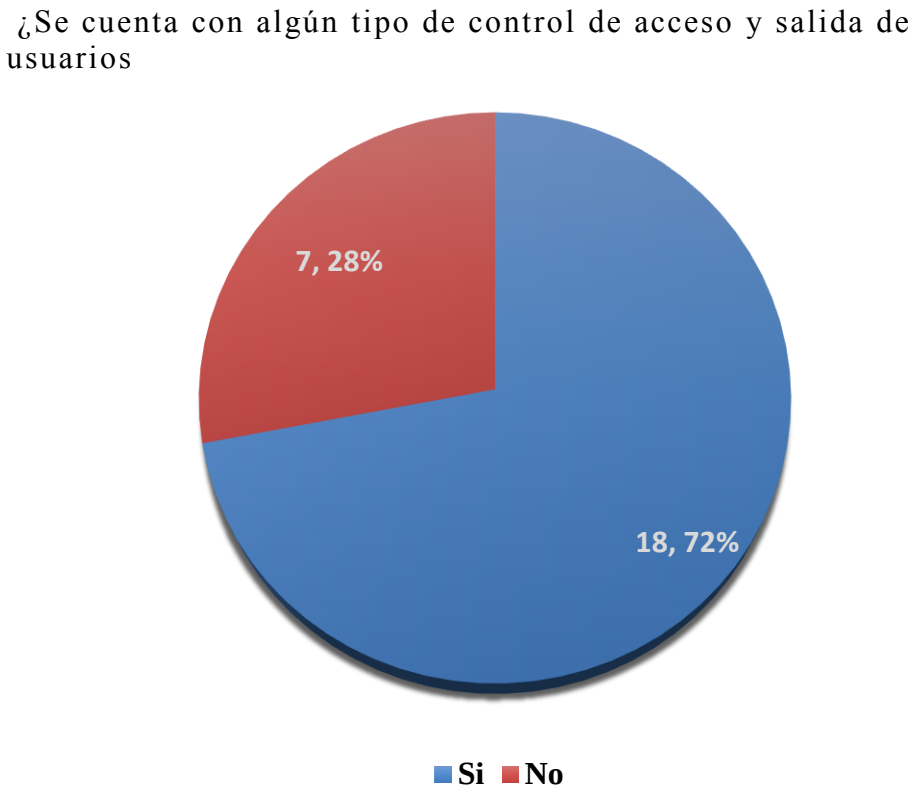
¿La institución le ha dado charla sobre la seguridad de la información?



Fuente: Tabla 14 del apéndice c.

En el gráfico 13 que ilustra la respuesta de los encuestados acerca de que si la institución ha dado charlas sobre seguridad de la información en la Fiscalía el 80% contestó que no han recibido charlas y solo el 20% contestó sí la han recibido.

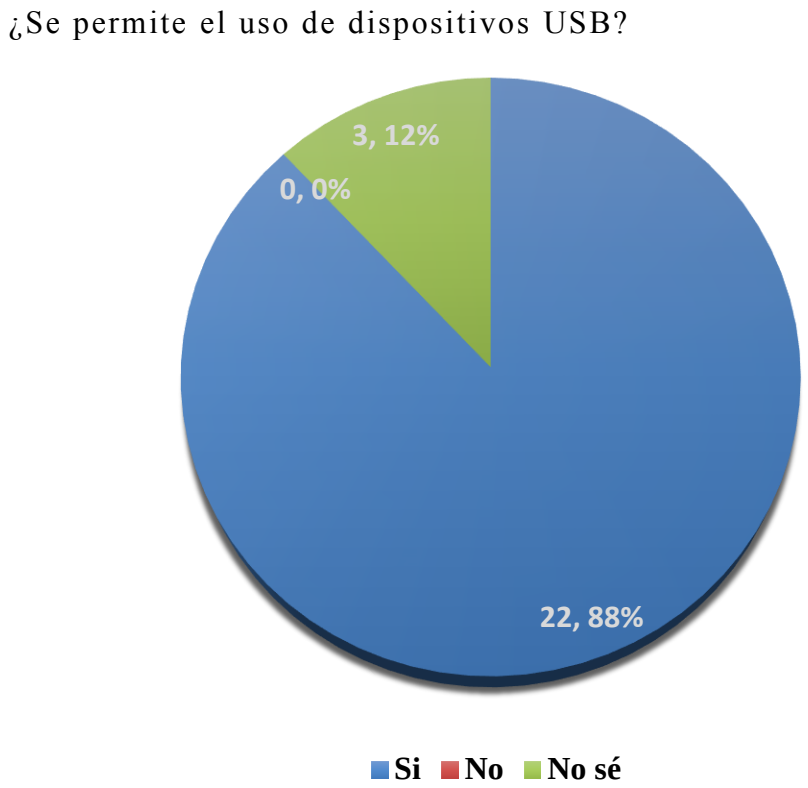
Gráfico 14



Fuente: Tabla 15 del apéndice c.

En el gráfico 14 que ilustra las respuestas de los encuestados acerca de que si cuenta con algún tipo de control de acceso y salida de usuarios en la Fiscalía, el 28% contestaron que sí hay control de acceso y el 28% contestaron no.

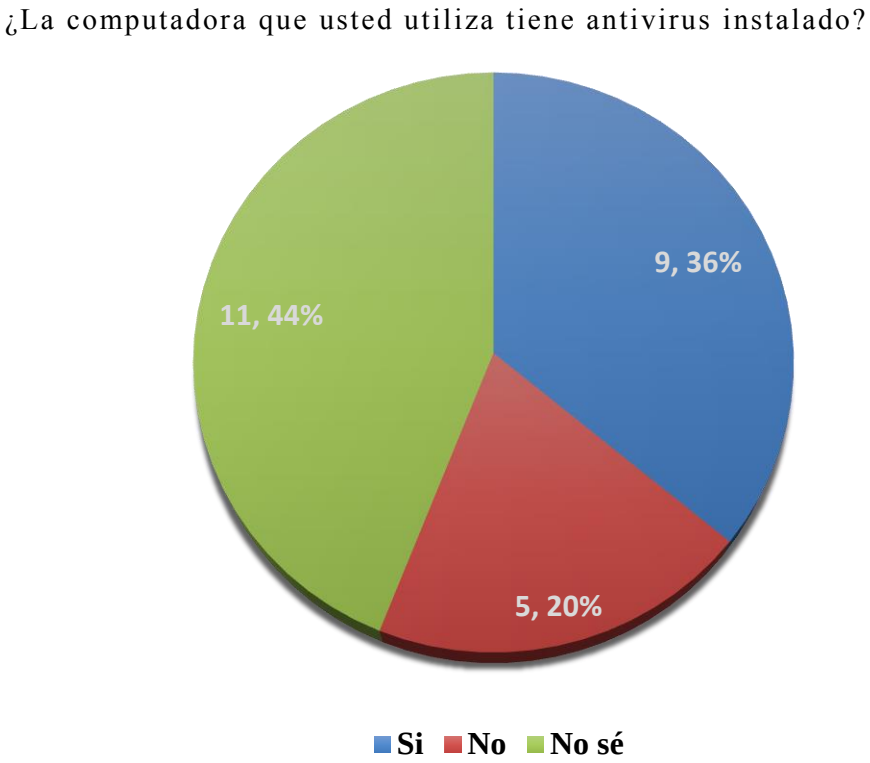
Gráfico 15



Fuente: Tabla 16 del apéndice c.

En el gráfico 15 que ilustra la respuesta de los encuestados acerca de que sí se permite el uso de dispositivos USB el 88% contestaron que sí se permite y el 12% contestaron no sé y no un se permite 0%.

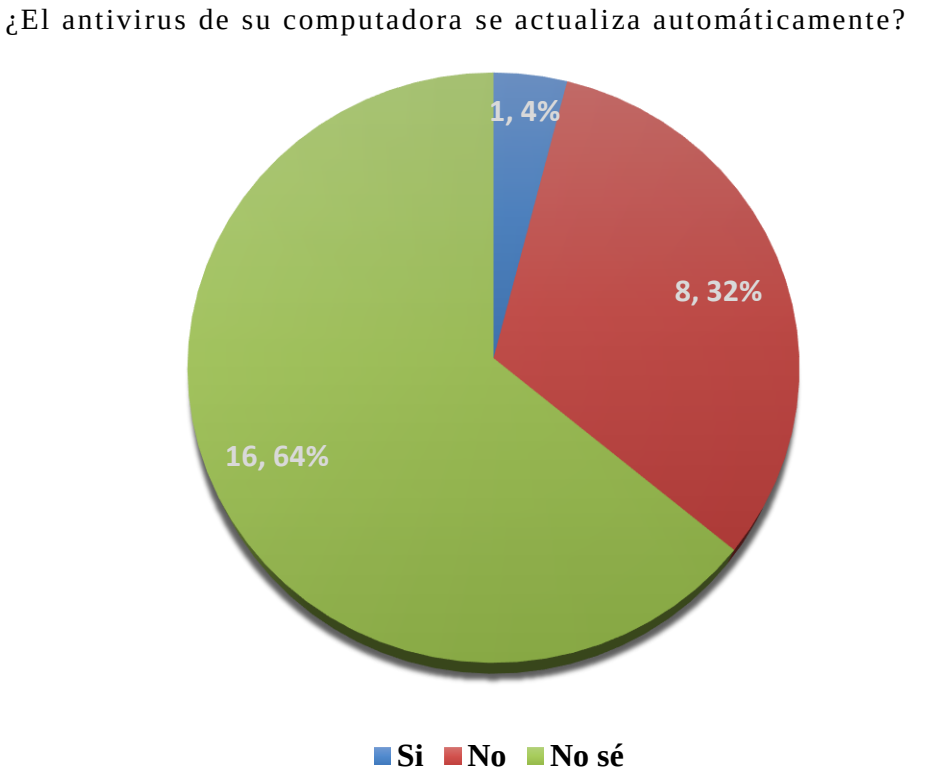
Gráfico 16



Fuente: Tabla 17 del apéndice c.

El gráfico 16 representa los resultados de las respuestas de la pregunta para determinar sí las computadoras tienen antivirus instalado el 36% contestó que sí tienen, el 20% contestó que no y el 44% no sabe sí tiene antivirus.

Gráfico 17

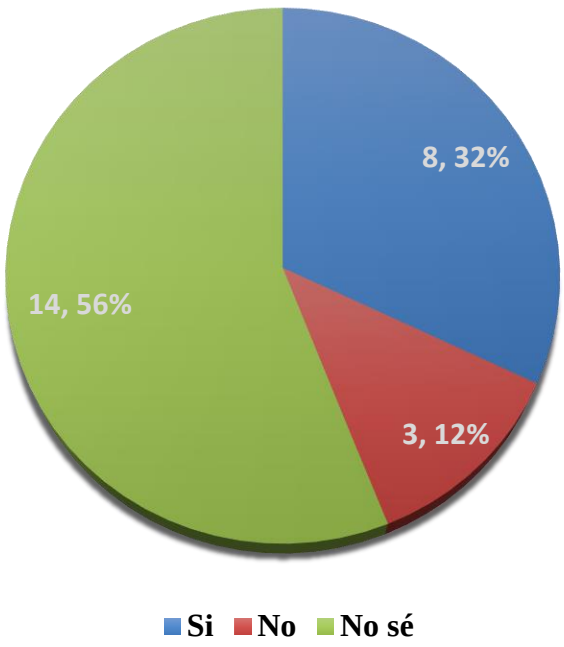


Fuente: Tabla 18 del apéndice c.

El gráfico 17 muestra en forma porcentual las respuestas a la pregunta de que sí lo antivirus se actualizan automáticamente a lo que el 4% contestó que si se actualizan, 32% contestó que no, y el 64% no sabe si se actualizan.

Gráfico 18

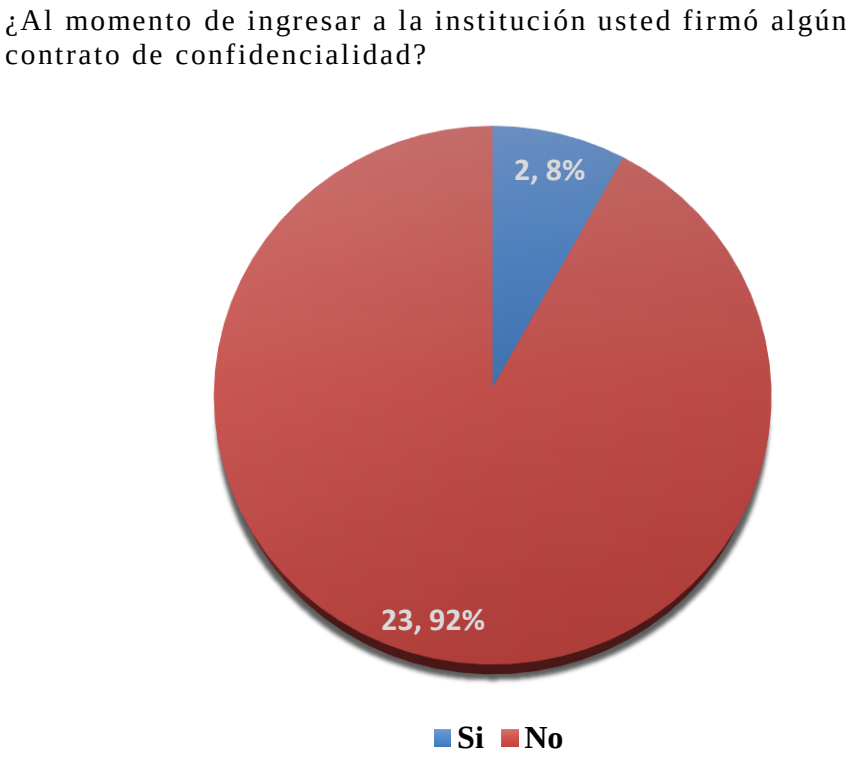
¿Las páginas web de la institución utilizan el protocolo https://?



Fuente: Tabla 19 del apéndice c.

El gráfico 18 representa de forma porcentual las respuestas de los encuestados sobre la pregunta de que sí las páginas web de la institución utilizan el protocolo https:// a lo que un 32% contestó que sí lo utilizan, el 12% contestó que no y el 56% contestó que no sabe si se utiliza el protocolo.

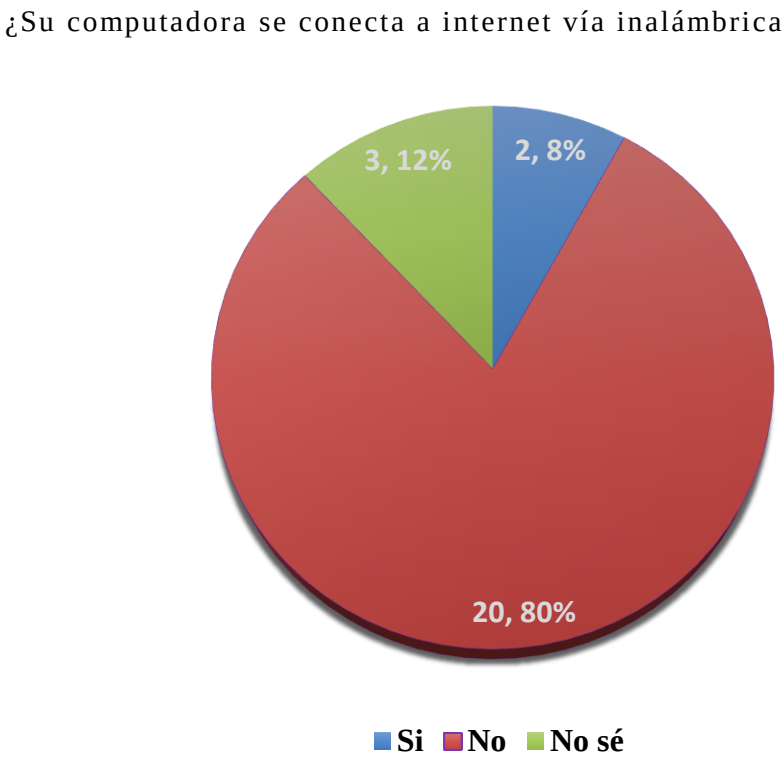
Gráfico 19



Fuente: Tabla 20 del apéndice c.

El gráfico 19 representa de forma porcentual las respuestas de los encuestados sobre la pregunta de que sí firmó contrato de confidencialidad al momento de ingresar a la institución a lo que solo un 8% contestó que sí firmo contrato y el otro 92% contestó no.

Gráfico 20



Fuente: Tabla 21 del apéndice c.

En el gráfico 20 ilustra las respuestas de los encuestados acerca de que sí su computadora se conecta a internet vía inalámbrica, a lo que el 8% contestaron que sí se conecta vía inalámbrica, el 12% contestaron no sé y 80% contestaron no.

Análisis.

En el gráfico uno que representa la pregunta realizada a los empleados de la Fiscalía, para saber sí comparten entre ellos las computadoras, como la mayoría de empleados comparte las computadoras, ósea, el 60% contestaron que sí la comparte, lo que la institución debe de establecer políticas que establezcan una computadora para cada usuario según lo planteado en la siguiente cita: La política de uso de las computadoras extiende la ley en lo que respeta a quien puede utilizar los sistemas de cómputos y como

pueden ser utilizados. Gran parte de la información en esta política parece de simple sentido común, pero si la organización no define una política de propiedad y uso de las computadoras, la organización queda es puesta a demandas legales por parte de los empleados. (Eric Maiwald 2005)

Los resultados porcentuales en el gráfico dos muestran que el 92% de los encuestados tienen perfil de usuario creado para poder usar una computadora, lo que permitirá a la institución poder organizar mejor el control de los usuarios y estandarizar algunas políticas de seguridad según establece el autor en la siguiente cita "El perfil de usuario es un conjunto a medida de opciones de configuración (fondo de escritorio, protector de pantalla, sonido, etc.), que fijan el funcionamiento y el aspecto del equipo para una cuenta de usuario determinada. Los perfiles de usuario permiten que se usen las preferencias fijadas en ellos al iniciar sesión.

Cada cuenta de usuario tiene asociado como un perfil que se crea cuando se crea la cuenta y que posteriormente puede modificarse; por lo tanto, para crear un perfil hay que crear previamente la cuenta a la que se va a asociar. Las propiedades que se asignen inicialmente a esa cuenta al crearla constituyen su perfil inicial". (Pérez Marqués, 2010)

Los resultados obtenidos en la gráfico tres en cuanto a si la institución tiene políticas de seguridad para el uso de las computadoras, el 0% del encuestado contestó que no, 16% no sabe si la institución tiene políticas de seguridad y el 84% contestó que sí existen políticas de seguridad para el uso de las computadoras. Por lo que es importante para la institución involucrar más a los empleados para que conozcan y sean parte de las políticas

de seguridad de la institución según lo establecido por el autor en la siguiente cita: “la política de seguridad recoge las directrices u objetivos de una organización con respecto a la seguridad de la información. Forma parte de su política general y, por tanto, ha de ser aprobada por la dirección”. (Aguilera López, 2010, pág. 21)

A demás según lo planteado por (Eric Maiwald 2005) “Se debe enseñar a los empleados porque la seguridad es importante para la organización. También deben ser capacitados en la identificación y la protección de la información confidencial. El entrenamiento de concientización de la seguridad proporcionada a los empleados la información necesaria en las áreas de política organizacional, selección de contraseña y prevención contra los ataques de ingeniería social”

En el gráfico cuatro que ilustra la respuesta de los encuestados acerca del conocimiento de las políticas de seguridad que se implementan en la Fiscalía el 40% contestó que no tiene conocimiento y el 60% contestó sí tiene conocimiento de las políticas de seguridad. Con respecto a las políticas de seguridad el siguiente autor plantea que: “El objetivo principal de la redacción de una política de seguridad es la de concienciar a todo el personal de una organización, y en particular al involucrado directamente con el sistema de información, en la necesidad de conocer qué principios rigen la seguridad de la entidad y cuáles son las normas para conseguir los objetivos de seguridad planificados. Por tanto, la política de seguridad deberá redactarse de forma que pueda ser comprendida por todo el personal de una organización”. (Aguilera López, 2010, pág. 21)

Los gráficos cinco y seis muestran que hay un gran porcentaje de los empleados que puede navegar en internet y también pueden enviar correos externos. Según lo establecido

por (Maiwald, 2005) “La política del uso del Internet define los usos apropiados de esta (como la investigación relacionada con los negocios, las adquisiciones o las comunicaciones a través de correo electrónico). También puede definir los usos inapropiados (como visitas a sitios web no relacionados con el negocio, descargas de software protegido por derechos del autor, el comercio o intercambio de archivos de música o él envió de cadenas de correspondencia)”. Por lo que es necesario controlar el acceso a las páginas que se puede navegar y lo que se puede descargar.

En el gráfico seis se muestra el porcentaje de los usuarios que tienen acceso a enviar correos externos y cuáles no, lo que indica el que 80% tiene permitido enviar correos externos y el otro 20% no puede enviar correos hacia un correo fuera de la institución.

El gráfico siete muestra el porcentaje de los empleados que tiene acceso a las redes sociales de los que solo un 8% puede acceder a ellas y 92% no tiene acceso a redes sociales. Las redes sociales deben estar muy bien controladas, según lo planteado por el autor en la siguiente cita: “ Los administradores de red tienen que incrementar todo lo concerniente a la seguridad de sus sistemas, debido a que se expone la organización privada de sus datos así como la infraestructura de su red a los expertos de internet (internet Crackers). Para superar estos temores y proveer el nivel de protección requerida, la organización necesita seguir una política de seguridad para prevenir el acceso no autorizado de los usuarios a los recursos y protegerse contra la exportación privada de información”. (Echeverria Peña, 2013). Es muy importante controlar el acceso a internet y las redes sociales en la institución o empresa porque esto aumenta el riesgo de fuga de información y tiempo que los empleados utilizan en ellas.

El gráfico ocho ilustra sobre los empleados que tiene acceso a todas las páginas web internas de la institución a lo que el 64% respondió que sí, el 12% entendió que no y el 24% no sabe si puede acceder. Según lo establecido en el siguiente texto "El uso de las computadoras proporcionadas por la organización también tendrá efectos en el software que estará cargado en los sistemas. Puede ser apropiado para la organización establecer que ningún software no autorizado puede ser cargado en los sistemas de cómputos. En dicho caso la deberá definir quién puede cargar el software autorizado y como obtener autorización para software". (Maiwald, 2005). La institución debe establecer a que páginas web puede y debe acceder cada empleado dependiendo el papel que desempeña.

El gráfico nueve que muestra de manera porcentual lo respondido por los encuestados con respecto a sí tiene privilegio de instalar y quitar programas el 28% contestó no sé, el 72% contestó no y la respuesta sí un 0% de las veces. Según lo planteado por el siguiente autor "la instalación de aplicaciones sin control puede suponer un gasto en la empresa, porque el software instalado puede provocar un sistema inestable, por ejemplo, si un usuario instala un software y el sistema empieza a dar errores por causas relacionadas con la instalación. La empresa será la perjudicada ya que esto supondrá que se pare la realización de servicios y que el personal de sistemas tenga que diagnosticar y reparar el equipo. Estas operaciones requieren un gasto para las empresas". (Aranda Vera, 2014). La instalación y desinstalación de software no debe estar permitido para los empleados porque esto puede provocar múltiples problemas y fallas de seguridad para la institución.

El gráfico diez ilustra las respuestas de que cuando hay un fallo de energía un 60% de las computadoras se apagan y el otro 40% no se apagan. Lo que quiere decir que una

gran cantidad de los equipos se apagan cuando hay un fallo de energía, lo que puede provocar perdida de información y perdida de energía según lo establecido por el autor en la siguiente cita: “Debe existir un plan de contingencias ante amenazas a cualquiera de los activos del sistema de información que puedan poner en peligro la continuidad de un negocio. El plan de contingencias es un instrumento de gestión que contiene las medidas (tecnológicas, humanas y de organización) que garanticen la continuidad del negocio protegiendo el sistema de información de los peligros que lo amenazan o recuperándolo tras un impacto”. (Aguilera López, 2010, pág. 23)

El gráfico once muestra el porcentaje de respuesta con respecto a lo preguntado a los empleados para saber sí ellos realizan o han realizado copias de seguridad algún día a lo que el 52% contestó sí y el 48% contestó no. Es imprescindible que se realicen copias de seguridad de manera sistemática y no solo por parte de los empleados según lo estable el autor en la siguiente cita” Para garantizar la plena seguridad de los datos y de los ficheros de una organización no solos es necesario contemplar la protección de la confidencialidad, sino que también se hace imprescindible salvaguardar su integridad y disponibilidad. Para garantizar dos aspectos fundamentales de la seguridad es necesario que existan procedimientos de realización de copias de seguridad y de recuperación que que en caso de fallos del sistema informático permiten recuperar y en su caso reconstruir los datos y ficheros dañados o eliminados”. (Gomez Vieites, 2014)

El gráfico doce nuestra los resultados de la pregunta para identificar sí algunas vez los empleados han perdido información en las computadoras a los que un 32% contestaron que sí un 68% contestó no. El 32% que contestó que sí el cual es un

porcentaje muy alto tomando en cuenta que siempre se deben realizar copias de seguridad para cualquier daño que ocurra en el hardware o software la información quede resguardada según lo que establece el autor en la siguiente cita" Ante una amenaza, se aplican medidas preventivas para evitar que se produzca un daño. Por ejemplo, crear y conservar en lugar seguro copias de seguridad de la información, instalar pararrayos o hacer simulacros de incendio". (Aguilera López, 2010, pág. 23)

En el gráfico trece que ilustra la respuesta de los encuestados acerca de que si la institución ha dado charlas sobre seguridad de la información en la Fiscalía el 80% contestó que no y solo el 20% contestó sí. Lo que indica que casi nunca se les educa a los empleados sobre la seguridad de la información, y esto es algo que debe ser de conocimiento de todos los involucrados para ayudar a proteger la información que manejan dentro de la institución y saber que hacer en cada caso que ocurra, según lo planteado por el autor en lo citado a continuación: "La política de seguridad recoge las directrices u objetivos de una organización con respecto a la seguridad de la información. Forma parte de su política general y, por tanto, ha de ser aprobada por la dirección. El objetivo principal de la redacción de una política de seguridad es la de concienciar a todo el personal de una organización, y en particular al involucrado directamente con el sistema de información, en la necesidad de conocer qué principios rigen la seguridad de la entidad y cuáles son las normas para conseguir los objetivos de seguridad planificados. Por tanto, la política de seguridad deberá redactarse de forma que pueda ser comprendida por todo el personal de una organización". (Aguilera López, 2010, pág. 21)

En el gráfico catorce que ilustra las respuestas de los encuestados acerca de que si

cuenta con algún tipo de control de acceso y salida de usuarios en la Fiscalía el 28% contestaron que sí hay control de acceso y el 28% contestaron no. Según lo establecido por el autor en la siguiente cita: “ El espacio en el que se encuentre el hardware debe contar con diferentes restricciones de acceso a personas, en función del impacto que tendría sobre la zona el robo o el deterioro de los equipos y, sobre todo, de la información. Por esa razón, es obvio que el área o las habitaciones en las que se entren los servidores tendrán la máxima protección del conjunto de espacios en los que se concentre el hardware”. (Aguilera López, 2010, pág. 31). Por lo que resulta necesario controlar el acceso para que solo puedan acceder a los lugares de trabajo las personas autorizadas.

En el gráfico quince que ilustra la respuesta de los encuestados acerca de que sí se permite el uso de dispositivos USB el 88% contestaron que sí se permite y el 12% contestaron no sé y no un se permite 0%. Como hay una gran cantidad de computadoras en las que se puede utilizar dispositivos USB esto representa una gran falla de seguridad porque casi siempre son la principal forma para expandirse los virus, según lo establecido por la siguiente cita “Los equipos de los usuarios y estaciones de trabajo también deben estar sometidos a las directrices establecidas en las Políticas de Seguridad de la organización. La organización podría implantar determinadas soluciones para facilitar el control de la conexión de dispositivos USB (como los pendrives) o Firewall (IEEE 1394) en los equipos de los usuarios, así como el control del acceso a puertos de comunicaciones como los puertos serie, puertos paralelo o puertos de infrarrojos (IrDA)”. (Gomez Vieites, 2014)

El gráfico dieciséis representa los resultados de las respuestas de la pregunta para determinar sí las computadoras tienen antivirus instalado el 36% contestó que sí tienen, el 20% contestó no y el 44% no sabe sí tiene antivirus. Por lo que la gran mayoría de las computadoras o no tiene antivirus instalados y por los menos los usuarios lo desconocen algo que resulta muy importante para una computadora tener un antivirus que la proteja de acuerdo con lo planteado por el siguiente autor. "Los antivirus detectan e impiden la entrada de virus y otro software malicioso. En el caso de infección tienen la capacidad de eliminarlos y de corregir los daños que ocasionan en el sistema, preventivo, detector y corrector. Protege la integridad de la información". (Aguilera López, 2010, pág. 17)

El gráfico diecisiete muestra en forma porcentual las respuestas a la pregunta de que sí lo antivirus se actualizan automáticamente a lo que el 4% contestó que si se actualizan, 32% contestó no, y el 64% no sabe si se actualizan. Los antivirus siempre deben actualizarse automáticamente para proporcionar mejor protección a los equipos según lo planteado en la siguiente cita: "Las actualización del antivirus es tan importante, o más que la del sistema operativo sí no contamos con una versión actualizada del archivo de definiciones de virus, el funcionamiento de la aplicación será pobre y no podrá detectar los últimos virus. Estos resultan ser lo más peligrosos, porque son aquellos contra los cuales el sistema tiene menos formas de defenderse". (Burgos, 2010)

El gráfico dieciocho representa de forma porcentual las respuestas de los encuestados sobre la pregunta de que sí las páginas web de la institución utilizan el protocolo https:// a lo que un 32% contestó que sí lo utilizan, el 12% contestó no y el 56% contestó no sé. Las páginas web deben utilizar https (http seguro) porque esto

proporciona una conexión cifrada y que protege mejor los datos de los usuarios, según lo planteado por el autor en la siguiente cita: “El protocolo que habitualmente se utiliza para el cifrado en internet se llama SSL (Secure Socket Layer) o Protocolo de Capa de Conexión Segura. El protocolo HTTPS utiliza el cifrado basado en SSL/TTL. Una buena forma para saber sí los datos que introducimos en una web viajan de forma segura, es observar en la barra de direcciones de nuestro navegador si aparece https:// lo que indicaría que es una web segura, o en su lugar aparece http:// que significa que no cuenta con cifrado SSL. Siempre que sea posible trabajaremos con cifrados, lo que es fácilmente configurable con la mayoría de navegadores actuales desde las Opciones de Internet o Preferencias”. (Aguilera López, 2010, pág. 152)

El gráfico diecinueve representa de forma porcentual las respuestas de los encuestados sobre la pregunta de que sí firmó contrato de confidencialidad al momento de ingresar a la institución a lo que solo un 8% contestó que sí firmo contrato y el otro 92% contestó no. Es necesario que la empresa establezca políticas de seguridad para que los empleados tengan compromiso para proteger las informaciones que manejan según lo que establece el autor en la siguiente cita: “Otra política de seguridad con respecto al empleado es establecer convenio de confidencialidad. Documento en el que las partes reflejan, de forma expresa, la protección jurídica de la información aportada en fase de actos preparatorios a la firma del contrato definitivo. Ello implica que cualquier uso fraudulento y doloso de la misma, además poder producir el desistimiento en el negocio por el afectado, dará lugar a la consiguiente indemnización por los daños y perjuicios causados. El convenio debe de contener los datos referentes a la información protegida, su ámbito geográfico de aplicación y el plazo en el que se mantendrá en vigor”. (Gómez

Cáceres & Cárle, 2004)

En el gráfico veinte ilustra las respuestas de los encuestados acerca de que sí su computadora se conecta a internet vía inalámbrica, a lo que el 8% contestaron que sí se conecta vía inalámbrica, el 12% contestaron no sé y 80% contestaron no. "Las redes inalámbricas están popularizándose, y no es raro que los departamentos establezcan una red inalámbrica sin hacerlo del conocimiento del departamento (Tecnología de la Información) TI. La política de seguridad debería definir las condiciones bajo la cual se permitirá operar una red inalámbrica y como tener autorización para tener una red de esta naturaleza". (Maiwald, 2005). Es importante para la institución establecer políticas que controlen cuales son los equipos específicos que pueden conectarte de forma inalámbrica porque esto puede abrir una gran falla de seguridad porque las redes de conexiones inalámbricas (wifi) son muy vulnerables.

A continuación la entrevista realizada al encargado del departamento de tecnología de la información de la Fiscalía de Santiago, con sus respectivas respuestas. Esta no permitió representarla gráficamente ya que la población la conforma una sola persona.

Pregunta 1. ¿Los lugares donde se localizan los equipos informáticos están protegidos de inundaciones, robo o cualquier otra situación que pueda ponerlo en peligro?

El encargado contestó que casi todos los equipos.

Pregunta 2. ¿El local cuenta con aire acondicionado?

El encuestado contestó positivamente.

Pregunta 3. ¿La ubicación de los aires acondicionado es estratégica en el sentido de que no se vayan a mojar los equipos informáticos?

El encuestado contestó positivamente.

Pregunta 4. ¿Se cuenta con alarma contra incendio?

El encuestado contestó negativamente.

Pregunta 5. ¿El local cuenta con extintores y se localizan estos en lugares adecuados?

El encuestado contestó positivamente.

Pregunta 6. ¿Se cuenta con algún tipo de control de entrada y salida de usuarios al área de informática?

El encuestado contestó positivamente.

Pregunta 7. ¿Los equipos se encuentran en buen estado?

El encuestado contestó que casi todos.

Pregunta 8. ¿Tienen acceso a las instalaciones donde están los equipos informáticos personas no autorizadas?

El encuestado contestó que nunca.

Pregunta 9. ¿Se han instalado equipos que protejan la información y los dispositivos en caso de variación de voltaje, como reguladores de voltajes, supresores pico, UPS, generadores de energía, etc.?

El encuestado contestó positivamente.

Pregunta 10. ¿Se tiene un control eficaz en cuanto al personal y al uso de los equipos en la institución?

El encuestado contestó que solo a veces.

Pregunta 11. ¿Hay alguna persona encargada de la seguridad lógica en el área de informática de la Fiscalía?

El encuestado contestó negativamente.

Pregunta 12. ¿La institución cuenta con equipos destinados a la seguridad lógica de las redes informáticas?

El encuestado contestó negativamente.

Pregunta 13. ¿Se ha implementado el uso de VPN para acceso seguro?

El encuestado contestó que siempre se utiliza VPN.

Pregunta 14. ¿Los usuarios tienen acceso controlado a las computadoras?

El encuestado contestó positivamente.

Pregunta 15. ¿Los usuarios normales pueden instalar programas y realizar cambios en las computadoras?

El encuestado contestó negativamente.

Pregunta 16. ¿Se permite el uso de USB a los usuarios?

El encuestado contestó positivamente.

Pregunta 17. ¿En el firewalls del sistema operativo hay otros puertos abiertos que no sean los de compartir archivos e impresoras y de acceso remoto?

El encuestado contestó casi nunca.

Pregunta 18. ¿En las aéreas de acceso al público se encuentran puntos de red habilitados?

El encuestado contestó negativamente.

Pregunta 19. ¿Qué tipo de sistema operativo se utilizan en la institución?

El encuestado contestó Windows.

Pregunta 20. ¿Los sistemas operativos cuentan con licencia?

El encuestado contestó casi todos.

Pregunta 21. ¿Los sistemas operativos tienen activada las actualizaciones automáticas?

El encuestado contestó que algunos.

Pregunta 22. ¿Las computadoras tienen instalado antivirus?

El encuestado contestó casi todos.

Pregunta 23. ¿Los antivirus se actualizan automáticamente?

El encuestado contestó que algunos.

Pregunta 24. ¿Son antivirus de paga?

El encuestado contestó ninguno.

Pregunta 25. ¿Los antivirus se actualizan en cualquier momento o se establece el horario por política de seguridad?

El encuestado contestó que nunca.

Pregunta 26. ¿Todas las computadoras se utilizan con las mismas configuraciones?

El encuestado contestó que todas.

Pregunta 27. ¿Se utiliza un dominio local para implementar las políticas de seguridad?

El encuestado contestó positivamente.

Pregunta 28. ¿Se utilizan estándares de seguridad?

El encuestado contestó negativamente.

Pregunta 29. ¿La parte de la instalación de los cables de red, se utiliza algún estándar internacional?

El encuestado contestó positivamente.

Pregunta 30. ¿Se realizan copias de seguridad de los datos y de las configuraciones de los servidores y equipos de red?

El encuestado contestó a veces.

Pregunta 31. ¿Se cuenta con copias de seguridad en lugares distintos a las instalaciones de la institución?

El encuestado contestó negativamente.

Pregunta 32. ¿Cómo se realizan las copias se seguridad de la institución?

El encuestado contestó que manual

Pregunta 33. ¿Se supervisa si las copias de seguridad se realizan correctamente?

El encuestado contestó siempre.

CAPÍTULO 5. CONCLUSIONES Y RECOMENDACIONES.

En este capítulo se presentan las conclusiones y recomendaciones del presente estudio, en el cual después de haberse realizado las entrevistas, observaciones y luego de haber tabulado, analizado y graficado los resultados, se logró satisfacer los objetivos generales y específicos.

Conclusiones

A continuación se muestran las conclusiones como resultado comparaciones con el marco teórico y todas las observaciones reveladas durante todo el ciclo de vida de este proyecto. Al mismo tiempo se hacen todas las recomendaciones pertinentes relacionadas con el análisis de la seguridad de las redes informáticas de la Fiscalía de Santiago.

Al llegar al final de esta monografía se ha llegado a las siguientes conclusiones para cada objetivo específico:

Objetivo 1. Determinar el nivel de seguridad física y lógica de redes informáticas de la Fiscalía de Santiago.

En cuanto al nivel de seguridad física y lógica de las redes informáticas de las Fiscalía, con los resultados de los datos tabulados y con las respuestas del encargado de TI de la institución se llegó a la conclusión de que se deben cumplir algunas políticas de seguridad que ya existen y en otros casos crear otras políticas de seguridad para proteger la parte físicas de las redes y equipos que se utilizan en la institución. Además hay muchas políticas de seguridad que según el resultado del análisis de datos los empleados desconocen. Lo que coincide con la siguiente monografía: “Plan de seguridad informática para una entidad financiera”.

Cuya conclusión fue la siguiente "La clave para desarrollar con éxito un programa de seguridad de información consiste en recordar que las políticas, estándares y procedimientos de seguridad son un grupo de documentos interrelacionados. La relación de los documentos es lo que dificulta su desarrollo, aunque es muy poderosa cuando se pone en práctica. Muchas organizaciones ignoran esta interrelación en un proceso por simplificar su desarrollo. Sin embargo, estas mismas relaciones son las que permiten que las organizaciones exijan y cumplan los requisitos de seguridad". (Córdoba Rodríguez, 2003)

Objetivo 2. Comprobar las actualizaciones del software que se utilizan en la institución.

Relacionado con las actualizaciones de software se llegó a la conclusión de que la mayoría de empleados opinan que los antivirus de las computadoras que utilizan no se actualizan y en la respuesta de la entrevista al encargado de TI también se comprueba que muchas computaras no se actualizan automáticamente, lo que coincide con las conclusiones a que se llegó en la siguiente monografía "Aseguramiento de los sistemas computacionales de la empresa sitiosdima.net". Sustentada por (Robayo López & rodríguez, 2015). En esa monografía los autores llegaron a la conclusión de que "la verificación de los diferentes elementos de seguridad y configuraciones en los sistemas operativos hacen parte del procedimiento de aseguramiento, tener en cuenta la aplicación de políticas de seguridad y la buena configuración del sistemas permite tener un grado de confianza para poder generar un buen funcionamiento en el sistema. Los ataques en profundidad regularmente son ataques agresivos y que hacen parte de una estrategia planeada y desarrolla muy técnicamente, con el fin de lograr el objetivo final que es

explotar vulnerabilidades y mantener el sistema controlado, por ello se debe implementar un proceso técnico de aseguramiento que combinado con políticas de seguridad permita estabilidad y armonía entre el usuario y el sistema operativo".

Objetivo 3. Determinar los estándares de seguridad que se pueden implementar para aumentar la seguridad de las redes informáticas de la Fiscalía.

Según lo contestado por el encargado de tecnología de la fiscalía y las observaciones que se realizaron en la estructura de redes, se comprobó que no hay definido ningún estándar internacional que rija la institución en el área de tecnología de la información, lo que coincide con lo establecido en las conclusiones de la siguiente tesis: "Diseño de un modelo para la implementación de un sistema de seguridad de información, basado en el estar ISO/IEC 27001: 2005. Caso: Cooperativa la Altagracia, Santiago, 2012-2013". Sustentada por (Antigua Reinoso & Padilla Estévez, 2015) en la que se concluyó que "el establecimiento de un SGSI resulta ser de gran valor para cualquier organización, ya que se buscara proveer una metodología y estrategia adecuada, que garantice la confidencialidad, la integridad de la información

Objetivo 4. Identificar si los equipos informáticos realizan copias de seguridad en otros lugares fuera de los edificios donde opera la Fiscalía o en la nube.

Con la relación a las copias de seguridad se llegó a la conclusión de que si se realizan copias de seguridad y que estas se realizan de forma manual y que nunca se hacen copias de seguridad fuera de la institución o en la nube y por eso en algunas ocasiones se ha perdido información.

Finalizando este trabajo de investigación el cual tuvo como objetivo general:

Analizar la situación de seguridad de las redes informáticas de la Fiscalía de Santiago para proporcionar posibles mejoras en la protección de los datos de la importante institución del Estado.

Se ha llegado a la conclusión de que al momento en que se realizó esta monografía el nivel de seguridad es bajo en algunas áreas, como es el caso de que se permite el uso de dispersivos USB, en algunas áreas no hay acceso restringido para el público. Los antivirus en la mayoría de casos no se actualizan y tampoco muchos sistemas operativos se actualizan automáticamente. Además de eso no existe un estándar de seguridad por la cual se rija la institución en lo tiene que ver con el área de informática. También cuando hay fallos de energía eléctrica hay un gran porcentaje de equipos que se apagan.

Recomendaciones.

Después de haber concluido la presente monografía se hacen las siguientes recomendaciones, dirigidas al departamento de tecnología de la información y a los directivos de la Fiscalía de Santiago: Crear e implementar más políticas de seguridad físicas y lógicas las cuales son un factor muy importante en cualquier empresa o institución y en caso de que se involucren a los empleados estos deben conocerlas a cabalidad para que entiendan cuáles son sus deberes y responsabilidades para ayudar a proteger la información que se maneja en la institución.

Buscar la forma de que todas las computadoras reciban actualizaciones automáticas, los antivirus deben de tener licencia y recibir actualizaciones constantemente para que permitan una mayor protección. Escoger el estándar ISO 27001 sobre sistema de gestión de seguridad de la información para que permita la normalización de todos los procesos,

para poder darle un mejor seguimiento y tener mejor control de las redes informáticas.

Controlar el acceso no autorizado a los sitios web que no son necesarias para desempeñar una función en el trabajo. Además de eso controlar que las páginas web utilicen el protocolo seguro de transferencia.

Realizar copias de seguridad de forma periódica y sistemáticamente, esto así para que en caso de pérdida de información existan copias de respaldo de los datos con fecha reciente. Además de eso deben de guardarse las copias de seguridad redundantes, tanto dentro de la institución como fuera de la misma para que en caso de catástrofes no haya pérdida de información.

También se recomienda un sistema alternativo de energía para que en momentos de que ocurran fallas de energía eléctrica los equipos no se apaguen de repente y esto pueda provocar que los mismos se dañen, o que provoque la perdida de archivos en los que se esté trabajando.

Se recomienda instalar equipos firewall para controlar el tráfico de información tanto de entrada como de salida.

Las recomendaciones ya mencionadas deben empezar a aplicarse en el menor tiempo posible para aumentar la seguridad del activo más importante en este caso que es la información. Además, se recomienda que después que se aplique lo recomendado anteriormente, en un tiempo promedio volver a realizar un estudio como este o una auditoria informática al menos dos veces al año, para determinar en qué ha mejorado la seguridad de las redes informáticas de la institución.

Apéndice.

Apéndice A. Cuestionario 1.

Cuestionario dirigido a los empleados de la Fiscalía de Santiago con el fin de determinar el nivel de seguridad de las redes informáticas de la institución.

1. ¿Comparte usted con otros usuarios la computadora que utiliza?

   Sí___ No___

2. ¿Tienen perfil de usuario creado, clave y contraseña para entrar?

   Sí___ No___

3. ¿La institución tiene políticas de seguridad para el uso de las computadoras?

   Sí___ No___ No sé___

4. ¿Tiene usted conocimientos de las políticas de seguridad que se implementan en la institución?

   Sí___ No___

5. ¿Tiene usted acceso a internet?

   sí___ No___

6. ¿Puede enviar y recibir correo externo?

   Sí___ No___

7. ¿Tiene usted acceso a las redes sociales?

   Sí___ No___

8. ¿Tiene acceso a todas las páginas internas de la institución?

   Sí___ No___ No sé___

9. ¿Tiene privilegio de instalar o quitar programas?

   Sí___ No___ No sé___

10. ¿Cuándo hay un fallo de energía se le apaga la computadora?

    Sí___ No___

11. ¿Hace usted mismo la copia de seguridad en caso de realizado algún día?

    Sí___ No___

12. ¿En algún momento se le ha perdido información?

    Sí___ No___

13. ¿La institución le ha dado charla sobre la seguridad de la información?

    Sí___ No___

14. ¿Se cuenta con algún tipo de control de acceso y salida de usuarios?

    Sí___ No___

15. ¿Se permite el uso de dispositivos USB?

    Sí___ No___ No sé___

16. ¿La computadora que usted utiliza tiene antivirus instalado?

    Sí___ No___ No sé___

17. ¿El antivirus de su computadora se actualiza automáticamente?

    Sí___ No___ No sé___

18. ¿Las páginas web de la institución utiliza en el nombre el protocolo https://?

    Sí___ No___ No sé___

19. ¿Al momento de ingresar a la institución usted firmo algún contrato de confidencialidad?

    Sí___ No___

20. ¿Su computadora se conecta a internet vía inalámbrica?

    Sí___ No___ No sé___

Apéndice B. Cuestionario 2.

Cuestionario dirigido al encargado del departamento de tecnología de la información de la Fiscalía de Santiago con el fin de determinar el nivel de seguridad de las redes informáticas de la institución.

1 ¿Los lugares donde se localizan los equipos informáticos están protegidos de inundaciones, robo o cualquier otra situación que pueda ponerlo en peligro?

1- Todos___ 2- Casi todos___ 3- Algunos___ 4- Ninguno___

2 ¿El local cuenta con aire acondicionado?

1- Sí___ 2- No___

3 ¿La ubicación de los aires acondicionado es estratégica en el sentido de que no se vayan a mojar los equipos informáticos?

1- Sí___ 2- No___

4 ¿Se cuenta con alarma contra incendio?

1- Sí___ 2- No___

5 ¿El local cuenta con extintores y se localizan estos en lugares adecuados?

1- Sí___ 2- No___

6 ¿Se cuenta con algún tipo de control de entrada y salida de usuarios al área de informática?

1- Sí___ 2- No___

7 ¿Los equipos se encuentran en buen estado?

1- Todos___ 2- Casi todos___ 3- Algunos___ 4- Ninguno___

8 ¿Tienen acceso a las instalaciones donde están los equipos informáticos personas no autorizadas?

1- Nunca___ 2- Casi nunca___ 3- A veces___ 4- Siempre___

9 ¿Se han instalado equipos que protejan la información y los dispositivos en caso de variación de voltaje, como reguladores de voltajes, supresores pico, UPS, generadores de energía, etc.?

1- Sí___ 2- No___

10 ¿Se tiene un control eficaz en cuanto al personal y al uso de los equipos en la institución?

1- Nunca___ 2- Casi nunca___ 3- A veces___ 4- Siempre___

11 ¿Hay alguna persona encargada de la seguridad lógica en el área de informática de la Fiscalía?

1- Sí___ 2- No___

12 ¿La institución cuenta con equipos destinados a la seguridad lógica de las redes informáticas?

1- Sí___ 2- No___

13 ¿Se ha implementado el uso de VPN para acceso seguro?

1- Nunca___ 2- Casi nunca___ 3- A veces___ 4- Siempre___

14 ¿Los usuarios tienen acceso controlado a las computadoras?

1- Sí___ 2- No___

15 ¿Los usuarios normales pueden instalar programas y realizar cambios en las computadoras?

1- Sí___ 2- No___

16 ¿Se permite el uso de USB a los usuarios?

1- Sí___ 2- No___

17 . ¿En el firewalls del sistema operativo hay otros puertos abiertos que no sean los de compartir archivos e impresoras y de acceso remoto?

1- Nunca___ 2- Casi nunca___ 3- A veces___ 4- Siempre___

18 ¿En las aéreas de acceso al público se encuentran puntos de red habilitados?

1- Si___ 2- No___

19 ¿Qué tipo de sistema operativo se utilizan en la institución?

1- Windows____

2- MacOS_____

3- Linux____

4- Otros____

20 ¿Los sistemas operativos cuentan licencia?

1- Todos___ 2- Casi todos___ 3- Algunos___ 4- Ninguno___

21 ¿Los sistemas operativos tienen activada las actualizaciones automáticas?

1- Todos___ 2- Casi todos___ 3- Algunos___ 4- Ninguno___

22 ¿Las computadoras tienen instalado antivirus?

1- Todos___ 2- Casi todos___ 3- Algunos___ 4- Ninguno___

23 ¿Los antivirus se actualizan automáticamente?

1- Todos___ 2- Casi todos___ 3- Algunos___ 4- Ninguno___

24 ¿Son antivirus de paga?

1- Todos___ 2- Casi todos___ 3- Algunos___ 4- Ninguno___

25 ¿Los antivirus se actualizan en cualquier momento o se establece el horario por política de seguridad?

1- Nunca___ 2- Casi nunca___ 3- Abecés ___ 4- Siempre___

26 ¿Todas las computadoras se utilizan con las mismas configuraciones?

1- Todas___ 2- Casi todas___ 3- Algunas___ 4- Ninguna___

27 ¿Se utiliza un dominio local para implementar las políticas de seguridad?

1- Sí___ 2- No___

28 ¿Se utilizan estándares de seguridad?

1- Sí___ 2- No___

29 ¿La parte de la instalación de los cables de red, se utiliza algún estándar internacional?

1- Si___ 2- No___

30 ¿Se realizan copias de seguridad de los datos y de las configuraciones de los servidores y equipos de red?

1- Nunca___ 2- Casi nunca___ 3- A veces___ 4- Siempre___

31 ¿Se cuenta con copias de seguridad en lugares distintos a las instalaciones de la institución?

1- Sí___ 2- No___

32 ¿Cómo se realizan las copias se seguridad de la institución?

1- Manual_____

2- Automática____

3-Manual y automática___

4- Ninguna____

33 ¿Se supervisa si las copias de seguridad se realizan correctamente?

1- Nunca___ 2- Casi nunca___ 3- A veces ___ 4- Siempre___

Apéndice C. Tablas.

Tabla 2

Pregunta 1-¿Comparte usted con otros usuarios la computadora que utiliza?

Opciones	**Frecuencia**	**%**
Sí	15	60%
No	10	40%
Total	25	100%

Fuente: Encuesta realizada a los empleados de la Fiscalía de Santiago.

Tabla 3

Pregunta 2-¿Tienen perfil de usuario creado, clave y contraseña para entrar?

Opciones	**Frecuencia**	**%**
Sí	23	92%
No	2	8%
Total	25	100%

Fuente: Encuesta realizada a los empleados de la Fiscalía de Santiago.

Tabla 4

Pregunta 3-¿La institución tiene políticas de seguridad para el uso de las computadoras?

Opciones	**Frecuencia**	**%**
Sí	21	84%
No	0	16%
No sé	4	0%
Total	25	100%

Fuente: Encuesta realizada a los empleados de la Fiscalía de Santiago.

Tabla 5

Pregunta 4-¿Tiene usted conocimientos de las políticas de seguridad que se implementan en la institución?

Opciones	**Frecuencia**	**%**
Sí	10	40%
No	15	60%
Total	25	100%

Fuente: Encuesta realizada a los empleados de la Fiscalía de Santiago.

Tabla 6

Pregunta 5-¿Tiene usted acceso a internet?

Opciones	**Frecuencia**	**%**
Sí	10	40%
No	15	60%
Total	25	100%

Fuente: Encuesta realizada a los empleados de la Fiscalía de Santiago.

Tabla 7

Pregunta 6-¿Puede enviar y recibir correo externo?

Opciones	**Frecuencia**	**%**
Sí	20	80%
No	5	20%
Total	25	100%

Fuente: Encuesta realizada a los empleados de la Fiscalía de Santiago.

Tabla 8
Pregunta 7-¿Tiene usted acceso a las redes sociales?

Opciones	Frecuencia	%
Sí	23	92%
No	2	8%
Total	25	100%

Fuente: Encuesta realizada a los empleados de la Fiscalía de Santiago.

Tabla 9
Pregunta 8-¿Tiene acceso a todas las páginas internas de la institución?

Opciones	Frecuencia	%
Sí	16	64%
No	3	12%
No sé	6	24%
Total	25	100%

Fuente: Encuesta realizada a los empleados de la Fiscalía de Santiago.

Tabla 10
Pregunta 9-¿Tiene privilegio de instalar o quitar programas?

Opciones	Frecuencia	%
Sí	0	0%
No	18	72%
No sé	7	28%
Total	25	100%

Fuente: Encuesta realizada a los empleados de la Fiscalía de Santiago.

Tabla 11
Pregunta 10-¿Cuándo hay un fallo de energía se le apaga la computadora?

Opciones	Frecuencia	%
Sí	15	60%
No	10	40%
Total	25	100%

Fuente: Encuesta realizada a los empleados de la Fiscalía de Santiago.

Tabla 12
Pregunta 11-¿Hace usted mismo la copia de seguridad en caso de realizado algún día?

Opciones	Frecuencia	%
Sí	13	52%
No	12	48%
Total	25	100%

Fuente: Encuesta realizada a los empleados de la Fiscalía de Santiago.

Tabla 13
Pregunta 12-¿En algún momento se le ha perdido información?

Opciones	Frecuencia	%
Sí	8	32%
No	17	68%
Total	25	100%

Fuente: Encuesta realizada a los empleados de la Fiscalía de Santiago.

Tabla 14
Pregunta 13-¿La institución le ha dado charla sobre la seguridad de la información?

Opciones	Frecuencia	%
Sí	3	20%
No	22	80%
Total	25	100%

Fuente: Encuesta realizada a los empleados de la Fiscalía de Santiago.

Tabla 15
Pregunta 14- ¿Se cuenta con algún tipo de control de acceso y salida de usuarios

Opciones	Frecuencia	%
Sí	18	28%
No	7	72%
Total	25	100%

Fuente: Encuesta realizada a los empleados de la Fiscalía de Santiago.

Tabla 16
Pregunta 15- ¿Se permite el uso de dispositivos USB?

Opciones	Frecuencia	%
Sí	22	88%
No	0	0%
No sé	3	12%
Total	25	100%

Fuente: Encuesta realizada a los empleados de la Fiscalía de Santiago.

Tabla 17

Pregunta 16- ¿La computadora que usted utiliza tiene antivirus instalado?

Opciones	***Frecuencia***	***%***
Sí	*9*	*36%*
No	*5*	*20%*
No sé	*11*	*44%*
Total	*25*	*100%*

Fuente: Encuesta realizada a los empleados de la Fiscalía de Santiago.

Tabla 18

Pregunta 17- ¿El antivirus de su computadora se actualiza automáticamente?

Opciones	**Frecuencia**	**%**
Sí	1	4%
No	8	32%
No sé	16	64%
Total	25	100%

Fuente: Encuesta realizada a los empleados de la Fiscalía de Santiago.

Tabla 19

Pregunta 18- ¿Las páginas web de la institución utilizan en el protocolo https://?

Opciones	**Frecuencia**	**%**
Sí	8	32%
No	3	12%
No sé	14	56%
Total	25	100%

Fuente: Encuesta realizada a los empleados de la Fiscalía de Santiago.

Tabla 20

Pregunta 19- ¿Al momento de ingresar a la institución usted firmó algún contrato de confidencialidad?

Opciones	**Frecuencia**	**%**
Sí	2	8%
No	23	92%
Total	25	100%

Fuente: Encuesta realizada a los empleados de la Fiscalía de Santiago.

Tabla 21

Pregunta 20- ¿Su computadora se conecta a internet vía inalámbrica?

Opciones	**Frecuencia**	**%**
Sí	2	8%
No	20	80%
No sé	3	12%
Total	25	100%

Fuente: Encuesta realizada a los empleados de la Fiscalía de Santiago.

Bibliografía.

Aguilera López, P. (2010). *Segurifad Informatica.* Madrid, España: Editex.

Antigua Reinoso, H. D., & Padilla Estévez, P. E. (2015). *Diseño de un modelo para la implementación de un sistema de seguridad de información, basado en el estar ISO/IEC 27001 : 2005. Caso: Cooperativa la Altagracia, Santiago , 2012-2013.* Santiago, Rep. Dom.

Aranda Vera, Á. (2014). *Instalación y parametrización del software.* Málaga, España: IC Editora.

Baca Urbina, G. (2016). Norma ISO 27000. En *Introduccion a la seguridad informatica* (pág. 264). Mexico: Grupo Editorial patria.

Bellido Quintero, E. (2013). En *Instalacion y actualizaciones de sistemas operativos* (pág. 10). Malaga: ic editorial.

Burgos, A. (2010). *Seguridad de PC.* Buenos Aires, Argentina: Creative Andina.

Caballero, C., & Clavero, J. A. (2016). Salvaguarda y recuperacion de los datos. En *Salvaguarda y Seguridad de los Datos* (pág. 27). España: Ediciones Paraninfo, S.A.

Córdoba Rodríguez, N. E. (2003). *Plan de seguridad informática para una entidad financiera.* Lima Perú.

Echeverria Peña, G. (2013). *Procedimientos y Medidas de Seguridad Informatica.* Guatemala.

Gallego, J. C., & Folgado, L. (20011). Montaje y manteniemiento de equipos. Editorial Editex.

Gómez Cáceres, D., & Cárle, G. C. (2004). *Los contratos en el marketing internacional.* Madrid, España: Gráfica Dehon.

Gomez Vieites, A. (2014). En A. Gomez Vieites, *Enciclopedia de la seguridad informatica* (pág. 145). Madrid: RA-MA, S.A.

Jara, H., & Pacheco, F. G. (2012). *Etical Hacking 2.0.* Buenos Aires: Fox Andina.

M. A., BAUDRU, S., CROCFER, R., N. C., F. E., J. H., . . . R. R. (2013). *Seguridad informatica.* Madrid: Ediciones ENI.

Maiwald, E. (2005). *Fundamentos de seguridad de redes.* México: McGraw-Hill.

Paulino, A. A., & Madera Fernández, B. E. (2015). *Nivel de seguridad de COBIT 5 para la seguridad de la información como están de seguridad informática en el sector cooperativo, Santiago, región norte Rep. Dom.* Santiago República Dominicana.

Pellejero, I., Andreu, F., & Lesta, A. (2006). *Fundamentos y aplicaciones de seguridad en redes.* Barcelona, España: MARCOMBO.

Pérez Marqués, M. (2010). *Claves Windows 7.* Madrid, España: RC Libros.

Robayo López, I. J., & rodríguez, I. R. (2015). *Aseguramiento de los sistemas computacionales de ka empresa sitiosdima.net.* Colombia DC.

Rodríguez, A. (18 de enero de 2016). *TrusDimension*. Recuperado el 02 de marzo de 2018, de http://www.trustdimension.com/la-importancia-de-la-seguridad-informatica

Vargas, C. A., Jiménez, M. d., & Hernández, J. M. (2013). *Seguridad informática en las pequeñas empresas de San Francisco de Macorís. Caso: Zigma computers año 2012* . Santiago República Dominicana.